VIII. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Landesbeauftragter für den Datenschutz - Postfach 1947 - 39009 Magdeburg

Telefon	(0391) 8 18 03 - 0
Bürgertelefon	(0800) 9 15 31 90
Fax	(0391) 8 18 03 33
Internet	http://www.datenschutz.sachsen-anhalt.de

Dienstgebäude: Berliner Chaussee 9 - 39114 Magdeburg

Vorwort

Im Rahmen der Veranstaltung des Landtagspräsidenten im April 2005 zur Verabschiedung meines Amtsvorgängers und meiner Amtseinführung hatte ich in meiner Ansprache als für einen Datenschützer hilfreiche Eigenschaften Beharrlichkeit, Gewissenhaftigkeit und Gelassenheit bezeichnet. Letztere kann angesichts der atemberaubenden Entwicklungen bei den Datensammlungen von Staat und Wirtschaft schon verloren gehen. Viele Maßnahmen lassen eine sachliche und verantwortungsbewusste Abwägung mit den Freiheitsgrundrechten vermissen. Die Tendenzen zur Überwachungsgesellschaft sind unverkennbar.

Der auch von mir gewünschte öffentliche Diskurs über das Verhältnis von Rechtsstaat und Gesellschaft und speziell über das Gleichgewicht von Freiheit und Sicherheit wird kaum geführt, jedenfalls wird die Debatte sehr durch die Terrorismusbekämpfung dominiert. Wir sollten uns stets darüber vergewissern, was uns, ja dass uns Freiheit, Freiheit vom Staat, etwas wert ist.

Die rechtliche Ordnung bedarf des Vertrauens ihrer Bürger, ein verlässlicher Datenschutz trägt dazu bei. Traut der Staat aber seinen Bürgern? Die Verwirklichung des Grundrechts auf informationelle Selbstbestimmung ist Maßstab der Freiheitlichkeit des Gemeinwesens.

Der VIII. Tätigkeitsbericht umfasst den Zeitraum vom 1. April 2005 bis zum 31. März 2007. Bei einzelnen Beiträgen wurden noch darüber hinaus reichende aktuelle Sachstände aufgenommen (Redaktionsschluss: 26. Mai 2007).

Ein besonderer Dank gilt wiederum meinen Mitarbeiterinnen und Mitarbeitern in der Geschäftsstelle.

Magdeburg, den 11. Juni 2007

Dr. Harald von Bose
Landesbeauftragter für den Datenschutz Sachsen-Anhalt

Inhaltsverzeichnis

Anlagenverzeichnis

1. Entwicklung und Situation des Datenschutzes

„Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist von dem Grundrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verbürgt [in der Landesverfassung Sachsen-Anhalts siehe Art. 6 Abs.1]. *Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.*
Das Grundrecht dient dabei auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was und bei welcher Gelegenheit über ihn weiß. Die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden, kann dadurch wesentlich gehemmt werden.
Ein von der Grundrechtsausübung abschreckender Effekt fremden Geheimwissens muss nicht nur im Interesse der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird hierdurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist.“
(Bundesverfassungsgericht, Urteil vom 2. März 2006, 2 BvR 2099/04, BVerfGE 115, 166 (188), unter Hinweis auf das Urteil zum Volkszählungsgesetz vom 15. Dezember 1983, BVerfGE 65, 1 ff. (43))

Der VIII. Tätigkeitsbericht des Landesbeauftragten umfasst den Zeitraum vom 1. April 2005 bis 31. März 2007. Die Maßstäbe des Bundesverfassungsgerichts aus dem Volkszählungsurteil von 1983 gelten fort und sind hochaktuell. Der Landesbeauftragte weiß sich in der Verantwortung seines Amtes diesen Maßstäben verpflichtet.

Der Datenschutzbericht dient

- der Unterrichtung des Landtages, zusammen mit der zum Bericht abzugebenden Stellungnahme der Landesregierung (§ 22 Abs. 4a Satz 1 und 2 DSG-LSA)
- der Öffentlichkeitsarbeit (§ 22 Abs. 4a Satz 3 DSG-LSA)
- der Information der Behörden und behördlichen Datenschutzbeauftragten und interessierter Bürgerinnen und Bürger

Der Bericht enthält insofern datenschutzpolitische Feststellungen und greift Grundsatzthemen auf. Er enthält Informationen, Kritik und Lob zu rechtlichen und technischen Entwicklungen. Er enthält Materialien und praxisbezogene Hinweise aus anschaulichen Einzelfällen und dazu erfolgten Beratungen und Kontrollen.

Der VII. Tätigkeitsbericht (2003 - 2005) wurde nach Beratung in den Ausschüssen des Landtages für Inneres und Recht und Verfassung auch im Plenum im Rahmen einer Debatte zur Kenntnis genommen. Diese gegenüber den Vorgängerberichten abweichende Verfahrensweise geht auf einen Vorschlag des Landesbeauftragten zurück, sie entspricht Wortlaut und Sinn der o.a. Gesetzesregelung

und dem Gegenstand. Eine öffentliche Debatte zum Datenschutzbericht empfiehlt sich auf Dauer.

1.1 Freiheit und Sicherheit

Datenschützer sind oft einsame Wächter. Die Bundesjustizministerin Zypries führte dazu beim Juristentag 2006 in Stuttgart aus: „Der Datenschutz hat es derzeit nicht leicht. Wer auf die strikte Beachtung bürgerlicher Freiheiten pocht, macht sich nur wenig Freunde. Schnell gilt man als Bedenkenträger, der den Ernst der Lage nicht erkannt habe. Wer heute dem Publikum gefallen will und Beifall sucht, der muss mit markigen Forderungen auftrumpfen."

Immerhin finden Datenschützer immer wieder Unterstützung durch kritische Bürgerinnen und Bürger, also die Grundrechtsträger, um die es geht, durch (Verfassungs)Gerichte, Medien und Wissenschaft. Doch selbst besonnene Kritik und die sachlich vorgetragene Bitte, bei Eingriffsbefugnissen Augenmaß an den Tag zu legen, verhallen leider schnell.

Die Lage des Datenschutzes nach der Bundestagswahl 2005 kommt in der Koalitionsvereinbarung auf Bundesebene wie folgt zum Ausdruck: Zwar wird vom notwendigen Gleichgewicht zwischen Freiheit und Sicherheit gesprochen. Dann aber: „Die Sicherheitsbehörden in Deutschland sind gut aufgestellt [im Hinblick auf Kriminalitäts- und Terrorismusbekämpfung]. Wir werden jedoch die im Grundsatz bewährte Sicherheitsarchitektur wo es nötig ist weiterentwickeln und überprüfen, inwieweit rechtliche Regelungen, etwa des Datenschutzes, einer effektiven Bekämpfung des Terrorismus und der Kriminalität entgegenstehen."
Das ist aus Sicht des Landesbeauftragten nichts anderes als der altbekannte Vorwurf, der Datenschutz sei **Täterschutz** (vgl. zur Diskussion VII. Tätigkeitsbericht, Ziff. 1). Auch durch eine Wiederholung dieser Behauptung wird diese nicht zutreffender. Datenschutz ist weder Hindernis noch Luxus.

Die insbesondere seit 2001 stetig vorangetriebenen Sicherheitsgesetze und -maßnahmen (z.B. Terrorismusbekämpfungspakete von 2002 und 2005) sind bekannt. Hinzu kommt aber die Entwicklung des Sicherheitsverständnisses des Staates hin zu einem **Präventionsstaat.** Dabei findet unverkennbar eine Verschiebung weg von der gezielten Erfassung tatsächlich Verdächtiger hin zur präventiven Rundumüberwachung statt. Daten werden im Vorfeld von Gefahren und Strafverfolgung erfasst. Beispiele sind die Vorratsdatenspeicherung in der Telekommunikation (siehe Ziff. 23.1) und die Videoüberwachung (siehe Ziff. 17.5). Auch die geplante Mautdatenerfassung (siehe Ziff. 25.4) gehört dazu. Und auch die Antiterrordatei kann in diesem Zusammenhang genannt werden (siehe Ziff. 24.3). Der Perspektivwechsel im Sicherheitsgebaren des Staates ist grundlegend; mit der Vorratsdatenspeicherung wird in besonderem Maße ein Tabu angegriffen, doch der öffentliche Diskurs ist schwach. Das mag auch daran liegen, dass die Maßnahmen nacheinander und in Teilen eingeführt werden, ein Aufschrei wie Anfang der 80er Jahre des 20. Jahrhunderts bei der Volkszählung wäre vielleicht dann zu erwarten, wenn die Grundrechtseingriffe in einem Vollprogramm durchgesetzt würden.

Der Staat legitimiert seine Sicherheitsmaßnahmen mit dem Schutzbedürfnis der Bevölkerung. Der **Schutzauftrag des Staates** ist unbestritten. Die Bedrohung der Freiheit der Bürgerinnen und Bürger durch den Terrorismus, auch durch Kriminalität, ist nicht zu leugnen. Nicht Polizei und Verfassungsschutz bedrohen allgemein die Freiheitsrechte. Im Falle wachsender konkreter Bedrohung darf der Staat die Schutzmaßnahmen verstärken. Zur Bekämpfung des Terrorismus und der Kriminalität sollte man aber nicht radikal vorgehen, d.h. nicht die Wurzeln des Rechtsstaates beschädigen. Der Rechtsstaat beweist seine Stärke und Eigenart - wie es das Bundesverfassungsgericht in der Rasterfahndungsentscheidung (Beschluss vom 4. April 2006, 1 BvR 518/02, BVerfGE 115, 320) formuliert hat - gerade darin, dass er sich auch im Umgang mit seinen Gegnern den allgemein geltenden Grundsätzen unterwirft. Doch wenn es um die Freunde des Rechtsstaats geht, die zu allermeist unverdächtigen rechtstreuen Menschen, sind die Eingriffsschranken höher. Aber die Nichtverdächtigen lassen viel mit sich geschehen: **„Ich habe nichts zu verbergen."** Da unbescholtene Menschen von staatlicher Kontrolle - vermeintlich - nichts zu befürchten haben, entfällt für sie das Problem der Reichweite, auch der Dauer, und der Intensität der Kontrolle, ja auch ein unberechtigter Verdacht schadet ja nicht. Bisher gilt rechtlich betrachtet noch, dass man sich nicht rechtfertigen muss, wenn man etwas zu verbergen hat. Für den Bereich der Strafverfolgung wird dies mit dem Prinzip der Unschuldsvermutung gewährleistet. Im Bereich der Gefahrenabwehr wirkt der Verhältnismäßigkeitsgrundsatz, wozu auch das Verbot der Gefahrerforschungseingriffe gehört. Ob man etwas zu verbergen hat oder nichts zu verbergen hat, wenn der Sicherheitsstaat die Daten haben will, darauf kommt es letztlich jedoch gar nicht mehr an: Den Präventionsstaat interessiert das nicht, denn er sammelt alles. Jedermann ist potenzieller Täter bzw. ein Sicherheitsfaktor, der Generalverdacht kann Alltag werden. Wenn vorsorglich alle erfasst werden, wird die Freiheit geopfert.

Die Mahnung des Bundesverfassungsgerichts in der Rasterfahndungsentscheidung, die **Balance zwischen Freiheit und Sicherheit** zumal angesichts von Streubreite und Persönlichkeitsrelevanz staatlicher Maßnahmen zu wahren bzw. wiederherzustellen, sollte ernst genommen werden. Die diesbezüglichen Aussagen des Gerichts sind sehr grundsätzlich und richtungsweisend. Die Balance stellt sich nicht von allein ein.
Das Grundanliegen besteht darin, das Gewicht der Freiheit zu stärken. Freiheit - weil es um ganz überwiegend unbeteiligte unverdächtige Bürger geht. Freiheit - weil es bei der Ausübung auch anderer Grundrechte um den Schutz vor Einschüchterung geht, wenn für den einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Freiheit - weil insofern über den einzelnen Grundrechtsträger hinaus das Gemeinwohl des Gemeinwesens, zu dem die Selbstbestimmung seiner Bürger gehört, beeinträchtigt wird.

Freiheit und Sicherheit - das beinhaltet zugleich die Feststellung, dass es kein Grundrecht auf Sicherheit gibt. Die Schutzpflichten des Staates resultieren grundrechtstheoretisch aus der objektiven Wertordnung der Grundrechte. Das Bundesverfassungsgericht betont in seiner Rasterfahndungsentscheidung dabei, dass die Schutzpflichten aber nicht den Abwehrcharakter der Grundrechte aushebeln dürfen.

Balance - das bedeutet angesichts dieses Befundes zugleich, dass nicht jeder Abwägungsvorgang mit dem Verhältnismäßigkeitsprinzip harmonisiert werden kann. Nur wenn der **Primat der Freiheit** beachtet wird, kann die Balance noch gelingen. Der gewisse Widerstreit von Sicherheit und Freiheit, die wir beide brauchen, wird so nicht zu Lasten der Freiheit geführt. Der Landesbeauftragte sieht seine Aufgabe darin, zur Stärkung der Balance und zum Erhalt des Spannungsverhältnisses zwischen beiden Polen mittels Betonung des Freiheitsprinzips beizutragen. Dazu gehört Augenmaß, aber auch Klarheit.

Die Dominanz der Bekämpfung des internationalen Terrorismus prägt die Debattenbeiträge der Sicherheitspolitiker seit September 2001. In Zeiten globaler und asymmetrischer Bedrohungen verschwimmen zudem die Grenzen zwischen äußerer und innerer Sicherheit, kommt es zu Netzwerken der Zusammenarbeit und neuen Architekturen. Dabei besteht auch die Gefahr, dass das verfassungsrechtliche **Trennungsgebot** zwischen Polizeien und Nachrichtendiensten verletzt wird (siehe Ziffn. 24.2, 24.3).

Bekämpft man den Terrorismus erfolgreich nur mit Mitteln des Sicherheitsstaates? Im Sinne eines erweiterten Sicherheitsbegriffes ist seit langem anerkannt, dass auch andere Politikfelder im Rahmen einer erweiterten Sicherheit wie z.B. Außenpolitik und Integrationspolitik dazugehören. Manche Stimmen lassen diese Einsicht vermissen. Die Frage nach den Ursachen des Terrorismus ist auch ein gesellschaftspolitisches Thema. Hektische Forderungen nach mehr Sicherheitsmaßnahmen, zumal gepaart mit Symbolismus wie bei der Forderung nach allumfassender flächendeckender Videoüberwachung (in die richtige Richtung geht der Beschluss der Innenministerkonferenz vom 4. September 2006, Videoüberwachung (nur) an Gefahrenschwerpunkten zu verstärken), suggerieren dagegen die Erfüllung eines Sicherheitsversprechens, das nicht zu halten ist. Es gibt keine absolute Sicherheit.

Doch die Vorschläge reißen nicht ab, es gibt kein Innehalten. Im Aktionismus verliert sich schnell der Blick auf verfassungsrechtliche Grenzen und die mangelnde Eignung mancher Maßnahme, da eine Verhältnismäßigkeitsprüfung nicht vorgenommen wird.
Noch einmal die Bundesjustizministerin beim Juristentag 2006: „Den Terrorismus der Gegenwart erleben wir als eine reale, aber zugleich diffuse Gefahr. Diese wenig fassbare Bedrohung verleitet manche dazu, wenigstens dort konkret zu werden, wo sie die vermeintlichen Hemmnisse einer effektiven Verbrechensbekämpfung vermuten. Da wird dann der Datenschutz an den Pranger gestellt, als ‚Täterschutz' missdeutet und der Eindruck erweckt, wenn nur dieses eine Gesetz, diese eine fehlende Datenbank geschaffen werde, dann sei endlich alles im Lot."

Jüngstes Beispiel der Sicherheitsschraube, von manchen schon als „Sicherheitshysterie" bezeichnet, ist der Vorschlag zur heimlichen Online-Durchsuchung privater PC (siehe Ziff. 18.3). Generell und hier ganz besonders passt die Aussage: **Der Zweck heiligt nicht jedes Mittel.**

Die Sicherheitsgesetze sind nicht unzureichend. Sie bedürfen vielmehr der Anpassung im Sinne einer Eingrenzung an die Maßgaben des Bundesverfassungs-

gerichts. Doch schon werden im Zusammenhang mit neuen Befugnissen des Bundeskriminalamtes Lockerungen bei den Voraussetzungen der Rasterfahndung und des großen Lauschangriffs gefordert. Und im neuen Sicherheitskatalog befindet sich der Online-Zugriff der Polizei nicht nur auf die digitalisierten Passbilder der Bürger, sondern auch auf deren Fingerabdrücke in den Meldebehörden (siehe Ziff. 6.3).

Zu den wichtigen Entscheidungen des Bundesverfassungsgerichts in 2005 und 2006 gehören insoweit:

- 12. April 2005 (2 BvR 581/01, BVerfGE 112, 304, NJW 2005, 1338) - polizeiliche Überwachung mittels GPS
- 27. Juli 2005 (1 BvR 668/04, BVerfGE 113, 348, NJW 2005, 2603) - vorbeugende polizeiliche Telefonüberwachung
- 9. Januar 2006 (2 BvR 443/02, NJW 2006, 1116) - Einsichtsrecht in Unterlagen
- 2. März 2006 (2 BvR 2099/04, BVerfGE 115, 166, NJW 2006, 976) - Zugriff auf im Herrschaftsbereich des Teilnehmers vorhandene Telekommunikationsverbindungsdaten
- 4. April 2006 (1 BvR 518/02, BVerfGE 115, 320, NJW 2006, 1939) - polizeiliche Rasterfahndung

Darüber hinaus bleibt das Urteil vom 3. März 2004 (1 BvR 2378/98, 1 BvR 1084/99, BVerfGE 109, 279, NJW 2004, 999) zur akustischen Wohnraumüberwachung (sog. Großer Lauschangriff) im Hinblick auf die Beachtung des Schutzes des Kernbereichs privater Lebensgestaltung maßgeblich. Die Menschenwürde bzw. das Grundrecht auf informationelle Selbstbestimmung ist - das darf dabei nicht übersehen werden - im Übrigen nicht auf den Kernbereich oder die Privatsphäre im engeren Bereich, etwa die Wohnung, beschränkt; das Grundrecht beansprucht Geltung bei jeglicher Kommunikation und Betätigung. Das übersehen jene Politiker, die etwa Computerfahndung mittels heimlicher Internet-Streife dadurch verniedlichen, indem sie feststellen, man sei hier doch nicht an die Verbotszone von Guantanamo und Folter herangekommen. Außerhalb des Kernbereichs sind lediglich die Eingriffsschranken niedriger. Bei Datenerhebungen, die den Kernbereich betreffen, findet keine Abwägung im Rahmen der Verhältnismäßigkeitsprüfung statt, denn der Schutz ist hier absolut.

1.2 Soziales

ALG II

Mit der Zusammenlegung der Sozial- und der Arbeitslosenhilfe unter Beteiligung von zwei Leistungsträgern in verschiedenen Formen (Arbeitsgemeinschaften, Optionskommunen usw.) ist auch der Schutz der Sozialdaten nicht einfacher geworden. Neben der komplizierten Vorfrage der datenschutzrechtlichen Kontrollzuständigkeit waren häufig die Inhalte der Datenerhebungen, insbesondere hinsichtlich der Erforderlichkeit, und das Verfahren der Erhebung (Telefonaktion, Kopieanforderung, Hausbesuch) zu würdigen (siehe Ziffn. 20.3 - 20.9).

JobCard/ELENA
Bei dem Projekt „Elektronischer Einkommensnachweis“ („ELENA“) ist aus datenschutzrechtlicher Sicht besonders brisant, dass eine zentrale Datensammlung auf Vorrat entsteht (siehe Ziff. 20.1).

Gesundheitskarte
Mit der vorgesehenen Einführung der elektronischen Gesundheitskarte werden nicht nur sensible Gesundheitsdaten gespeichert, sondern vielmehr auch das Patientengeheimnis und die Verfügungsbefugnis der Versicherten über ihre Daten tangiert (siehe Ziff. 10.1).

1.3 eGovernment und Technik

Die technische Entwicklung im nicht-öffentlichen Bereich und auch im öffentlichen Bereich, etwa beim eGovernment, ist bereits Thema früherer Tätigkeitsberichte gewesen (vgl. VII. Tätigkeitsbericht, Ziff. 1 und Ziff. 7.1). Naturgemäß sieht der Landesbeauftragte nicht in erster Linie die Chancen neuer Technologien, sondern deren Risiken für Datenschutz und Datensicherheit. Neue Technologien, u.a. die RFID-Technologie (beim elektronischen Pass seit November 2006 und voraussichtlich 2008 beim elektronischen Personalausweis) - siehe Ziff. 4.4 - und Voice over IP („Internet-Telefonie“ - siehe **Anlage 8**), finden bereits Anwendung im öffentlichen Bereich oder sind in Planung.

Zur Sicherung eines angemessenen Schutzniveaus für die Grundrechte ist eine Anpassung der gesetzgeberischen Maßnahmen an die Herausforderungen durch die faktischen Entwicklungen in den einzelnen Lebensbereichen erforderlich. Viele Bereiche bedürfen klarer gesetzlicher Regelungen, auch wenn das Grundanliegen von Normensparsamkeit und Deregulierung nicht aus dem Auge verloren werden darf. Der Anpassungsbedarf besteht gerade aufgrund der technischen Entwicklungen. Das Recht muss moderne Techniken einfangen, wenn sich aus diesen Risiken für den Grundrechtsschutz ergeben (vgl. Bundesverfassungsgericht, Beschluss vom 12. April 2005, 2 BvR 581/01, BVerfGE 112, 304). Insoweit gilt der Grundsatz, dass nicht alles, was technisch möglich ist, auch rechtlich zulässig ist.
Notwendig ist zudem eine datenschutzkonforme Technikgestaltung unter Beachtung der Grundsätze der Datensparsamkeit und Datenvermeidung. Datenschutz muss von vornherein und dauerhaft in die automatisierten Verarbeitungsprozesse personenbezogener Daten integriert werden.

Im Zentrum aller Aktivitäten zur Verwaltungsmodernisierung, als Basis der Kommunikationsinfrastruktur des Landes Sachsen-Anhalt, ob beim IT-Konzept der Landesverwaltung, beim eGovernment-Maßnahmenplan der Landesregierung oder beim Masterplan des Landesportals Sachsen-Anhalt (LPSA) steht nach wie vor das „Informationstechnische Netz des Landes Sachsen-Anhalt“ (ITN-LSA), welches die Grundlage der Kommunikation der Landesverwaltung untereinander, mit den Kommunen, mit den Bürgerinnen und Bürgern sowie mit der Wirtschaft bildet.

Obwohl die Verfügbarkeit der zentralen Kommunikationsdienste und eine sehr hohe Verfügbarkeit der Transportfunktionalität dieses Netzes dem Betreiber, dem Technischen Polizeiamt des Landes Sachsen-Anhalt (TPA), am 1. Dezember 2006 durch eine erneute Zertifizierung durch einen externen unabhängigen Gutachter bestätigt wurde (allerdings nicht nach den national und international anerkannten Common Criteria), sind die durch den Landesbeauftragten bereits in seinem VI. Tätigkeitsbericht 2003 (Ziff. 7.3) aufgezeigten Defizite einer verbindlichen IT-Sicherheitspolitik nicht ausgeräumt.
Die im IT-Konzept der Landesverwaltung - Fortschreibung 2005 - zur Umsetzung der IT-Strategie und zum Aufbau der Sicherheitsarchitektur festgestellte immer größere Bedeutung der Gewährleistung der IT-Sicherheit bei allen anstehenden Geschäftsprozessen (insbesondere also auch Geschäftsprozessen des eGovernment) und die in diesem IT-Konzept daraus abgeleitete Notwendigkeit einer Anpassung der IT-Grundsätze (vom 1. Juni 1992) und des Netzerlasses zum ITN-LSA (vom 7. Februar 1994) sind auch im April 2007 nach wie vor nicht erfolgt. Diese Situation wird den festgelegten Zielen des IT-Einsatzes gemäß IT-Konzept der Landesverwaltung und der Sicherstellung von Datenschutz und Datensicherheit bei der automatisierten Verarbeitung personenbezogener Daten nicht gerecht und ist auch unter Beachtung der Anforderungen für eine sichere Abwicklung von eGovernment-Prozessen so nicht mehr akzeptabel (siehe Ziff. 4.1).

Das Datenschutzgesetz des Landes wurde im November 2005 novelliert (durch Artikel 15 des Ersten Rechts- und Verwaltungsvereinfachungsgesetzes vom 18.11.2005, GVBl. LSA S. 698, 701 - vgl. Ziff. 3.2). Die wichtigste Änderung betrifft die Neufassung und Erweiterung der **Unterrichtungspflicht der Landesbehörden über automatisierte Datenverarbeitungen,** die der Regelung zur Verantwortung und Selbstkontrolle der Verwaltung für die Einhaltung datenschutzrechtlicher Vorgaben in § 14 Abs. 1 Satz 2 (zuvor § 22 Abs. 4 Satz 2) DSG-LSA angefügt wurde: *„Der Landesbeauftragte für den Datenschutz ist rechtzeitig über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu unterrichten“.* Die Regelung unterstützt die Beratungsaufgabe im Vorfeld der Einführung neuer Verfahren und ergänzt § 40 der Gemeinsamen Geschäftsordnung der Ministerien (Allgemeiner Teil), wonach der Landesbeauftragte vor der Erstellung neuer Regelungen, einschließlich Rechtsvorschriften, mit Datenschutzrelevanz zu beteiligen ist.

Der Landesbeauftragte musste feststellen, dass gerade die obersten Landesbehörden es mehrmals versäumten, rechtzeitig im Sinne einer Bringschuld über neue eGovernment-Pläne zu informieren. Dies betrifft etwa und insbesondere das Ministerium des Innern beim eGovernment-Maßnahmenplan 2007 (Ziff. 4.2), die Staatskanzlei (siehe Ziffn. 4.1 und 23.2) und das Ministerium der Justiz (siehe Ziff. 18.13).

Infolge eines grundsätzlichen kritischen Hinweises des Landesbeauftragten informierte der Chef der Staatskanzlei im Februar 2007 die Staatssekretärskonferenz über die Rechtslage.

Der Landesbeauftragte geht davon aus, dass zukünftig durch eine rechtzeitige Unterrichtung seitens der Ressorts seine Beteiligung bei Planungen des Landes erfolgt, hierzu gehören u.a. die eGovernment-Leitprojekte und die eGovernment-Basiskomponenten, aber auch z.B. das IT-Infrastrukturdienste-Konzept für das ITN-LSA oder die Einführung von Voice over IP in der Landesverwaltung. Nur so wird er in die Lage versetzt, seinen gesetzlichen Beratungsauftrag (§ 22 Abs. 4 DSG-LSA) zeitnah und effizient zu erfüllen (vgl. Ziff. 4.2).

1.4 Zusammenfassung und Ausblick

Wo stehen wir im Datenschutz? Ein gesellschaftlicher Diskurs über die aufgeworfenen Fragen findet im Grunde nicht statt, auch wenn die Medien sich stärker diesen Themen zuwenden und in der Bevölkerung das Unbehagen über die Datensammlungen im privaten und öffentlichen Bereich zunimmt. Das **Datenschutzbewusstsein** ist ambivalent, es ist nicht vorhanden beim Einsatz von Kundenkarten, es ist durchaus vorhanden im privaten Bereich, wenn es um unverlangte Spam-Werbung geht, und mehr noch bei Gesundheitsdaten und Kontodaten, dagegen praktisch nicht vorhanden bei den Themen der inneren Sicherheit. Hier gibt es keinen Protest, sondern Desinteresse, Duldung und Gewöhnung, vielleicht auch infolge der Technikprägung der modernen Informationsgesellschaft wie durch das Internet und einer Technologiebereitschaft der Betroffenen.

Der Landesbeauftragte hat schon in der Vergangenheit, so im VII. Tätigkeitsbericht 2005 (Ziff. 1), darauf aufmerksam gemacht, dass es deutliche Tendenzen zum **„gläsernen Bürger“** infolge mehrerer Vorhaben gibt, zum Beispiel: Kontenkontrolle, Jobkarte, Gesundheitskarte, biometrische Ausweise, Telekommunikationsdatenspeicherung, DNA-Analyse zur Strafverfolgung. Hinzu kamen und kommen: Videoüberwachung, verdeckte Ermittlungen, Auskünfte zur Terrorismusprävention. Und natürlich kann der nicht-öffentliche Bereich nicht ausgeblendet werden: Kundenkarten, Scoring, Auskunfteien. Von daher ist die Feststellung, dass sich die freie offene Gesellschaft zu einer „Überwachungsgesellschaft“ entwickelt, nicht nur eine Behauptung von Datenschützern. Die Vermischung von öffentlicher und privater Datenverarbeitung trägt dazu bei.

Im staatlichen Bereich, also das Verhältnis des Grundrechtsträgers zum Staat betreffend, mag die eine oder andere Maßnahme, etwa eine Videoüberwachung an einem Kriminalitätsschwerpunkt, rechtsstaatlich gerechtfertigt sein. Das kann auch für eine zweckgebundene Datenerfassung für die Terrorismusabwehr gelten. Auch die Gesundheitskarte kann doch noch zu einer Erfolgsgeschichte werden. Aber: Häufung und Intensität der Vorhaben geben Anlass zu großer Sorge. Denn es drohen Tendenzen zur umfassenden Überwachung, gestützt durch die technischen Entwicklungen und entsprechenden Möglichkeiten, z.B. mittels der RFID-Technik, und durch die Verknüpfung der Datenverbünde, unterstützt durch eine Vernachlässigung des datenschutzrechtlichen Zweckbindungsgrundsatzes. Besonderes Gefährdungspotential erwächst aus zentralen Datenbeständen (JobCard/ELENA; Melderegister). Das Bundesverfassungsgericht hat in seiner Entscheidung zur GPS-Überwachung (Beschluss vom 12. April 2005, 2 BvR 581/01, BVerfGE 112, 304) erneut vor einer Rundumüberwachung und der Erstellung von

Persönlichkeitsprofilen gewarnt und insoweit von der **Gefahr „additiver Grundrechtseingriffe“** gesprochen.
Der Überwachungsstaat wäre nicht mehr Rechtsstaat. Nur ein verlässlicher Datenschutz schafft Vertrauen, Transparenz bewirkt Akzeptanz. Datenschutz ist Maßstab der Freiheitlichkeit des Gemeinwesens.

Der Ausblick kann nur lauten: Mehr Datenschutz. Aber Anspruch und Wirklichkeit klaffen auseinander. Eine Anhörung im Innenausschuss des Deutschen Bundestages am 5. März 2007 zur Modernisierung des Datenschutzrechts machte Defizite im Bereich des Kredit-Scorings, der RFID-Technik und darüber hinaus erneut des allgemeinen Datenschutzrechts, des BDSG einschließlich der Auditverfahren (das Gesetz zu § 9a BDSG steht seit Jahren aus), deutlich. Das Landesdatenschutzgesetz soll nach Einschätzung aus dem Ministerium des Innern erst nach einer Novellierung des BDSG angefasst werden.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mehrere Regelungsbereiche benannt, die angegangen werden müssen. Die Fortentwicklung des Datenschutzrechts bleibt auf der Agenda (siehe im Einzelnen Ziff. 3.1).

2. Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Die Zahl der schriftlichen Geschäftseingänge (zunehmend mittels E-Mail) und der telefonischen Anfragen, der Eingaben der Bürgerinnen und Bürger und der Beratungs- und Informationsanfragen der öffentlichen Stellen des Landes ist weiter gewachsen. 2005 gab es 3.120 registrierte schriftliche Eingänge, im Jahre 2006 3.412. In die datenschutzrechtliche Auswertung wurden auch alle Landtagsdrucksachen und eine Vielzahl von Bundestags- und Bundesratsdrucksachen einbezogen. Insgesamt in 2005/2006 wurden 1570 schriftliche Stellungnahmen verfasst, darunter befanden sich 115 Petentenfälle.

Im Berichtszeitraum gab es **eine förmliche Beanstandung** nach § 24 DSG-LSA (siehe Ziff. 14.1), daneben in mehreren Fällen erhebliche Rechtsverstöße. Das Niveau des Selbstdatenschutzes der öffentlichen Stellen gemäß § 14 Abs. 1 Satz 1 DSG-LSA ist steigerungsfähig. Die Aufgabe des Datenschutzes darf nicht auf die behördlichen Datenschutzbeauftragten (§ 14a DSG-LSA) reduziert werden. Zu deren Befugnissen ist erneut auf Anlage 20 des VI. Tätigkeitsberichts zu verweisen.

Anlassunabhängige Kontrollen wurden in Ausländerbehörden, Sozialämtern, Kindertagesstätten, Schulen, Kommunalämtern, einer Optionskommune nach ALG II, Justizvollzugsanstalten, dem Landesverwaltungsamt, im Landeskriminalamt, Gerichten sowie einem Finanzamt durchgeführt.

In Vorträgen und Fortbildungsveranstaltungen haben der Landesbeauftragte und die Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle Grundlagen erläutert und für Belange des Datenschutzes geworben.

Der Landesbeauftragte hat zudem seine Presse- und Öffentlichkeitsarbeit insgesamt verstärkt (siehe auch Ziff. 2.4).

Das aktuelle Organigramm der Geschäftsstelle ist diesem Bericht beigefügt (**Anlage 35**).
Zum Ende des Berichtszeitraums lief eine Ausschreibung für eine zunächst auf fünf Jahre befristete IT-Referentenstelle in der Geschäftsstelle; der Landesbeauftragte hatte hierzu im Vorfeld der Beschlussfassung des Landtags zum Haushalt 2007 im Ältestenrat, in Gesprächen mit den Fraktionen und im Finanzausschuss des Landtages für einen Personalaufwuchs geworben und den Bedarf einer zusätzlichen Personalausstattung begründet. In Zeiten von Trends zur Überwachungsgesellschaft und von zunehmenden Gefährdungen des Grundrechts durch automatisierte Datenverarbeitungen wäre es fatal, ausgerechnet beim Datenschutz zu sparen.

Die sachliche Ausstattung des Dienstgebäudes bedarf entsprechender Anpassung. Bei der technischen Ausstattung wurden im Berichtszeitraum Server- und Firewallleistungen verbessert.

2.2 Schwerpunkte - Empfehlungen an Landtag und Landesregierung

Schwerpunkte der Tätigkeit des Landesbeauftragten und der Geschäftsstelle betrafen, wie bereits unter Ziffn. 1.1 bis 1.3 eingeführt, die Bereiche

- innere Sicherheit (Polizei, Rechtspflege, Verfassungsschutz - siehe Ziffn. 17, 18, 22, 24)
- Sozialdatenschutz (siehe Ziffn. 20, 10)
- eGovernment, Technikentwicklung und technisch-organisatorischer Datenschutz (siehe Ziffn. 4, 12).

Die von der Kultusministerkonferenz geplante Einführung eines nationalen Bildungsregisters mit Schülerindividualdaten auf der Basis eines einheitlichen Kerndatensatzes wirft eine ganze Reihe von Fragen verfassungsrechtlicher, statistikrechtlicher und technischer Art auf (siehe Ziff. 19.1).

Im Bereich des Themenfeldes Kindesschutz hat der Landesbeauftragte innerhalb der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Erfahrungsaustausch zu Recht und Praxis von Datenübermittlungen zur Vermeidung und Beseitigung von Kindeswohlgefährdungen angestoßen (siehe Ziff. 20.19).

<u>Empfehlungen an Landtag bzw. Landesregierung</u>

- **Regelung gemäß der Grundsätze des Bundesverfassungsgerichts zum Kernbereichsschutz privater Lebensgestaltung im Polizeigesetz und Verfassungsschutzgesetz**
- **Überprüfung der Struktur und Aufgaben des GIAZ - Trennungsgebot ernst nehmen**

- **Zuverlässigkeitsüberprüfungen bei Großveranstaltungen rechtsstaatlich regeln**
- **Festhalten an der Ablehnung einer Beteiligung an einer nationalen Schülerdatenstatistik**
- **Einführung eines Informationsfreiheitsgesetzes mittels Vollregelung**
- **generelle Befristung und Evaluierung von Eingriffsgesetzen, strenge Zweckbindung der Datenerhebungen**
- **Einbeziehung des Landesbeauftragten in Planungen des eGovernment**
- **Technikfolgenabschätzung des Gesetzgebers**

2.3 Zusammenarbeit mit anderen Institutionen

Die Zusammenarbeit mit dem **Landtag** insbesondere im Zusammenhang mit der Beratungsaufgabe des Landesbeauftragten (siehe § 22 Abs. 4 DSG-LSA) war wiederum intensiv. Erstmals wurde der Landesbeauftragte durch einen Landtagsausschuss um eine Prüfung in einem Einzelvorgang ersucht (§ 22 Abs. 5 DSG-LSA - siehe Ziff. 17.3).

Die Zusammenarbeit mit den **Landtagspräsidenten** Prof. Dr. Adolf Spotka und - seit der im April 2006 begonnenen 5. Legislaturperiode - Dieter Steinecke und seiner Landtagsverwaltung war vertrauensvoll. Die Geschäftsstelle des Landesbeauftragten ist beim Landtagspräsidenten eingerichtet. Die vorübergehende Wahrnehmung der Aufgaben der behördlichen Datenschutzbeauftragten der Landtagsverwaltung durch eine Mitarbeiterin aus der Geschäftsstelle des Landesbeauftragten hat sich tatsächlich nicht bewährt und wurde auch aus rechtlichen Gründen - um eine Aufgabenkollision zu vermeiden - aufgegeben.

Die Beratung und Kontrolle der **Exekutive**, der Landesregierung wie deren nachgeordneten Behörden und den Kommunen, verlief wiederum sachorientiert. Auffällig war der Umstand, dass erbetene Stellungnahmen (vgl. § 23 Abs. 1 Satz 1 und Satz 2 Nr. 1 DSG-LSA) nicht selten zu lange auf sich warten ließen. Dies betrifft den Geschäftsbereich insbesondere der Ministerien der Justiz und des Innern und hängt auch damit zusammen, dass diese Ressorts bei öffentlichen Stellen aus ihrem Geschäftsbereich auf der hinderlichen Einhaltung des Dienstweges bestehen (siehe z.B. für den Bereich der Polizei RdErl. des Ministeriums des Innern vom 9. September 2002, MBl. LSA S. 1140, insbesondere Abschnitt II.). Das wird der unübersehbaren datenschutzrechtlichen Verantwortung der jeweiligen öffentlichen Stelle (§ 14 Abs. 1 Satz 1 DSG-LSA) ebenso wenig gerecht wie der vorerwähnten Verpflichtung zur Unterstützung des Landesbeauftragten, die keine Verzögerungen erlaubt. Ganz allgemein formuliert: Informationsnachfragen und Kontrollen dienen nicht der Skandalsuche, sondern der Sensibilisierung für die Belange des Datenschutzes und der Stärkung der Selbstkontrolle. Das Gesetz sieht im Übrigen im Falle von Beanstandungen die Beteiligung der obersten Landesbehörde vor (§ 24 Abs. 1 Nr. 1 DSG-LSA). Kontrollbesuche werden in aller Regel vorab angekündigt. Der Landesbeauftragte wird trotz der Sorge des Ministeriums, es könne etwas an ihm vorbeigehen, nicht gänzlich von Ad-hoc-Kontrollen absehen können. Selbst wenn auf eine Kenntnisnahme der Stellungnahme (die vom Ministerium aber hier und da auch noch geändert wird) etwa einer Polizeidienststelle nicht verzichtet werden kann, sollte doch in Betracht kommen, jedenfalls ein

Verfahren zu akzeptieren, das neben der unmittelbaren Unterrichtung des Landesbeauftragten eine parallele Kopie an die Aufsichtsbehörde gemäß Dienstweg vorsieht. Der Landesbeauftragte hat dies dem Ministerium des Innern im November 2006 erneut vorgeschlagen und wartet auf eine Antwort.

Gibt es in den Grundsatzfragen und -themen nur wenig datenschutzrechtliche Verbesserungen, so gelingt es andererseits in der alltäglichen Kleinarbeit, zumal im Umgang mit den Behörden anhand konkreter Einzelfälle, auf datenschutzrechtliche Veränderungen hinzuwirken und Maßgaben durchzusetzen. Dieser Tätigkeitsbericht enthält dazu wiederum viele Beispiele.

Mit den **Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich,** dem für Datenschutz zuständigen Referat im Ministerium des Innern als oberster und dem Landesverwaltungsamt als oberer Aufsichtsbehörde (vgl. § 38 BDSG), wurden auf Initiative des Landesbeauftragten Erfahrungsaustausche durchgeführt (siehe auch § 22 Abs. 7 Satz 1 DSG-LSA). Der Landesbeauftragte beteiligte sich auch weiterhin am Erfahrungsaustauschkreis (ERFA-Kreis) Sachsen-Anhalt von betrieblichen Datenschutzbeauftragten.

Zur Frage nach der Unabhängigkeit der Datenschutzaufsicht im nicht-öffentlichen Bereich wird auf eine Darstellung an anderer Stelle verwiesen (Ziff. 3.3).

Sachsen-Anhalt übernahm im Jahre 2006 erstmals den Vorsitz in der **Konferenz der Datenschutzbeauftragten des Bundes und der Länder.** Dies bedeutete zusätzliche inhaltliche Koordinierungsaufgaben und einen erheblichen organisatorischen Aufwand für die Vorbereitung und Durchführung der beiden Tagungen in Magdeburg im März und in Naumburg (Saale) im Oktober. Die Entschließungen der Konferenz zu aktuellen Themenfeldern sind im Anhang dieses Berichts aufgeführt. Eine Reihe von Aufgabenstellungen aus der Vorsitzfunktion wirkten im Jahr 2007 weiter (siehe Ziff. 19.1). Dazu zählte auch die maßgeblich unter Mitwirkung des Landesbeauftragten initiierte Veranstaltung zum **Ersten Europäischen Datenschutztag** am 29. Januar 2007 in der Landesvertretung Sachsen-Anhalts in Berlin (siehe Ziff. 7.4).

Der Landesbeauftragte stieß in der Konferenz eine Grundsatzdiskussion unter Einbeziehung der in Ziff. 1 beschriebenen Entwicklungen an, bei der der nicht-öffentliche Bereich, also etwa die Datensammlungen bei Kunden und Verbrauchern, von Arbeitnehmern und Kreditnehmern nicht außen vor blieb (vgl. auch Ziff. 3.1).

Europäische Themen beherrschen in mehreren Bereichen die Diskussion und Rechtssetzung in Deutschland (siehe Ziffn. 7. und 23.1).
Der Landesbeauftragte nahm an der Internationalen Datenschutzkonferenz im Herbst 2005 teil (siehe Ziff. 7.3 und **Anlage 30**).

2.4 Informationsangebote

2.4.1 Die Internet-Homepage des Landesbeauftragten

Der Landesbeauftragte führt im Internet unter www.datenschutz.sachsen-anhalt.de bereits seit dem Jahr 2000 ein eigenes und Jahr für Jahr umfangreicher werdendes Informationsangebot, das sich außer an die öffentliche Verwaltung Sachsen-Anhalts natürlich auch an die Bürgerinnen und Bürger und die interessierte Fachöffentlichkeit richtet. Die jährlich um ca. 50 % steigenden Besucherzahlen (z.B. im Jahr 2006 monatlich mehr als 40.000 Seitenaufrufe) zeigen, dass das Angebot als informativer und aktueller Bestandteil der Öffentlichkeitsarbeit des Landesbeauftragten im Sinne von § 22 Abs. 4a DSG-LSA wahrgenommen wird. Allerdings hatte das Angebot mit der fortlaufenden Entwicklung weder optisch noch technologisch Schritt halten können, vielmehr war der Landesbeauftragte im Berichtszeitraum zu der Auffassung gelangt, dass das Angebot einer Modernisierung und eines Redesigns bedürfe. Dem kam das Angebot der Staatskanzlei entgegen, das Web-Angebot des Landesbeauftragten, unter Nutzung des Corporate-Design der Landesregierung, in das Landesportal Sachsen-Anhalt unter www.sachsen-anhalt.de zu migrieren. Für die dem Landesbeauftragten von Seiten der Staatskanzlei bei der Migration zuteil gewordene Unterstützung bedankt er sich an dieser Stelle noch einmal. Seit Mitte Januar 2007 erscheint die Website des Landesbeauftragten unter unveränderter Adresse im modernen Design des Landesportals. Dadurch wurde auch die Anzeige dynamisch generierter html-Seiten ermöglicht, die die tele- und medienrechtlich korrekte Darstellung seines Impressums und der anderen gesetzlich vorgeschriebenen Inhalte verbessert. Der Landesbeauftragte wird auch zukünftig seine Internetpräsenz als Informationsquelle weiter ausbauen und pflegen.

Insbesondere für den mit Artikel 1 Nr. 16 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 21. August 2001 (GVBl. LSA S. 348) gem. § 14a DSG-LSA eingeführten “Beauftragten für den Datenschutz” bei öffentlichen Stellen des Landes soll die Homepage, mangels bestehender bzw. begrenzter Fortbildungsmöglichkeiten für diesen Personenkreis, eine Unterstützung bei der täglichen Arbeit bieten. Ein positives Echo aus zahlreichen Anrufen und Nachfragen von behördlichen Datenschutzbeauftragten zu dieser Homepage des Landesbeauftragten zeigt, dass auch in dieser Hinsicht dieses Informationsangebot angenommen und genutzt wird.

2.4.2 Das Virtuelle Datenschutzbüro

Bereits seit einigen Jahren existiert im Internet unter www.datenschutz.de das Virtuelle Datenschutzbüro, das sich als gemeinsamer Service verschiedener Datenschutzinstitutionen versteht. Projekt- und Kooperationspartner sind die Datenschutzbeauftragten des Bundes und der Länder und viele weitere in- und ausländische Datenschutzinstitutionen. Es stellt als öffentliches Portal im WWW eine zentrale Informations- und Anlaufstelle für Datenschutzfragen dar. Zum 1. Januar 2006 ist auch der Landesbeauftragte auf seinen Antrag hin förmlich als Projektpartner des Virtuellen Datenschutzbüros aufgenommen worden. Damit hat er die Möglichkeit, seinen Zuständigkeitsbereich betreffende Belange des Datenschut-

zes von überregionaler Bedeutung einem wesentlich größeren Interessentenkreis zu vermitteln.

3. Allgemeines Datenschutzrecht - aus der Alltagspraxis

3.1 Fortentwicklung des Datenschutzrechts

Bereits vor Inkrafttreten der letzten BDSG-Novelle im Mai 2001 hat das Bundesministerium des Innern ein Gutachten zur „Modernisierung des Datenschutzrechts“ bei Fachleuten aus den Bereichen Datenschutzrecht und Informatik in Auftrag gegeben. Das im November 2001 fertiggestellte Gutachten enthält eine Fülle von Anregungen und Vorschlägen zur Optimierung datenschutzrechtlicher Bestimmungen (Vereinfachungen; Stärkung der Selbstbestimmung).
Der Deutsche Bundestag hat in seinem Beschluss „Umfassende Modernisierung des Datenschutzrechts voranbringen“ (BT-Drs. 14/9709) bereits die Notwendigkeit der Modernisierung des Datenschutzrechtes zum Ausdruck gebracht. Die Bundesregierung hatte in der Koalitionsvereinbarung für die 15. Legislaturperiode auch ein entsprechendes Vorhaben aufgenommen.

Die Datenschutzbeauftragten des Bundes und der Länder hatten hierzu auf ihrer 65. Konferenz am 27./28. März 2003 die Entschließung „Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung“ gefasst (vgl. VII. Tätigkeitsbericht, Anlage 1).
Anlässlich der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 wurde das Anliegen in einer ausführlichen Entschließung „Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz“ bekräftigt (**Anlage 2**).

Ob das Vorhaben der Modernisierung des Datenschutzrechts weiterverfolgt wird, erscheint leider offen. Die Koalitionsvereinbarung für die 16. Legislaturperiode enthält dazu nichts Konkretes. Ebenso ist fraglich, ob das Vorhaben eines Durchführungsgesetzes zu § 9a BDSG (Audit-Gesetz) weiterverfolgt wird. Auch hierzu enthält die Koalitionsvereinbarung für die 16. Legislaturperiode nichts Konkretes. Die Koalitionsvereinbarung vom 11. November 2005 sah allerdings vor zu prüfen, ob im Hinblick auf den Abbau überflüssiger Bürokratie Änderungen vorgenommen werden können. Das erste Gesetz zum Abbau bürokratischer Hemmnisse, insbesondere in der mittelständischen Wirtschaft, vom 22. August 2006 (BGBl. I S. 1970) enthält danach einige Änderungen des BDSG. Diese betreffen die Lockerung der Meldepflicht zu automatisierten Verfahren bzw. der Bestellung von betrieblichen Beauftragten für den Datenschutz, deren Position allerdings gestärkt wurde.

Im Innenausschuss des Bundestages hat am 5. März 2007 eine Anhörung zum Thema „Modernisierung des Datenschutzes“ stattgefunden. Mehrere Datenschutzbeauftragte haben dort die Gelegenheit nutzen können, auf den Bedarf gesetzlicher Optimierung hinzuweisen. Dies betrifft die Themenbereiche u.a. der Harmonisierung des Datenschutzrechtes, die Datenschutz-Gütesiegel, den Datenschutz durch Technik und den Verbraucherdatenschutz. Erwähnt wurde auch

die Gewährleistung des Datenschutzes durch ein Prozessmanagement in den datenverarbeitenden Stellen.

Am 29. März 2007 folgte der Deutsche Bundestag einer Beschlussempfehlung des Innenausschusses vom 28. März 2007, BT-Drs. 16/4882, zum 20. Tätigkeitsbericht (2003 und 2004) des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Darin wird ebenfalls die zügige Modernisierung und Weiterentwicklung des Datenschutzrechts gefordert. Erwähnt sind insbesondere ein Datenschutzauditgesetz, Regelungen zur RFID-Technologie und zur Begrenzung von Profilbildungen sowie zur Genomanalyse, ein Auskunftsanspruch gegenüber der Steuerverwaltung sowie das internationale Datenschutzniveau.

Auch eine seit langem ausstehende differenzierte Regelung der vielschichtigen datenschutzrechtlichen Probleme im Rahmen von Arbeitsverhältnissen (Arbeitnehmerdatenschutzgesetz) konkretisiert sich nicht. Der Deutsche Bundestag hatte schon in seiner Entschließung zum 19. Tätigkeitsbericht (2001 und 2002) des Bundesbeauftragten für den Datenschutz (BT-Drs. 15/4597) auf die Notwendigkeit hingewiesen, Rechtssicherheit für Arbeitgeber und Arbeitnehmer zu schaffen. Die Bundesregierung hat jedoch in ihrer Antwort auf eine Große Anfrage der FDP-Fraktion (BT-Drs. 15/4725) mitgeteilt, dass es vor der Schaffung gesetzlicher Regelungen sinnvoll sei, Überlegungen auf der Ebene der Europäischen Kommission zum Arbeitnehmerdatenschutz abzuwarten. Der Koalitionsvereinbarung für die 16. Legislaturperiode ist hierzu ebenfalls nichts Konkretes zu entnehmen. Die 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007 hat erneut die Regelungsnotwendigkeit erörtert und die Entschließung „GUTE ARBEIT in Europa nur mit gutem Datenschutz“ gefasst (**Anlage 23**).

3.2 Änderungen im Datenschutzgesetz Sachsen-Anhalt

In den Berichtszeitraum fiel das Verfahren zur Verabschiedung des Ersten Rechts- und Verwaltungsvereinfachungsgesetzes. Dieses Gesetz vom 18. November 2005 bezieht sich in Art. 15 auch auf das Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA - GVBl. LSA, S. 698, 701).

Ergänzt wurde die Regelung des § 15 Abs. 1 Satz 1 Nr. 1 DSG-LSA. Danach ist dem Betroffenen auf Antrag Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen. Hier wurde ergänzt, dass sich die Auskunft auch auf erfolgte Übermittlungen an Dritte erstrecken soll. Bedenken, dass hiermit die Verpflichtung zur Speicherung jeglicher Übermittlung und damit erheblicher Verwaltungsaufwand begründet werden könnte, konnten ausgeräumt werden. Der Landesbeauftragte konnte darauf hinweisen, dass es sich auch nach der Begründung des Gesetzentwurfs um eine Klarstellung handelt. Lediglich sofern entsprechende Angaben bereits gespeichert sind, ist auch darüber Auskunft zu erteilen. Eine gesonderte Speicherung für Auskunftszwecke ist dagegen nicht erforderlich.

Weiterhin wurde die gesetzliche Regelung des § 22 Abs. 4 Satz 2 DSG-LSA, wonach der Landesbeauftragte über Planungen des Landes zu automatisierten In-

formationssystemen zu unterrichten ist, systematisch sinnvoll an anderer Stelle platziert. In § 14 Abs. 1 DSG-LSA wurde als Satz 2 angefügt, dass der Landesbeauftragte rechtzeitig über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu unterrichten ist. Hierzu konnte der Landesbeauftragte vor dem Ausschuss für Inneres des Landtages von Sachsen-Anhalt nochmals darauf hinweisen, dass der Gesetzgeber damit eine **„Bringschuld“** der Landesbehörden formuliert. Schon in seinem VII. Tätigkeitsbericht hatte der Landesbeauftragte zu Ziff. 7.1 (eGovernment-Konzept in Sachsen-Anhalt) auf die Notwendigkeit rechtzeitiger Unterrichtung hingewiesen. Auf diesbezügliche Defizite ist bereits oben unter Ziff. 1.3 eingegangen worden.

In ihrer Stellungnahme zum Tätigkeitsbericht hat die Landesregierung mitgeteilt, dass sie rechtzeitige Vorkehrungen zum Datenschutz durch die Beteiligung des Landesbeauftragten für wichtig hält. Seine frühzeitige Einbindung kann späteren zeit- und kostenintensiven Umplanungen entgegenwirken. Eine besondere Form der Unterrichtung sei aber nicht vorgesehen. Sie könne, soweit rechtzeitig und vollständig, auch im Koordinierungssausschuss Informationstechnik (IT-KA) erfolgen.

Der Landesbeauftragte muss von den Landesbehörden so umfassend und frühzeitig informiert werden, dass die von ihm einzubringenden datenschutzrechtlichen Belange noch ausreichende Berücksichtigung finden können. Es geht um vorwirkenden Grundrechtsschutz. Auch wenn die Unterrichtung nicht an eine besondere Form gebunden ist, reicht die - möglicherweise zu späte - Gelegenheit der Kenntnisnahme im Rahmen von Besprechungen und Ausschusssitzungen in der Regel nicht aus. Es besteht allenfalls die schlichte Möglichkeit für den Landesbeauftragten, sich selbst als Gast im IT-KA zu informieren. Der datenschutzrechtliche Prüfungsumfang geht zudem meist über das im IT-KA behandelte Erörterungsspektrum hinaus. Der Landesbeauftragte weist daher darauf hin, dass § 14 Abs. 1 S. 2 DSG-LSA der Landesregierung eine Pflicht zu einer (Unterrichtungs-)Handlung auferlegt.

Unter anderem die Änderungen durch das Erste Rechts- und Verwaltungsvereinfachungsgesetz machten es erforderlich, die **Verwaltungsvorschriften zum DSG-LSA** zu ändern. Ein erster Entwurf lag erst ein Jahr nach Inkrafttreten der Gesetzesänderung vor. Der Landesbeauftragte wurde durch das Ministerium des Innern beteiligt. Dank der konstruktiven Zusammenarbeit war es möglich, in wesentlichen Punkten zur Optimierung und Erhöhung der Verständlichkeit beizutragen. Dies betraf u.a. die Darstellungen zu den Vereinigungen im Sinne des § 3 Abs. 1 DSG-LSA und damit auch die Frage nach der Kontrollzuständigkeit für die eher wirtschaftlich orientierten Einrichtungen. Betroffen war auch die Erläuterung zur Pflicht der frühzeitigen Beteiligung des Landesbeauftragten nach § 14 Abs. 1 Satz 2 DSG-LSA. Die geänderten Verwaltungsvorschriften sind auch im Mai 2007 noch nicht veröffentlicht.

3.3 Unabhängigkeit der Datenschutzaufsicht

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bestimmt in Art. 28 Abs. 1 Satz 1 und 2, dass die Mitgliedstaaten öffentliche Stellen vorsehen, die die Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften überwachen. Weiterhin ist ausdrücklich geregelt, dass diese Stellen die ihnen zugewiesenen Aufgaben in **völliger Unabhängigkeit** wahrnehmen. Die Ausgestaltung der aufsichtsbehördlichen Datenschutzkontrolle in den Bundesländern ist unterschiedlich. Grundsätzlich sind die Landesbeauftragten für den Datenschutz zuständig für die Kontrolle im öffentlichen Bereich. Einige Landesbeauftragte sind darüber in unterschiedlicher Ausgestaltung auch zuständig für die datenschutzrechtliche Kontrolle im nicht-öffentlichen Bereich (Aufsichtsbehörde nach § 38 Abs. 6 BDSG). In Sachsen-Anhalt ist das Landesverwaltungsamt im Ressort des Ministeriums des Innern Aufsichtsbehörde für die Datenverarbeitung nicht-öffentlicher Stellen nach § 38 BDSG. Auch in anderen Bundesländern wird die Datenschutzaufsicht im nicht-öffentlichen Bereich durch Behörden der allgemeinen Landesverwaltung wahrgenommen. Soweit Landesbeauftragte für den Datenschutz die Aufgaben nach § 38 BDSG wahrnehmen, unterliegen sie teilweise nicht nur der Rechtsaufsicht, sondern auch der Fachaufsicht.

Aufgrund dieser Aufsichtsstruktur und der Vorgabe der Datenschutzrichtlinie der EG zur völligen Unabhängigkeit hat die Kommission der Europäischen Gemeinschaften im Juli 2005 gegen die Bundesrepublik Deutschland ein Vertragsverletzungsverfahren eingeleitet. Sie verweist auf den Erwägungsgrund 62 der Richtlinie, wonach die Errichtung unabhängiger Kontrollstellen in den Mitgliedstaaten ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten ist. Auch das Zusatzprotokoll zum Europäischen Übereinkommen des Europarates zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr SEV Nr. 181 vom 8. November 2001 verlangt die „völlige Unabhängigkeit“ der Kontrollstellen. Der erläuternde Bericht zum genannten Zusatzprotokoll sieht dabei folgende Umstände, die die Unabhängigkeit ausmachen können:

- Zusammensetzung der Kontrollstelle
- Art und Weise der Ernennung ihrer Mitglieder
- Bedingungen zur Beendigung des Amtes
- Zuweisung ausreichender Mittel an die Kontrollstelle
- Keine Anweisungen oder Einmischungen von außen bei der Beschlussfassung.

Unter Zugrundelegung der vorgenannten Rechtsauffassung kommt die Europäische Kommission zur Annahme, dass die Organisationsformen der Kontrollstellen und damit die Datenschutzaufsicht in einzelnen Bundesländern daher nicht „völlig unabhängig“ seien.

Die Stellungnahme der Bundesregierung gegenüber der EU-Kommission im Vorverfahren, zuletzt im Februar 2007, geht demgegenüber davon aus, dass „Unabhängigkeit“ in der Richtlinie eine funktionelle Unabhängigkeit bezeichnet. Eine darüber hinausgehende organisatorische Unabhängigkeit verlange die Richtlinie dagegen nicht. Eine organisatorische Unabhängigkeit sei im ursprünglichen Richtlinienentwurf noch vorgesehen gewesen, die Formulierung sei jedoch zugunsten des jetzt geltenden Wortlautes aufgegeben worden. Maßgeblich sei die Unabhängigkeit von sachfremden Einflüssen. Zudem erforderten das in Art. 20 Abs. 2, Art. 28 Abs. 1 GG verankerte Demokratieprinzip und der Grundsatz der parlamentarischen Verantwortung der Regierung die Abhängigkeit der Amtsleiter von Weisungen des zuständigen Ressortministers. Dies gelte insbesondere bei möglichen Eingriffen in die Rechte der Bürger und Unternehmen. Die Datenschutzaufsichtsbehörden für die Privatwirtschaft könnten nämlich in subjektive Rechte von Unternehmen und Bürgern durch Anordnungen, Betretungs- und Einsichtsbefugnisse eingreifen (Art. 28 Abs. 3 Richtlinie 95/46/EG).

Die 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 hat sich ebenfalls mit der Unabhängigkeit der Datenschutzaufsicht befasst. Einzelne Länder berichteten von Plänen, die Kontrolle über den öffentlichen Bereich mit der Aufsicht über den nicht-öffentlichen Bereich in ihren Ländern zusammenzulegen. Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen unterliegen. Es wurde die Entschließung „Unabhängige Datenschutzkontrolle in Deutschland gewährleisten“ (**Anlage 3**) gefasst. In Niedersachsen ist, nachdem zwischenzeitlich das Innenministerium die Datenschutzkontrolle über den privatwirtschaftlichen Bereich an sich gezogen hatte, wieder der Landesbeauftragte für den nicht-öffentlichen Bereich zuständig. Auch andere Landesbeauftragte sind mit der Aufsicht für den nicht-öffentlichen Bereich betraut worden.

3.4 Akteneinsicht beim Landesbeauftragten

Ein Petent hatte sich an den Landesbeauftragten gewandt, da er in den Akten eines Sozialamtes, in die er anlässlich eines Gerichtsverfahrens um Sozialhilfeleistungen Einsicht nahm, umfängliche Informationssammlungen zu seiner Person und seinen Bekannten gefunden hatte, u.a. zur kriminellen Vergangenheit. Auch war seinem weiteren Antrag auf Akteneinsicht beim Sozialamt nicht in der gewünschten Form Rechnung getragen worden. Der Landesbeauftragte hatte das Sozialamt auf die datenschutzrechtlichen Erfordernisse hingewiesen und dem Petenten Anregungen zur Präzisierung seines Antrags gegeben (vgl. §§ 25, 83 SGB X). Siehe im Übrigen Ziff. 20.28

Einige Zeit später meldete sich der Prozessbevollmächtigte des Petenten und bat um Akteneinsicht beim Landesbeauftragten. Dem Prozessbevollmächtigten konnte die Problematik zur Akteneinsicht beim Landesbeauftragten zu seiner Zufriedenheit ausführlich dargelegt werden.

Ein eigenständiger Anspruch auf Akteneinsicht gegenüber dem Landesbeauftragten für den Datenschutz ist nicht gegeben. Auch darüber hinaus kam eine Akteneinsicht nach Berücksichtigung der Gesamtumstände und der Interessen der Beteiligten nicht in Betracht. Insbesondere war hierzu auf § 15 Abs. 2 DSG-LSA zu verweisen, wonach Abs. 1 (Auskunftsanspruch des Betroffenen) nicht für personenbezogene Daten gilt, die ausschließlich Zwecken der Datenschutzkontrolle dienen. § 21 Abs. 1a i.V.m. § 10 Abs. 4 DSG-LSA weisen ebenfalls auf die besonders enge Zweckbindung der durch den Landesbeauftragten erhobenen Daten hin. Weiterhin wurde auf § 15 Abs. 6 DSG-LSA verwiesen, wonach der Landesbeauftragte für den Datenschutz von der verantwortlichen Stelle eine Auskunft erhält, falls diese dem Betroffenen verweigert worden ist. Auch dann darf die Mitteilung des Landesbeauftragten an den Betroffenen keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen.
Auch unter Bezugnahme auf obergerichtliche Rechtsprechung wurde erläutert, dass die Entscheidung über die Akteneinsicht bei der aktenführenden Stelle verbleiben soll. Der Landesbeauftragte hat nach § 23 DSG-LSA umfänglichen Zugang zu den Unterlagen der kontrollierten öffentlichen Stellen. Sie überlassen ihm in der Regel die erforderlichen Vorgänge im Vertrauen auf die Bindung an den Zweck der Datenschutzkontrolle. Da der Landesbeauftragte die Vorgänge nicht inhaltlich bearbeitet, ist die Entscheidung über den Zugang zu den darin enthaltenen Informationen lediglich bei der verantwortlichen Stelle sachgerecht angesiedelt.

3.5 Informationsfreiheitsgesetz

Unter Ziff. 1. des VII. Tätigkeitsberichtes hat der Landesbeauftragte im Rahmen eines Ausblicks auf die künftige Entwicklung des Datenschutzes auch die Frage nach einem Informationsfreiheitsgesetz des Landes angesprochen. Auch in der 5. Legislaturperiode ist durch einen Teil der Opposition ein Gesetzentwurf für ein Informationszugangsgesetz des Landes eingebracht worden, wie schon in der 3. und 4. Legislaturperiode.

Inhaltlich gibt es eine Vielzahl von tatsächlichen und vermeintlichen Aspekten, die bei der Schaffung eines Anspruchs des Bürgers auf Zugang zu amtlichen Informationen aus dem Weg geräumt werden müssen. Diskutiert werden u.a. eine befürchtete Mehrbelastung des Personals, fiskalische Interessen, Sicherheitserwägungen sowie das Interesse an der Geheimhaltung von Betriebs- und Geschäftsgeheimnissen. Diese teilweise spekulativen Bedenken sind Ausdruck eines Verständnisses einer öffentlichen Verwaltung, die aus obrigkeitlichen Ursprüngen herrührend vom Verbot der unbefugten Offenbarung von Amtsgeheimnissen geprägt war. Demgegenüber steht das nachvollziehbare Anliegen, das demokratische Staatswesen im Zeitalter der Informationsgesellschaft durch Schaffung und Stärkung von Bürgerrechten zu unterstützen. Wie so oft ist der sachgerechte Ausgleich gefragt zwischen den freiheitlichen Bürgerrechten auf der einen und den sicherheitsorientierten Verwaltungsinteressen auf der anderen Seite. Hierbei ist, wie der Landesbeauftragte bereits im VII. Tätigkeitsbericht darlegte, Gelassenheit und der Blick über die Landesgrenzen angezeigt.

Zur Zeit der Erörterung des Gesetzentwurfs in den Ausschüssen des Landtages in der 4. Legislaturperiode hatten bereits vier Bundesländer entsprechende Informationszugangsregelungen. Parallel lief das Verfahren zum Erlass des Informationsfreiheitsgesetzes des Bundes. Der Gesetzesbeschluss des Bundestages zum Informationsfreiheitsgesetz hat am 8. Juli 2005 den Bundesrat passiert, so dass das Gesetz zum 1. Januar 2006 in Kraft treten konnte (BGBl. I 2005, S. 2722).

Kurz vor der maßgeblichen Entscheidung des Bundesrates hatten die beteiligten Ausschüsse des Landtages den Gesetzentwurf für ein Informationszugangsgesetz abgelehnt. Der Landesbeauftragte hat daraufhin öffentlich deutlich gemacht, dass der Umstand, dass der Bundesrat das Informationsfreiheitsgesetz des Bundes gebilligt hat, Anlass sein sollte, auch in Sachsen-Anhalt nochmals über ein eigenes Landesgesetz nachzudenken. Die Erfahrungen in den Bundesländern, die bereits Informationsfreiheitsgesetze haben, seien positiv. Auch der internationale Vergleich gebiete, erneut über die Angelegenheit nachzudenken. Die demokratischen Akteneinsichtsrechte der Bürger führen zur Transparenz der Verwaltung in der Informationsgesellschaft. Rechte Dritter könnten im Verfahren selbst hinreichend beachtet werden.

Anfang 2007 besitzen bereits acht Bundesländer ein Informationszugangsgesetz. Die Beratungen des erneuten Entwurfs in den Ausschüssen des Landtages werden daher mit besonderem Interesse zu beobachten sein, zumal die Landesregierung für den Sommer 2007 einen eigenen Entwurf angekündigt hat. Zu einem Referentenentwurf des Ministeriums des Innern konnte der Landesbeauftragte bereits kritisch Stellung nehmen, u.a. zur (inzwischen aufgegebenen) Absicht, ein anwenderunfreundliches Verweisungsgesetz auf die Bundesregelung vorzusehen.

3.6 Aus Einzelfällen der täglichen Beratungen

Zuständigkeit

Der Landesbeauftragte erhält viele Anrufe besorgter Bürger mit der Frage, ob bestimmte Verfahren datenschutzrechtlich zulässig wären. Häufig beziehen sich diese Anfragen auf den nicht-öffentlichen Bereich. Nach § 19 DSG-LSA können sich Betroffene jedoch nur an den Landesbeauftragten wenden, wenn sie der Ansicht sind, durch öffentliche Stellen in ihren Rechten verletzt worden zu sein. Zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich nach § 38 BDSG ist das Landesverwaltungsamt in Halle. Geht es daher um datenschutzrelevante Verhaltensweisen von Unternehmen oder Geschäftsleuten, muss der Landesbeauftragte die Anrufer an das Landesverwaltungsamt in Halle verweisen.

Ein Beispiel ist die Anfrage eines Anrufers zur Videoanlage an der Wohnung seines Nachbarn in einem Mietshaus. Der überwachte sein vor dem Haus auf der Straße abgestelltes Auto. Der Anrufer hielt dies für datenschutzrechtlich bedenklich.

Erläuterungen zum Zuständigkeitsbereich des Landesbeauftragten für den Datenschutz betreffen nicht nur die Abgrenzung zum nicht-öffentlichen Bereich, sondern vor allem auch die Beschränkung auf spezifisch datenschutzrechtliche Fragen. Gelegentlich liegt der Schwerpunkt der Anfrage bei der Suche nach einer höheren Instanz in Sachen materieller Gerechtigkeit. Die Frage nach konkreten Datenverarbeitungsprozessen wird getragen von der Unzufriedenheit über bestimmte gesetzliche Vorgaben oder deren Umsetzung durch öffentliche Stellen. Dazu ist dann häufig darauf hinzuweisen, dass es nicht Aufgabe des Landesbeauftragten ist, für die Befriedigung materieller Ansprüche Sorge zu tragen, sondern lediglich die Einhaltung der persönlichkeitsschützenden datenschutzrechtlichen Vorschriften zu kontrollieren.

DSG-Kommentar

Gelegentlich wird der Landesbeauftragte gefragt, ob und welche Literatur zum Datenschutzrecht er den anfragenden öffentlichen Stellen empfehlen könne. Insbesondere richtet sich das Interesse auf eine aktuelle Kommentierung zum DSG-LSA. Es ist leider darauf hinzuweisen, dass es derzeit keine aktuelle Kommentierung zum DSG-LSA gibt. Hinweise zur Interpretation des Gesetzestextes lassen sich daher zunächst nur aus den Verwaltungsvorschriften (VV-DSG-LSA vom 31. August 2002, MBl. LSA S. 1091) entnehmen (vgl. oben Ziff. 3.2). Weitere Hinweise können sich aus Kommentierungen zu Datenschutzgesetzen anderer Länder oder zum Bundesdatenschutzgesetz ergeben. Dabei ist jedoch stets zu berücksichtigen, dass die gesetzlichen Regelungen zwar ähnlich sind, im Einzelfall aber entscheidende Abweichungen enthalten können.

Videoüberwachung

Häufig sind Planungen zur Einrichtung von Videoüberwachungen Anlass für Anfragen beim Landesbeauftragten. Hierzu hatte der Landesbeauftragte schon wiederholt in Tätigkeitsberichten Stellung genommen (vgl. u.a. VII. Tätigkeitsbericht, Ziffn. 11.2, 14.2, 17.1.2).
Der behördliche Datenschutzbeauftragte eines Landkreises war vom Leiter des Berufschulzentrums in Trägerschaft des Landkreises auf die Problematik angesprochen worden. Geplant war die Vergabe zu einer Videoüberwachung der sieben Notausgänge der Einrichtung. Hierzu konnte der Landesbeauftragte in einer ersten fernmündlichen Beratung auf die Rahmenbedingungen nach § 30 DSG-LSA hinweisen. Unbeschadet der Möglichkeiten, zum Schutz des Eigentums oder Besitzes oder zur Kontrolle von Zugangsberechtigungen Videoüberwachungen durchführen zu können, war zunächst zu prüfen, ob geeignete Maßnahmen in Betracht kommen, um die befürchteten Gefahren anderweitig abzuwenden (milderes Mittel). Auf die Notwendigkeit der Einhaltung technisch-organisatorischer Maßnahmen nach § 6 DSG-LSA wurde hingewiesen. Der Grundsatz der Verhältnismäßigkeit der Überwachungsmaßnahme wurde erörtert (Überwachung nur außerhalb der Öffnungszeiten). Für den Fall, dass eine Aufzeichnung überhaupt in Betracht kommen sollte, wurde auf die Einhaltung kurzer Löschungsfristen hingewiesen.

Bestellung des behördlichen Datenschutzbeauftragten

Aus einer Verwaltungsgemeinschaft kam die Anfrage, ob ein Formular für die Bestellung eines behördlichen Datenschutzbeauftragten vorläge. Zur Institution des behördlichen Datenschutzbeauftragten wurde zunächst auf die ausführliche Darstellung auf der Homepage des Landesbeauftragten hingewiesen. Die Anlage 4 zu den Verwaltungsvorschriften (VV-DSG-LSA) vom 31. August 2002, MBl. LSA S. 1091, ist ein Formularmuster zur Einsetzung zur/zum Beauftragten für den Datenschutz nach § 14a Abs. 1 DSG-LSA.

Akteneinsicht durch Praktikanten

Ein Krankenhaus eines Landkreises fragte an, ob Praktikanten, die bei einem Dritten (Dienstleister) in Ausbildung sind und im Krankenhaus ein Praktikum absolvieren, Personalaktendaten zur Kenntnis erhalten dürfen. Hierzu wurde darauf hingewiesen, dass es sich bei dem Krankenhaus um eine öffentliche Stelle nach § 3 Abs. 1 DSG-LSA handelt. Nach § 28 Abs. 1 DSG-LSA i.V.m. § 3 Abs. 2 Nr. 1 DSG-LSA gelten daher für den Umgang mit Personalaktendaten die Vorschriften des Beamtengesetzes. Nach § 90 Abs. 3 BG LSA dürfen nur Beschäftigte zu Personalaktendaten Zugang haben, die mit der Bearbeitung beauftragt sind. Es gilt das Personalaktengeheimnis. Im Interesse des zu schützenden Persönlichkeitsrechts des Personals begegnet der Zugang von Außenstehenden zu Personalakten daher grundsätzlich Bedenken. Andererseits ist zu berücksichtigen, dass Aus- und Fortbildung eine Notwendigkeit ist, die sich in realistischer und effizienter Form zumeist nicht ohne Kenntnisnahme von personenbezogenen Informationen durchführen lässt. Unter Einhaltung bestimmter datenschutzrechtlicher Rahmenbedingungen ist daher die Kenntnisnahme personenbezogener Informationen durch Praktikanten grundsätzlich möglich. Notwendige Voraussetzung dürfte u.a. sein, dass die Praktikanten auf das Datengeheimnis (§ 5 DSG-LSA) sowie nach dem Verpflichtungsgesetz zur Verschwiegenheit verpflichtet sind. Zudem dürfen sie nur Einsicht in diejenigen Unterlagen erhalten, die für die jeweilige Praktikumarbeit unbedingt erforderlich sind. Die Kenntnisnahme von besonders sensiblen Daten bzw. Daten von Personen, die den Praktikanten bekannt sein können, sollte möglichst vermieden werden. Der Datenzugriff hat sich daher im Einzelfall an der Erforderlichkeit zu orientieren.

Soweit Kenntnisse in der Lohnbuchhaltung zur Ausbildung von Berufen des Gesundheitswesens gehören, ist es danach vertretbar, Praktikanten mit der Betreuung personalwirtschaftlicher Vorgänge zu beauftragen und im erforderlichen Umfang Einsicht in Personalakten zu gewähren. Weitere Hinweise zum Einsatz von Praktikanten finden sich im II. Tätigkeitsbericht, Ziff. 20.13 und Ziff. 21.18 sowie im III. Tätigkeitsbericht, Ziff. 11.3 und 21.18.

Überwachung dienstlicher Telefonate

Ein Personalratsmitglied einer Kommune erkundigte sich besorgt nach der datenschutzrechtlichen Zulässigkeit der Überprüfung der dienstlichen Telefonate durch den Amtsleiter. Aufgrund eines konkreten Hinweises war in einem Einzelfall nach Überprüfung festgestellt worden, dass ein Mitarbeiter private Telefonate nicht als

solche geführt und abgerechnet, sondern als Dienstgespräche geführt hat. Nunmehr beabsichtige der Amtsleiter, eine Telefonliste der Mitarbeiter zu deren Dienstgesprächen zu kontrollieren. Hierzu konnte darauf hingewiesen werden, dass ein legitimes Interesse des Arbeitgebers besteht, den wirtschaftlichen, sparsamen und dienstlich veranlassten Umgang mit den vorhandenen Haushaltsmitteln zu kontrollieren (Kostenkontrolle). Dabei dürfte allerdings das Interesse der Beschäftigten am Schutz ihrer Persönlichkeit nicht übersehen werden. Grundsätzlich gehört zwar die Beobachtung ihres dienstlichen Verhaltens zu den Ausflüssen des Beschäftigungsverhältnisses, die keine unzumutbare Beeinträchtigung des Persönlichkeitsrechtes darstellen. Allerdings darf die legitime Kontrolle des dienstlichen Verhaltens des Mitarbeiters nicht in eine persönlichkeitsbeeinträchtigende und damit unzulässige Vollkontrolle ausufern. Der Landesbeauftragte hat daher angeregt, in Absprache mit der Dienststelle ein angemessenes Verfahren zu finden, das die beteiligten Interessen in einen sachdienlichen Ausgleich bringt. In diesem Zusammenhang kann auf die Darstellungen im VII. Tätigkeitsbericht zur Erfassung von dienstlichen Telefonaten von Personalratsmitgliedern und dortigen weiteren Hinweise verwiesen werden (Ziff. 16.12).

Verwendung von Protokolldaten

Der Hauptamtsleiter eines Landkreises teilte mit, dass man in seiner Dienststelle mit einem Antivirenprogramm wiederholt einen Virus im Netz des Landkreises festgestellt habe. Der Administrator habe daraufhin einen einzelnen PC und damit eine bestimmte nutzende Person festgestellt, die im Internet pornographische Seiten aufgerufen hatte, die virenbehaftet waren. Die private Nutzung des Internet war verboten. Nunmehr frage man sich, ob die Nutzung der Protokolldaten beispielsweise zur Darlegung des Umfangs der unzulässigen Nutzung des dienstlichen Internet gegenüber dem Gericht mit der Regelung des § 28 Abs. 4 DSG-LSA vereinbar sei. § 28 Abs. 4 DSG-LSA sieht vor, dass Daten der Beschäftigten, die im Rahmen technischer und organisatorischer Maßnahmen nach § 6 DSG-LSA gespeichert wurden, nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden dürfen. Hierzu konnte zunächst darauf hingewiesen werden, dass die Nutzung der Daten jedenfalls dann noch dem Zweck der technisch-organisatorischen Maßnahmen dient, wenn die Informationen dazu verwendet werden, die sicherheitsrelevante Fehlnutzung des Internets zu unterbinden. Zu den Zwecken der Datenschutzkontrolle, der Datensicherung und der Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage gehören aber nicht nur beispielsweise die Sperrung des Zugangs zu einzelnen Internetseiten. Vielmehr gehört hierzu das gesamte Spektrum der erforderlichen Maßnahmen zur abschließenden Unterbindung von festgestellten Datenschutzverstößen. Die Verwendung der Protokolldaten für konkrete Folgemaßnahmen gegenüber dem festgestellten Mitarbeiter ist damit noch von der Zweckbindung erfasst. Die vorgenannte Regelung soll die Verwendung der Daten für Routinekontrollen ausschließen, nicht die Verfolgung von delinquenten Zufallsfunden.

4. Entwicklung der automatisierten Datenverarbeitung - eGovernment

4.1 IT-Konzept der Landesverwaltung Sachsen-Anhalt

Am 15. November 2005 wurde das vom Ministerium des Innern vorgelegte IT-Konzept - Fortschreibung 2005 - vom Kabinett zustimmend zur Kenntnis genommen. Mittelfristig beruht die IT-Strategie des Landes auf einer Zusammenführung aller zentralisierbaren Rechenzentrumsdienstleistungen (einschließlich der IT-Infrastruktur), der Standardisierung der IT-Landschaft sowie der Institutionalisierung der Kooperation mit der kommunalen Ebene zur gemeinsamen Nutzung einheitlicher IT-Standards. Durch eine interministerielle Arbeitsgruppe unter Federführung des Ministeriums des Innern, in der auch der Landesbeauftragte mitgewirkt hatte, wurde diese Kabinettvorlage vorbereitet und ausgearbeitet. Durch die Mitarbeit in der Arbeitsgruppe haben wesentliche datenschutzrechtliche Belange Berücksichtigung bei den Zielen und Leitlinien sowie bei der Umsetzung der IT-Strategie im IT-Konzept gefunden.

Hierzu gehören u.a.

- die in den Leitlinien festgelegte Beachtung des Rechts auf informationelle Selbstbestimmung als grundlegende Voraussetzung bereits bei Planungen von IT-/eGovernment-Vorhaben,

- die Aufnahme eines eigenen Kapitels „Datenschutz und Datensicherheit“ mit der Darstellung der wesentlichen Änderungen der DSG-LSA-Novelle vom 21. August 2001 (GVBl. LSA S. 348) sowie den daraus resultierenden datenschutzrechtlichen Anforderungen bei Planung und Umsetzung von IT-Vorhaben,

- im Rahmen der Definition von Standards für den IT-Einsatz die Nutzung datenschutzgerechter Protokolle (z.B. OSCI-Transport) für einen sicheren Transport und die Realisierung der „Ende-zu-Ende-Verschlüsselung“,

- die Berücksichtigung datenschutzrechtlicher Belange beim Aufbau und der Umsetzung der Sicherheitsarchitektur im ITN-LSA durch die Erstellung einer IT-Sicherheitsrichtlinie unter Federführung des Ministeriums des Innern und die dementsprechende Anpassung des Netzerlasses für das ITN-LSA vom 7. Februar 1994 und der IT-Grundsätze vom 1. Juni 1992 sowie der Aufbau eines zentralen IT-Sicherheitsmanagement zum schnellen Erkennen von und Reagieren auf Gefährdungen der IT der Landesverwaltung in der Form eines CERT-LSA („Computer Emercency Response Team“).

Eine jährliche Anpassung an aktuelle Entwicklungen und die Fortschreibung dieses IT-Konzeptes 2005, wie in der Zusammenfassung des Konzeptes selbst festlegt, erfolgte allerdings nicht. Der Aufforderung zur Fortschreibung des Konzeptes und dessen erneute Vorlage durch das Ministerium des Innern im Kabinett bis spätestens November 2006, auch nochmals durch den Kabinettsbeschluss vom 15. November 2005 bekräftigt, kam das Ministerium des Innern nicht mehr nach.

Einer der Gründe für diese nicht erfolgte Fortschreibung oder deren Verzögerung liegt wahrscheinlich in den Ergebnissen eines externen Gutachtens „Zusammenführung aller zentralisierbaren Rechenzentrumsdienstleistungen in eine übergreifende Organisationsstruktur in der Landesverwaltung Sachsen-Anhalt“ vom 6. Februar 2006, dessen Erstellung bereits am 28. Februar 2005 durch den „Ständigen Staatssekretärsausschuss Informationstechnologie“ beschlossen worden war und für den die Staatskanzlei dann als Auftraggeber fungierte.
Anzumerken ist in diesem Zusammenhang, dass dieses Gutachten durch die Staatskanzlei den Ressorts bereits am 10. Februar 2006 zur Verfügung gestellt wurde, der Landesbeauftragte aber in dieser doch grundsätzlich auch für ihn wesentlichen Angelegenheit noch nicht einmal nachrichtlich davon in Kenntnis gesetzt wurde und erst auf Nachfrage beim nunmehr zuständigen Referat der Staatskanzlei seiner Bitte um Zusendung des besagten Gutachtens am 16. Januar 2007 entsprochen wurde.

Im Ergebnis dieses Gutachtens wird der Landesregierung eine **IT-Neuorganisation** dringend empfohlen, bei gleichzeitiger Verlagerung der Aufgabenwahrnehmung der IT-Strategie vom Ministerium des Innern (ehemals Landesleitstelle für Informationstechnik - LIT) in die Staatskanzlei (Landesleitstelle für IT-Strategie - LIS). Mit der operationellen Steuerung und Umsetzung des gesamten Prozesses der IT-Neuorganisation soll ein gleichzeitig zu bildender Aufbaustab beauftragt werden. Für die Abarbeitung der ressortübergreifenden Aufgaben wird die Bildung nachfolgend genannter neun Kompetenzteams für dringend notwendig erachtet:

Kompetenzteam	Team-Führung
Nutzerbetreuung	Ministerium des Innern (TPA)
Software-Verteilung	Ministerium des Innern (TPA)
Terminal-Server-Technik	Ministerium des Innern (TPA)
SAP	Ministerium des Innern (TPA)
Security / Netzinfrastruktur	Ministerium des Innern (TPA)
Druckstraße	Ministerium der Finanzen (FRZ)
Solaris	Ministerium der Finanzen (FRZ)
Storage / Archivierung	Ministerium der Finanzen (FRZ)
E-Mail/ Intranet, Internet	Ministerium des Innern (LIZ)

Die Konsolidierung von 307 IT-Fachbereichen auf 15 neue IT-Fachbereiche soll durch die Bildung von ressortinternen Projektteams unterstützt werden.

Als weiteres zentrales Ziel im Gutachten ist, neben dieser Konsolidierung der IT-Fachbereiche, die Schaffung eines zentralen IT-Dienstleisters für die Landesverwaltung Sachsen-Anhalt benannt. Nach zunächst ressortinterner Konsolidierung der IT-Fachbereiche sollen diese dann zu einem ressortübergreifenden Rechenzentrum zusammengeführt werden.

Folgerichtig zog die Landesregierung entsprechende Konsequenzen aus diesem Gutachten. Mit Kabinettsbeschluss vom 14. November 2006 leitete sie die Neuausrichtung der IT-Organisation und eine neue Aufgabenverteilung und -abgrenzung zwischen der Staatskanzlei, dem Ministerium des Innern und dem Ministerium der Finanzen ein.

Seit dem 1. Dezember 2006 liegt nunmehr die Verantwortung für die **IT-Strategie** bei der LIS. Die Leitung des Landesportals sowie die Koordinierung der eGovernment-Angebote für die Öffentlichkeit werden ebenfalls durch die Staatskanzlei in Abstimmung mit dem Ministerium des Innern wahrgenommen.
Dem Ministerium des Innern obliegt wie bisher die Koordinierung des **eGovernment** in der Landesverwaltung.
Das Ministerium der Finanzen wird mit der Bildung eines Aufbaustabes „Konsolidierung des IT-Betriebes“ beauftragt. Dieser soll solange bestehen bleiben, bis die neue **IT-Organisation** gesichert arbeitet. Bis spätestens zum 30. Juni 2007 hat das Ministerium der Finanzen dem Kabinett über die Einrichtung dieses Aufbaustabes, die Konzepte zur Konsolidierung des IT-Betriebes und die Zeitplanung zu berichten.

Auch im Fall dieses Kabinettsbeschlusses vom 14. November 2006 erachtete es die Staatskanzlei nicht für nötig, den Landesbeauftragten zumindest nachrichtlich durch Übersendung des gefassten Kabinettsbeschlusses in Kenntnis zu setzen. Erst auf Nachfragen des Landesbeauftragten erreichten diesen Anfang Januar 2007 die Unterlagen. Der Landesbeauftragte hofft nunmehr, dass nach Bekundungen einer zukünftig frühzeitigen Unterrichtung Taten folgen werden und damit die offene und vertrauensvolle Zusammenarbeit seitens der Staatkanzlei auch unter Beweis gestellt wird.
Es bleibt festzuhalten, dass auch durch die Staatskanzlei die Regelung zur rechtzeitigen Unterrichtung des Landesbeauftragten gem. § 14 Abs. 1 Satz 2 DSG-LSA beachtet bzw. die Beteiligung des Landesbeauftragten sichergestellt werden muss. Hier kann die Staatskanzlei ein Zeichen für eine offene und vertrauensvolle Zusammenarbeit mit dem Landesbeauftragten setzen, die gleichzeitig Vorbildcharakter für andere Ressorts haben könnte.

Der Landesbeauftragte geht davon aus, dass er zu gegebener Zeit, aber rechtzeitig, im Rahmen der Aufnahme der Tätigkeit der **Kompetenzteams** entsprechend beteiligt wird, denn gerade auch bei der Neustrukturierung und Neuordnung von Verarbeitungskapazitäten, sowie Themenbereichen wie Nutzerbetreuung, Security/Netzinfrastruktur, Terminal-Server-Technik, Storage/Archivierung und der Nutzung von E-Mail, Intranet, Internet bestehen enge Bezüge auch zu Datenschutz und Datensicherheit. Dieser Datenschutzbezug wird leider von den Verantwortlichen oft nicht erkannt, obwohl der Landesgesetzgeber mit der Novellierung des DSG-LSA vom 21. August 2001 mit § 14a DSG-LSA das Institut des „behördlichen Beauftragten für den Datenschutz“ geschaffen hat, der in jedem Ressort bzw. auch in jeder anderen öffentlichen Stelle des Landes gerade bei Planungen neuer und Veränderung bestehender automatisierter Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beteiligt werden sollte. Nach dem Kenntnisstand des Landesbeauftragten erfolgt diese Beteiligung der behördlichen Datenschutzbeauftragten, gerade wenn es um grundsätzliche bzw. Leitungsentscheidungen der Ressorts geht, zum Teil gar nicht oder nur ungenügend oder zu spät.

Der Landesbeauftragte verkennt nicht die Schwierigkeiten der nunmehr von der Staatskanzlei übernommenen Aufgaben zur Planung, Gestaltung und Umsetzung der IT-Strategie für das Land Sachsen-Anhalt. Er hofft, dass nach der Ist-Analyse,

d.h. einer Sichtung und Strukturierung der vom Ministerium des Innern übernommenen Aufgaben, die Erörterung der von ihm angesprochenen Problemfelder und Informationsdefizite ab dem 2. Halbjahr 2007 intensiv auf der Arbeitsebene fortgesetzt und damit eine vertrauensvolle Zusammenarbeit erreicht werden kann.

Nach letzten Verlautbarungen aus der Staatskanzlei ist beabsichtigt, das IT-Konzept der Landesverwaltung im 4. Quartal 2007 fortzuschreiben. Der Landesbeauftragte bietet hierzu seine Mitarbeit und Unterstützung an.

4.2 eGovernment-Maßnahmenplan 2007

Der Landesbeauftragte hatte zuletzt in seinem VII. Tätigkeitsbericht (Ziff. 7.1) über die Aktivitäten der Landesregierung zur Umsetzung ihres eGovernment-Konzeptes mit dem Aktionsplan für die Jahre 2004 bis 2010 und dem daraus abgeleiteten Maßnahmenplan 2005/2006 berichtet. Für die Mehrzahl der dort vorgestellten Projekte und Verfahren in Form der 16 Leitprojekte und für alle sechs Basiskomponenten ist ein datenschutzrechtlicher Bezug gegeben, auch wenn das von mancher Seite so nicht sofort erkannt und interpretiert wird.
Die Landesregierung hatte in ihrer damaligen Stellungnahme zu Ziff. 7.1 (LT-Drs. 4/2524 vom 1. Dezember 2005, S. 7) zum VII. Tätigkeitsbericht des Landesbeauftragten (LT-Drs. 4/2189 vom 25. Mai 2005) darauf verwiesen, die alte, eher unauffällig platzierte Regelung des § 22 Abs. 4 Satz 2 DSG-LSA zur *frühzeitigen Unterrichtung* des Landesbeauftragten stärker in das Blickfeld der zur Unterrichtung verpflichteten Stellen gerückt zu haben. Die besagte Regelung wurde durch Artikel 15 des Ersten Rechts- und Verwaltungsvereinfachungsgesetzes vom 18. November 2005 (GVBl. S. 698) dementsprechend in *§ 14 DSG-LSA als Satz 2* übernommen und zugleich inhaltlich dahingehend modifiziert, dass diese Unterrichtungspflicht zukünftig neben der Planung auch für die grundlegende Änderung automatisierter Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten Anwendung finden sollte. Der Landesbeauftragte sollte nach Aussage der Landesregierung zukünftig rechtzeitig über *grundlegende* Planungen zum Aufbau und zur Änderung von automatisierten Verfahren unterrichtet werden. In dieser Stellungnahme der Landesregierung sind auch Planungen zur Gestaltung der technischen Infrastruktur, wie z.B. das eGovernment-Konzept, ausdrücklich erwähnt worden (siehe auch Ziff. 3.2 mit Hinweisen zu den geänderten Verwaltungsvorschriften). Dieser selbst auferlegten Verpflichtung ist die Landesregierung im Rückblick auf den Berichtszeitraum nicht immer nachgekommen.

Dies gilt insbesondere für die länderübergreifenden Leitprojekte des eGovernment-Maßnahmenplanes 2005/2006. Mit dem Ministerium der Justiz hat der Landesbeauftragte deshalb z.B. einen jährlichen, kontinuierlichen Informationsaustausch über den Einführungsstand von IT-Projekten in dessen Geschäftsbereich vereinbart, der seitens des Ministeriums der Justiz auch eingehalten wird.
Trotzdem erfolgte z.B. die Beteiligung beim Vorhaben des Ministeriums der Justiz zu Errichtung und Betrieb eines **bundesweiten Registerportals der Länder** unter Beteiligung des Landes Sachsen-Anhalts, welches zum 1. Januar 2007 in Betrieb gehen sollte, viel zu spät. Zudem waren die erforderlichen rechtlichen Grundlagen für die hoheitliche Verarbeitung personenbezogener Daten durch eine Stelle außerhalb der rechtlichen Zuständigkeit Sachsen-Anhalts noch nicht geschaf-

fen, da der Staatsvertrag bis Jahresende 2006 weder geschlossen noch ratifiziert werden konnte (siehe Ziff. 18.13).

Die Leitprojekte aus dem Bereich des Ministeriums des Justiz (Nr. 13: Elektronische Einsichtnahme in maschinell geführte Register, Nr. 14: Automatisiertes gerichtliches Mahnverfahren, Nr. 15: Elektronischer Rechtsverkehr in Grundbuchsachen) sowie des Ministeriums der Finanzen (Nr. 16: Elektronische Steuererklärung) sind bundesländerübergreifende Leitprojekte. In diesen Ressorts besteht eine zentralisierte Führung des nachgeordneten Bereiches und durch die Länder werden bundesrechtliche Regelungen wie z.B. der Grundbuchordnung und der Abgabenordnung umgesetzt und ausgeführt. Hier scheint deshalb teilweise die Meinung der Ressortverantwortlichen vorzuherrschen, dass damit eine rechtzeitige Beteiligung des Landesbeauftragten gem. § 14 Abs. 1 Satz 2 DSG-LSA nicht mehr erforderlich sei, weil ja schon alles, auch die datenschutzrechtlichen Fragestellungen und Themen, in den dazu eingerichteten Bund-Länder-Gremien abschließend behandelt worden seien und es damit nur noch einer Umsetzung im eigenen Bundesland bedürfe. Das ist aber, wie die Praxis zeigt, oft ein Irrtum. Der Landesbeauftragte lässt sich bei seiner datenschutzrechtlichen Prüfung und Beurteilung nicht von der „Wirkung“ bereits abgeschlossener Staatsverträge oder Verwaltungsvereinbarungen zwischen den Bundesländern beeinflussen. Oft stellt sich bei solchen Nachprüfungen heraus, dass entweder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit auf Bundesebene oder die Landesbeauftragten für den Datenschutz über ihre Landesressorts nicht rechtzeitig unterrichtet oder beteiligt worden sind.

Eine Beteiligung des Landesbeauftragten mit Gelegenheit zur Stellungnahme zum **eGovernment-Maßnahmenplan 2007** vor Beschlussfassung der Landesregierung wäre geboten gewesen, wurde aber von den einzelnen Ressorts weder für ihre neu aufgenommenen Leitprojekte noch durch das mit der Erstellung des e-Government-Maßnahmenplanes 2007 federführend befasste Ministerium des Innern erkannt und ist offenbar vernachlässigt worden.

Gerade aber der zurückliegende Berichtszeitraum ist auf EU-, Bundes- und auch auf Landesebene von vielfältigen Aktivitäten, Programmen und Initiativen zum eGovernment gekennzeichnet, die selbst dem Landesbeauftragten Mühe bereiten, die Übersicht zu behalten. „eGovernment“ scheint zu einem Zauberwort der Politik geworden zu sein, welches synonym für die Verwaltungsmodernisierung durch Informations- und Kommunikationstechnologien verwendet wird.

Stellvertretend für diese Aktivitäten auf Bundesebene sei hier auf den sogenannten **„1. Nationalen IT-Gipfel“** am 18. Dezember 2006 am Hasso-Plattner-Institut in Potsdam verwiesen, zu dem die Bundeskanzlerin hochkarätige Experten aus Politik, Wissenschaft, Forschung und Wirtschaft eingeladen hatte, um über den Ausbau Deutschlands als Standort für Informations- und Kommunikationstechnologien (IKT) zu beraten. Nicht eingeladen waren die Datenschutzbeauftragten des Bundes und der Länder, für die Stellung und die Standortbestimmung des Datenschutzes in dieser Informationsgesellschaft geradezu ein fatales Zeichen in dieser Zeit. Der ausgegrenzte Bundesbeauftragte für den Datenschutz und die Informationsfreiheit forderte deshalb, schon bei der Konzeption von IT-Systemen ver-

stärkt Vorkehrungen zur Gewährleistung des Rechts auf informationelle Selbstbestimmung zu treffen und veröffentlichte hierzu zeitgleich zum 1. Nationalen IT-Gipfel „Zehn Thesen für eine datenschutzfreundliche Informationstechnik“ (**Anlage 27**), denen sich der Landesbeauftragte für seinen Zuständigkeitsbereich nur anschließen kann, gelten doch diese Forderungen auch für die Landesregierung bei der konzeptionellen Gestaltung weiterer Vorhaben des eGovernment in Sachsen-Anhalt.

Zu den wesentlichen Einflussfaktoren hinsichtlich der weiteren Gestaltung und Umsetzung des eGovernment-Prozesses in Sachsen-Anhalt zählen aus Sicht des Landesbeauftragten nachfolgend bezeichnete EU-Richtlinien, EU-Initiativen, Initiativen des Bundes sowie die Rahmenvereinbarung der Landesregierung mit den Kommunalen Spitzenverbänden.

Europäische Union:

- **EU-Initiative „i2010** – Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung“ vom 1. Juni 2005,

- **EU-Initiative „Interoperabilität** für europaweite elektronische Behördendienste (eGovernment-Dienste) vom 13. Februar 2006,

- **E-Government-Aktionsplan** im Rahmen der i2010-Initiative: „Beschleunigte Einführung elektronischer Behördendienste in Europa zum Nutzen aller“ vom 25. April 2006,

- **i2010 Erster Jahresbericht** über die europäische Informationsgesellschaft vom 19. Mai 2006,

- **Richtlinie 2006/123/EG** des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (sog. „EU-Dienstleistungsrichtlinie“).

Bundesregierung und Bundesländer:

- **BundOnline 2005 - Abschlussbericht** - Status und Ausblick vom 24. Februar 2006

- **Aktionsplan Deutschland-Online** - Deutschland-Online Bund, Länder und Kommunen vom 22. Juni 2006 mit den fünf priorisierten Vorhaben:

  Querschnittsbereiche:
  - IT-Infrastruktur
  - Standardisierung

  ebenenübergreifende Fachverfahren:
  - Kfz-Wesen
  - Personenstandswesen (siehe Ziff. 6.4)
  - Meldewesen (siehe Ziff. 6.1.)

Diese **fünf priorisierten Vorhaben** werden durch eine Staatssekretärs-Lenkungsgruppe unter enger Einbindung der betroffenen Fachministerkonferenzen gesteuert und erhalten aus einem Bund-Länder-Fonds zentrale Unterstützung z. B. in Form von Beratungsleistungen.

- **E-Government 2.0** - Das Programm des Bundes - (Beschluss der Bundesregierung vom 13. September 2006: „Pogramm Zukunftsorientierte Verwaltung durch Innovationen“ einschließlich des Programms E-Government 2.0)

  Die Bundesregierung hat **vier Handlungsfelder** festgelegt, die in den kommenden Jahren bis 2010 gezielt ausgebaut werden, um den Modernisierungsprozess in der Verwaltung und den Standort Deutschland durch eGovernment zu fördern:

  A. Portfolio:
  Bedarfsorientierter qualitativer und quantitativer Ausbau des eGovernment-Angebots des Bundes,

  B. Prozessketten:
  Elektronische Zusammenarbeit zwischen Wirtschaft und Verwaltung durch gemeinsame Prozessketten,

  C. Identifizierung:
  Einführung eines **elektronischen Personalausweises** und Erarbeitung von E-Identity-Konzepten,

  D. Kommunikation:
  Sichere Kommunikationsinfrastruktur für Bürger, Unternehmen und Verwaltungen.

Land Sachsen-Anhalt:

- **Rahmenvereinbarung** zwischen dem Land Sachsen-Anhalt und den Kommunalen Spitzenverbänden vom 9. Januar 2006

Diese Aufzählung zeigt deutlich den hohen Koordinierungsaufwand, den zukünftig die Landesregierung bei der Umsetzung des eGovernment-Maßnahmenplanes 2007 und der Folgejahre zu bewältigen haben wird.
Der Landesbeauftragte will diesen Prozess datenschutzrechtlich begleiten und die Landesregierung entsprechend seines gesetzlichen Beratungsauftrages (§ 22 Abs. 4 DSG-LSA) bei der anstehenden Verwaltungsmodernisierung unterstützen. Er erwartet seitens der Ressorts eine direkte Unterstützung seiner Tätigkeit durch eine rechtzeitige Unterrichtung und weitere Beteiligung beim Aufbau und der Umsetzung der **Basiskomponenten:**

- 1 - Dienstleistungsportal (Landesportal www.sachsen-anhalt.de, in Verantwortung der Staatskanzlei),

- 2 - Formularserver (Pilotlösung eines Formularmanagementsystems im LIZ Halle),
- 3 - Zahlungsverkehrsplattform (Muster eShop und Aufbau der zentralen Nutzerverwaltung im LIZ Halle),
- 4 - Virtuelle Poststelle - VPS (Beginn Testbetrieb der VPS ab Februar 2007, Echtbetrieb geplant ab 4. Quartal 2007; Public Key Infrastruktur bereits seit 11. Oktober 2006 offiziell in Betrieb),
- 6 - Dokumentenmanagementsystem/Vorgangsbearbeitungssystem (DMS/VBS) (Pilotprojekt im Ministerium des Innern).

Insbesondere bei der Basiskomponente 1, dem Landesportal Sachsen-Anhalt (LPSA) in Verantwortung der Staatskanzlei, ihrer Weiterentwicklung und ihrem Ausbau, erwartet der Landesbeauftragte zukünftig eine rechtzeitige Beteiligung und Unterrichtung gem. § 14 Abs. 1 Satz 2 DSG-LSA.
Entsprechend dem Masterplan LPSA 2007-2011 (Bekanntmachung der Staatskanzlei vom 26. September 2006, MBl. LSA S. 657) soll das LPSA als Dienstleistungsportal ausgebaut werden. Damit wird die besondere Rolle des LPSA in der eGovernment-Strategie des Landes deutlich. Dabei verlagert sich der Schwerpunkt im eGovernment-Maßnahmenplan 2007 von reinen Informationsangeboten hin zur Transaktion, d.h. der eigentlichen Online-Erbringung von Dienstleistungen mit Bürgerinnen und Bürgern sowie der Wirtschaft. Damit ist zukünftig eine automatisierte Verarbeitung einer Vielzahl auch personenbezogener Daten von Kommunikationspartnern verbunden. Gerade hier ist die rechtzeitige Einbindung des Landesbeauftragten erforderlich, um durch die Prüfung und Abklärung der Fragen des Datenschutzes und der Datensicherheit Vertrauen in das Internetportal des Landes Sachsen-Anhalt und seine dort verfügbaren Online-Dienstleistungsangebote der Verwaltung zu erreichen (vgl. Ziff. 23.2).

Den gleichen Appell richtet der Landesbeauftragte an die Ressorts, welche die bereits begonnenen **Leitprojekte** (2, 3, 6, 9) aus 2005/2006 fortsetzen bzw. im Jahr 2007 nach Bereitstellung von Basiskomponenten weiterführen. Hierzu gehören die Leitprojekte 11, 12, 13, 14.
Beim Leitprojekt 15 (Elektronischer Rechtsverkehr in Grundbuchsachen - Federführung Ministerium der Justiz) erwartet der Landesbeauftragte eine rechtzeitige Beteiligung vor Abschluss des Feinkonzeptes.
Das Leitprojekt 1 (Fördermittelmanagement-System efREporter) ist mit Beteiligung des Landesbeauftragten erfolgreich abgeschlossen worden.
Weitere Leitprojekte (4, 5, 7, 8, 10, 16) gelten lt. eGovernment-Maßnahmenplan 2007 als abgeschlossen.

Bei den in **2007** vier neu geplanten **Leitprojekten** (18, 19, 20 und 21)

- **XAusländer** (Leitprojekt 18/Ministerium des Innern, Festlegung einheitlicher Standards für Datenaustauschformate auf Basis XML im Ausländerwesen),

- **XPersonenstand** (Leitprojekt 19/Ministerium des Innern, Festlegung von Standards für das Personenstandswesen (Version 1.0) auf der Grundlage von XMeld und OSCI-Transport),

- **EUREKA-FACH** (Leitprojekt 20/Ministerium der Justiz, Erweiterung des in den Fachgerichtsbarkeiten eingesetzten Justizfachverfahrens EUREKA-FACH für den Elektronischen Rechtsverkehr, einschließlich der Annahme und Archivierung von Verfahrensunterlagen in elektronischer Form sowie Workflow in der Verfahrensführung), und

- **web.sta** (Leitprojekt 21/Ministerium der Justiz, vollständige An- und Einbindung der Staatsanwaltschaften an die automatisierte Informationsbeschaffung und -verwaltung der Strafverfolgungsbehörden im Rahmen der europäischen Strafregistervernetzung; Ausbau von landesinternen Kommunikationsbeziehungen für Ermittlungsaufgaben in Wirtschaftsstrafsachen)

erinnert der Landesbeauftragte das Ministerium des Innern und das Ministerium der Justiz vorsorglich an ihre Unterrichtungspflichten.
Ein datenschutzrechtlicher Bezug wird wohl bei diesen neuen Leitprojekten nicht in Abrede gestellt werden.
Wie der Landesbeauftragte seitens des Ministeriums des Innern bei einem Gespräch in der Staatskanzlei informiert wurde, wird sich das Ministerium auch auf Grund der sog. „EU-Dienstleistungsrichtlinie“, deren IT-Umsetzung insbesondere für den Bereich der Wirtschaftsüberwachung zusätzlich in den Aktionsplan Deutschland-Online aufgenommen werden soll, verstärkt den Basiskomponenten und deren Umsetzung widmen.

4.3 Sicherheitsinfrastruktur in Sachsen-Anhalt

Mit der Veröffentlichung des Runderlasses des Ministeriums des Innern vom 14. März 2006 „Organisation und Aufgaben der Sicherheitsinfrastruktur des Landes Sachsen-Anhalt“ (MBl. LSA S. 233) wurden die organisatorischen Voraussetzungen für den Einsatz von fortgeschrittenen und qualifizierten Signaturen und Zertifikaten gemäß dem Signaturgesetz für den Einsatz bei der Signierung, Verschlüsselung und der Authentisierung in der Landesverwaltung in Sachsen-Anhalt geschaffen.
Die sog. „**Public Key Infrastruktur Land Sachsen-Anhalt - PKI LSA**“ bildet die wesentliche Grundlage für die Umsetzung der anspruchsvollen Ziele im Rahmen des eGovernment-Maßnahmenplanes 2007 der Landesregierung und ist zugleich notwendige Voraussetzung für die Umsetzung des ab dem 1. Januar 2007 gesetzlich vorgeschriebenen bundesweiten, nur noch elektronisch durchzuführenden Rückmeldeverfahrens im Meldewesen.
Das Land konnte mit der Inbetriebnahme des „Intermediär LSA“ auch die Integration des Standards OSCI-Transport erfolgreich abschließen. Damit wurde in Sachsen-Anhalt für die Datenübermittlung zwischen den Meldebehörden, vom Versand bis zum Empfang einer Nachricht, die Ende-zu-Ende-Verschlüsselung sichergestellt.
Mit dem Sicherheitsstandard **OSCI** (Online Services Computer Interface) werden die Vertraulichkeit, Integrität und Authentizität personenbezogener Daten bei der Übertragung über unsichere Netze, wie dem Internet, zwischen den öffentlichen Stellen in Bund, Ländern und Kommunen gewährleistet.
Insbesondere die Entwicklung von OSCI-Transport zu einem Protokollstandard für einen rechtlich anerkannten elektronisch signierten und verschlüsselten Daten-

austausch sowie dessen Einsatz im Rahmen des eGovernment wurde in der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. Dezember 2005 „Sicherheit bei eGovernment durch Nutzung des Standards OSCI“ begrüßt (**Anlage 9**).

Der Landesbeauftragte hat die offizielle Inbetriebnahme der PKI LSA am 11. Oktober 2006 durch den Staatssekretär des Ministeriums des Innern gleichzeitig zum Anlass genommen, die Ressorts auf die sachgemäße Anwendung von Authentisierungs- und Signaturverfahren hinzuweisen.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und ziehen damit unterschiedliche Rechtsfolgen für die Nutzenden nach sich. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren Berücksichtigung finden.
Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind zur Zeit nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.
Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet.
In einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 „Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren“ werden auf die Problematik der Nutzung ungeeigneter oder weniger sicherer Verfahren hingewiesen und Forderungen für eine sachgerechten Einsatz von Signatur- und Authentisierungsverfahren erhoben (**Anlage 14**).

Darüber hinaus hat der Arbeitskreis eGovernment der Datenschutzkonferenz eine Orientierungshilfe zu Dokumentenmanagementsystemen erarbeitet, die auch Aussagen zur Nutzung sicherer Signaturverfahren enthält; diese Orientierungshilfe ist im Serviceangebot der Homepage des Landesbeauftragten verfügbar. Die Empfehlungen sollten bei der weiteren Entwicklung der Basiskomponente Dokumentenmanagementsystem beachtet werden.

4.4 RFID (Radio Frequency Identification) - Chancen und Risiken

Der Landesbeauftragte hatte in seinen einleitenden Bemerkungen zum VII. Tätigkeitsbericht (Ziff. 1) zur technischen Entwicklung in Bezug auf den fortschreitenden Einsatz von RFID-Technologie aufmerksam gemacht.
In ihrer damaligen Entschließung vom März 2004 hatte die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder sich voll inhaltlich einer Entschließung zu „Radio Frequency Identification“ der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre angeschlossen, in der erste Datenschutzhinweise gegeben wurden.

Seit dem ist eine rasante Entwicklung auf diesem Gebiet zu verzeichnen, die insbesondere diese sog. „Funk-Chips“ immer technologisch ausgereifter, aber auch kostengünstiger werden lässt, womit einem flächendeckenden Einsatz dieser Technologie in Wirtschaft und Verwaltung, in nicht mehr allzu ferner Zukunft, nichts mehr im Wege zu stehen scheint.

Mit der Ausstattung von Pässen ab November 2006 (ePass) und auch von Personalausweisen (ePA) ab 2008 mit einem RFID-Chip, der biometrische Merkmale des Ausweisinhabers speichert, hält RFID-Technologie auch Einzug in den öffentlichen Bereich (siehe Ziff. 6.3). Allerdings steht die Sicherheit, insbesondere die Schutzvorkehrungen gegen die Auslesbarkeit der Daten aus dem RFID-Chip durch unbefugte Dritte, zumindest bei den Pässen der „1. Generation“, in der Kritik. Für die Sicherheit der Daten will der Gesetzgeber bei der „2. Generation“ von Pässen, in denen dann auch Fingerabdrücke im RFID-Chip gespeichert werden, einen erweiterten Zugriffsschutz auf den RFID-Chip realisieren. Dieser erweiterte Zugriffsschutz - Extended Access Control - spezifiziert einen zusätzlichen Public-Key Authentisierungsmechanismus, mit dem sich zukünftig das Lesegerät als zum Lesen von Fingerabdrücken berechtigt gegenüber dem RFID-Chip im ePass oder später im ePA ausweisen muss. Das Lesegerät muss dazu ebenfalls mit einem eigenen Schlüsselpaar und einem vom RFID-Chip des ePass oder ePA verifizierbaren Zertifikat ausgestattet werden.

Auch u.a. aus diesem Grund hat sich der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ mit dieser als Basistechnologie für die Informationsgesellschaft bezeichneten RFID-Technologie kritisch auseinandergesetzt. Der Arbeitskreis hat hierzu eine Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“ (Stand 14. Dezember 2006) verabschiedet; diese ist auf der Homepage des Landesbeauftragten abrufbar.

Die zuvor von der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg verabschiedete Entschließung „Verbindliche Regelungen für den Einsatz von RFID-Technologien“ (**Anlage 18**) verdeutlicht nochmals die Möglichkeiten, aber auch die datenschutzrechtlichen Risiken dieser Technologie.
Zusammenfassend wird gefordert, dass bereits bei der Entwicklung, der Einführung, der Verwendung oder dem Einsatz von RFID-Technologien Datenschutzprinzipien materiell-rechtlich wie technisch berücksichtigt werden müssen. Eventuell ist auch ein gesetzgeberisches Tätigwerden erforderlich (vgl. Ziff. 3.1).
Zu erwähnen ist auch, dass die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, der sog. „Düsseldorfer Kreis“, am 8./9. November 2006 in einem inhaltlich gleichlautenden Beschluss diese Auffassung zum datenschutzkonformen Einsatz von RFID vertreten (**Anlage 25**).

Die Entschließung der 72. Konferenz hat einen hoffentlich fruchtbaren Diskussionsprozess in Gang gesetzt, das zeigt z.B. die „Gemeinsame Stellungnahme“ von Informationsforum RFID e.V., Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (BITKOM), Bundesverband der Deutschen Industrie (BDI), GS1 Germany und Hauptverband des Deutschen Einzelhandel e.V. (HDE) vom Dezember 2006 als Reaktion auf diese Entschließung.

In der Antwort des Vorsitzenden der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom April 2007 an diese Interessenverbände der Wirtschaft wird das Angebot unterbreitet, die Diskussion um eine datenschutzgerechte Ausgestaltung von RFID-Anwendungen gemeinsam konstruktiv fortzuführen. Die Forderungen nach Transparenz, Kennzeichnungspflicht, dem Verbot einer Profilbildung, der Vermeidung unbefugter Kenntnisnahme und frühzeitiger Deaktivierungsmöglichkeit beim Einsatz von RFID-Technologien werden weitgehend von den Interessenverbänden der Wirtschaft akzeptiert. In der Bewertung der aus dem RFID-Einsatz resultierenden Risiken gehen die Auffassungen der Datenschutzkonferenz und der Interessenverbände noch auseinander. Dieser Umstand steht aber einer konstruktiven Diskussion nicht im Wege.
Die Datenschutzbeauftragten des Bundes und der Länder erklären sich ausdrücklich bereit, RFID-Projekte zu begleiten, und fordern dabei eine umfassende Technikfolgenabschätzung ein.

Auf europäischer Ebene hat ebenfalls, initiiert durch die EU-Kommission, eine öffentliche Konsultation zu RFID im Jahr 2006 stattgefunden. Bis Mitte des Jahres 2007 soll eine RFID-Interessengruppe eingerichtet werden, an der auch die Artikel-29-Datenschutzgruppe beteiligt ist. Die gemeinsame RFID-Strategie der EU hat das Ziel, die europäische Datenschutzrichtlinie für die elektronische Kommunikation so zu überarbeiten, dass RFID-Anwendungen unter diese Richtlinie fallen. Bis Ende des Jahres 2007 soll eine „Empfehlung über die Wahrung der Sicherheit und Privatsphäre“, die europaweit gültig sein wird, erarbeitet werden, die zugleich der IT-Branche als Rahmenrichtlinie dienen soll.

5. Archivwesen

5.1 Stasiunterlagengesetz

Am 29. Dezember 2006 endete die in § 20 Abs. 3 und § 21 Abs. 3 des Stasiunterlagengesetzes (StUG) bestimmte Frist von 15 Jahren, innerhalb der die Nutzung von Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR zulässig war, um die in § 20 Abs. 1 Nrn. 6 und 7 und § 21 Abs. 1 Nrn. 6 und 7 StUG genannten Personen zu überprüfen. Nach Ablauf der Frist sollte die Tatsache einer Tätigkeit für den Staatssicherheitsdienst dem Mitarbeiter im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwendet werden dürfen.

Wäre diese Rechtslage so eingetreten, hätte sich wohl ein erheblicher Beratungsbedarf für den Landesbeauftragten ergeben. Aufgrund der erfolgten Regelanfragen hätten sich sehr viele Dienststellen mannigfaltigen Problemen gegenübergesehen. Demgemäß hatte sich der Landesbeauftragte an einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und einiger Länder zu diesem Thema beteiligt. Dabei wurde u.a. diskutiert, ob auch das Ergebnis aus der Nutzung der Unterlagen von dem Anwendungsbereich der Vorschriften erfasst ist. Die weitere Aufbewahrung bzw. Archivierung wurden ebenso erörtert wie die Möglichkeit, an einen individuellen Tilgungsanspruch zu denken. In der zweiten Hälfte des Jahres 2006 wurde die Problematik der Verwendung von Stasiunterlagen aufgrund von Gesetzesentwürfen sowohl im Bundesrat (BR-Drs. 425/06) als auch im Bundestag (BT-Drs. 16/2969) eingehend behandelt. In der Fassung der Beschlussemp-

fehlung des Ausschusses für Kultur und Medien (BT-Drs. 16/3938) wurde das Stasiunterlagengesetz geändert (Siebtes Gesetz zur Änderung des StUG vom 21. Dezember 2006, BGBl. I S. 3326; Bekanntmachung der Neufassung des StUG vom 18. Februar 2007, BGBl. I S. 162). Nunmehr besteht lediglich die Möglichkeit, das Führungspersonal in den Bereichen der Politik, der Verwaltung und des Sports auf eine Zusammenarbeit mit dem Staatssicherheitsdienst der DDR für weitere fünf Jahre zu überprüfen. In Absatz 3 der §§ 20 und 21 StUG ist nunmehr vorgesehen, dass die Verwendung von Unterlagen für die Überprüfung des nunmehr benannten Personenkreises nach dem 31. Dezember 2011 unzulässig ist. Unterlagen zu Auskünften und Mitteilungen, die im Zusammenhang mit früheren Überprüfungen bei den anfordernden Stellen angefallen sind, sind dem Bundesarchiv oder dem zuständigen Landesarchiv anzubieten.

Demgemäß ist die gravierende Änderung der Rechtslage nach der alten Fassung des Stasiunterlagengesetzes ausgeblieben. Auch wenn jedoch kein ausdrückliches Verwertungsverbot mehr formuliert ist, wird dadurch kein freizügiger Umgang mit den Unterlagen gestattet. Vielmehr ist die besondere Sensibilität der Mitteilungen der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) zu beachten. Insbesondere ist die Zweckbindung des § 29 StUG zu berücksichtigen. Ob und inwieweit jemandem seine frühere Tätigkeit für den Staatssicherheitsdienst in arbeits- oder dienstrechtlichen Rechtsverhältnissen vorgehalten werden kann, ist auch künftig im Einzelfall zu prüfen. Auch sollen in die im Zusammenhang mit den früheren Überprüfungen angefallenen Unterlagen nicht grundsätzlich vernichtet werden. Vielmehr sollen sie dem zuständigen Archiv angeboten werden. Maßstab für die Aufbewahrung in den jeweiligen Personal- oder Überprüfungsvorgängen ist der Grundsatz der Verhältnismäßigkeit. Bei der Frage, ob einzelne Vorgänge nunmehr zu archivieren sind, ist daher neben der Notwendigkeit für die laufende Verwaltung auch der im Disziplinarrecht geltende Resozialisierungs- und Tilgungsgedanke zu berücksichtigen.

5.2 Verwaltungsrechtliche Rehabilitierung

Ein Petent beklagte sich gegenüber dem Landesbeauftragten darüber, dass das seinerzeit für eine verwaltungsrechtliche Rehabilitierung zuständige Regierungspräsidium zu ihm als Antragsteller bei der BStU eine Anfrage durchgeführt hatte. Erst im Zuge der Akteneinsicht im gerichtlichen Klageverfahren habe er von der Anfrage bei der BStU erfahren.

Der Landesbeauftragte hat den Vorgang intensiv mit dem zwischenzeitlich zuständigen Landesverwaltungsamt diskutiert. Im Ergebnis war das Verfahren der zuständigen Behörde aus datenschutzrechtlicher Sicht letztendlich nicht zu beanstanden.

Die verwaltungsrechtliche Rehabilitierung ist nach § 2 Abs. 2 VwRehaG ausgeschlossen, wenn der Berechtigte oder derjenige, von dem er seine Rechte herleitet, gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen oder in schwerwiegendem Maße seine Stellung zum eigenen Vorteil oder zum Nachteil anderer missbraucht hat. Nach der Rechtsprechung des Bundesverwal-

tungsgerichtes hat sich an den Grundsätzen der Menschlichkeit oder Rechtsstaatlichkeit vergangen, wer zur Stützung des repressiven Systems der ehemaligen DDR freiwillig und gezielt, insbesondere auch durch Eindringen in die Privatsphäre anderer und Missbrauch persönlichen Vertrauens, Informationen über Mitbürger gesammelt, an die auch in der DDR für ihre repressive und menschenverachtende Tätigkeit bekannte Staatssicherheit weitergegeben und dabei jedenfalls in Kauf genommen hat, dass diese Informationen zum Nachteil der denunzierten Person, namentlich zur Unterdrückung ihrer Menschen- und Freiheitsrechte, benutzt werden könnten. Daher haben die Antragsteller im Antragsvordruck die Frage zu beantworten, ob sie hauptamtlicher oder inoffizieller Mitarbeiter des Ministeriums für Staatssicherheit bzw. des Arbeitsgebiets 1 der Kriminalpolizei der Volkspolizei gewesen sind. Im Rahmen der Antragsbearbeitung ist die zuständige Behörde dann verpflichtet, das Vorliegen von Ausschließungsgründen zu überprüfen. Da Angaben über eine frühere Tätigkeit für das Ministerium für Staatssicherheit nach bisherigen Erfahrungen auch gegenüber der Landesverwaltung häufig verschwiegen oder bagatellisiert werden, wurde eine Überprüfung der Angaben des Antragstellers für erforderlich gehalten.
Zumeist wird den Antragstellern im Rehabilitierungsverfahren verdeutlicht, dass eine entsprechende Überprüfung der Angaben bei der BStU erfolgen wird. Diese wünschenswerte Information war bei der Antragstellung im konkreten Fall leider vergessen worden. Sie ist allerdings auch nicht zwingend notwendig. Zunächst drängt sich angesichts des Frageinhalts schon auf, dass die Angabe des Antragstellers wohl nicht ungeprüft übernommen werden kann. Unbeschadet dessen ist jedoch die Anfrage bei der BStU gem. § 9 Abs. 2 Nr. 1 DSG-LSA i.V.m. § 21 Abs. 1 Nr. 1, § 30 Abs. 1 und 2 StUG oder § 9 Abs. 2 Satz 2 Nr. 2a i.V.m. § 10 Abs. 2 Nr. 4 DSG-LSA ohne vorherige Einwilligung und Information des Betroffenen zulässig. In § 21 Abs. 1 Nr. 1 StUG ist vorgesehen, dass Unterlagen der BStU für Rehabilitierungsverfahren Verwendung finden können. § 30 StUG sieht vor, dass die BStU den Betroffenen grundsätzlich nachträglich über die übermittelten Daten und den Empfänger unterrichtet. Diese Information kann allerdings auch entfallen. Dies gilt u.a., wenn der Betroffene auf andere Weise von der Übermittlung Kenntnis erlangen kann, wie hier beispielsweise durch eine entsprechende Bescheidung durch die zuständige Rehabilitierungsbehörde.

6. Ausweis- und Melderecht, Personenstandsrecht

6.1 Änderungen im Melderecht

In den letzten Jahren erfolgten Änderungen im Melderechtsrahmengesetz, welche auch grundlegende Änderungen im Melderecht des Landes Sachsen-Anhalt nach sich zogen (GVBl. LSA 2004, S. 506).

Eine solche Änderung war die Abschaffung der Verpflichtung zur Abmeldung bei Umzügen im Inland. Daneben wurden im Melderecht die erforderlichen Rahmenbedingungen für die Nutzung moderner Informations- und Kommunikationstechniken geschaffen, um insbesondere die Auskunftserteilung an Behörden und Privatpersonen mittels elektronischer Verfahren zu ermöglichen.

Die Verpflichtung zur Abmeldung bei Umzügen wurde durch Datenübermittlungen zwischen den Meldebehörden, die sogenannte Rückmeldung, überflüssig. So hat nun die Meldebehörde , bei der sich der neue Einwohner der Gemeinde anmeldet, die bisher zuständige Meldebehörde zu unterrichten. Dies hat unverzüglich, jedoch spätestens nach drei Werktagen zu erfolgen. Dabei sollte die Rückmeldung auf automatisiert verarbeitbaren Datenträgern oder durch Datenübertragung erfolgen.

Im Jahr 2004 wurde das Melderecht dahingehend konkretisiert, dass die Daten nach der Anmeldung nur noch durch Datenübertragung zu übermitteln sind. Eine Übergangsfrist wurde bis zum 31. Dezember 2006 gewährt. In dieser Zeit vollzog auch das Land Sachsen-Anhalt und damit seine Meldebehörden die Voraussetzungen für eine sichere Datenübertragung.

Damit alle Meldebehörden im gesamten Bundesgebiet reibungslos Meldedaten mittels automatisierter Datenübertragung austauschen können, wurden gemeinsame Standards wie „OSCI–xMeld“ und „OSCI-Transport“ (Online Services Computer Interface) entwickelt. xMeld ist somit ein bundeseinheitliches Datenaustauschformat für das Meldewesen. Bei OSCI-Transport erfolgen eine Trennung von Nutzungs- und Inhaltsdaten und Verschlüsselung sowie Signatur mittels signaturgesetzkonformer Signaturkarte.

Das Land Sachsen-Anhalt schreibt diese Standards auch für Datenübermittlungen zwischen den Meldebehörden des Landes vor, indem sie in der Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden von Sachsen-Anhalt für die Datenübermittlung für Zwecke des Rückmeldeverfahrens die Erste Bundesmeldedatenübermittlungsverordnung (1. BMeldDÜV) für anwendbar erklärt hat. In § 2 1. BMeldDÜV werden Form und Verfahren der Datenübermittlung mittels OSCI-xMeld und OSCI-Transport vorgeschrieben.

Auch die Datenschutzbeauftragten des Bundes und der Länder begrüßten in einer Entschließung vom 15. Dezember 2005 die mit dem OSCI-Transport angestrebte Ende-zu-Ende-Sicherheit vor allem für die Übermittlung personenbezogener Daten zwischen den Kommunen und empfehlen den flächendeckenden Aufbau einer OSCI-basierten Infrastruktur (**Anlage 9**); vgl. auch Ziff. 4.3.

6.2 Änderung des Melderechts aufgrund der Föderalismusreform

Im Rahmen der Föderalismusreform ist das Meldewesen zum 1. September 2006 in die ausschließliche Gesetzgebungskompetenz des Bundes überführt worden.

Das Meldewesen soll in neue Strukturen übergeleitet werden, d.h., bundeseinheitliche Verfahren sollen die Nutzung der Melderegister vereinfachen. Bei ersten Überlegungen wird auch von der Schaffung eines zusätzlichen zentralen Melderegisters gesprochen - nicht nur für Datenschützer ein kritisch zu betrachtendes Szenario. Ein einheitliches Personenkennzeichen wäre unzulässig.

Die Datenschutzkonferenz des Bundes und der Länder hat daraufhin eine Arbeitsgruppe zum Arbeitskreis Meldewesen ins Leben gerufen, welche das Ge-

setzgebungsverfahren in den kommenden Jahren datenschutzrechtlich begleiten wird.

6.3 Biometrische Merkmale in Reisepässen

In seinem VI. Tätigkeitsbericht (Ziff. 5.1) hatte der Landesbeauftragte bereits von der Absicht der Bundesregierung berichtet, Reisepässe „zur Erhöhung der inneren Sicherheit“ mit biometrischen Merkmalen zu versehen.

Mittlerweile werden seit dem 1. November 2005 Reisepässe ausgestellt, die einen Chip enthalten, auf dem biometrische Daten des Gesichts gespeichert sind. Ob sie dadurch sicherer geworden sind, ist durchaus umstritten. In Presse und Fachliteratur ist mehrfach von erfolgreichen Versuchen, den Chip zu „knacken“ und damit Reisepässe zu verfälschen, berichtet worden (vgl. Ziff. 4.4; siehe auch Entschließung der Datenschutzkonferenz vom Juni 2005, **Anlage 1**).

Inzwischen liegt ein Gesetzentwurf der Bundesregierung vor, wonach ab November 2007 die Aufnahme von Fingerabdruckdaten in den Reisepass geplant ist. Um diesen Gesetzentwurf ist in der Öffentlichkeit eine rege Diskussion entbrannt. Zum Einen, weil der Bundesrat eine Ausweitung der Befugnisse der Sicherheitsbehörden zu erreichen versucht, zum Anderen, weil sich die Entstehung eines „Fingerabdruckregisters“ abzeichnete.

So sollen

- die Polizeivollzugsbehörden die zur Überprüfung der Identität des Inhabers erhobenen Daten mit ihren erkennungsdienstlichen Dateien abgleichen dürfen (sog. 1:n-Vergleich).

- alle Passregisterdaten (einschließlich der Lichtbilder) von den Sicherheitsbehörden automatisch abgerufen werden können.

Dem hat die Bundesregierung (noch) widersprochen. Sie will es bei der Identitätsüberprüfung beim sog. 1:1-Vergleich belassen und den automatisierten Abruf auf Lichtbilder beschränken (vgl. BT-Drs. 16/4138 und 16/4456).

Außerdem mehren sich die Stimmen, die eine Speicherung der Fingerabdrücke fordern (so auch die EU-Kommission in ihrer „Strategieplanung für 2008“) - entweder im Passregister oder sogar im Melderegister.
Der Landesbeauftragte teilt dazu die kritische Einschätzung des Innenministers, der sich an die „Zentrale Einwohnermeldekartei der DDR“ erinnert fühlt.

Am 23. April 2007 hat eine Anhörung im Bundestag stattgefunden. Danach ist die Bundesregierung von ihrer Absicht, Fingerabdrücke zu speichern, wieder abgekommen. Der Landesbeauftragte hofft, dass es dabei bleibt (vgl. auch **Anlage 31**).

6.4 Personenstandsgesetz

Wie unter Ziff. 4.2 dargelegt, ist das Personenstandswesen eines der Fachprojekte des Aktionsplans Deutschland-Online. Das einzuführende elektronische Personenstandsregister ist ein Schwerpunkt des Vorhabens. Der elektronische Datenbestand soll für einen vereinfachten Ausdruck von Personenstandsurkunden und die Mitteilungen an andere Behörden genutzt werden. Rechtliche Grundlage hierzu ist das am 23. Februar 2007 verkündete Gesetz zur Reform des Personenstandsrechts (BGBl. I, S. 122). Das Gesetz tritt am 1. Januar 2009 in Kraft, einige Regelungen gelten bereits jetzt, wie u.a. die Möglichkeit der Länder, zentrale elektronische Personenstandsregister zur Erprobung einzurichten. Einzelheiten sind in Rechtsverordnungen des Bundes bzw. der Länder zu regeln. So sind die Länder auch zum Erlass von Mitteilungspflichten ermächtigt (§ 74 Abs. 1 Nr. 6 Personenstandsgesetz).

Der Landesbeauftragte hatte Gelegenheit, gegenüber dem Ministerium des Innern des Landes Sachsen-Anhalt zu ersten Entwürfen Stellung zu nehmen. Auch andere Landesbeauftragte haben jeweils Stellung genommen. Während einzelne kritisierte Formulierungen optimiert wurden, bleiben die grundsätzlichen datenschutzrechtlichen Bedenken gegenüber zentralen Datenbeständen bestehen. Die Entwicklung ist weiter zu begleiten, insbesondere angesichts der Darstellungen in der Begründung zum Gesetzentwurf. Sie spricht von länderübergreifender Zusammenarbeit, ausländischen Stellen und internationalen Organisationen ebenso wie von der Frage, ob bei der Beurkundung der Geburt ein persönliches Identifikationsmerkmal zu vergeben ist.

7. Europäischer und internationaler Datenschutz

7.1 „Europäischer Informationsverbund“ - Austausch für Polizei- und Sicherheitsbehörden

„Europa gelingt gemeinsam“ - hinter diesem Titel verbirgt sich das Präsidentschaftsprogramm der Bundesregierung zur EU-Ratspräsidentschaft vom 1. Januar bis 30. Juni 2007. Auf 25 Seiten erklärt die Bundesregierung, was sie in der ersten Jahreshälfte 2007 für und in Europa bewegen will.

In der Einleitung kann man lesen: „Deutschland möchte während seiner Präsidentschaft einen Beitrag leisten, damit den internen und externen Herausforderungen der Europäischen Union effektiv begegnet werden kann. Dabei werden im Vordergrund stehen: die Fortführung des Verfassungsprozesses, die Zukunftsfähigkeit des europäischen Wirtschafts- und Sozialmodells, der Raum der Freiheit, der Sicherheit und des Rechts sowie der Ausbau des europäischen Sicherheits- und Stabilitätsraumes.“ Ein paar Seiten weiter: „Vor dem Hintergrund internationaler Krisen, des Terrorismus, der Verbreitung von Massenvernichtungswaffen, ... wurde im Jahr 2003 die Europäische Sicherheitsstrategie verabschiedet. Gemäß den darin enthaltenen Vorgaben wird sich die deutsche Präsidentschaft für eine effizientere und kohärente Außenpolitik und eine vertiefte Zusammenarbeit mit den Partnern einsetzen.“

Als vorläufiges Ergebnis des Einsatzes hat die deutsche Ratspräsidentschaft Mitte März einen neuen Vorschlag für einen **EU-Rahmenbeschluss zum Datenschutz im Sicherheitsbereich** unterbreitet. Nach dem deutschen Vorschlag soll der besonders umkämpfte Austausch von Polizeidaten mit Drittstaaten von diesen Regelungen unberührt bleiben. Ein Drittstaat in diesem Sinne ist auch die USA. Und dass die USA ein erhöhtes Interesse an europäischen Polizeidaten hat, weiß man nicht erst seit dem transatlantischen Abkommen zur nach wie vor umstrittenen Übermittlung von Flugpassagierdaten (siehe Ziff. 7.5). Gefasst wurde ein solcher EU-Rahmenbeschluss auf Vorschlag der deutschen Ratspräsidentschaft bisher nicht.

Allerdings haben bereits 15 Mitgliedsstaaten die Vernetzung von Gen- und Fingerabdruckdaten beschlossen. Der EU-Datenschutzbeauftragte Peter Hustinx kritisierte in diesem Zusammenhang die nicht ausreichende rechtliche Grundlage für einen solchen Vertrag und das Fehlen eines übergeordneten Datenschutzkonzeptes für den Austausch personenbezogener Informationen.

Auch der **Vertrag von Prüm** - den die Bundesregierung mit auf den Weg gebracht hat und der 2005 zwischen sieben Staaten vereinbart wurde und einen elektronischen Datenaustausch etwa von DNA- und Fahrzeugregisterdaten vorsieht - soll nun eiligst in den Rechtsrahmen der EU überführt werden, um die polizeiliche Zusammenarbeit zu verbessern. Der EU-Datenschutzbeauftragte bemängelt hier, dass der Vertrag nicht im regulären Gesetzgebungsverfahren der EU geschlossen wurde. Einem solchen Vertrag hätte ein Rahmenbeschluss des EU-Rates für die Zusammenschaltung von Polizeidatenbanken vorausgehen müssen.

Vor diesem Hintergrund erscheint das im Präsidentschaftsprogramm als „... Ausbau des europäischen Sicherheits- und Stabilitätsraumes“ beschriebene Ziel der deutschen Ratspräsidentschaft datenschutzrechtlich keineswegs zurückhaltend. Vielmehr scheint die Bundesregierung sich gezielt für einen immer umfangreicheren Datenaustausch zwischen den Polizei- und Sicherheitsbehörden in Europa einzusetzen. Dass der EU-Datenschutzbeauftragte dabei nach eigener Einschätzung nicht angemessen beteiligt wurde, spricht für sich.

7.2 Europol

Über die Entwicklung bei Europol hat der Landesbeauftragte immer wieder berichtet (vgl. zuletzt VII. Tätigkeitsbericht, Ziff. 6.2).

Inzwischen sind die Europol-Befugnisse durch drei Änderungsprotokolle zum Europol-Übereinkommen weiter ausgebaut worden. Damit soll Europol eine deutlich größere Rolle bei der Bekämpfung grenzüberschreitender schwerer Straftaten spielen. So darf Europol jetzt an gemeinsamen Ermittlungsgruppen der Mitgliedsstaaten teilnehmen und mit ihnen Informationen, d.h. auch personenbezogene Daten, austauschen. Europol darf jetzt außerdem einzelne Mitgliedsstaaten um die Aufnahme von Ermittlungen ersuchen, und auf das Informationssystem bei Europol dürfen weitere nationale Behörden zugreifen.

Geplant ist weiterhin die Umwandlung des Europol-Übereinkommens in einen Ratsbeschluss. Damit wäre bei zukünftigen Änderungen die demokratische Kontrolle durch das EU-Parlament oder den Bundestag ausgehebelt.

7.3 Europäische und internationale Datenschutzkonferenzen

Im Berichtszeitraum fanden mehrere europäische und internationale Datenschutzkonferenzen statt.

Die Europäische Datenschutzkonferenz am 25./26. April 2005 in Krakau hat sich in einer einstimmig angenommenen Entschließung für einen verbesserten Datenschutz bei der grenzüberschreitenden Kriminalitätsbekämpfung ausgesprochen. Zudem hielten es die Datenschutzbeauftragten für dringend erforderlich, den europäischen Datenschutz umfassend und einheitlich für den öffentlichen und privaten Bereich zu regeln. Nur so würde dem in der Charta der Europäischen Grundrechte und im Entwurf der Europäischen Verfassung verankerten Grundrecht auf Datenschutz Genüge getan (**Anlagen 28** und **29**).

Zu dem Thema „Veränderte Sicherheitslage und Datenschutz im europäischen Staatenverbund“ hat sich auch das 14. Wiesbadener Forum Datenschutz am 23. Juni 2005 Gedanken gemacht. Unter anderem hat man sich dort mit den folgenden Fragen beschäftigt: Wie können wir eine Harmonisierung des Datenschutzes auf möglichst hohem Niveau erreichen? Wie können wir unser hohes Datenschutzniveau gegen europäische Nivellierung schützen? Brauchen wir für den europäischen Sicherheitsbereich einheitliche Datenschutzregelungen vergleichbar mit der EU-Datenschutzrichtlinie oder reichen jeweils „projektbezogene Regelungen“ aus? (vgl. dazu die Entschließung der 71. Datenschutzkonferenz am 16./17. März 2006 in Magdeburg; **Anlage 10**)

Auf der Europäischen Datenschutzkonferenz am 24./25. April 2006 in Budapest wurde eine Erklärung zur Notwendigkeit datenschutzrechtlicher Regelungen bei der polizeilichen und justiziellen Zusammenarbeit in der EU (sog. „Dritter Pfeiler“) verabschiedet (**Anlage 32**). Wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit dazu erklärte, wird mit der zu erwartenden Intensivierung des Austausches personenbezogener Informationen der Polizei- und Justizbehörden in Europa die Schaffung eines hohen und einheitlichen Datenschutzstandards auch für diesen Bereich immer dringender. In diesem Sinne äußerten sich die Europäischen Datenschutzbehörden erneut in London am 2. November 2006 (**Anlage 33**).

Die 27. Internationale Datenschutzkonferenz in Montreux vom 14. bis 16. September 2005 ist in einer Schlusserklärung („Erklärung von Montreux“, **Anlage 30**) übereingekommen, die Anerkennung des universellen Charakters der Datenschutzgrundsätze zu fördern.

Auf der 28. Internationalen Datenschutzkonferenz, die vom 2. bis 3. November 2006 in London stattfand, standen die Gefahren einer Überwachungsgesellschaft im Mittelpunkt. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat dazu hervorgehoben, dass der weltweit feststellbare Datenhunger der

Wirtschaft und das Interesse staatlicher Stellen an möglichst umfassenden Ermittlungsansätzen eine äußerst brisante Mischung bilden.

7.4 Erster Europäischer Datenschutztag

Der Europarat hat den 28. Januar zum Europäischen Datenschutztag erklärt, der zukünftig jährlich begangen wird. An diesem Datum wurde im Jahr 1981 die Unterzeichnung der Europaratskonvention 108 begonnen. Mit der Konvention wollten die unterzeichnenden Staaten die Achtung der Rechte und Grundfreiheiten, insbesondere das Recht auf einen Persönlichkeitsbereich bei der automatisierten Datenverarbeitung sicherstellen.

Aus Anlass des ersten Europäischen Datenschutztages am 28. Januar 2007 haben die Datenschutzbeauftragten des Bundes und der Länder eine zentrale Veranstaltung in der Vertretung des Landes Sachsen-Anhalt beim Bund durchgeführt, die auf große Resonanz gestoßen ist.

Thema der Veranstaltung war die Fragestellung: Datenschutz ist Grundrechtsschutz – Wie schützt der Staat die Freiheit? Ausgangspunkt war die Beobachtung, dass die Sicherheit fast unumstritten ganz oben auf der politischen Agenda steht. Vielfältige staatliche Informationsbeschaffungen zur Gefahrenabwehr und Strafverfolgung legen nahe, dem Datenschutz wieder größeres Gewicht zu verleihen. Anti-Terror-Datei, Kontenüberwachung, Passagierdatenübermittlung bzw. die Speicherung von Telekommunikationsverbindungsdaten auf Vorrat sind Beispiele für Datenverarbeitungen, die das Verhältnis zwischen Sicherheitsgewinn und Freiheitsverlust diskussionswürdig erscheinen ließen. In Vorträgen und Podiumsdiskussion mit Teilnehmenden aus Bundesregierung, Parlamenten, Verfassungsgerichtsbarkeit, Wissenschaft und Datenschutzkontrolle wurde der Frage nachgegangen, wie die Verantwortlichen in der Politik die Freiheit der Bürgerinnen und Bürger schützen.

7.5 Übermittlung von Flugpassagierdaten in die USA

Gegen den Widerstand des Europäischen Parlamentes und ohne die Bedenken der Artikel 29-Datenschutzgruppe[1] zu berücksichtigen, hat 2004 die Europäische Kommission ein Abkommen mit den USA über die Weitergabe von Daten über Flugpassagiere, die in die USA einreisen, gebilligt. Auch die Datenschutzbeauftragten des Bundes und der Länder haben sich gegen die weitreichenden und aus ihrer Sicht zum Teil überflüssigen Datenübermittlungen ausgesprochen. Im April 2004 hat das Europäische Parlament beschlossen, den Europäischen Gerichtshof deswegen anzurufen. Dieser hat mit Urteil vom 30. Mai 2006 die Entscheidung der Kommission für nichtig erklärt, allerdings ohne datenschutzrechtliche Aspekte

[1] Die Artikel 29-Gruppe wurde 1996 gemäß Artikel 29 der Europäischen Datenschutzrichtlinie eingerichtet. Ihre Aufgabe ist es, gegenüber der Allgemeinheit und den Organen der EU Empfehlungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten auszusprechen sowie die Kommission datenschutzrechtlich zu beraten und ihr gegenüber zu Fragen des Datenschutzes Stellungnahmen abzugeben. Sie besteht insbesondere aus den Datenschutzbeauftragten der Mitgliedsstaaten und wird zur Zeit vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit geleitet.

zu prüfen. Danach haben sich die Europäische Kommission und die USA im Oktober 2006 auf ein „Interimsabkommen“ zur Übermittlung von Flugpassagierdaten geeinigt, wonach die Daten zunächst wie bisher übermittelt werden. Zuletzt haben das Europäische Parlament einen Entschließungsantrag verabschiedet, in dem festgestellt wird, dass die in Aussicht genommenen Lösungen u.a. zum Passagierdatenabkommen nicht ausreichen, um die Daten der EU-Bürger zu schützen, und die Artikel 29-Gruppe einen Workshop veranstaltet, auf dem man sich darüber einig war, dass jedes weitere Übereinkommen die Grundrechte garantieren und technische und organisatorische Sicherheitsmaßnahmen gewährleisten muss. Der Landesbeauftragte verfolgt die weitere Entwicklung, obwohl sie nicht unmittelbar in seinen Zuständigkeitsbereich fällt, mit Interesse.

7.6 SWIFT

Die Society for Worldwide Interbank Financial Telecommunication (SWIFT) dürfte bis Mitte des vergangenen Jahres wohl nur Eingeweihten ein Begriff gewesen sein. Seit SWIFT nach dem 9. September irgendwie und warum auch immer alle dort bekannt gewordenen Auslandsgeldtransaktionen an US-amerikanische Behörden weitergegeben haben soll, hat sich dies geändert.

Doch was ist und was macht SWIFT, dass es für US-Behörden so interessant erscheinen lässt? SWIFT ist ein weltweit agierender Geldüberweisungsdienst zur Übermittlung von internationalen Zahlungsanweisungen. SWIFT speichert alle Überweisungsdaten für 124 Tage in zwei Rechenzentren. Eines der Rechenzentren befindet sich in Belgien, das andere in den USA. Die Rechenzentren haben denselben Datenbestand, weil die Daten „gespiegelt“ werden. Die Zahlungsanweisungen, die verarbeitet werden, enthalten diverse personenbezogene Daten. So ist u.a. der Name des Zahlungsanweisenden und des Zahlungsempfängers ausgewiesen. Und diese Informationen sind für die US-Behörden zur Terrorismusbekämpfung von großem Interesse. Denn wer die Geldströme kennt, kann die Strukturen dahinter verstehen.

Im Namen der Terrorismusbekämpfung traten nun US-amerikanische Behörden und auch die US-Notenbank an SWIFT mit Offenlegungsbeschlüssen heran. Sie wollten an Informationen über Finanztransaktionen von Verdächtigen mit Verbindungen zu Al Qaida gelangen. Nach Angaben von SWIFT sei durch das US-Finanzministerium die vertrauliche Behandlung der Daten zugesichert worden. SWIFT übermittelte daraufhin die gewünschten Daten.

Nach langen, auch öffentlich geführten Diskussionen hat sich die Artikel 29-Gruppe auf ihrer Sitzung am 21. und 22. November 2006 zu einer gemeinsamen Stellungnahme zum Vorgehen von SWIFT verständigt.
Nach Auffassung der Artikel 29-Gruppe ist die EG-Datenschutzrichtlinie von 1995 auf den Austausch von personenbezogenen Daten durch SWIFT anwendbar. SWIFT und die Finanzinstitute tragen die Verantwortung für die Verarbeitung der personenbezogenen Daten gemeinsam. SWIFT trägt zwar die Hauptverantwortung, die Finanzinstitute sind in gewissem Umfang allerdings mitverantwortlich. Bei den in Rede stehenden Übermittlungen an US-Behörden haben SWIFT und die Finanzinstitute die Vorgaben der EG-Datenschutzrichtlinie nicht beachtet.

Die Artikel 29-Gruppe forderte daher SWIFT und die Finanzinstitute auf, die Rechtsverletzungen zu beenden und zu einer rechtmäßigen Datenverarbeitung zurückzukehren. Weiterhin wurde gegenüber den Zentralbanken eine Klärung der Aufsichtsstrukturen bei SWIFT angemahnt. Und letztendlich wurden die Finanzinstitute aufgefordert, ihre Kunden gem. der Artikel 10 und 11 der EG-Datenschutzrichtlinie darüber zu unterrichten, wie deren Daten verarbeitet werden und welche Rechte sie als Betroffene haben. Sie haben ihre Kunden auch darüber zu informieren, dass US-Behörden Zugriff auf die Daten haben können.

Die obersten deutschen Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich hatten zuvor bereits solche Forderungen erhoben (siehe **Anlage 26**).

Der Bundestag hat die Bundesregierung aufgefordert, sich für eine das Bankgeheimnis sowie das informationelle Selbstbestimmungsrecht der Bankkunden berücksichtigende Lösung des Konflikts einzusetzen.

7.7 Terrorlisten der Vereinten Nationen

Nach den Anschlägen vom 11. September 2001 haben die Vereinten Nationen sog. Terrorlisten eingeführt. Auf ihnen sind bekannte Terroristen, aber auch zahlreiche andere Personen mit arabischen Namen aufgeführt. Den dort genannten Personen dürfen Banken, Ämter und andere Institutionen kein Geld zur Verfügung stellen. In der EU wurden die von den Vereinten Nationen vorgegebenen Maßnahmen auf der Grundlage des „Gemeinsamen Standpunktes 2001/931/ GASP“ des Europäischen Rates vom 27. Dezember 2001 mit einer Verordnung (EG) umgesetzt.

Das wollten die Datenschutzbeauftragten des Bundes und der Länder nicht hinnehmen und haben deshalb auf der 71. Datenschutzkonferenz vom 16./17. März 2006 in Magdeburg die Bundesregierung aufgefordert, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz (**Anlage 11**).

Im Dezember 2006 hat der Sicherheitsrat der Vereinten Nationen eine Resolution verabschiedet, in der die Einrichtung eines sog. Focal Point bei den Vereinten Nationen beschlossen wurde, an den sich Privatpersonen direkt wenden können, um die Entfernung ihres Namens von den Terrorlisten zu beantragen. Ob dies für den Individualrechtsschutz entscheidenden Fortschritt bringt, ist fraglich, da der Focal Point den Antrag an den Staat weiterleitet, der das Listing vorgeschlagen hat; ohnehin entscheidet wie bisher das Sanktionskomitee.

Während es gegen die Aufnahme in eine Terrorliste der Vereinten Nationen bislang keinen hinreichenden Rechtsschutz gibt, hat das Europäische Gericht 1. Instanz beim Gerichtshof der Europäischen Gemeinschaften in Luxemburg dagegen Rechtsschutz bei EU-Sanktionslisten gewährt.

8. Finanzwesen

8.1 Identifikationsnummer im Besteuerungsverfahren

Nicht aufzuhalten war die „Einführung dauerhafter Identifikationsnummern in Besteuerungsverfahren“ (vgl. VII. Tätigkeitsbericht, Ziff. 8.1.1). Inzwischen ist auch die erforderliche Rechtsverordnung nach § 139d AO erlassen worden (vgl. LT-Drs. 5/618). Damit wird zum 1. Juli 2007 auf der Grundlage von Meldedatenübermittlungen erstmals ein zentrales Register geschaffen, in dem neben den Identifikationsnummern gem. § 139b AO auch die Personalien und Anschriften der gesamten Bevölkerung (einschließlich der Neugeborenen und aller anderen Kinder, die noch gar nicht steuerpflichtig sind) erfasst sind. Auch wenn die Landesregierung das Vorhaben im Hinblick auf einen wirksamen Gesetzesvollzug gutheißt (Stellungnahme zum VII. Tätigkeitsbericht, LT-Drs. 4/2524, zu 8.1.1, S. 9), bleiben gerade auch deswegen datenschutzrechtliche Zweifel.

8.2 Kontenabrufverfahren

Über die u.a. den Finanzbehörden nach § 93 Abs. 7 AO neu eingeräumte Möglichkeit, über das Bundeszentralamt für Steuern einzelne Kontodaten bei den Kreditinstituten abzurufen, hatte der Landesbeauftragte bereits kritisch berichtet (vgl. VII. Tätigkeitsbericht, Ziff. 8.1.2).

In der Folge haben die Datenschutzbeauftragten der Länder das Verfahren bei den Finanzämtern überprüft. Dabei sind verschiedene Mängel aufgefallen, die zum großen Teil den Vordrucken zur Dokumentation im Kontenabrufverfahren geschuldet waren; so fiel auch bei der Kontrolle eines Finanzamtes in Sachsen-Anhalt auf, dass die Benachrichtigungspflicht gegenüber dem Betroffenen nach dem Kontenabruf vernachlässigt wurde. Deshalb haben sich die Datenschutzbeauftragten des Bundes und der Länder zusammengesetzt und gemeinsam ein datenschutzgerechtes Formular entwickelt. Dieser Vordruck wurde von der Finanzverwaltung zwar nicht 1:1 übernommen, doch enthalten die jetzt in den Ländern verwendeten Formulare zahlreiche datenschutzrechtliche Verbesserungen.

Anzumerken bleibt, dass die Entscheidung des Bundesverfassungsgerichts zur Rechtmäßigkeit des Kontenabrufverfahrens im Hauptsacheverfahren immer noch aussteht.

8.3 Elektronische Signatur in der Finanzverwaltung

Im VII. Tätigkeitsbericht (Ziff. 8.2) hatte der Landesbeauftragte bereits die Entscheidung der Finanzverwaltung kritisiert, bei der elektronischen Steuererklärung - ELSTER auf eine qualifizierte elektronische Signatur zu verzichten. Seine und die Kritik der anderen Datenschutzbeauftragten des Bundes und der Länder hat leider nicht gefruchtet. Inzwischen sind sowohl die Abgabenordnung (§ 87a AO) als auch die Steuerdatenübermittlungsverordnung (§ 6 StDÜV) den Wünschen der Finanzminister angepasst worden.

Insbesondere die Änderungen der Steuerdatenübermittlungsverordnung haben die Datenschutzbeauftragten mit einem Schreiben an den Präsidenten des Bundesrats unter Hinwies auf Unstimmigkeiten zur Rechtsgrundlage in der Abgabenordnung zu verhindern versucht. Das war jedoch vergeblich, so dass sich der § 6 StDÜV jetzt so liest, als wenn bei der elektronischen Übermittlung nicht nur keine qualifizierte elektronische Signatur mehr erforderlich ist, sondern auch kein anderes sicheres Verfahren.

8.4 Auskunftsersuchen eines Finanzamtes

Im Berichtszeitraum hat ein Finanzamt eine Stadt aufgefordert, alle Baugenehmigungen mit Baukosten von über einer halben Million Euro für einen Zeitraum von fünf Monaten aufzulisten. Aus der Aufstellung sollten Name und Anschrift des Bauherrn, der Entwurfsverfasser mit Anschrift, die Art des Bauvorhabens und die geschätzten Baukosten hervorgehen. Darüber hinaus sollten auch die durch die Stadt selbst vergebenen Bau- und Dienstleistungen aufgelistet werden. Zu diesen Leistungen sollten die Art der Leistung, der leistende Unternehmer mit Anschrift, die Angebotssumme, die Differenz zum Nächstgebot und der Zeitraum der Leistungserbringung angegeben werden. Begründet hatte das Finanzamt seine Anforderung mit der Einführung des Gesetzes zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung (SchwarzArbG) und Erfahrungen aus Prüfungen, die zeigten, dass Angebotspreise oftmals nur durch Einschaltung von Dumpingsubunternehmen erzielt werden können. Innerhalb von Subunternehmerketten erfülle meist ein Subunternehmer die steuerlichen und Sozialabgabenpflichten nicht.

Trotz anfänglicher Skepsis ergab die datenschutzrechtliche Überprüfung, dass das Finanzamt grundsätzlich ein Recht auf die geforderten Angaben hat. Nach § 2 SchwarzArbG obliegt die Prüfung der Erfüllung steuerlicher Pflichten den zuständigen Landesfinanzbehörden; in Sachsen-Anhalt den Steuerfahndungsstellen bei den Finanzämtern. Die Aufdeckung und Ermittlung unbekannter Steuerfälle ist nach § 208 AO auch Aufgabe dieser Steuerfahndungsstellen. Eine solche Ermittlung nach unbekannten Steuerfällen im Bereich der Schwarzarbeit wollte das bei der Stadt anfragende Finanzamt durchführen. Als Ausgangspunkt für weitere Ermittlungen sollten die Daten der Stadt dienen.

Gänzlich voraussetzungslos darf aber auch eine Steuerfahndungsstelle bei der Ermittlung unbekannter Steuerfälle nicht tätig werden. Ermittlungen „ins Blaue hinein“, „Rasterfahndungen“, Ausforschungsdurchsuchungen oder ähnliche Ermittlungsmaßnahmen sind unzulässig. Die Steuerfahndung darf erst dann tätig werden, wenn ein hinreichender Anlass dazu besteht. Ein solcher Anlass liegt nach der Rechtsprechung vor, wenn aufgrund konkreter Anhaltspunkte – z.B. wegen der Besonderheit des Objektes oder der Höhe des Wertes – oder aufgrund allgemeiner Erfahrung die Möglichkeit einer Steuerverkürzung in Betracht kommt.

Von Ermittlungen „ins Blaue hinein“ konnte vorliegend nicht ausgegangen werden. Die Steuerfahndung hat sich auf Erfahrungen aufgrund von Prüfungen berufen. Danach sei die Einschaltung von Dumpingsubunternehmen und die Wahrscheinlichkeit, dass ein Subunternehmer in der Subunternehmerkette die steuerlichen und Sozialabgabenpflichten nicht erfüllt, hinreichend groß. Die Darstellung

der Steuerfahndungsstelle des Finanzamtes erschien nachvollziehbar und plausibel.

Aber auch wenn das Finanzamt grundsätzlich zu einer solchen Anfrage berechtigt ist, finden derlei Maßnahmen ihre Grenzen in der Abgabenordnung. Vorliegend bestanden datenschutzrechtlich zumindest Bedenken gegen den Umfang der angeforderten Daten. So erklären sich die Angaben zum Bauherrn und seiner Anschrift, der Art des Bauvorhabens und zur geschätzten Bausumme von selbst. Wozu jedoch die Angaben zum Entwurfsverfasser erforderlich waren, erschloss sich nicht. Die Stadt wurde darauf hingewiesen, dass Bedenken gegen die Erforderlichkeit dieses Datums bestehen. Ihr wurde vorgeschlagen, das Finanzamt zunächst die Erforderlichkeit begründen zu lassen und dann über die datenschutzrechtliche Zulässigkeit zu entscheiden.

Die Verhältnismäßigkeit des Auskunftsersuchens war vorliegend dadurch gewahrt, dass nicht wahllos jedes, sondern nur Bauvorhaben mit einem Bauvolumen von mehr als 500.000 € bzw. Dienst- und Werkleistungen von mehr als 50.000 € erfasst werden sollten.

8.5 KONSENS

Im März 2006 erhielt der Landesbeauftragte davon Kenntnis, dass die Bundesländer den Abschluss eines Verwaltungsabkommens zu KONSENS („Koordinierte neue Softwareentwicklung der Steuerverwaltung“) beabsichtigen.

Inhalt des Abkommens ist es u.a., dass sich die Bundesländer als Vertragspartner verpflichten, entsprechend einem verbindlich festgelegten Einsatzplan flächendeckend eine einheitliche Software für das Besteuerungs-, Straf- und Bußgeldverfahren einzuführen. Auch wenn grundsätzlich gegen den Einsatz einheitlicher Software keine Bedenken bestehen, so muss diese doch den jeweiligen landesrechtlichen Vorschriften entsprechen.

Nun kann man natürlich einräumen, dass die Steuergesetzgebung Bundesrecht ist und damit sowieso bundeseinheitlich. Aber die Einführung von Software bei Landesbehörden - und die Oberfinanzdirektionen und Finanzämter sind Landesbehörden - ist nicht nur unter steuerrechtlichen Gesichtspunkten zu betrachten. Vielmehr kommt auch und vor allem den datenschutzrechtlichen Landesvorschriften große Bedeutung zu.

Allein der Verpflichtung nach § 14 Abs. 1 Satz 2 DSG-LSA, dass der Landesbeauftragte rechtzeitig über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu unterrichten ist, kann das Land bei gemeinsamen Entwicklungen nur schwerlich nachkommen. Das Datenschutzrecht der einzelnen Bundesländer stellt auch ganz unterschiedliche Anforderungen an Softwareentwicklungen. Bereits vor diesem Hintergrund konnten die Landesbeauftragten dem Vorschlag der Finanzverwaltung, der KONSENS-Arbeitsgruppe der Finanzverwaltung eine entsprechende Arbeitsgruppe der Datenschutzbeauf-

tragten gegenüberzustellen, mit der die datenschutzrechtlichen Probleme verbindlich geklärt werden, nicht folgen.

In der Sitzung des Arbeitskreises Steuerverwaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im April 2006 wurde der Vorschlag zwar diskutiert; aber mit dem Ergebnis, dass kein Gremium die Prüfungskompetenz der einzelnen Landesbeauftragten ausschließen kann. Eine frühzeitige Einbindung der Landesbeauftragten in den Entwicklungsprozess einheitlicher Software wäre wünschenswert, weil wegen der hohen Entwicklungskosten spätere datenschutzrechtliche Einwände oft übergangen werden. Gegebenenfalls könnte der Finanzverwaltung jedoch insoweit entgegengekommen werden, als der Landesbeauftragte, in dessen Bundesland eine bestimmte Software entwickelt wird, als Ansprechpartner fungiert und dann seinerseits die Verteilung von Unterlagen und Vorlage von Stellungnahmen veranlasst bzw. koordiniert.

9. Forschung

9.1 Allgemeines

Der Landesbeauftragte wurde im Berichtszeitraum bei 29 neuen Forschungsprojekten beteiligt. Auch hat er bereits laufende Forschungsvorhaben datenschutzrechtlich begleitet.
In diesem Berichtszeitraum war allerdings auffällig, dass doch immer ähnliche datenschutzrechtliche Problemkreise in den verschiedenen Projekten auftraten.
Betroffen war die Forschung mit medizinischen Daten und die Forschung von nicht-öffentlichen Stellen.

Außerdem fanden auch in den Schulen Sachsen-Anhalts im Jahr 2006 erneut die internationalen Schulleistungsuntersuchungen PISA und IGLU statt, die Studie TIMSS hat begonnen. Diese Projekte werden unter Ziff. 19.2 und 19.3 näher beschrieben.

9.2 Forschung mit medizinischen Daten

Häufig sind Forscher bei öffentlichen Stellen auf personenbezogene medizinische Daten angewiesen, ohne selbst eine Einwilligung der Betroffenen einholen zu können. Eine Datenübermittlung von öffentlichen Stellen (z.B. öffentlich-rechtlich organisierte Krankenhäuser, Gesundheitsämter) an die Forscher ist nach § 28 Abs. 8 i.V.m. Abs. 6 Nr. 4 BDSG i.V.m. § 3 Abs. 2 Nr. 1 DSG-LSA bzw. § 26 Abs. 1 Nr. 6 i.V.m. § 27 und § 11 Abs. 1 i.V.m. § 10 Abs. 2 Nr. 9 DSG-LSA unter den dort genannten Voraussetzungen zulässig.

Neben den datenschutzrechtlichen Vorschriften ist allerdings zu berücksichtigen, dass Gesundheitsdaten darüber hinaus auch der ärztlichen Schweigepflicht unterliegen (§ 9 Berufsordnung der Ärztekammer Sachsen-Anhalt) können.
Gemäß § 203 Abs. 1 StGB ist das unbefugte Offenbaren von anvertrauten fremden Geheimnissen unter Strafe gestellt. Ein schutzwürdiges Geheimhaltungsinteresse besteht z.B. bereits für den Namen des Patienten sowie für die Tatsache, dass dieser überhaupt den offenbarenden Arzt konsultiert hat. Für eine Daten-

übermittlung an den Forscher benötigt der Arzt somit eine Offenbarungsbefugnis. In Rechtsprechung und Literatur sind vier Offenbarungsbefugnisse entwickelt worden, die es dem Arzt ermöglichen, ein Patientengeheimnis rechtmäßig zu offenbaren. Diese sind die Einwilligung, die mutmaßliche Einwilligung des Patienten, gesetzliche Offenbarungspflichten oder -rechte und aus dem Güterabwägungsprinzip der sog. rechtfertigende Notstand gem. § 34 StGB.
Nach § 1 Abs. 3 Satz 2 BDSG bzw. § 3 Abs. 3 Satz 2 DSG-LSA bleibt die Verpflichtung zur Wahrung von Berufsgeheimnissen unberührt. Bei der ärztlichen Schweigepflicht handelt es sich um ein solches Berufsgeheimnis. Der Sonderschutz der Geheimnisse dieser Berufsgruppe soll nicht durch Regelungen des BDSG bzw. DSG-LSA verringert werden. Dies bedeutet, dass das BDSG bzw. das DSG-LSA und die standesrechtlichen Anforderungen nebeneinander gelten. Dies hat zur Folge, dass eine Übermittlung des Arztes an den Forscher nur dann zulässig ist, wenn beide Regelungen dies erlauben. Die allgemeinen datenschutzrechtlichen Regelungen stellen daher keine Offenbarungsbefugnis dar.
Hier kommt somit zunächst die Einwilligung der Betroffenen als Offenbarungsbefugnis in Betracht. Soweit deren Einholung nicht durchführbar ist, müssen Alternativen, wie z.B. die Pseudonymisierung der Daten oder das Adressmittlungsverfahren, geprüft werden.

9.3 Forschung von nicht-öffentlichen Stellen

Wenn nicht-öffentliche forschende Stellen von einer öffentlichen Stelle Daten benötigen, ist eine andere Übermittlungsgrundlage erforderlich. Dies kann eine spezialgesetzliche Norm, wie z.B. § 476 Abs. 1 StPO, oder auch die allgemeine Regelung des § 12 Abs. 1 i.V.m. § 10 Abs. 2 Nr. 9 DSG-LSA sein. In beiden Fällen muss die Datenübermittlung zur Durchführung wissenschaftlicher Forschung erforderlich sein, das wissenschaftliche bzw. öffentliche Interesse das entgegenstehende Betroffeneninteresse erheblich überwiegen und der Forschungszweck mit anonymisierten Daten nicht erreichbar sein. Nach § 12 Abs. 1 Nr. 1 DSG-LSA muss die Übermittlung an die Forscher zudem zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich sein. Sonst wären die Voraussetzungen nach § 12 Abs. 1 Nr. 2 DSG-LSA zu erfüllen.

Die Erforderlichkeit der einzelnen Datenübermittlungen zur Durchführung der Forschung ist normalerweise unproblematisch, da die Forscher dazu ggf. Stellung beziehen und bei Bedarf auch auf einzelne Informationen verzichten. Das wissenschaftliche oder öffentliche Interesse wird meist durch eine Entscheidung des zuständigen Ministeriums belegt. Bei der Darstellung, warum der Forschungszweck nicht mit anonymisierten Daten erreicht werden kann, bestehen zuweilen Unsicherheiten, da genau erläutert werden muss, warum personenbezogene Daten für den Forschungszweck unerlässlich sind. In der Praxis argumentieren die Forscher oftmals, dass der Name des Betroffenen überhaupt nicht erhoben wird. Allerdings ist es aufgrund der sonstigen Informationen häufig trotzdem möglich, eine bestimmte Person diesem Datensatz zuzuordnen. Die Festlegung, ob es sich um Daten einer bestimmbaren Person oder um anonymisierte Daten handelt, ist daher immer im Einzelfall zu klären.

Bei einem Forschungsvorhaben einer nicht-öffentlichen Stelle hat der Landesbeauftragte darauf hingewiesen, dass gem. § 476 Abs. 3 StPO eine Datenübermittlung nur an solche Personen erfolgt, die nach dem Verpflichtungsgesetz zur Geheimhaltung verpflichtet worden sind. Der Forscher wandte ein, dass er auch Professor an einer Fachhochschule und somit bereits Amtsträger im Sinne des § 476 Abs. 3 StPO sei. Der Sinn dieser Bestimmung, eine Strafbewehrung zu bewirken, setzt jedoch voraus, dass die personenbezogenen Informationen dem Empfänger im Zusammenhang mit seiner Eigenschaft als Amtsträger anvertraut oder bekannt geworden sind. Der Amtsträgerstatus als solcher bzw. datenschutzgerechtes Verhalten allein reichen daher nicht aus. Da weder dem Forschungsauftrag noch der Projektbeschreibung zu entnehmen war, dass der Forscher im Rahmen dieses Forschungsprojektes als Hochschullehrer tätig wird, hat der Landesbeauftragte die förmliche Verpflichtung weiterhin für erforderlich gehalten.

9.4 Biomaterialbanken für die Forschung

Biomaterialbanken sind Einrichtungen, die Proben menschlicher Körpersubstanzen (z. B. Zellen, Gewebe, Blut, ganze Organe) sammeln bzw. Anteile solcher Substanzen extrahieren (z. B. Serum oder DNS), diese durch personenbezogene und krankheitsbezogene Daten des Probanden ergänzen und diese Proben und Daten für Forschungszwecke zur Verfügung stellen. Probensammlungen, die im Rahmen der Krankenversorgung entstehen und nur intern zur Forschung genutzt werden, ohne dass die Proben oder Analyseergebnisse dauerhaft für weitergehende Forschungszwecke zur Verfügung gestellt werden, sind keine Biomaterialbanken.
Im Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde in Zusammenarbeit mit der Telematikplattform für Medizinische Forschungsnetze (TMF) ein Generisches Datenschutzkonzept für Biomaterialbanken erstellt und abgestimmt. Die TMF ist eine Interessengemeinschaft öffentlich geförderter medizinischer Forschungsverbünde und zahlreicher Koordinierungszentren für klinische Studien in Deutschland. Sie soll die Interessen der Forschungsverbünde in der Entwicklung und im Auf- und Ausbau leistungsfähiger IT-Infrastrukturen für die medizinische Forschung koordinieren. Durch die Entwicklung eines allgemeinen generischen Konzeptes für Biomaterialbanken ist eine Übertragbarkeit auf einzelne Biomaterialbanken möglich und auch bereits realisiert. Eine kontinuierliche Weiterentwicklung des Konzeptes von 2006 wurde durch die TMF zugesichert. Das Datenschutzkonzept entspricht im Wesentlichen einer Stellungnahme des Nationalen Ethikrates von 2004 und dem Endbericht des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag von 2006.

Aus datenschutzrechtlicher Sicht sind insbesondere die Themenbereiche der Einwilligungserklärungen, der Trennung der Datenbestände und Verantwortlichkeiten und der Möglichkeit der Anonymisierung zu begleiten.
Wenn ein Proband Materialien seines Körpers zu Zwecken der biomedizinischen Forschung zur Verfügung stellen möchte, darf dies nur mit seiner Einwilligung erfolgen. Die Einwilligungserklärung muss insbesondere folgende Sachverhalte enthalten: Der Forschungszweck, d.h. der Umfang der Nutzung der Biomaterialien, ist so konkret wie möglich zu formulieren; zukünftige, unbestimmte Zwecke

sind nicht ausgeschlossen. Die Nutzungsdauer bzw. der vorgesehene Zeitpunkt der Löschung bzw. Vernichtung der Daten/Proben ist mitzuteilen. Der Nutzerkreis ist zu benennen. Die Art und Weise der Verarbeitung (anonym, pseudonym oder personenbezogen) ist darzulegen.
Eine Rückidentifizierung des Probanden darf nur bei Eintritt vorher festgelegter Bedingungen stattfinden. Das Risiko einer versehentlichen oder mutwilligen Rückidentifizierung ist daher durch technische und organisatorische Maßnahmen zu minimieren. Materialien, medizinische und identifizierende Daten werden daher getrennt gespeichert. Die Verwaltung der Daten erfolgt in getrennter Verantwortung. Die Bereithaltung der Biomaterialien und der dafür erforderlichen Daten erfolgt in einer „Probenbank“. Die Daten des Probanden einschließlich möglicher Analyseergebnisse werden in „Datenbanken“ abgelegt. Die Probenbank ist daher in der Regel an einem Labor oder einem biomedizinischen Institut angesiedelt. Ein Pseudonym dient der Zusammenführung der Daten, z.B. für fallbezogene Auswertungen.
Eine vollkommene Anonymisierung von Gendaten einer Person ist nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht möglich, da das Ergebnis einer einzelnen Genomanalyse immer durch eine spätere Referenzanalyse wieder re-individualisiert werden kann. Wenn das dazu notwendige Zusatzwissen (Referenzprobe) nur mit unverhältnismäßig großem Aufwand erlangt werden kann, liegt eine faktische Anonymisierung vor. Eine solche Anonymisierbarkeit ist in Abhängigkeit der Rahmenbedingungen der Einlagerung und Nutzung aus heutiger Sicht möglich.

9.5 Genetisches Wissen und Datenschutz

Der Landesbeauftragte hat die in Ziff. 9.4 aufgeworfenen Fragen in die Arbeit einer interdisziplinären Arbeitsgruppe eingebracht, die seit 2005 auf Initiative der Evangelischen Akademie Sachsen-Anhalt und des Interdisziplinären Zentrums Medizin – Recht – Ethik der Martin-Luther-Universität Halle tagt. Dabei geht es um die Begrifflichkeiten des „genetischen Wissens“ und seiner Kontexte, exemplarisch an den Bereichen der individuellen medizinischen genetischen Beratung und der staatlichen Maßnahmen eines Public Health Genetics (Integration genetischen Wissens in öffentliche Gesundheitsvorsorge) verdeutlicht. Die Anwendungsbereiche genetischen Wissens und der daraus abgeleiteten Risikoabschätzungen berühren aus ethisch-rechtlicher Sicht nicht nur Medizin, Diagnose und Forschung, sondern auch die Bereiche der Abstammung (vgl. Bundesverfassungsgericht, Urteil vom 13. Februar 2007, 1 BvR 421/05, NJW 2007, 753 - Verbot heimlicher Vaterschaftstests) und der DNA-Analyse im Strafverfahren (siehe Ziff. 18.8), den Arbeitnehmerdatenschutz und Versicherungsverhältnisse. Der Bedarf für ein umfassendes Gendiagnostikgesetz auf der Grundlage der Prinzipien der Einwilligung für jegliche Datenverarbeitung und des Rechts auf Nichtwissen besteht unverändert (vgl. auch Ziff. 3.1).

10. Gesundheitswesen

10.1 Elektronische Gesundheitskarte

Die elektronische Gesundheitskarte sollte die heutige Krankenversichertenkarte zum 1. Januar 2006 ablösen (siehe VII. Tätigkeitsbericht, Ziff. 10.2). Dieses Ziel wurde nicht erreicht. Die elektronische Gesundheitskarte ist bis zum Ende des Berichtszeitraumes noch nicht einmal abschließend getestet. Die 10.000er Tests haben im Dezember 2006 in sieben Modellregionen begonnen. Im Land Sachsen-Anhalt befindet sich keine Testregion. Die 100.000er Tests sollen sich anschließen.
Die Tests erfolgen nach der Verordnung über Testmaßnahmen zur Einführung der Gesundheitskarte vom 5. Oktober 2005, zuletzt geändert am 2. Oktober 2006 (Neufassung, BGBl. I S. 2199).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zur Einführung der Tests der Gesundheitskarte u.a. Folgendes betont: Die differenzierten Zugriffsrechte der Versicherten nach § 291a Abs. 3 SGB V sollten ebenfalls Inhalt der Testverfahren sein. Einwilligung, Dokumentation auf der Karte, Widerruflichkeit und Beschränkung auf einzelne Anwendungen sowie die in § 291a Abs. 5 SGB V geforderten technischen Vorkehrungen zur Zugriffsautorisierung durch den Versicherten sind essentielle Vorraussetzungen für die Datenschutzkonformität der Karte. Ihre Realisierung vorzubereiten, muss ein wesentliches Ziel der Testverfahren sein.
Die Entwicklung, insbesondere die verfahrensmäßige Absicherung der Patientenrechte, wird vom Landesbeauftragten weiterhin beobachtet (vgl. auch Ziff. 10.2).

10.2 Elektronischer Heilberufsausweis

Um die Sicherheit der gespeicherten Daten zu gewährleisten, fordert § 291a SGB V den Besitz eines elektronischen Heilberufsausweises als Voraussetzung für den Zugriff auf die auf der elektronischen Gesundheitskarte gespeicherten Daten. Gemäß § 291a Abs. 5 Satz 3 SGB V muss der elektronische Heilberufsausweis eine qualifizierte Signaturfunktion besitzen. Der Empfängerkreis dieser Ausweise ist in § 291a Abs. 4 SGB V beschrieben und umfasst neben Ärzten, Zahnärzten und Apothekern (verkammerte Berufe) u.a. auch sonstige Erbringer ärztlich verordneter Leistungen (nicht verkammerte Berufe). Das sind z.B. Physiotherapeuten und Hörgeräteakustiker. Wer eine solche Karte ausgeben darf, wurde im SGB V nicht geregelt. Aus diesem Grund wurde bereits im Juni 2005 unter Beteiligung des Landesbeauftragten § 5 Abs. 1 des Gesetzes über die Kammern für Heilberufe Sachsen-Anhalt um Nr. 9 erweitert, die den Kammern als weitere Aufgabe die Ausstellung elektronischer Heilberufsausweise zuweist.

Darüber hinaus ist jedoch noch offen, welche Stelle die Ausgabe der Heilberufs- und Berufsausweise für die nicht verkammerten Berufe übernehmen könnte. Eine Projektgruppe hat im Rahmen einer Bestandsaufnahme eine Berufematrix erstellt und u.a. festgestellt, dass es über 40 eigenständige Heilberufe und Berufe im Gesundheitswesen in Deutschland und dazugehörend eine Vielzahl von zuständigen Berufserlaubnisbehörden gibt. Insgesamt gibt es in diesen Berufsgruppen ca.

2 Millionen Beschäftigte (ohne Arzthelferinnen und Heilpraktiker). Aufgrund dessen schlägt die Arbeitsgruppe nunmehr vor, ein „Nationales Berufsregister“ einzurichten, dass als einzig zuständige Stelle in Deutschland die Ausgabe der Heilberufs- und Berufsausweise für nicht verkammerte Berufe vornehmen soll. Dazu soll eine bundesweit zentrale Sammlung personenbezogener Dokumente entstehen, die Aufschluss über die Zuerkennung der Berufsbezeichnung geben. Aus datenschutzrechtlicher Sicht ist fraglich, ob eine solche Datensammlung überhaupt erforderlich ist, wenn die Aufgaben auch dezentral von den bisher zuständigen Behörden wahrgenommen werden können. Die Entscheidung darüber, inwieweit sich Sachsen-Anhalt am Register beteiligen wird, steht noch aus.

10.3 Datenbank über gefälschte Rezepte

Die Apothekerkammer teilte dem Landesbeauftragten mit, dass Rezeptfälschungen über verschreibungspflichtige Arzneimittel ständig zunehmen würden. Man habe sich daher aus Gründen der Fürsorgepflicht gegenüber den Kammermitgliedern überlegt, eine Datenbank zu erstellen, in der wesentliche Anhaltspunkte für gefälschte Rezepte (Namen, Arzneimittelverordnung, verschreibender Arzt, Kassenrezept bzw. Privatrezept) gesammelt werden können. Die Daten sollten in einer länderübergreifenden, netzbasierenden Plattform vorgehalten werden, die es registrierten Kammermitgliedern möglich gemacht hätte, entsprechende Daten abzufragen. Es sollte mit dem Einverständnis der betroffenen Ärzte gehandelt werden, die Daten zu Patienten seien unbeachtlich, da sie zumeist fingiert seien.

Hierzu hat der Landesbeauftragte die Apothekerkammer wie folgt beraten:
Die Führung einer entsprechenden Datenbank wäre kaum unter die Wahrnehmung der beruflichen Belange der Kammerangehörigen unter Beachtung der Interessen der Allgemeinheit im Sinne von § 5 Abs. 1 Nr. 1 des Gesetzes über Kammern für Heilberufe Sachsen-Anhalt zu subsumieren. Auch wenn die Apothekerkammer häufig mit der Problematik gestohlener oder gefälschter Verordnungsblätter konfrontiert wurde, dürften die Belange der Apotheker allenfalls u.a. betroffen sein. Darüber hinaus sind jedoch weitere Personenkreise und Einrichtungen in das Gesamtproblem involviert. Das gilt insbesondere für die Kassenärztliche Vereinigung, die Ärztekammer, einzelne Polizeidienststellen sowie einzelne Arztpraxen. Die beabsichtige Datenerhebung und Verarbeitung wäre daher möglicherweise nützlich gewesen, nicht aber zwingend für die Aufgabenerledigung der Kammer erforderlich. Die Erforderlichkeit der Datenerhebung und -verarbeitung wäre jedoch Voraussetzung, um zumindest eine Grundlage im DSG-LSA zu finden. Auch in der Regelung des § 17 Abs. 8 Apothekenbetriebsordnung konnte keine Rechtsgrundlage gesehen werden, da diese Regelung keine Grundlage für die Verarbeitung personenbezogener Daten darstellt, sondern lediglich eine Norm zur Zuweisung von Aufgaben an das pharmazeutische Personal.

Demgemäß wäre das Erheben, Speichern und Übermitteln durch Bereithalten von personenbezogenen Daten zur Einsicht lediglich auf der Grundlage der Einwilligung der Betroffenen zulässig gewesen. Zu den wirksamen Voraussetzungen einer Einwilligung hat der Landesbeauftragte auf § 4 Abs. 2 DSG-LSA verwiesen.

Unzulässig war es jedoch, personenbezogene Informationen aus den Angaben auf dem Rezept zu übernehmen, da diese im Normalfall fingiert sind. Zwar sind nach § 2 Abs. 1 DSG-LSA personenbezogene Daten nur Einzelangaben in Bezug auf natürliche Personen. Nicht existierende Personen sind daher nicht vom Anwendungsbereich des DSG-LSA erfasst. Da jedoch nicht mit Sicherheit ausgeschlossen werden konnte, dass die auf dem Rezept aufgeführten Personen dennoch existieren bzw. dass aus den vorhandenen Angaben auf existierende Personen geschlossen werden kann, wäre auch insoweit jeweils die Einwilligung erforderlich gewesen.

Zudem steht eine Änderung der Sach- und Rechtslage an. Die Einführung der elektronischen Gesundheitskarte soll zumindest die Funktion des elektronischen Rezepts beinhalten. Es ist daher abzusehen, dass der Bedarf an Maßnahmen zum Schutz des Papierrezepts stark abnehmen wird.

10.4 Mammographie-Screening

Die Einführung des Mammographie-Screenings soll der Senkung der Brustkrebssterblichkeit dienen. Bereits im VII. Tätigkeitsbericht (Ziff. 10.6) hat der Landesbeauftragte die daraus resultierenden Probleme aus datenschutzrechtlicher Sicht dargestellt.
Das Gesundheitsministerium plant, die Zentrale Stelle für das Land Sachsen-Anhalt beim Gesundheitsamt Bremen einzurichten. Damit wäre die Grundvoraussetzung für die Verwendung von Meldedaten für das Einladungswesen, eine öffentliche Stelle, erfüllt. In Bremen sehen die dortigen gesetzlichen Regelungen vor, dass das Gesundheitsamt Bremen diese zentrale Stelle für das Land Bremen ist, diese aber auch für andere Bundesländer tätig werden darf.

Für den beabsichtigten Abgleich des Mammographie-Screenings mit dem Krebsregister wurde der Staatsvertrag zum Gemeinsamen Krebsregister bereits geändert, die Ratifizierung steht noch aus.

Inzwischen ist auch der Entwurf des Gesetzes zur Änderung des Gesundheitsdienstgesetzes durch die Landesregierung im Landtag eingebracht worden, in dem die Schaffung der Zentralen Stelle vorgesehen ist. Die Details zur späteren Umsetzung (Aufgabenübertragung an die Hansestadt Bremen, Transfer der Daten, Verfahren beim Gesundheitsamt Bremen, Korrespondenz mit den Screening-Stellen) bedürfen weiterer datenschutzrechtlicher Beratung. An dem Erfordernis einer informierten Einwilligung als Rechtsgrundlage für die eigentliche Datenerhebung ändert sich nichts.

10.5 Einschulungsuntersuchungen

Ein Vater, der neben der Einladung zur Einschulungsuntersuchung seines Sohnes auch einen Informations- und Anamnesebogen erhalten hatte und diesen ausgefüllt zur Untersuchung mitbringen sollte, fragte beim Landesbeauftragten an, ob der Umfang der darin abgefragten medizinischen und soziodemographischen Daten (z.B. Elternbildung, Erwerbstätigkeit, Personen im Haushalt) tatsächlich für die Einschulungsuntersuchung erforderlich sei. Die optische und inhaltli-

che Trennung der im Zusammenhang mit der Einschulungsuntersuchung und auch der schulärztlichen Untersuchung stehenden Sachverhalte im Informations- und Anamnesebogen wurde nicht nur mit dem betroffenen Gesundheitsamt, sondern auch mit dem Verband der Ärzte im Öffentlichen Gesundheitsdienst im Land Sachsen-Anhalt e.V. ausführlich erörtert.
Im Ergebnis war Folgendes festzustellen: Gemäß § 37 Abs. 2 SchulG LSA i.V.m. § 9 Abs. 2 GDG LSA führt der Öffentliche Gesundheitsdienst vor der Aufnahme in die Schule eine Untersuchung durch, um den Gesundheits- und Entwicklungsstand der Kinder festzustellen. Es handelt sich daher um eine Pflichtuntersuchung und der Amtsarzt darf damit die dafür erforderlichen Angaben zur Anamnese gem. § 26 Abs. 1 Nr. 8 DSG-LSA erheben.

Die Angaben zum Impfstatus sind ebenfalls bei der Einschulungsuntersuchung nach § 34 Abs. 11 IfSG zu erheben. Das Gesundheitsamt leitet diese gewonnenen aggregierten und anonymisierten Daten über die oberste Landesbehörde an das Robert-Koch-Institut weiter. Die darüber hinausgehende Impfberatung ist jedoch freiwillig. Hierbei ist noch zu beachten, dass Angaben zum Impfstatus bei schulärztlichen Untersuchungen in den dritten und sechsten Schuljahrgängen nach § 38 SchulG LSA i.V.m. § 9 Abs. 2 GDG LSA nur ausschließlich freiwillig erhoben werden können, da § 34 Abs. 11 IfSG hierfür keine Erhebungsgrundlage bietet.

Die soziodemographischen Daten sollen im Rahmen der Einschulungsuntersuchung für begleitende wissenschaftliche Studien erhoben werden. Da dies nicht für die Feststellung des Entwicklungsstandes des Kindes erforderlich ist, ist eine solche Erhebung nur freiwillig nach § 26 Abs. 1 Nr. 2 DSG-LSA möglich.
Der Erhebungsbogen wird derzeit überarbeitet.

Darüber hinaus begleitet das Gesundheitsministerium in Zusammenarbeit mit dem Landesamt für Verbraucherschutz die Einführung des EDV-Programms „Oktoware“. Durch Verwendung dieses Programms in allen Gesundheitsämtern Sachsen-Anhalts soll zukünftig u.a. eine einheitliche Datenerhebung bei der Einschulungsuntersuchung erreicht werden. Der Landesbeauftragte berät die Beteiligten hinsichtlich der datenschutzrechtlichen Aspekte.

10.6 Rettungsdienstgesetz Sachsen-Anhalt

Im Rahmen des Gesetzgebungsverfahrens zum Entwurf eines Rettungsdienstgesetzes Sachsen-Anhalt (RettDG LSA) der Landesregierung (LT-Drs. 4/2254) hatte der Landesbeauftragte bereits im Oktober 2004 gegenüber dem Ministerium für Gesundheit und Soziales des Landes Sachsen-Anhalt keine datenschutzrechtlichen Bedenken geäußert. Dies bezog sich vornehmlich auf die Bestimmungen zum Datenschutz in § 14 des Entwurfs, der § 23 des bisherigen Gesetzes entsprach.

Im anschließenden Anhörungsverfahren zum Gesetzentwurf im Ausschuss für Gesundheit und Soziales des Landtages wurde der Landesbeauftragte nicht beteiligt.

Da der Landesbeauftragte noch Klärungsbedarf insbesondere zur beabsichtigten Verlängerung der Aufbewahrung von Tonaufzeichnungen von mindestens drei Monaten (§ 1 Abs. 2 Satz 4 RettDG LSA) auf künftig feststehende sechs Monate (§ 5 Abs. 1 Satz 6) sah, hielt er es für geboten, sich schriftlich gegenüber dem Ausschuss für Gesundheit und Soziales zu äußern.
In der Begründung zum RettDG LSA ging die Landesregierung davon aus, dass ein Zeitraum von drei Monaten zu kurz sei, um Fehlverhalten des Personals im Rettungsdienst zu untersuchen. Der Landesbeauftragte wies aus datenschutzrechtlicher Sicht darauf hin, dass möglicherweise ein kürzerer Zeitraum für die Wahrung der beteiligten Interessen ausreichen würde. Zumindest sei die Ausweitung des Zeitraums der Tonaufzeichnungen von drei Monaten auf sechs Monate anhand der in der Begründung des Entwurfs angesprochenen Erfahrungen näher zu erläutern.

In der Anhörung erklärte die Ärztekammer Sachsen-Anhalt, dass die vorgesehene Aufbewahrungspflicht von Tonbandaufzeichnungen auf ein Jahr verlängert werden sollte, da häufig Folgen von schweren Verletzungen erst nach sechs Monaten ersichtlich werden und ggf. Ansprüche erst dann angemeldet werden könnten. Bei einer kürzeren Frist seien die Tonbandaufzeichnungen dann nicht mehr vorhanden.

Das Gesetz kam mit diesem Vorschlag zustande (GVBl. LSA 2006, S. 84). Datenschutzrechtliche Zweifel an der Ausweitung der Tonbandaufzeichnungen auf 12 Monate wurden nicht laut.

10.7 Angabe von Diagnosen auf Verordnungen bei Krankentransporten

Ein Petent wandte sich im Rahmen der Abrechnung von Krankentransporten im Rettungswesen an den Landesbeauftragten. Die Angabe von Diagnosen auf Bescheinigungen für Rettungsfahrten widerspräche u.a. dem Rettungsdienstgesetz des Landes Sachsen-Anhalt (RettDG LSA) und § 203 StGB.

Der Landesbeauftragte führte aus, dass personenbezogene Daten im Rettungswesen nur insoweit übermittelt werden dürfen, als sie für die Abwicklung eines Beförderungsauftrages, insbesondere für die Abrechnung der erbrachten Leistung erforderlich sind. Die Rechtsgrundlage für eine Offenbarung ergibt sich jetzt aus § 14 Abs. 2 Satz 2 i.V.m. § 14 Abs. 1 Nr. 1 RettDG LSA.

Die Leistungserbringer nach dem Rettungsdienstgesetz zählen zu den sog. „sonstigen Leistungserbringern“ im Sinne von § 302 SGB V. Die durch die sonstigen Leistungserbringer für Zwecke der Abrechnung zulässigerweise zu übermittelnden Daten ergeben sich aus § 302 Abs. 1 SGB V.
Daraus folgt, dass zwar die Notarzt- bzw. Einsatzprotokolle für Abrechnungszwecke der sonstigen Leistungserbringer entsprechend der Auflistung in § 302 Abs. 1 SGB V und auch im Sinne des § 14 Abs. 1 RettDG LSA nicht erforderlich sind und als Folge den Krankenkassen grundsätzlich nicht offenbart werden dürfen. Dies gilt insbesondere, soweit Notarztprotokolle Informationen für den weiterbehandelnden Arzt enthalten. Solche Angaben dienen einem anderen Zweck als der Feststellung eines Grundes für die Notwendigkeit eines bestimmten Transportmit-

tels. Sie dürfen daher nicht für die Abrechnungszwecke der Krankenversicherung verwendet werden.

Ausgehend vom Grundsatz der Erforderlichkeit dürfen Krankenkassen zu Abrechnungszwecken personenbezogene Daten (Sozialdaten) auf der Grundlage des § 284 Abs. 1 Satz 1 Nr. 8 SGB V erheben. Von den Leistungserbringern erhalten die Krankenkassen Daten zu Abrechnungszwecken gem. § 294 i.V.m. § 302 SGB V. Danach hat der Notarzt aber u.a. eine Verordnung mit der Diagnose und den erforderlichen Angaben über den Befund vorzulegen. Maßgeblich sind hierfür die §§ 60, 133 SGB V.

Die Krankenkassen sind gem. § 60 i.V.m. § 133 SGB V verpflichtet, die Kosten der Kranken- bzw. Rettungstransporte zu übernehmen, wenn sie aus zwingenden medizinischen Gründen notwendig sind. Hierbei muss es sich um zwingende und unvermeidlich entstehende Aufwendungen handeln. Knappe, grundlegende Angaben sind daher ausreichend.
Eine weitergehende Begründung der medizinischen Notwendigkeit wäre dagegen nicht zulässig. Wenn Zweifel an der medizinischen Notwendigkeit des Transportmittels und damit der Leistungspflicht der Krankenkasse bestehen, hat die Krankenkasse gem. § 275 Abs. 1 Nr. 1 SGB V den Medizinischen Dienst der Krankenversicherung einzuschalten und eine gutachterliche Stellungnahme einzuholen.

10.8 Namensschilder an Patiententüren

Ein Patient im Maßregelvollzug teilte dem Landesbeauftragten mit, dass gelegentlich Besuchergruppen und auch Fernsehteams über die Flure des Krankenhauses geleitet werden und dabei Gelegenheit haben, die Patienten zu sehen. Außerdem sind an den Zimmertüren auf den Fluren Namensschilder angebracht.

Der Landesbeauftragte hat das Krankenhaus darauf hingewiesen, dass Namensschilder an den Türen nur ausnahmsweise und ggf. in bestimmten Fällen aus verwaltungsorganisatorischen Gründen (Gewährleistung medizinischer Nothilfe, Optimierung der Essensausteilung) erforderlich sein können. Überwiegende Interessen der Betroffenen können dem jedoch entgegenstehen, wenn durch, auch nur gelegentlichen, Publikumsverkehr die Offenbarung des Patientengeheimnisses zu befürchten ist. Werden also Fernsehteams und/oder andere Besucher über die Flure geleitet, ist die Verwendung von Namensschildern zu diesem Zeitpunkt unzulässig (Datenübermittlung an Dritte nach § 12 Abs. 1 DSG-LSA).
Ähnlich verhält es sich mit der Einsichtnahme von Fernsehteams in die Zimmer der Patienten. Können Besucher zur Kenntnis nehmen, wer in diesem Zimmer wohnt bzw. den Patienten selbst sehen, wäre diese Informationsübermittlung nur mit vorliegender Einwilligung des betroffenen Patienten zulässig.

Das Krankenhaus erläuterte, dass die Patienten im Vorfeld über die Filmaufnahmen informiert wurden. Außerdem wurde den Patienten die Möglichkeit gegeben, sich in Bereichen aufzuhalten, in denen nicht gefilmt wurde. In den Zimmern konnten die Patienten zuvor ihre persönlichen Gegenstände wegräumen. Soweit dennoch Personen oder persönliche Sachen im Film zu sehen waren, wurden diese im Film unkenntlich gemacht.

Bezüglich der Beschriftung der Türen teilte das Krankenhaus mit, dass dies aufgrund der Größe der Klinik und der derzeitigen Überbelegung erforderlich sei, um eine bessere Orientierung bei der Notfallversorgung auch für neues Personal oder für die Polizei zu erreichen. Das Krankenhaus hat sich dennoch entschlossen, die Namensschilder von den Patientenzimmern zu entfernen.

Im parallel dazu laufenden Gerichtsverfahren beschloss das zuständige Landgericht, dass bei der Abwägung der beiderseitigen Interessen die von der Klinik vorgetragenen Argumente vorgehen und das Persönlichkeitsrecht des Antragstellers (Patienten) insoweit zurücktreten muss. Das Gericht stellte in seiner Begründung hauptsächlich auf die Besonderheiten des Maßregelvollzugs ab. Hier seien bei Notfällen oder Evakuierungen des Gebäudes zum Schutz der Patienten und Mitarbeiter sofortige Überprüfungen, ob und welche Patienten noch im Gebäude sind und wo diese sich aufhalten können, erforderlich. Auch ein vorübergehendes Verdecken von Namen bei Besuchen von Dritten wird nicht als geeignete Maßnahme angesehen, da Notfälle jederzeit eintreten könnten. Die Nutzung der Namensschilder sei aus Gründen der Sicherheit und Ordnung innerhalb der Maßregelvollzugseinrichtung erforderlich.
Das Krankenhaus hat daraufhin angekündigt, die Namensschilder wieder an den Türen anzubringen.

10.9 Übermittlung einer Stellungnahme eines Krankenhauses an die Polizei

Ein Petent im Maßregelvollzug wandte sich an den Landesbeauftragten, da das Krankenhaus im Rahmen eines vom Petenten angestrengten Ermittlungsverfahrens eine ausführliche Stellungnahme zu Krankheitsbild und Therapieverlauf und zum sozialen Verhalten des Petenten abgegeben hatte.

Das Krankenhaus verwies auf eine vom Petenten unterschriebene Schweigepflichtsentbindung und erläuterte, dass die außerordentlich umfassende Darstellung des komplexen Krankheitsbildes erforderlich war, um das Verhalten des Petenten für den Nichtmediziner begreiflich zu machen.
Parallel laufend wurde gerichtlich festgestellt, dass die Übersendung der Stellungnahme rechtswidrig war. Das Gericht begründete den Beschluss damit, dass eine Entbindungserklärung keinen Verzicht auf die Geheimhaltung sensibler Daten in toto bedeutet, sondern nur in Bezug auf den jeweiligen Verfahrensgegenstand, dessen Umfang im Einzelfall ggf. auch durch Auslegung zu bestimmen ist. Die Angabe zu Vorgängen, die nicht mit den o.g. Anschuldigungen in Verbindung stehen, gehen über die Entbindung von der Schweigepflicht hinaus.
Der Begründung des Gerichts schließt sich der Landesbeauftragte vollumfänglich an. Eine Entbindung von der Schweigepflicht kann nicht zur Folge haben, dass sämtliche Gesundheitsdaten übermittelt werden. Vielmehr ist im Sinne der Erforderlichkeit und Verhältnismäßigkeit im Einzelfall abzuwägen, welche Daten direkt mit dem Vorgang in Verbindung stehen. In diesem Rahmen ist eine Datenübermittlung an die Polizei zulässig.
Die Klinikleitung hat erklärt, dies zukünftig zu berücksichtigen.

11. Gewerbe und Wirtschaft

11.1 Die Handwerksrolle

Anlässlich einer bereits im vergangenen Berichtszeitraum begonnenen Kontrolle einer Handwerkskammer wurde dem Landesbeauftragten auch der „Antrag auf die Eintragung in die Handwerksrolle, das Verzeichnis der handwerkähnlichen Gewerbe bzw. zulassungsfreien Handwerke“ (Handwerksrolle) vorgelegt. Ein Vergleich der mit diesem Antrag erhobenen Datenarten mit denen, die gemäß Anlage D der Handwerksordnung (HandwO) in die Handwerksrolle aufzunehmen sind, ergab eine überschießende Datenerhebung. Der Antrag sah die Erhebung von Geburtsort und Wohnanschrift des Inhabers, der persönlich haftenden Gesellschafter einer Personengesellschaft oder der Geschäftsführer einer juristischen Person oder des fachlichen Betriebsleiters, falls dieser nicht gleichzeitig Geschäftsführer ist, vor.
Die Handwerkskammer, mit der Unzulässigkeit dieses Tuns konfrontiert, ließ sich zwar dazu bewegen, auf die Erhebung des Geburtsortes o.g. Personenkreises zum Zweck der Eintragung in die Handwerksrolle fortan zu verzichten, die Wohnanschrift sei jedoch erforderlich. Aus der Praxis sei z.B. gefordert worden, dass doch Betriebsleiter mittels ihrer Wohnadresse über die Löschung ihres Handwerksbetriebes aus der Handwerksrolle informiert werden müssten.
Auf eine solche Diskussion ließ sich der Landesbeauftragte nicht ein. In der Anlage D zur HandwO, die die Art der personenbezogenen Daten in der Handwerksrolle festlegt, heißt es: „In der Handwerksrolle dürfen folgende Daten gespeichert werden:“. Der Bundesgesetzgeber hat mit dieser Formulierung und der folgenden abschließenden Aufzählung seiner Absicht Ausdruck verliehen, dass die Aufzählung eben gerade nicht nach Belieben der mit der Gesetzesausführung befassten Kammern erweitert werden kann, wenn dies nützlich oder für die Erledigung irgendeiner Aufgabe geeignet erscheint. Damit bestände auch für die ergänzende Anwendung des DSG-LSA, im Besonderen § 4 Abs. 1 (Einwilligungsklausel) oder § 9 Abs. 1 (Erforderlichkeitsgrundsatz der Datenerhebung), keinerlei Raum, denn „soweit andere Rechtsvorschriften“ - und sei es eine ihrer Anlagen - „auf personenbezogene Daten anwendbar sind, gehen sie den Vorschriften dieses Gesetzes (des DSG-LSA) vor“ (§ 3 Abs. 3 DSG-LSA).

Der Landesbeauftragte konnte der Kammer jedoch eine Lösung anbieten. Der Handwerkskammer stehen nämlich die Datenarten Geburtsort und Wohnanschrift zur Erfüllung ihrer Aufgaben nach § 91 HandwO aus den ihnen nach § 14 Abs. 5 Ziff. 2 GewO zu übermittelnden Daten schon zur Verfügung. Zu den an die Kammern von den zur Entgegennahme der Gewerbeanzeigen zuständigen Stellen zu übermittelnden Daten aus den Gewerbeanzeigen (Anlagen 1 bis 3 zu § 14 Abs. 4 GewO) zählen diese Angaben der Betroffenen bereits. Die genannten Datenarten dürfen nicht in der Handwerksrolle gespeichert werden, wohl aber, auch automatisiert, als Teil der zur Mitgliederbetreuung geführten Sachakten, die der Erfüllung der Kammeraufgaben dienen.

Der Landesbeauftragte drückte der Kammer gegenüber seine Erwartung aus, dass diese durch Veranlassen geeigneter und nachprüfbarer Maßnahmen dafür Sorge trägt, dass die Mitarbeiter der Kammer nur auf die zur jeweiligen Aufga-

benerfüllung erforderlichen Datenarten Zugriff haben, beispielsweise ausschließlich die mit der Führung der Handwerksrolle befassten Mitarbeiter auf die in Anlage D der HandwO genannten Daten der Handwerksrolle. Auf technische und organisatorische Maßnahmen zur Revisionsfähigkeit und auf die Transparenz des Verfahrens muss besonderer Augenmerk gelegt werden.
Die Kammer änderte inzwischen auch ihr Antragsformular. Damit entsteht nicht mehr der Eindruck, die Daten würden unzulässig in der Handwerksrolle gespeichert.

11.2 Inkasso von Handwerkskammerbeiträgen

Der Landesbeauftragte wurde vom zuständigen Ministerium zu der Absicht einer Handwerkskammer befragt, die die Beitreibung der ausstehenden Mitgliedsbeiträge im Vorfeld der Vollstreckung an ein Inkassobüro abgeben wollte.

Die Beauftragung eines privaten Inkassounternehmens mit der Beitreibung von Beitragsforderungen einer Handwerkskammer war aus datenschutzrechtlicher Sicht zwar nicht grundsätzlich ausgeschlossen, begegnete aber einigen Vorbehalten.

Nach § 113 Abs. 3 HandwO sind grundsätzlich die Gemeinden für Einziehung und Beitreibung der Beiträge zuständig. Die grundsätzliche Zulässigkeit der Übertragung von Inkassogeschäften ergibt sich, speziell für die Gemeinden, aus § 107 GO LSA. Eine entsprechende Regelung für die Handwerkskammern fehlt. Die auf der Grundlage von § 113 Abs. 3 S. 3 HandwO erlassene Verordnung über die Einziehung von Beiträgen zur Handwerkskammer berechtigte die dort genannten Kammern lediglich zur Beitreibung in eigener Zuständigkeit.

Die Beitreibung öffentlich-rechtlicher Forderungen betrifft in der Regel sensible personenbezogene Informationen. Zwar waren im vorliegenden Fall spezifische Geheimnisse, die einer Beauftragung ggf. hätten entgegen stehen können, wie etwa das Steuergeheimnis oder das Sozialgeheimnis, nicht betroffen. Zu berücksichtigen war aber die Regelung des § 1 Abs. 1 VwVfG LSA i.V.m. § 30 VwVfG, die den Anspruch formuliert, Betriebs- und Geschäftsgeheimnisse und damit auch Informationen über die wirtschaftlichen Verhältnisse des Betriebsinhabers nicht unbefugt zu offenbaren.

Nach § 4 Abs. 1 DSG-LSA bedarf die Handwerkskammer als öffentliche Stelle im Sinne des § 3 Abs. 1 DSG-LSA für die Übermittlung personenbezogener Informationen zum Beitragspflichtigen (Beitragsbescheid) an ein externes Inkassounternehmen als Dritten einer rechtlichen Grundlage.

Die Vorschriften über die Datenverarbeitung im Auftrag nach § 8 DSG-LSA waren nicht einschlägig. Der dem Vorhaben beigefügte Vertragsentwurf beschrieb den Leistungsumfang. Danach wurde deutlich, dass ein umfängliches eigenverantwortliches Handeln des Inkassounternehmens insbesondere mit der Freiheit der Maßnahmenwahl (u.a. aktives und passives telefonisches Inkasso, Adressermittlung, Bonitätsprüfung, Abschluss von Ratenzahlungen usw.) vorgesehen

war. Daher war letztlich von einer Übertragung der Beitreibungsfunktion und nicht von einer reinen Hilfstätigkeit auszugehen.

Als Rechtsgrundlage für die Datenübermittlung kam § 12 Abs. 1 Nr. 1 DSG-LSA in Betracht. Fraglich erschien dabei, ob diese Übermittlung an ein Inkassobüro letztendlich als zur Aufgabenerfüllung erforderlich betrachtet werden kann. Die Handwerkskammer hatte als öffentliche Stelle den verfassungsmäßigen Grundsatz der Verhältnismäßigkeit zu berücksichtigen.

Zunächst war einerseits ein erhebliches öffentliches Interesse an der rechtzeitigen und möglichst vollständigen Beitreibung öffentlicher Forderungen gegeben. Es besteht ein erhebliches Allgemeininteresse an der vollständigen Beitragszahlung zur finanziellen Sicherung der Erledigung öffentlicher Aufgaben.

Andererseits waren die Interessen der Betroffenen an der Geheimhaltung zu berücksichtigen. Oftmals sind sensible personenbezogene Informationen betroffen. Zu berücksichtigen wäre wohl auch, dass gerade Handwerksbetriebe gelegentlich unverschuldet in eine finanziell komplizierte Situation gelangt sind.

Besonders problematisch erschien die Übermittlung solch sensibler Daten zur Finanzlage gerade an Inkassounternehmen, die ggf. gleichzeitig Auskunfteien betreiben oder ggf. bundesweit mit anderen entsprechenden Unternehmen verbunden sind. Die informationstechnologische Vernetzung und evtl. Zugriffsregelungen hätten einer besonderen Beobachtung bedurft. In diesen Punkten wäre das Gebot der Zweckbindung der Daten lediglich für den konkreten Inkassoauftrag besonders zu beachten und umzusetzen gewesen.

Die Erforderlichkeit im engeren Sinne erforderte zudem, dass es der Handwerkskammer ohne die Einschaltung eines Inkassobüros nicht oder nur unter unverhältnismäßig großen Schwierigkeiten möglich wäre, die Aufgabe der Beitragseinziehung zu erledigen. Dabei war zunächst zu berücksichtigen, dass die Beitreibung grundsätzlich durch die Gemeinden nach den landesrechtlichen Vorschriften weiterhin möglich war. Die Gemeinden haben als Vollstreckungsbehörden (§ 6 VwVG LSA) die Befugnis, die Leistungsbescheide der Handwerkskammern als der Aufsicht des Landes unterstehende Körperschaften öffentlichen Rechts (§ 1 VwVG LSA) mit den Zwangsmitteln des Vollstreckungsrechts (§§ 27 ff VwVG LSA) zu vollstrecken. Die Möglichkeiten gingen also erheblich weiter als bei Inkassobüros als privatrechtlichen Einrichtungen, denen keine eigenständige Vollstreckungskompetenz zukommt. Die Erforderlichkeit der Einschaltung eines Inkassobüros im außergerichtlichen Bereich und jenseits des Vollstreckungsrechts hätte einer differenzierten Begründung bedurft.

Die Effizienz der Einschaltung eines Inkassounternehmens wäre darzulegen gewesen. Zunächst wäre eine befristete Regelung vorzuziehen, die nach einem angemessenen Zeitraum eine Evaluierung der Effizienz der Beauftragung des Inkassounternehmens ermöglicht.

Nach bisheriger Erkenntnis ist das Verfahren nicht weiter verfolgt worden, da zunächst nach einer kammerübergreifenden Lösung gesucht wurde.

12. Hinweise zum technischen und organisatorischen Datenschutz

12.1 Auftragsdatenverarbeitung - mit bekannten Problemen

Im Rahmen seiner planmäßigen Kontrollen bei öffentlichen Stellen des Landes Sachsen-Anhalt hat der Landesbeauftragte Ende des Jahres 2006 im Bereich der Justiz die Überprüfung der Auftragsdatenverarbeitung in einer zentralen Servicestelle zur Betreuung der Informationstechnik vorgenommen.
Zuvor hatte sich der Landesbeauftragte, wie üblich, wenn „Neuland“ in einem Prüfbereich betreten wird, im Rahmen eines Informationsgespräches über die Aufgaben dieser zentralen Servicestelle informiert. In diesem Zusammenhang war für den Landesbeauftragten von besonderem Interesse, dass diese Stelle für den gesamten Justizbereich die Entsorgung von Personalcomputern vornahm und die Vernichtung der Festplatten dieser Personalcomputer einem privaten Unternehmen in einem anderen Bundesland übertragen hatte.

Die allerdings bei der Kontrolle vorgefundene Ablauforganisation bei der Entgegennahme und Lagerung dieser auszusondernden Computertechnik und die Vertragsgestaltung gaben dem Landesbeauftragten doch Anlass zur Kritik.
Zur Kontrolle selbst konnte ein schriftlicher Vertrag mit dem Unternehmen nicht vorgelegt werden. Eine Kontrolle des Auftraggebers beim Auftragnehmer zur Überprüfung dessen Eignung, insbesondere im Hinblick auf die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen, war nicht erfolgt und eine Unterrichtung des Landesbeauftragten für den Datenschutz über die Auftragsdatenverarbeitung lag ebenfalls nicht vor.
Nur die umgehende Erfüllung der im Prüfbericht des Landesbeauftragten festgelegten, auch zeitlichen, Auflagen bewahrte diese öffentliche Stelle vor einer formellen Beanstandung gem. § 24 Abs. 1 DSG-LSA.

Eigentlich sollten die gesetzlichen Regelungen zur Auftragsdatenverarbeitung (§ 8 DSG-LSA) und die damit verbundenen Verpflichtungen für eine öffentliche Stelle mittlerweile ausreichend bekannt sein, denn in fast allen bisherigen Tätigkeitsberichten wurde auf die Problematik der Auftragsdatenverarbeitung eingegangen. Bereits in seinem II. Tätigkeitsbericht 1995, Ziff. 13.2, also vor fast 12 Jahren, hat der Landesbeauftragte ausführlich hierzu berichtet!

Trotzdem nochmals die nachfolgenden Hinweise zu den Pflichten des öffentlichen Auftraggebers bei der Beauftragung eines privaten (nicht öffentlichen) Auftragnehmers:
Bei der Datenverarbeitung im Auftrag bleibt der Auftraggeber die rechtlich verantwortliche Stelle (§ 8 Abs. 1 Satz 1 DSG-LSA). Der Auftrag ist gem. § 8 Abs. 2 Satz 2 DSG-LSA schriftlich zu erteilen. Gemäß § 8 Abs. 2 Satz 4 DSG-LSA hat sich der Auftraggeber von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Diese Maßnah-

men müssen den für den Auftraggeber geltenden Bestimmungen des § 6 DSG-LSA entsprechen.
Bei einem privaten (nicht öffentlichen) Auftragnehmer, auf den die Vorschriften des DSG-LSA nicht anwendbar sind, ist gem. § 8 Abs. 6 DSG-LSA vertraglich sicherzustellen, dass dieser die Bestimmungen des DSG-LSA befolgt und sich der Kontrolle (§§ 22 bis 24 DSG-LSA) durch den Landesbeauftragten für den Datenschutz unterwirft. Der Landesbeauftragte ist über die Beauftragung zu unterrichten.
Der § 8 Abs. 7 des DSG-LSA berücksichtigt noch den Sonderfall der Wartung von Datenverarbeitungsanlagen oder -verfahren durch Dritte. Er ist durch Art. 1 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 21. August 2001 (GVBl. LSA S. 348) in § 8 eingefügt worden.

Der Landesbeauftragte fordert die öffentlichen Stellen, insbesondere aber die Beauftragten für den Datenschutz in den Landesbehörden und auch im kommunalen Bereich auf, in ihrem Verantwortungsbereich zu prüfen, ob eine Auftragsdatenverarbeitung durch private Dritte erfolgt, inwieweit bei vorliegenden Verträgen die Bestimmungen des § 8 DSG-LSA berücksichtigt sind und ob eine Unterrichtung des Landesbeauftragten erfolgt ist. Denn auch die beim Landesbeauftragten geführte Übersicht zu Unterrichtungen über eine Auftragsverarbeitung enthält in den letzten zwei Jahren Eingänge im einstelligen Bereich.

12.2 Festplattenlöschung - aber sicher!

Eine untere Landesbehörde hatte sich als Ersatz für die völlig veraltete Technik mehrere neue Computer zugelegt. Um die Kosten der Entsorgung der ausgesonderten Computer zu minimieren, vielleicht sogar Gewinn aus der Entsorgung zu schlagen und der interessierten Belegschaft etwas zu gönnen, war von der übergeordneten Behörde die Erlaubnis eingeholt worden, diese alten Computer an die Mitarbeiterinnen und Mitarbeiter verkaufen zu dürfen. Um die Geheimhaltung der auf den Festplatten der Computer gespeicherten sensiblen personenbezogenen Daten zu gewährleisten, war Teil der Verwertungserlaubnis eine sog. Löschdiskette, mit der die Festplatten vor der Abgabe noch zu löschen seien.
Tatsächlich, und das ergab später eine Kontrolle durch den Landesbeauftragten, war auf dieser Diskette, die ursprünglich vom BSI stammte, aber von der Aufsichtsbehörde nachträglich nutzerfreundlicher gemacht wurde, ein selbst für die Löschung von Verschlusssachendaten geeignetes Programm, nämlich VS-Clean des BSI.

Um zu verstehen, was dieses spezielle Datenlöschprogramm von anderen Löschprogrammen bzw. -funktionen, z.B. aus der Bordmittel-Toolbox des Betriebssystems unterscheidet, muss man folgendes wissen:
Während das „Löschen“ einer Computerdatei mit der Entf-Taste, die diese Datei lediglich in den Papierkorb befördert, mit dem Versuch zu vergleichen ist, eine aufgeschriebene Information zu vergessen, wirken das Formatieren der ganzen Festplatte oder das Löschen der Festplattenpartitionen nicht wirklich anders. Deren Wirkung ist mit dem Durchstreichen oder bestenfalls dem Herausreißen des Inhaltsverzeichnisses eines Geheimdossier vergleichbar, um es unlesbar zu machen - also auch nicht viel besser!

Niemand erwartet doch, ernstgenommen zu werden, wenn er behauptet, der Inhalt eines solchen Dokuments wäre nur deshalb nicht mehr lesbar, weil das Inhaltsverzeichnis fehlt. Der einzige Weg, die Daten eines magnetischen Datenträgers, wie einer Festplatte, aber auch eines USB-Speichers oder eines wiederbeschreibbaren optischen Datenträgers, gründlich und unumkehrbar zu löschen, ist das Überschreiben **aller** Daten. Und genau das leistet z.B. das BSI-Tool VS-Clean. Es überschreibt jeden einzelnen Datensektor der Festplatte mehrmals mit uncharakteristischen, also zufälligen Zahlenmustern oder alternierend mit Nullen und Einsen und kontrolliert nach jedem Schreibvorgang den Erfolg.

Jedoch stößt man bei der Benutzung solcher Überschreibprogramme auf ein Problem in Form einer physikalischen Beschränkung. Um eine Festplatte von mehreren Gigabyte Größe komplett zu überschreiben, benötigt eine solche Software mehrere Stunden. Bei einer einzelnen zu löschenden Festplatte ist das über Nacht erledigt, nicht so im Fall der kontrollierten Behörde, die mehrere Dutzend PC ausgesondert hatte und diese, so war ihr aufgegeben worden, in ganz kurzer Zeit zu verwerten hatte. Ihr war daher von der übergeordneten Stelle geraten worden, das für solche Fälle sich auf der Löschdiskette ebenfalls befindliche schnelle Löschprogramm zu verwenden. Und dieses Programm löschte eben nur die Festplattenpartition, eigentlich die Partitionstabelle, also das Inhaltsverzeichnis - und das ging ruck, zuck! Leider jedoch nicht datenschutzgerecht, denn es gibt im Internet kostenlose Datenrettungsprogramme, die - ebenso ruck, zuck! - versehentlich oder bewusst gelöschte Partitionstabellen wieder herstellen können. Das hatte einer der Computererwerber getan und angesichts einer schier unglaublichen Fülle nun sichtbarer personenbezogener Daten aus der ursprünglichen Behörde den Landesbeauftragten durch Zusendung der Festplatte verständigt. Dieser hat das Verfahren gegenüber den beteiligten Behörden gerügt.

Dem vorgefundenen Datenschutzproblem rechnet der Landesbeauftragte mehrere Ursachen zu. Zunächst war festzustellen, dass durch das Hinzufügen einer Wahlmöglichkeit zwischen einem vermeintlich besonders nutzerfreundlichen Schnell-Lösch-Tool und der langsamen, jedoch sicheren BSI-Software ein eigentlich zuverlässig wirkendes Datenlöschwerkzeug unsicher wurde. Außerdem wäre zu erwarten gewesen, dass sich der für die restlose Datenlöschung verantwortliche Mitarbeiter der vom Landesbeauftragten kontrollierten Behörde selbständig Informationen verschafft, welches der zur Wahl stehenden Löschprogramme wie wirkt und wie sicher diese Wirkung ist.
Alle erforderlichen Angaben und die Software zum Ausprobieren der entsprechenden Wirkungen wären dem Internet entnehmbar gewesen. Im Web-Angebot des Landesbeauftragten ist z.B. in der Rubrik Service-Orientierungshilfen eine Orientierungshilfe des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum „Sicheren Löschen magnetischer Datenträger“ enthalten, die Grundlagen, Werkzeuge und Empfehlungen aus Sicht des Datenschutzes ausführlich beschreibt. Der Landesbeauftragte rät allen öffentlichen Stellen, sich deren Inhalt vor der Herausgabe magnetischer Datenträger zu eigen zu machen und strikt zu beachten.

12.3 Computerkriminalität

Die Computerkriminalität ist eine Kriminalitätsform, deren Erscheinungsbild in den zurückliegenden Jahren einem erheblichen Wandel unterworfen war. Wer glaubt, Ziele und Opfer von Angriffen auf Computersysteme und die darin gespeicherten Daten seien stets „die anderen“, z.B. die Global Player an den internationalen Wirtschaftsmärkten oder öffentliche Stellen, bei denen ganz besonders interessante personenbezogene Daten gespeichert werden, der irrt gefährlich. Das gilt auch für die öffentlichen Stellen des Landes Sachsen-Anhalt.
Während im Jahr 1996 laut polizeilicher Kriminalitätsstatistik in 930 Fällen öffentliche Stellen des Landes Sachsen-Anhalt von der trivialsten Form der Computerkriminalität betroffen waren, nämlich dem Computerdiebstahl, ist diese Zahl seitdem zwar ständig rückgängig. Gleichwohl darf sich kein Nutzer eines vernetzten PC in Sicherheit wähnen. Moderne Angriffe auf Computernetze und die gespeicherten personenbezogenen Daten werden mit der Maus ausgeübt, weniger mit der Brechstange. Der Direktor des Landeskriminalamtes formulierte im Juli 2006 treffend: „Der Computer ist das Tatmittel der Zukunft.“. Und die Täter sitzen nicht unbedingt nur in Deutschland.

Die polizeiliche Kriminalitätsstatistik weist für das Jahr 2005 beispielsweise allein in Sachsen-Anhalt über 1.500 Fälle von Computerkriminalität aus. Unter den ca. 1.700 dabei Geschädigten waren neben 367 Firmen auch 13 öffentliche Stellen, möglicherweise zuzüglich einer hohen Dunkelziffer.

Eine der Kriminalitätsformen mit zunehmender Tendenz ist das sog. „Pishing“, das Fischen nach Bankzugangsdaten. Die Nutzer werden dabei mit Links in E-Mails mit gefälschten Absendern auf nachgemachte Bankportale geleitet und zur Eingabe ihrer Zugangsdaten nebst TAN „zur Sicherheitsüberprüfung“ überredet. Ehe dem hereingelegten Nutzer überhaupt klar wird, was passiert ist, befindet sich der Inhalt seines Online-Banking-Kontos bereits auf der anderen Seite des Globus. Seit einiger Zeit haben viele Banken ihr Online-Angebot so umgestellt, dass für eine Transaktion eine ganz bestimmte TAN verlangt wird. Außerdem hat sich inzwischen herumgesprochen, dass Banken niemals E-Mails versenden, in denen zur Eingabe von Zugangsdaten aufgefordert wird.

Doch auch die Kriminellen haben aufgerüstet. Als wichtigster im Berichtszeitraum zu verzeichnender Trend in Sachen Computerkriminalität hat eine renommierte Computerzeitschrift (c’t 2007, Heft 2) die Professionalisierung der Angreifer ausgemacht. Während noch vor wenigen Jahren eine in Microsoft Windows gefundene Sicherheitslücke durch den Wurm Sasser verwendet worden sei, der nichts weiter tat, als sich zu vermehren - und als besonders unprofessioneller Nebeneffekt die betroffenen Rechner herunterfuhr -, so sehe die Verwertung eines solchen Fundes heute so aus: Die gefundene Sicherheitslücke wird in Untergrundauktionen versteigert, dann für gezielte Spionage eingesetzt und schließlich für den Aufbau von Bot-Netzen verwendet. Es sei eine regelrechte Industrie entstanden, die von Datenspionage, Spam-Versand und selbst Lahmlegen von Webservern lebe. Und die Helfershelfer bei diesen Machenschaften sind harmlos aussehende PC in deutschen Wohnungen, selbst im ITN-LSA hält der Landesbeauftragte solches für möglich, wenn selbst die NASA schon betroffen gewesen sein

soll. Das Problem sitzt, so hatte der Landesbeauftragte bei Kontrollen im Land oder bei Informationsgesprächen mehrmals feststellen müssen, nämlich häufig vor dem Monitor. Getrieben von Neugier und Unwissenheit werden hemmungslos Dateianhänge (Attachments) von E-Mails der sonderbarsten Absender mit den merkwürdigsten Betreffs angeklickt, denn in der E-Mail, und sei sie noch so unerwartet im Posteingang aufgetaucht, heißt es doch: „Klicken Sie hier und Sie werden sehen!“. Man sieht dann zwar doch nichts, aber das Unheil nimmt seinen Lauf. Das Attachment war beispielsweise eher nicht von der Telekom, die auf eine besonders hohe Rechnung hinweisen wollte, sondern von Angreifern. Kaum ausgeführt, installiert das Attachment unter Ausnutzung einer bisher ungepatchten Sicherheitslücke eine Hintertür, durch die später ein Angreifer den PC und womöglich das ganze angeschlossene Netz übernehmen kann, oder einen Bot-Net-Client.

Dieser, zuweilen durch Rootkit-Techniken getarnt, kann lange Zeit unbemerkt im PC sein Unwesen treiben. Gelegentlich nimmt er Kontakt mit einem Bot-Master auf, von dem er Arbeitsaufträge erhält, z.B. das Generieren von Spam oder das Mitwirken an DoS-Attacken gegen Server. Spätestens an dieser Stelle kommt der Schutz personenbezogener Daten ins Spiel. Wenn nämlich unter der Last hunderter, tausender oder gar zigtausender Bots Informationssysteme, z.B. Web- oder Mailserver, an den Rand ihrer Leistungsfähigkeit gelangen oder gar völlig ausfallen, ist § 6 Abs. 2 Ziff. 3 DSG-LSA tangiert. Die auf diesen Systemen gespeicherten personenbezogenen Daten stehen dann nicht mehr, nicht mehr vollständig oder nicht mehr aktuell zur Verfügung, die Verfügbarkeit der Daten ist massiv beeinträchtigt.

Bei seinen Kontrollen und Beratungen achtet der Landesbeauftragte stets auch darauf, dass auf den verwendeten PC die Betriebssysteme aktuell gepatcht sind, wirksame Schutzsoftware gegen Computerviren und geeignete Tools zum Auffinden und Bekämpfen von Rootkits vorhanden sind. Die wichtigste Waffe gegen Schadsoftware sind jedoch gesundes Misstrauen und bei regelmäßigen Fortbildungsveranstaltungen erworbenes Wissen um die Gefahren bei der Internetnutzung.

Unterstützung kommt dabei möglicherweise demnächst von Seiten des Bundesgesetzgebers. Das Bundeskabinett hatte am 20. September 2006 den Regierungsentwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität beschlossen, der hauptsächlich das StGB ändern und mit dem die Umsetzung der auch von Deutschland ratifizierten „Convention of Cybercrime“ erreicht werden soll. Dieser Gesetzentwurf, der inzwischen als BT-Drs. 16/3656 parlamentarisch beraten wird, sieht z.B. vor, dass der unbefugte Zugang zu besonders gesicherten Daten unter Überwindung von Sicherheitsvorkehrungen unter Strafe gestellt wird. Der Straftatbestand der Computersabotage, bisher nur gegen Betriebe und Behörden anwendbar, soll auch auf Private ausgedehnt werden. „DoS-Attacken“ sollen ebenso unter Strafe gestellt werden wie gefährliche Vorbereitungshandlungen, wie das Herstellen, Überlassen, Verbreiten oder sich oder anderen Verschaffen von als „Hacker-Tools“ bezeichneter Software. Dabei wird der Bundesgesetzgeber auch einer Bitte des Bundesrates in seiner Stellungnah-

me zum Gesetzentwurf nachzukommen haben, Tools zur Sicherheitsüberprüfung von IT-Systemen vor einer ungewollten Kriminalisierung zu schützen.
Allerdings werden diese Sanktionen nur bei Straftaten greifen, deren Begehungsort im Geltungsbereich des Grundgesetzes liegt, was im Internet eine erhebliche Einschränkung darstellen wird.

12.4 Schutzprofil für den datenschutzgerechten Einsatz von Videoüberwachungssystemen

Angesichts der zunehmenden Videoüberwachung, auch durch öffentliche Stellen des Landes, insbesondere im kommunalen Bereich und im Bereich der Polizei zur Gefahrenabwehr, stellt sich die Frage, wie dabei der Datenschutz gewahrt werden kann, immer stärker.
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat auf der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. März 2007 in Erfurt hierzu berichtet.
Das vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Auftrag gegebene Schutzprofil entstand mit Hilfe des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), das diesen Katalog mit dem Titel „Software zur Verarbeitung von Bilddaten“ mit dem Report BSI-PP-0023-2007 zertifiziert hat.
Schutzprofile stehen in engem Zusammenhang mit den Common Criteria - CC - (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik; Version 2.1, August 1999).
Die auf den CC basierenden „Schutzprofile (Protection Profile - PP) für Software zur Verarbeitung von personenbezogenen Bilddaten“ vom 15. Januar 2007 beschreiben die Mindestanforderungen, welche die Software zur Verarbeitung personenbezogener Bilddaten erfüllen muss.

Dieses Schutzprofil definiert technische Anforderungen, die von den Videosystemen erfüllt sein müssen, damit sie gemäß den Bestimmungen der Datenschutzgesetze des Bundes und der Länder eingesetzt werden können. Das Schutzprofil entbindet die öffentlichen Stellen des Landes allerdings nicht davon, den Einsatzbereich der Videoüberwachung entsprechend den gesetzlichen Vorgaben vorzunehmen bzw. zu begrenzen.

Es ermöglicht ihnen jedoch, die Einhaltung dieser Vorgaben technisch zu realisieren und zu kontrollieren. Dazu fordert der Landesbeauftragte auf. Bei Ausschreibungen für Videoüberwachungstechnik (einschließlich Betriebs- und Auswertungssoftware) sollte dieses Schutzprofil durch die öffentlichen Stellen zugrunde gelegt werden.
Abrufbar ist dieses Schutzprofil auch auf der Homepage des Landesbeauftragten.

12.5 E-Mail-Verteiler

Pressemitteilungen einer obersten Landesbehörde enthielten häufig „als Vorspann“ E-Mail-Verteilerlisten. Auf diesen Verteilerlisten waren für jeden Empfänger die jeweils anderen Empfänger mit Mail-Adresse und teilweise mit fachlicher Zuordnung erkennbar.

Es lagen bereits einige Eingaben von Journalisten vor, die dieses Verfahren der Listenübermittlung beklagten. Zudem hatte der Landesbeauftragte die Behörde zuvor bereits fernmündlich auf die Problematik aufmerksam gemacht. Er bat erneut, künftig auf die Übermittlung der Verteilerlisten zu verzichten.
Die oberste Landesbehörde teilte mit, dass es sich um Versehen gehandelt habe und künftig das empfohlene Verfahren eingehalten werde. Nur wenige Wochen später erhielt der Landesbeauftragte erneut Pressemitteilungen der Behörde mit mehrseitigen Verteilerlisten. Es war daher ein nachdrückliches Aufgreifen der Angelegenheit durch den Landesbeauftragten geboten.

Es ist nicht zu verkennen, dass eine E-Mail-Adresse regelmäßig dazu dient, in gesellschaftliche bzw. berufliche Kommunikation zu treten. Allerdings ist die Erforderlichkeit der Übermittlung der in der Verteilerliste enthaltenen personenbezogenen Informationen einschließlich der Information, überhaupt auf der Verteilerliste der Behörde verzeichnet zu sein, äußerst fraglich. Diese Verarbeitung widerspricht dem für alles Verwaltungshandeln maßgeblichen Grundsatz der Datensparsamkeit (§ 2 Abs. 2 Satz 1 DSG-LSA). Eine Rechtsgrundlage für die Übermittlung ist nicht ersichtlich.

Auch technische Zwänge sind nicht bestimmend. Vielmehr ist es technisch schon beim E-Mail-Versenden ohne Weiteres möglich, beim Empfänger nur jeweils seine eigene E-Mail-Adresse erscheinen zu lassen .
Bei allen gängigen E-Mail-Programmen gibt es drei mögliche Felder, um einen Adressaten einzutragen:

„**to**“ (an) ist für den Hauptempfänger bestimmt, d.h. Empfänger im offenen Versand.
„**cc**“ ist die Abkürzung für „carbon copy" und steht für den aus dem „guten alten Büro“ mit Schreibmaschinenausstattung übernommenen Begriff „Durchschlag“ (mit Kohlepapier), d.h. weitere Empfänger im offenen Versand.
„**bcc**" ist die Abkürzung von „**blind carbon copy“** und kann mit **Blindkopie** oder verdeckte/unsichtbare Kopie übersetzt werden, d.h. Empfänger im verdeckten Versand (Blindkopie).

Dieses am wenigsten geläufige, weil in einigen E-Mail-Programmen nicht automatisch angezeigte, aber wichtige 3. Adressaten-Feld kann die oben beschriebenen Probleme mit „ellenlangen“ Verteilerlisten lösen. Bei Adressierung in bcc bleiben darunter eingetragene Empfänger für sämtliche weitere Empfänger **unsichtbar**.

Der Datenschutz kann auch schon beim Versenden von E-Mails sehr einfach beachtet werden, wenn man damit beginnt, das richtige, nämlich das bcc-Adressatenfeld des E-Mail-Programms zu nutzen. Nützlicher Nebeneffekt ist die Papierersparnis beim häufig noch anzutreffenden Ausdruck von E-Mails.

13. Hochschulen

13.1 Hochschulmedizingesetz

Mit dem Hochschulmedizingesetz des Landes Sachsen-Anhalt vom 12. August 2005 (HMG-LSA, GVBl. LSA S. 508) wurden die Universitätsklinika als rechtsfähige Anstalten errichtet. Durch die Verbesserung der Rahmenbedingungen für eine effizientere Wirtschafts- und Betriebsführung sollte den steigenden Anforderungen hinsichtlich der Finanzierung von Forschung und Lehre sowie der Einbindung in die regionale Krankenversorgung Rechnung getragen werden.

Bezüglich des Personals, das im Aufgabenspektrum der Medizinischen Fakultäten und der Klinika tätig wird, wurden der Rechtsformänderung entsprechende differenzierte Regelungen getroffen. Das wissenschaftliche und sonstige Personal der Medizinischen Fakultäten wird demnach bei der Hochschule beschäftigt mit der Maßgabe, ggf. auch in der Krankenversorgung tätig sein zu müssen (§ 6 HMG-LSA). Ein Teil der ärztlichen Beschäftigten sowie die sonstigen Beschäftigten wurden den Klinika zugewiesen (§ 20 HMG-LSA).

In der Vorbereitung der Umsetzung des HMG-LSA wurden die personalwirtschaftlichen Konsequenzen deutlich. Die Beibehaltung der Personalverwaltung, die bisher für Klinikum und Medizinische Fakultät durch das Klinikum wahrgenommen wurde, erschien einigen Beteiligten sinnvoll. Dem standen jedoch datenschutzrechtliche Bedenken entgegen.

Dies konnte der in der Vorbereitungsphase beteiligte Landesbeauftragte bestätigen. Er wies auf die vielfältigen, zum Teil deutlichen Hinweise im HMG-LSA auf eine getrennte Zuständigkeit hin. Im Ergebnis bewirkt das HMG-LSA eine Zuweisung des bisherigen Personals an zwei Dienstherrn. Die Verwaltung des der Hochschule zugewiesenen Personals durch das Klinikum hätte daher eine Übermittlung von Personalakten an einen anderen Dienstherrn erforderlich gemacht. Diese Übermittlung von Personalaktendaten hätte einen Eingriff in das Grundrecht der Beschäftigten auf informationelle Selbstbestimmung bewirkt, so dass hierfür eine Rechtsgrundlage erforderlich gewesen wäre.

Die Einwilligung der Betroffenen als Grundlage wäre wenig praktikabel gewesen. Eine gesetzliche Grundlage war nicht gegeben. Nach den §§ 28 Abs. 1 DSG-LSA i.V.m. 90 g) Abs. 1, 90 d) BG LSA ist die Übermittlung an einen anderen Dienstherrn nicht zulässig. Hierauf hat der Landesbeauftragte unter Bezugnahme auf einschlägige obergerichtliche Rechtsprechung hingewiesen. Auch die Regelung des § 19 Abs. 1 S. 3 Nr. 5 HMG-LSA, die auf die „Verwaltung“ für die Medizinische Fakultät durch das Klinikum hinweist, erfüllte nicht die verfassungsrechtlichen Anforderungen an eine normenklare Eingriffsgrundlage.

Entsprechend den Beratungen des Landesbeauftragten haben die Beteiligten Verfahren gefunden, die eine datenschutzkonforme Personaldatenverarbeitung durch Mitarbeiter des jeweiligen Dienstherrn gewährleisten.
Offenbar soll nunmehr, nach beratender Beteiligung des Landesbeauftragten, eine Änderung der einschlägigen Regelungen auf den parlamentarischen Weg ge-

bracht werden. Eine normenklare Bestimmung soll Grundlage der Personaldatenverarbeitung durch die Klinika für die Medizinischen Fakultäten werden.

14. Kommunalverwaltung

14.1 Ratsinformationssystem

Über Ratsinformationssysteme hat der Landesbeauftragte erst im letzten Tätigkeitsbericht ausführlich informiert (VII. Tätigkeitsbericht, Ziff. 14.1).
Wie man es nicht machen darf, zeigt das Beispiel einer Stadt, die in ihrem Rats- und Amtsinformationssystem, auf das neben den Stadträten auch alle Amts- und Betriebsleiter Zugriff hatten, Informationen über das disziplinarrechtliche Vorermittlungsverfahren gegen einen Amtsleiter eingestellt hatte, die personenbezogen waren.

Da anfangs uneinsichtig und trotz Hinweises auf die Rechtslage und die die Verwaltung bindenden Verwaltungsvorschriften zum Gesetz zum Schutz personenbezogener Daten der Bürger nicht in der Lage, das Verfahren datenschutzgerecht zu regeln, musste eine Beanstandung (§ 24 Abs.1 Nr. 2 DSG-LSA) gegenüber der Stadt ausgesprochen werden; zumal hier verschärfend hinzukam, dass es sich bei den personenbezogenen Daten um Personaldaten handelte. Danach wurden geeignete Maßnahmen getroffen.

Der Landesbeauftragte weist aus diesem Anlass ausdrücklich darauf hin, dass die Einstellung von personenbezogenen Daten in ein Ratsinformationssystem als Datenweitergabe innerhalb einer Behörde zumindest eine Nutzung von personenbezogenen Daten darstellt, für die die Voraussetzungen des § 10 DSG-LSA unbedingt vorliegen müssen.

14.2 Einwohnerliste für den Stadtrat

In einer Stadt verlangte der Stadtrat von der Verwaltung die Vorlage einer Liste aller Einwohner. In dieser Liste sollten dann alle Hundebesitzer mit der Anzahl der Hunde kenntlich gemacht sein, und der Stadtrat wollte diese in der nächsten - immerhin nicht-öffentlichen - Sitzung „auf Vollständigkeit“ überprüfen.

Das ging natürlich nicht. Denn die Feststellung aller Hundesteuerpflichtigen fällt nicht in die Zuständigkeit des Stadtrates, sondern ist eine Aufgabe der laufenden Verwaltung, die gem. § 63 Abs. 1 GO LSA dem Bürgermeister obliegt.
Dem Stadtrat bleibt es aber unbenommen, der Verwaltung strengere Vorgaben bei der Überprüfung der Hundesteuerpflichtigen zu machen, wenn er der Meinung ist, die Verwaltung handhabe dies zu lasch.

15. Landtag

15.1 Landtagsverwaltung und Öffentlichkeitsarbeit

Bereits in vorherigen Berichten (VI. Tätigkeitsbericht, Ziff. 15 und VII. Tätigkeitsbericht, Ziff. 15.1) hatte sich der Landesbeauftragte mit der Veröffentlichung von Papieren des Landtags befasst. Nach seiner Auffassung ist die Landtagsverwaltung rechtlich nicht gehindert, das weltweite Internet zu Zwecken der Öffentlichkeitsarbeit zu nutzen. Die damit gegebene Möglichkeit, schnell und unkompliziert Informationen verbreiten zu können, entbindet sie indessen nicht von der Pflicht, sorgsam auf möglicherweise in den einzustellenden Drucksachen vorhandene personenbezogene Daten zu achten. Die Verfassung und die aus ihr folgenden gesetzlichen Regelungen zum Datenschutz unterscheiden hinsichtlich des Beeinträchtigungspotentials nicht in erster Linie nach den die Information tragenden Medien, sondern u.a. danach, an welchen Empfänger(-kreis) personenbezogene Daten übermittelt werden könnten. Dass damit Informationsträger, welche eine geografisch unbegrenzte Verfügbarkeit gewährleisten, nur mit besonderer Sensibilität genutzt werden dürfen, versteht sich eigentlich von selbst. Der Landesbeauftragte hatte bei den entsprechenden Beratungen mit der Landtagsverwaltung den Eindruck gewonnen, dass sie seine rechtliche Einschätzung teilte.
Trotzdem beschwerte sich erneut ein Petent beim Landesbeauftragten darüber, dass Daten über seine Person im Internetangebot des Landtags veröffentlicht worden seien und er darum bereits wirtschaftliche und persönliche Nachteile gehabt habe. Auf dessen Beschwerde und die sofortigen Hinweise des Landesbeauftragten hin entfernte die Landtagsverwaltung die entsprechende Drucksache und stellte eine „neutralisierte“ Fassung ein. Der Betroffene berichtete in einem Dankschreiben an den Landesbeauftragten, dass die Korrekturen Erfolg gehabt hätten und seine Daten mit den allgemein üblichen Suchmechanismen im Internet nun nicht mehr auffindbar seien.

Der Landesbeauftragte weist in diesem Zusammenhang jedoch auf die Stellungnahme der Landesregierung zum VII. Tätigkeitsbericht zu diesem Themenbereich hin (LT-Drs. 4/2524, S. 17), welche er mit Unverständnis zur Kenntnis genommen hat. Die Landesregierung hatte erklärt, es wirke praxisfern, „wenn der Landesbeauftragte den Zugang zu allgemein zugänglichen Unterlagen wie Landtagsdrucksachen von einer vorherigen Filterung auf darin enthaltene schutzwürdige personenbezogene Daten abhängig machen will“. Dies macht den Eindruck, als solle entgegen der bestehenden verfassungsrechtlichen Lage mit dem Scheinargument der Praktikabilität einer Missachtung der Grundrechte von Bürgerinnen und Bürgern das Wort geredet werden. Es ist nach den Vorstellungen des Verfassungsgesetzgebers im Gegenteil so, dass die Vereinfachung der Öffentlichkeitsarbeit von öffentlichen Stellen dadurch, dass große Informationsmengen sehr leicht zur Verfügung gestellt werden können, nicht mit einer Beschränkung der Grundrechte einhergehen darf, nur weil der Prüfungsaufwand hinsichtlich des Inhalts der Veröffentlichungen zugleich steigt. Verwaltungsbequemlichkeit reicht zur Rechtfertigung eines Grundrechtseingriffs nie aus.
Der Informationszugang zu den Drucksachen über eine Einsichtnahme beim Landtag hat schon im Tatsächlichen nicht die Auswirkungen wie eine Übermittlung über das Internet.

15.2 Anschluss der Mitglieder des Landtags und der Fraktionen an das Intranet der Landesverwaltung

Im Laufe des Jahres 2007 werden die Landtagsabgeordneten und die Fraktionen des Landtags Zugang zum internen Verwaltungsnetz der Landesverwaltung/Intranet erhalten können. Damit geht ein seit Ende 2004 betriebener Vorgang in die letzte Runde bzw. in die praktische Umsetzung. Für einen mit dem Staatsgefüge nicht so vertrauten Leser mutet es auf den ersten Blick u.U. seltsam an, dass die Landtagsabgeordneten einen solchen Zugang noch nicht haben sollen. Schließlich ist in der allgemeinen Wahrnehmung alles im öffentlichen Bereich irgendwie Eins. Dies entspricht aber weder der gelebten noch der rechtlichen Wirklichkeit. Die gegenseitige Kontrolle durch die Trennung der staatlichen Gewalten in Gesetzgebung, Vollziehende Gewalt und Rechtsprechung drückt sich auch in einer notwendigen Selbständigkeit aus, die es nicht erlaubt, außerhalb eines genau geregelten Verfahrens Informationen zwischen diesen drei Bereichen hin und her zu schieben. Neben dieser staatsorganisatorischen Festlegung in der Verfassung (vgl. z.B. Art. 53 Landesverfassung), ist auch zu bedenken, dass, selbst in solch einem gesetzlich vorgesehenen Verfahren, nicht nur Sachinformationen, sondern auch personenbezogene Informationen übermittelt werden könnten. Für diese gelten besondere Schutzregelungen z.B. in der Landesverfassung und im DSG-LSA.
Durch einen Zugriff der Landtagsabgeordneten auf das Intranet der Landesverwaltung kann es zur Weitergabe personenbezogener Daten kommen; insoweit gelten Landtagsabgeordnete als private Dritte. Da die Datenweitergabe zudem automatisiert geschieht, sieht das DSG-LSA die Beteiligung des Landesbeauftragten für den Datenschutz vor.
Er war – allerdings erst nach einigem Hin und Her – im Rahmen seiner Zuständigkeit an der Einrichtung dieses sog. automatisierten Abrufverfahrens beteiligt worden. Der weit überwiegende Teil der erwünschten/zur Verfügung zu stellenden Informationen betrifft indessen keine personenbezogenen Daten. Daher war durch das Drängen auf die Beachtung datenschutzrechtlicher Vorgaben, entgegen einer von manch einem Beteiligten im Vorfeld geäußerten Besorgnis, auch keine wesentliche Behinderung des Informationsangebots zu erwarten - unabhängig davon, wie ein etwaiger Zugriff auf Personendaten vom Landesbeauftragten letztendlich eingeschätzt werden würde.

Soweit Zugriff auf die Daten von Bediensteten oder anderen Betroffenen gewährt werden sollte, war das Vorhaben unter Berücksichtigung des Grundrechts auf informationelle Selbstbestimmung anhand des DSG-LSA zu prüfen. Das Bereithalten personenbezogener Daten zum Abruf durch Landtagsabgeordnete hat den Anforderungen von § 7 Abs. 1 DSG-LSA zu genügen. Ein automatisiertes Abrufverfahren darf danach nur eingerichtet werden, soweit es unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen einerseits und der Aufgaben bzw. Geschäftszwecke der beteiligten Stellen andererseits angemessen ist. Die einfache Nutzbarkeit der elektronischen Datenverarbeitung für sich allein kann nicht als Rechtsgrundlage für Grundrechtseingriffe herhalten. Dass damit unter Umständen differenzierte Zugangsregelungen, z.B. in Abhängigkeit von der jeweils wahrgenommenen Funktion der Bediensteten, getroffen werden mussten, war

nicht vermeidbar. Das Bundesverfassungsgericht hat reine Zweckmäßigkeitserwägungen als Rechtsgrundlage für Eingriffe in das Datenschutzgrundrecht nicht ausreichen lassen. Insofern war für eine rechtliche Beurteilung des Abrufverfahrens die genaue inhaltliche und organisatorische Darstellung der beabsichtigten Informationsplattform notwendig. Nach etlichen Vorinformationen und der notwendigen Abstimmung der Zuständigkeiten für eine Informationsvorlage wurde dem Landesbeauftragten schließlich Anfang 2007 vom Ministerium des Innern eine Darstellung des Vorhabens zugeleitet, die den erforderlichen Detaillierungsgrad erfüllte.

Die Einrichtung des automatisierten Abrufverfahrens im Sinne von § 7 DSG-LSA erfordert die Unterrichtung des Landesbeauftragten nach § 7 Abs. 3 DSG-LSA. Neben der genauen Beschreibung von Verfahren und etwaiger Sicherungsmaßnahmen sind vor allem Anlass und Zweck, Art und Umfang der personenbezogenen Daten, die zur Übermittlung bereit gehalten werden sollen, darzulegen. Die Erforderlichkeit dieser Nutzung durch die Landtagsabgeordneten ist gem. § 7 Abs. 1 DSG-LSA zu begründen, die jeweilige Rechtsgrundlage ist in der Verfahrensbeschreibung zu benennen.

Auch weil der Datenbestand nach Kenntnis des Landesbeauftragten nicht zentral verwaltet werden soll, sind die jeweiligen Dienststellen eigenständig für die Vorabkontrolle des einzurichtenden Abrufverfahrens und die Unterrichtung des Landesbeauftragten zuständig (§ 14 Abs. 2 S. 2 DSG-LSA). Da obendrein die technischen und organisatorischen Voraussetzungen in jeder der mitwirkenden Dienststellen unterschiedlich sein dürften, geht der Landesbeauftragte davon aus, dass er über die Durchführung der Vorabkontrolle von jeder der beteiligten öffentlichen Stellen unterrichtet werden wird.
Bis zum Redaktionsschluss dieses Tätigkeitsberichtes lagen erst die Unterrichtungen von Landesrechnungshof, Ministerium des Innern und Ministerium für Wirtschaft und Arbeit vor. Der Landesbeauftragte erwartet, dass die anderen in absehbarer Zeit folgen werden und weist vorsorglich darauf hin, dass die Unterrichtung gesetzmäßig vor der Einrichtung des Abrufverfahrens zu erfolgen hat.

16. Personalwesen

16.1 Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung

Im Zuge einer immer weiter voranschreitenden Modernisierung der öffentlichen Verwaltung werden beim Bund und in den Ländern derzeit eine Vielzahl automatisierter Personalinformationssysteme bzw. Personalmanagementverfahren sowie automatisierte Verfahren zur betriebswirtschaftlichen Steuerung der Haushaltswirtschaft eingesetzt.

Aus diesem Grund hat der Arbeitskreis Personalwesen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im vergangenen Berichtszeitraum Handlungsempfehlungen zu diesem Thema erarbeitet. Diese Handlungsempfehlungen können über das Internetangebot des Landesbeauftragten

(www.datenschutz.sachsen-anhalt.de) im Bereich Service als Info-Material abgerufen werden.

Zusammenfassend bleibt festzustellen, dass personenbezogene Daten der Beschäftigten in technikunterstützten Verfahren nur in dem Umfang gespeichert, übermittelt und genutzt werden dürfen, in dem dies rechtlich zulässig und im Rahmen der festgelegten Zwecke zur Durchführung der der jeweiligen Stelle obliegenden personalwirtschaftlichen, organisatorischen und sozialen Aufgaben erforderlich ist (Grundsätze der Erforderlichkeit und der Zweckbindung). Besondere Beachtung sollten die Vorschriften des öffentlichen Dienstrechts und insbesondere die Regelungen über den Schutz von Personalaktendaten finden. In einem Berechtigungskonzept ist daher festzulegen, wer im Rahmen der ihm übertragenen Aufgaben für welche Zwecke und in welcher Form (Lesen / Verändern) befugt ist, auf personenbezogene Daten zuzugreifen bzw. Auswertungen vorzunehmen. Dabei ist der Grundsatz der Datenvermeidung und Datensparsamkeit zu berücksichtigen. Diese Grundsätze gelten zumal bei zentralen Datenbanken. So kann insgesamt vermieden werden, „gläserne Bedienstete“ zu schaffen. Die Rechte der Betroffenen und das Transparenzgebot sind stets zu beachten. Insbesondere im Rahmen von Auswertungen sollen Personaldaten soweit wie möglich anonym und pseudonym Verwendung finden. Technische und organisatorische Maßnahmen müssen das Erreichen der Sicherheitsziele des § 6 Abs. 2 DSG-LSA gewährleisten.

Auch in der Landesverwaltung Sachsen-Anhalt ist die Einführung eines ressortübergreifenden integrierten Stellen-, Personal- und Bezügemanagementsystems vorgesehen. Dieses Projekt wurde im IT-Konzept der Landesverwaltung aufgenommen. Ziel ist es, durch die Einführung einer landesweit einheitlichen Softwareausstattung eine Vereinheitlichung der Personal- und aufgabenbezogenen Prozesse in allen Organisationseinheiten zu erreichen.
Der Landesbeauftragte wurde durch die Staatskanzlei Ende 2005 gem. § 14 Abs. 1 Satz 2 DSG-LSA beteiligt und begleitet die Arbeit an diesem Projekt, zur Zeit insbesondere die Erstellung von Ausschreibungsunterlagen durch das Ministerium der Finanzen, in datenschutzrechtlicher Hinsicht.

16.2 Personaldatenübermittlung aus Anlass des Aufgabenübergangs

Im Zusammenhang mit gesetzlich vorgeschriebenen Änderungen in der Zuständigkeit bestimmter Aufgaben zwischen den Gemeinden und den Landkreisen kann es auch immer wieder zur Übernahme von Personal kommen.

In einem solchen Fall bat ein Landkreis eine Stadt um eine Aufstellung aller Mitarbeiter und Mitarbeiterinnen, die zur Zeit mit der Sachbearbeitung in einem bestimmten Aufgabenbereich betraut waren. Angaben wie Name, Vorname, Geburtsdatum, Familienstand, Kinder, Ausbildung, Weiterbildung, Lehrgänge, Vergütung, wöchentliche Arbeitszeit u.a. sollten aufgelistet werden. Die Aufforderung des Landkreises enthielt jedoch auch den ausdrücklichen Hinweis, aus datenschutzrechtlichen Gründen das Einverständnis für die Übermittlung der persönlichen Daten einzuholen.

Nicht alle Beschäftigten des Aufgabenbereiches der Stadt waren mit der Übermittlung der Daten einverstanden. Trotzdem versandte die Stadt eine Aufstellung aller Mitarbeiter und Mitarbeiterinnen mit den gewünschten Daten an den Landkreis.

Auf Nachfrage des Landesbeauftragten vertrat die Stadt die Ansicht, dass sie aus Fürsorgegründen und aufgrund des Tarifvertrages zur sozialen Absicherung die Verpflichtung habe, sich beim drohenden Wegfall von Arbeitsplätzen um eine Weiterbeschäftigung der betroffenen Mitarbeiter eventuell auch bei einem anderen Arbeitgeber des öffentlichen Dienstes zu bemühen.

Rechtlich lag hier eine Übermittlung personenbezogener Daten vor, die nur zulässig gewesen wäre, wenn eine gesetzliche Regelung diese Übermittlung erlaubt oder die Betroffenen eingewilligt hätten (vgl. § 4 Abs. 1 DSG-LSA).

Die Übermittlung der personenbezogenen Daten der Beschäftigten ist in § 28 Abs. 1 DSG-LSA i. V. m. § 90d Abs. 1 Satz 2 und Abs. 2 BG LSA geregelt. Die dort genannten Voraussetzungen waren hier nicht erfüllt. Auch der § 1 Abs. 2 des Tarifvertrages zur sozialen Absicherung begründet keine Übermittlung personenbezogener Daten.

Folglich hätte in jedem Einzelfall eine Einwilligung der Betroffenen vorliegen müssen. Da diese nicht vorlag, wäre eine Übermittlung der Daten nur in anonymisierter Form zulässig gewesen. Eine ausreichende Anonymisierung ist nach § 2 Abs. 7 DSG-LSA erst dann anzunehmen, wenn personenbezogene Daten derart verändert werden, dass 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.

Die Stadt handelte hier in dem Glauben, für die Vermeidung betriebsbedingter Kündigungen den Datenschutz der Betroffenen einschränken zu können. Durch sofortige Rückforderung der übersandten Listen und das Verlangen, alle auf Grund der Listen gespeicherten Daten durch den Landkreis umgehend zu löschen, wurde eine Schadensbegrenzung erreicht. Die Stadt wird in Zukunft sorgfältiger mit den personenbezogenen Daten der Mitarbeiter und Mitarbeiterinnen umgehen.

16.3 Erfolglose Bewerbungen in Personalunterlagen

Die Personalakten sind Grundlage für die Entscheidung über die dienstliche Entwicklung des Beschäftigten. Ihr Inhalt ist daher für den Betroffenen von erheblicher Bedeutung. Deshalb wird gelegentlich die Frage diskutiert, ob erfolglose Bewerbungen zur Personalakte zu nehmen sind. Im Interesse des Persönlichkeitsschutzes der Beschäftigten enthält allerdings § 90 Abs. 1 Satz 2 BG LSA hierzu eine klare Aussage. Danach dürfen nur Daten in der Personalakte aufgenommen werden, soweit sie mit dem Beschäftigungsverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Ergänzend sagt das Gesetz ausdrücklich, dass andere Unterlagen nicht in die Personalakte aufgenommen werden dürfen. Das

grundsätzliche Ziel der Datensparsamkeit und Datenvermeidung im Interesse des Persönlichkeitsschutzes wird hier nochmals besonders hervorgehoben.

Mit der Bewerbung verfolgt der Bewerber den Zweck, eine Veränderung seiner Beschäftigungssituation zu erreichen. Bleibt der Bewerbung jedoch der Erfolg versagt, hat sich der Zweck erledigt. Ein innerer Zusammenhang mit dem aktuell bestehenden Dienst- oder Beschäftigungsverhältnis besteht gerade nicht.

Nicht einmal auf Wunsch des Betroffenen können abgeschlossene Bewerbungen in die Personalakte aufgenommen werden. Dies würde dem Anliegen des Gesetzgeber zuwiderlaufen, mit der grundlegenden Regelung des Dienstrechts eine möglichst weitgehende Übereinstimmung des Personalaktenrechtes für die Beamten aller Dienstherren zu schaffen. Dieses Ziel wäre nicht zu erreichen, wenn die Akten entsprechend der Wünsche der Mitarbeiter unterschiedlich umfangreich ausgestaltet werden. Die Regelung, dass andere Unterlagen nicht aufgenommen werden können, ist zwingendes Recht und nicht abdingbar.

Der Erlass einer Obersten Landesbehörde zur Führung von Personalakten sah jedoch vor, dass erfolglose Bewerbungen innerhalb des Ressorts oder in den Geschäftsbereich einer anderen Obersten Landesbehörde in Sachakten aufzunehmen seien, während erfolglose Bewerbungen zu anderen Dienstherren sogar in die Personalakten (Teilakte) Eingang finden sollten. Die Oberste Landesbehörde ging davon aus, dass es die Fürsorgepflicht gebietet, Veränderungsbestrebungen der Beschäftigten im Blick zu halten und so den Neigungen und Entwicklungsvorstellungen der Beschäftigten optimal Rechnung tragen zu können. Zudem gelte es, auch im Hinblick auf Probleme bei Nachbesetzungen der Abwanderung von Bediensteten zu anderen Dienstherren entgegen zu wirken. Man sei für Versetzungen ohnehin zuständig und habe diesbezüglich umfänglichen Schriftverkehr zu bewältigen. Dies gelte insbesondere für die Anfertigung aktueller Beurteilungen, die für die ausschreibende Dienststelle für die Durchführung korrekter Auswahlverfahren erforderlich seien. Außerdem seien Bewerbungen auf dem Dienstweg durchzuführen und daher ohnehin bekannt.

Der Landesbeauftragte hat gegenüber der Obersten Landesbehörde zunächst darauf hingewiesen, dass sich der Zweck der Unterlagen mit Abschluss des Bewerbungsvorgangs erledigt habe. Den personalwirtschaftlichen Interessen an der Berücksichtigung von Veränderungsbestrebungen kann anders ausreichend Rechnung getragen werden. Wenn der Mitarbeiter von sich aus - freiwillig - den Wunsch nach Veränderung artikuliert, dürfte es eine sachdienliche Personalwirtschaft sogar gebieten, entsprechende Informationen zu speichern, um unter Berücksichtigung derartiger Wünsche einen optimalen Personaleinsatz zu gewährleisten. Diesbezügliche Unterlagen, die den Zwecken der Personalplanung und des Personaleinsatzes dienen, gehen aber der Zweckbestimmung nach über das einzelne Dienstverhältnis hinaus. Personalwirtschaftliche Unterlagen sind daher in Sachakten zu führen, nicht in Personalakten.

Die Aufbewahrung erfolgloser Bewerbungen in Personalakten für die Personalwirtschaft und -verwaltung ist nicht unerlässlich. Vielmehr steht dem das Persönlichkeitsrecht des Betroffenen (unbeobachtete Bewerbung) entgegen. Bewerbun-

gen enthalten oftmals Überschussinformationen, die den Dienstherrn nicht zu interessieren haben. Zudem besteht die Gefahr der Stigmatisierung. Eine größere Anzahl erfolgloser Bewerbungen begründet für den unbefangenen Betrachter zumindest die Vermutung, dass der Bewerber auf dem gegenwärtigen Dienstposten nicht zurecht kommt und auch auf dem Stellenmarkt keine Chancen hat. Die Versendung der aufgefüllten Personalakten mit alten, erfolglosen Bewerbungsvorgängen dürfte mit der von der Behörde betonten Fürsorge kaum zu vereinbaren sein.

Auch die Kenntnisnahme von Bewerbungen auf dem Dienstweg erscheint nicht zwingend. Zwar mag die Organisation der Personalwirtschaft im eigenen Geschäftsbereich entsprechende Verfahren vorgeben. Ein Dienstweg in den Geschäftsbereich einer anderen Obersten Landesbehörde oder gar eines anderen Dienstherrn erscheint aber fraglich. Für Letzteres sind beamtenrechtliche Vorgaben nicht ersichtlich. Dass die Behörde ggf. ohnehin Kenntnis von der Bewerbung ihres Mitarbeiters bekommt, wenn die ausschreibende Behörde die Personalakte anfordert, ist unerheblich. Die ausschreibende Behörde darf Personalakten nur dann anfordern, wenn der Bewerber in die engere Wahl kommt und nicht von vornherein ausscheidet. Zudem erfolgt die Anforderung nur mit der Einwilligung des Betroffenen.

Der Landesbeauftragte hat auch darauf hingewiesen, dass der für die Personalaktenqualität erforderliche unmittelbare innere Zusammenhang mit dem Beschäftigungsverhältnis auch nach Rechtsprechung und Literatur allenfalls im Einzelfall bei internen Bewerbungen gegeben sein kann.

Nunmehr sieht ein geänderter Erlass der Obersten Landesbehörde vor, dass Bewerbungen zu einem anderen Dienstherrn, soweit nur das Bewerbungsschreiben anfällt, Sachaktenqualität haben. Die Bewerbung zu anderen Dienstherrn, soweit dabei weiterer Schriftverkehr anfällt, sowie Bewerbungen zum gleichen Dienstherrn werden in der Personalakte aufgenommen. Die Oberste Landesbehörde hat also leider die Beratungen zum Anlass genommen, die Personalaktenführung zulasten des Persönlichkeitsrechts der Beschäftigten in höchst bedenklichem Umfang zu verschlechtern. Wenigstens wurde seitens der Behörde bekundet, dass man bemüht sei, eventuelle Sammlungen über eine Vielzahl von erfolglosen Bewerbungen bei der Anforderung von Personalakten nicht mitzusenden.

16.4 Umsetzung von Beurteilungsrichtlinien

Im VII. Tätigkeitsbericht hatte der Landesbeauftragte unter Ziff. 16.2 darauf hingewiesen, dass eine grundrechtsrelevante Bekanntgabe personenbeziehbarer Bewertungsdaten an Beurteilungsgremien einer Rechtsgrundlage entbehre. Demgegenüber verwies die Stellungnahme der Landesregierung auf ein Urteil des Oberverwaltungsgerichts des Saarlands (v. 15.01.1999, NVwZ-RR 2000, S. 450), wonach die sachlich begründete Verwendung einzelner Personalaktendaten als Grundlage einer behördeninternen Konferenz zur Vorbereitung dienstlicher Beurteilungen zulässig sei.
Nach Auffassung des Landesbeauftragten ist die Verwendung von Personalaktendaten im Rahmen der Personalverwaltung oder Personalwirtschaft nur in den

verfassungsrechtlichen Grenzen der Erforderlichkeit und Verhältnismäßigkeit zulässig. Nach § 90 Abs. 3 BG LSA dürfen nur Beschäftigte Zugang zu Personalakten haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur soweit dies für Zwecke der Personalverwaltung oder Personalwirtschaft erforderlich ist. Die reine Nützlichkeit von Informationen ist nicht ausreichend.

Unabhängig davon, ob und inwieweit das genannte Urteil verallgemeinerungsfähig ist, ist auch danach die Erforderlichkeit Maßstab. Das Urteil betraf lediglich einzelne, sachbezogen einschlägige Personalaktendaten. Zur Herbeiführung einheitlicher allgemeiner Beurteilungsmerkmale in Konferenzen ist es gerade nicht erforderlich, besonders vertrauliche Personalaktendaten, insbesondere Beurteilungsentwürfe, zu verwenden. Die Beurteilung von Stärken und Schwächen der zu Beurteilenden ist grundsätzlich nur unter den zuständigen Beurteilern zulässig. Ein Beurteilungsbasar ist und bleibt datenschutzrechtlich bedenklich.

16.5 Offener elektronischer Terminkalender

Ein Landesbetrieb erkundigte sich, ob gegen die Freischaltung der Funktion Kalender des Microsoftprogramms Outlook für alle PC-Arbeitsplätze im Landesbetrieb zu Zwecken der optimalen Terminkoordinierung datenschutzrechtliche Bedenken bestehen. Hierzu gab der Landesbeauftragte folgende Hinweise:

Grundsätzlich ist bei der Verwendung automatisierter Verfahren zur Gestaltung von Arbeitsabläufen eine Abwägung zwischen den beteiligten Interessen vorzunehmen. Das auch im Dienstverhältnis zu schützende Persönlichkeitsrecht steht den legitimen Interessen des Dienstherrn gegenüber, seine Aufgaben unter Einsatz technischer Hilfsmittel wirtschaftlich und effizient zu erfüllen.

In Terminkalendern dürften vornehmlich Informationen der Personalwirtschaft, insbesondere des Personaleinsatzes, enthalten sein, die als Sachakteninformationen über das einzelne Dienstverhältnis grundsätzlich hinausgehen und danach dem allgemeinen Datenschutzrecht unterliegen. Das Erheben, Speichern und Nutzen von terminlichen Informationen ist nach den §§ 9 Abs. 1, 10 Abs. 1 DSG-LSA zulässig, soweit dies zur Aufgabenerfüllung erforderlich ist. Gegen die Zusammenfassung der Kalenderfunktion aller PC-Arbeitsplätze im Landesbetrieb bestehen daher grundsätzlich keine datenschutzrechtlichen Bedenken, soweit dies für eine sachdienliche Terminkoordinierung erforderlich ist. Der Mitarbeiter muss bei der Verwendung dienstlich vorgegebener Systeme grundsätzlich damit rechnen, dass die dort eingetragenen Informationen auch dienstlich bekannt werden. Hier sollte allerdings im Interesse der Betroffenen für Transparenz gesorgt werden. Eine Grenze zulässiger Datenverarbeitung wäre erst bei einer Beeinträchtigung des Persönlichkeitsrechts der Mitarbeiter gegeben; dies könnte beispielsweise bei der Schaffung eines unverhältnismäßigen Überwachungsdruckes anzunehmen sein.
Im Hinblick auf die Grundsätze der Datensparsamkeit und Datenvermeidung (§ 1 Abs. 2 DSG-LSA) sollte geklärt werden, ob ein differenzierter Zugriff, also eine selektierte Freigabe, auf die Kalendereinträge bestimmter Mitarbeiter(-gruppen) möglich ist. Deshalb liegt eine Gestaltung nahe, nach der nur für ausgewählte

Mitarbeiter der Inhalt des Termins sichtbar ist, während für alle anderen Mitarbeiter der fragliche Zeitabschnitt im Kalender des betroffenen Mitarbeiters lediglich als „belegt“ gekennzeichnet ist. Sollte dies möglich sein, wäre zu prüfen, ob die Funktion im Hinblick auf die mögliche Verwendung unterschiedlicher Softwareversionen tatsächlich auf allen Arbeitsplätzen zur Verfügung steht. Zudem sollte auch bei differenzierten Zugriffen Transparenz gewährleistet sein, so dass jeder Mitarbeiter bei seinem Eintrag wissen kann, wer auf den vollen Inhalt des Eintrags zugreifen kann.

Die Eintragung privater Termine durch die Kennzeichnung als „privat“ erscheint vertretbar. Die Hintergründe (Gleitzeitausgleich, Arztbesuch) können hinreichend unterdrückt werden. Dennoch wird im Interesse des Dienstherrn deutlich, dass der Mitarbeiter zur fraglichen Zeit nicht für dienstliche Terminplanungen zur Verfügung steht. Datenschutzfreundlicher wäre auch hier ein neutralerer Hinweis („belegt“; „abwesend“).

Die vorgenannten Aspekte der Datensparsamkeit und Datenvermeidung sollten insbesondere bei sensiblen Terminen (Personalverwaltung) Berücksichtigung finden. In besonderem Maße beanspruchen die o.g. Grundsätze Geltung für die Termine des Personalrates.

16.6 Nutzung von E-Mail in der Personalverwaltung

Aufgrund voranschreitender Ausstattung mit moderner Technik in der Verwaltung kommt es in den letzten Jahren auch häufiger vor, dass sich Personalverwaltungen auf kurzem Dienstweg an ihre Mitarbeiter wenden. So werden organisatorische Informationen und Termine schnell als E-Mail verfasst und an alle betroffenen Bediensteten über eine Verteilerliste versandt.

Es mehren sich Anfragen beim Landesbeauftragten, ob es denn korrekt sei, dass durch diese Verfahrensweise z.B. weitere zehn Kollegen erfahren, dass jemand den ersten und vielleicht auch noch den Nachholtermin einer Pflichtveranstaltung verpasst hat und nun zum letzten Mal aufgefordert wird, hierzu einen Termin zu vereinbaren und diesen auch wahrzunehmen. Natürlich haben die weiteren zehn Kollegen bisher auch alle Termine versäumt, dies berechtigt sie jedoch nicht automatisch zu wissen, in welch nettem Kreis von Kollegen sie sich befinden.

Zu diesem Thema kann auf frühere Ausführungen (VII. Tätigkeitsbericht, Ziff. 16.3) zu Sammelverfügungen verwiesen werden. Auch in diesem Fall handelt es sich rein rechtlich um den Tatbestand einer Übermittlung nach § 2 Abs. 5 Nr. 3a) DSG-LSA, für den eine Rechtsgrundlage bestehen muss.

Jede Personalverwaltung sollte sich also genau überlegen, in welcher Form die Nutzung der modernen Technik möglich ist. Gegen eine Versendung einer Aufforderung zur Terminabsprache per E-Mail nur an den einen Betroffenen ist in der Regel nichts einzuwenden.

17. Polizei

17.1 SOG LSA - Kernbereichsschutz

Im Berichtszeitraum wurde das SOG LSA nicht geändert. Insoweit kann man sagen, dass es gegenüber dem, was der Landesbeauftragte in seinem VII. Tätigkeitsbericht (Ziff. 17.1) ausgeführt hat, nichts Neues gibt.

Das SOG LSA bedarf aber aus datenschutzrechtlicher Sicht in einigen Bereichen der Überarbeitung. Die Rechtsprechung hat z.B. zu Fragen der präventiven Telekommunikations- und Wohnraumüberwachung und der Rasterfahndung grundlegende Ausführungen gemacht, die eine Anpassung der derzeitigen Rechtslage in Sachsen-Anhalt bedingen.

Zum Urteil des Bundesverfassungsgerichtes vom 27. Juli 2005 (BVerfGE 113, 348) zur präventiven Telekommunikationsüberwachung hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits im Oktober 2005 dahingehend geäußert, „... dass der durch die Menschenwürde garantierte **unantastbare Kernbereich privater Lebensgestaltung** im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.
Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.
Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber auf Grund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.“ (**Anlage 5**).

Die Entscheidung des Verfassungsgerichtshofes Rheinland-Pfalz vom 29. Januar 2007 (VGH B 1/06, DVBl. 2007, 569), die sich mit Fragen der optischen und akustischen Wohnraumüberwachung befasst, stellt unmissverständlich klar, dass der Schutz des Kernbereichs privater Lebensgestaltung auch bei Vorfeldermittlungen im Bereich der Gefahrenabwehr zu beachten ist. Nicht nur bei der Strafverfolgung ist dieser Bereich unantastbar. Die entsprechenden Regelungen in § 17 Abs. 4 bis 6 SOG LSA sind auf ihre Vereinbarkeit mit diesem Grundsatz hin zu überprüfen.

Hinsichtlich der Entscheidung zur Rasterfahndung wird auf die Ausführungen unter Ziff. 17.2 verwiesen.

17.2 Rasterfahndung

In seinem VII. Tätigkeitsbericht (Ziff. 17.2) hat der Landesbeauftragte über die Beendigung der Rasterfahndung nach dem 11. September 2001 berichtet. Ihren

höchstrichterlichen Abschluss fand diese bundesweite Rasterfahndung nach bundeseinheitlichen Rasterkriterien aber erst im April 2006. Am 4. April 2006 hat das Bundesverfassungsgericht festgestellt, dass eine polizeiliche Rasterfahndung nur in Betracht kommt, wenn Tatsachen vorliegen, aus denen sich eine konkrete Gefahr ergibt (BVerfGE 115, 320).

Das Bundesverfassungsgericht traf seine Entscheidung im Rahmen der Überprüfung des Polizeigesetzes des Landes Nordrhein-Westfalen. Es führt grundlegend zur Rasterfahndung, deren Eingriffsintensität und der erforderlichen Eingriffsschwelle aus, dass „... eine Rasterfahndung nicht schon im Vorfeld einer konkreten Gefahr ermöglicht werden...“ darf, „... denn sie würde zu vollständig verdachtslos und mit hoher Streubreite erfolgenden Grundrechtseingriffen führen, die Informationen mit intensivem Persönlichkeitsbezug erfassen können.“

Von einer großen Streubreite ist immer dann auszugehen, wenn zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Grundrechtseingriffe mit großer Streubreite weisen grundsätzlich eine hohe Eingriffsintensität auf.

„Bei der Wahl der Mittel zur Erfüllung seiner Schutzpflicht ist der Staat auf diejenigen Mittel beschränkt, deren Einsatz mit der Verfassung in Einklang steht (...). Der staatliche Eingriff in den absolut geschützten Achtungsanspruch des Einzelnen auf Wahrung seiner Würde (...) ist ungeachtet des Gewichts der betroffenen Verfassungsgüter stets verboten (...). Aber auch im Rahmen der Abwägung nach Maßgabe des Grundsatzes der Verhältnismäßigkeit im engeren Sinne dürfen staatliche Schutzpflichten nicht dazu führen, dass das Verbot unangemessener Grundrechtseingriffe unter Berufung auf grundrechtliche Schutzpflichten leer läuft, so dass in der Folge allenfalls ungeeignete oder unnötige Eingriffe abgewehrt werden könnten.“
„Aus dem Gebot der Verhältnismäßigkeit im engeren Sinne kann unter bestimmten Voraussetzungen sogar die vollständige Unzulässigkeit der Vornahme bestimmter Grundrechtseingriffe zu Zwecken persönlichkeitsbezogener Ermittlungen im Bereich der inneren Sicherheit folgen.“

Das Bundesverfassungsgericht stellt klar, dass das Grundrecht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist. Aber der Einzelne muss nur solche Beschränkungen seines Grundrechtes hinnehmen, die durch ein überwiegendes Allgemeininteresse gerechtfertigt sind und auf einer verfassungsgemäßen gesetzlichen Grundlage stehen, die insbesondere dem Grundsatz der Verhältnismäßigkeit und dem Gebot der Normenklarheit entspricht. Im Fall der Rasterfahndung nach dem 11. September 2001 im Land Nordrhein-Westfalen war das nach Auffassung des Gerichts nicht der Fall. Für die entsprechende Rasterfahndung in Sachsen-Anhalt gibt es eine vergleichbare gerichtliche Entscheidung nicht. Es ist aber wahrscheinlich, dass auch die Rechtsgrundlage in § 31 SOG LSA für eine polizeiliche Rasterfahndung in Sachsen-Anhalt einer gerichtlichen Überprüfung nicht standhalten würde.

Dem Landesbeauftragten sind bisher keine Bestrebungen der Landesregierung bekannt, das SOG LSA in absehbarer Zeit zu ändern. Eine Überarbeitung der Vorschriften im SOG LSA ist allerdings auch zum Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Maßnahmen erforderlich (vgl. Ziff. 17.1).

17.3 Gesprächsaufzeichnungen bei der Polizei

Aus Presseveröffentlichungen im Zusammenhang mit einem Todesfall in einer Arrestzelle eines Polizeireviers erlangte der Landesbeauftragte davon Kenntnis, dass dienstliche Telefongespräche durch die Polizei aufgezeichnet werden. Er nahm dies sofort zum Anlass, um im Juni 2005 beim Ministerium des Innern als zuständiger oberster Landesbehörde zur grundsätzlichen Verfahrensweise anzufragen.

Ebenfalls im Juni 2005 beschloss der Ausschuss für Inneres des Landtages im Rahmen seiner Beratungen zu dem Todesfall, den Landesbeauftragten zu ersuchen (§ 22 Abs. 5 DSG-LSA), „ ... Hinweisen auf Probleme in der Anwendung datenschutzrechtlicher Bestimmungen bei der Aufzeichnung von fernmündlichen Gesprächen durch Dienststellen der Landespolizei nachzugehen.“ Um sich auch vor Ort einen Eindruck zu verschaffen, hat der Landesbeauftragte im Juni und Juli 2005 zwei Polizeireviere aufgesucht.

Im September 2005 wurde durch das Ministerium des Innern des Landes Sachsen-Anhalt eine erste Äußerung zur Anfrage des Landesbeauftragten vorgelegt. Im Ergebnis blieb vor allem festzustellen, dass es im Land unterschiedlichste Varianten von Aufzeichnungsmöglichkeiten gibt.
Unterschieden werden Langzeit- und Kurzzeitdokumentation. Die Langzeitdokumentation ist manipulationssicher und damit gerichtsverwertbar. Sie erfolgt für die jeweilige Dienststelle zentral und ist in aller Regel fest voreingestellt, d.h. der Nutzer eines Apparates entscheidet nicht für jedes Gespräch gesondert, ob er von der Aufzeichnungsmöglichkeit Gebrauch machen will. Die Kurzzeitdokumentation ist ein Arbeitsmittel, das dem Benutzer zum unmittelbaren Nachvollziehen des gesprochenen Wortes innerhalb eines zeitlich eng begrenzten Zeitraumes dient. Sie wird regelmäßig manuell zugeschaltet und erfolgt über einen geräteinternen Chip. Man kann sich das wie bei einem Anrufbeantworter vorstellen. Die Aufnahmemöglichkeit wird durch Betätigen einer bestimmten Taste ausgelöst.

Der Vielfalt der technischen Lösungen ist es geschuldet, dass nicht alle Aufzeichnungen stets im Rahmen der gesetzlichen Vorgaben veranlasst wurden. Nach § 23a SOG LSA kann die Polizei Anrufe über Notrufeinrichtungen aufzeichnen. Im Übrigen ist eine Aufzeichnung von Anrufen durch die Polizei nur zulässig, soweit sie im Einzelfall zur polizeilichen Aufgabenerfüllung erforderlich ist. Aufzeichnungen sind spätestens nach einem Monat zu löschen, es sei denn, sie werden zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt oder Tatsachen rechtfertigen die Annahme, dass die anrufende Person künftig Straftaten begehen wird, und die Aufbewahrung zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist.

Nach § 23a Satz 1 SOG LSA darf die Polizei Anrufe - gemeint sind in erster Linie eingehende Notrufe - über Notrufeinrichtungen (110, Notrufsäulen, Verbindung von der Rettungsleitstelle zum Polizeirevier) aufzeichnen. Darüber hinaus erlaubt diese Bestimmung in Satz 2 eine Aufzeichnung von Anrufen durch die Polizei im Übrigen nur dann, wenn sie im Einzelfall zur polizeilichen Aufgabenerfüllung erforderlich ist (z.B. Drohanrufe). Dies begegnet keinen grundsätzlichen datenschutzrechtlichen Bedenken, es kommt aber entscheidend auf die entsprechende Eingrenzung in der Praxis an.

Nach Veröffentlichungen durch die Medien hat es im Juni 2005 Weisungen des Ministeriums des Innern an die Polizeidienststellen und Hinweise auf diese Rechtslage gegeben. Die Praxis wurde entsprechend umgestellt, so dass nicht mehr jedwede Gespräche über die Notrufeinrichtungsapparate an den Bedienplätzen in den Lagezentren geführt werden, wo die Gespräche zwangsläufig aufgezeichnet werden. Zudem wurde auf die Löschfrist von einem Monat hingewiesen. Von der Änderung der Praxis konnte sich der Landesbeauftragte bei der Überprüfung von Einzelfällen überzeugen.

Auch der gesamte Sprechfunkverkehr der Polizei wird aufgezeichnet. Selbst wenn man davon ausgeht, dass das im dienstlichen Zusammenhang gesprochene Wort von Polizeibediensteten nicht in vollem Umfang dem Grundrechtsschutz unterliegen sollte, so werden doch regelmäßig die Grundrechte derer beeinträchtigt, über die sich die Polizeibediensteten via Sprechfunk verständigen. Mit der Aufzeichnung des Sprechfunkverkehrs werden zwangsläufig auch personenbezogene Daten der Dritten gespeichert. Zumindest insoweit bedarf die Aufzeichnung des Sprechfunkverkehrs einer rechtlichen Grundlage. § 22 Abs. 5 SOG LSA erlaubt es der Polizei, zur Vorgangsverwaltung oder zur befristeten Dokumentation behördlichen Handelns personenbezogene Daten zu speichern und zu nutzen. Eine befristete Dokumentation behördlichen Handelns soll u.a. übergeordnete Behörden in die Lage versetzen, geeignete Maßnahmen im Rahmen der Dienst- und Fachaufsicht zu treffen. Sie dient darüber hinaus dem späteren Nachweis der Rechtmäßigkeit getroffener Maßnahmen gegenüber Betroffenen bzw. Gerichten.

Im Übrigen unterstützt der Landesbeauftragte die Absicht des Ministeriums des Innern, eine einheitliche Struktur mit landeseinheitlicher Technik, zentralem Management und dezentraler Aufzeichnung einzurichten und verschlissene Technik zu ersetzen. Dabei sollen Auswahlmöglichkeiten geschaffen werden, ob Telefongespräche automatisch oder nur im Bedarfsfalle aufgezeichnet werden. Das Technische Polizeiamt hat eine Ausschreibung durchgeführt und einen Teil der Technik bereits erworben.

Die öffentliche Behandlung des Themas, die Hinweise des Landesbeauftragten - der auch den Innenausschuss des Landtages in einer ausführlichen Stellungnahme informierte - und des Ministeriums des Innern haben zu mehr Sensibilität geführt und die Aufmerksamkeit auf diese eher unbekannte Materie gelenkt. Der Landesbeauftragte hat seine Unterstützung bei der Einführung der neuen Technik angeboten. Das Ministerium des Innern seinerseits wollte umgehend einen Anwendungserlass erstellen und dem Landesbeauftragten zuleiten; zu einem Ent-

wurf vom September 2006 wurde im selben Monat Stellung genommen; doch auch bis Ende Mai 2007 kam der Vorgang im Ministerium nicht voran.

17.4 Fußball-Weltmeisterschaft - „Deutschland und der Sicherheitsfußball“

Nein - Deutschland ist nicht Fußball-Weltmeister 2006 geworden. Im Nachhinein betrachtet verlief das große Fußballfest ganz überwiegend friedlich und strafte damit alle „Sicherheitsbedenkenträger“ Lügen.

Aber warum ging es bei der Fußball-Weltmeisterschaft friedlich zu? Hat der enorme Sicherheits- und Überwachungsaufwand Probleme verhindert? Trotz der Sicherheitskonzepte der Sicherheitsbehörden war nicht jede polizeiliche oder sicherheitsbehördliche Maßnahme aus datenschutzrechtlicher Sicht zu begrüßen. Ganz im Gegenteil hat der Sicherheitseifer die Datenschutzbeauftragten immer wieder auf den Plan gerufen. Denn in datenschutzrechtlicher Hinsicht waren die Verfahren zum Ticketing, zur Akkreditierung und zum Public Viewing nicht von Anfang an hinnehmbar.

Bei aller Freude über eine Fußball-Weltmeisterschaft im eigenen Land darf man auch nicht vergessen, was so eine Veranstaltung rechtlich gesehen ist. Sie ist ein Vereinsfest; zwar das Vereinsfest eines „Welt-Vereins“, das zudem Deutschland in einen Ausnahmezustand versetzte, aber trotzdem nur ein Vereinsfest. Veranstalter der Fußball-Weltmeisterschaft war die FIFA, die Fédération Internationale de Football Association, d.h. die Internationale Föderation des Verbandsfußballs. Die FIFA ist der Weltfußballverband mit Sitz in Zürich. Er organisiert verschiedene Fußball-Wettbewerbe, darunter auch die Fußball-Weltmeisterschaft. Die FIFA ist ein im Handelsregister eingetragener Verein im Sinne von Art. 60 ff. des Schweizerischen Zivilgesetzbuches. Die FIFA besteht aus 207 Nationalverbänden. Und der Nationalverband Deutschland hatte von der FIFA den Zuschlag bekommen, die Fußball-Weltmeisterschaft 2006 im eigenen Land durchzuführen. Die Deutschen organisierten also den Fußball-Wettbewerb „Fußball-Weltmeisterschaft 2006“ der FIFA.

Der Deutsche Fußball-Bund (DFB) hat seinen Sitz in Frankfurt/Main. Der DFB ist ein eingetragener, gemeinnütziger Verein. Er ist damit dem nicht-öffentlichen Bereich zuzuordnen. Für Fragen des Datenschutzes im nicht-öffentlichen Bereich ist in Hessen das Regierungspräsidium Darmstadt zuständig. Die datenschutzrechtliche Beratung des DFB bei der Organisation des Vereinsfestes oblag demnach zuförderst dem Regierungspräsidium Darmstadt.

Weil aber öffentliche Stellen, wie z.B. die Polizeien und Verfassungsschutzbehörden der Länder und des Bundes, in die Organisation der Sicherheitsarchitektur des Vereinsfestes eingebunden waren, konnten sich die Datenschutzbeauftragten nicht zurücklehnen. Denn für die Polizeien und Verfassungsschutzbehörden nehmen sie die Datenschutzkontrolle wahr. Deshalb hat sich der Landesbeauftragte, auch in seiner Eigenschaft als Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2006, immer wieder in die Diskussionen rund um die Fußball-Weltmeisterschaft eingebracht.

Auch wenn Großereignisse wie eine Fußball-Weltmeisterschaft eine ganz eigene Dynamik entwickeln und ein seltenes Ereignis darstellen, so kann die Absicherung solcher Veranstaltungen nicht allein zu Lasten des Rechtes auf informationelle Selbstbestimmung gehen.

17.4.1 Ticketing-Verfahren

Ein Glückspilz - wer eines der begehrten Tickets für ein Spiel der Fußball-Weltmeisterschaft ergattern konnte. Die Tickets waren rar und das Verfahren, um auf ehrlichem Wege ein Ticket zu erlangen, eher beschwerlich. Mehrere Vergaberunden, eine Anmeldung über Internet und ein Losverfahren mussten überwunden werden, um dann ggf. zu den Auserwählten zu gehören, die eines der Spiele live erleben durften. Aber es kostete den an einem Ticket Interessierten nicht nur Zeit und Geld, sondern auch einen Teil seines „Lebens“ – nämlich seines Datenlebens.

Bereits bei der Anmeldung über das Internet mussten die Interessenten ihre persönlichen Daten, wie z.B. Name, Geburtsdatum, Adresse, Nationalität und sogar ihre Ausweisdaten angeben. Ziemlich viele Angaben dafür, dass man eine Eintrittskarte erwerben möchte und keinerlei Sicherheit hat, dass einem ein Ticket zugeteilt wird. Wer geht schon an die Kinokasse und klärt den Verkäufer über seinen Namen, sein Geburtsdatum, seine Adresse, seine Nationalität und seine Ausweisdaten auf, um sich dann sagen zu lassen, der Kinosaal ist bereits ausverkauft. Zugegeben, ganz vergleichbar ist das nicht, obwohl in der datenschutzrechtlichen Bewertung der beiden Vorgänge gar nicht so enorme Unterschiede liegen.

Die Begründung des Veranstalters war so einfach wie datenschutzrechtlich nicht zu begrüßen. Die WM-Tickets sollten personalisiert vergeben werden. Jedes ausgegebene Ticket sollte, auf einem RFID-Chip gespeichert, die persönlichen Daten des Ticketinhabers enthalten. An den Eingängen der Stadien sollten diese Daten über entsprechende Lesegeräte ausgelesen werden können und mit den Daten des mitzuführenden Ausweises abgeglichen werden. Um dieses Ziel zu erreichen, hätte es auch ausgereicht, die Daten von den Personen zu erheben, denen tatsächlich ein Ticket zugeteilt wurde.

Die Frage nach der Notwendigkeit solcher personalisierten Tickets stellt sich auch nach der Fußball-Weltmeisterschaft. Nach dem Kenntnisstand des Landesbeauftragten wurden nur sehr wenige Besucher daraufhin überprüft, ob die Daten des Stadionbesuchers mit denen des Ticketerwerbers auch übereinstimmen. Wo die Interessen des Veranstalters an personalisierten Tickets genau gelegen haben, ist nicht ganz nachvollziehbar. Zumindest hat der Veranstalter Unmengen von personenbezogenen Daten aufgrund der Erhebungen im Rahmen der Anmeldungen erhalten und es steht zu „... befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.“ So hat es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits in ihrer Entschließung anlässlich ihrer 69. Tagung im März 2005 in Kiel formuliert.

17.4.2 Akkreditierungsverfahren

Noch viel mehr als die Besucher von Weltmeisterschaftsspielen mussten Personen, die bei der Fußball-Weltmeisterschaft beruflich tätig werden wollten bzw. sollten, Sicherheitsmaßnahmen hinnehmen. Solche Personen mussten sich akkreditieren lassen, die u.a. als Ordnungs- und Sicherheitskräfte, als Servicepersonal, als Reinigungskräfte, als Journalisten und sonstige Helfer in den Stadien und sonstigen offiziellen WM-Arealen tätig werden wollten.

Die Akkreditierung sollte nach der Datenschutzinformation des Veranstalters dem Zweck dienen, einen friedlichen und störungsfreien Verlauf der Fußball-Weltmeisterschaft zu gewährleisten. In das Akkreditierungsverfahren für den privaten Veranstalter waren sowohl die Polizeien als auch die Verfassungsschutzbehörden mit einbezogen. Die Situation stellt sich im Ergebnis so dar, dass eine „Privatperson“ - hier der DFB - staatliche Stellen - Polizei und Verfassungsschutz - um Auskunft bittet, um die Zuverlässigkeit bei ihm Beschäftigter zu überprüfen. Dafür gibt es keine Rechtsgrundlage.

Also wurde den Betroffenen eine „Einverständniserklärung“ abverlangt, mit derer sie freiwillig in das Überprüfungsverfahren bei Polizei und Verfassungsschutz einwilligten. Diese Erklärung bildete dann die Grundlage des Verfahrens. Rechtliche Bedenken bleiben jedoch. Wenn es eine Rechtsgrundlage für die Beteiligung von Polizei und Verfassungsschutzbehörden in Akkreditierungsverfahren privater Veranstalter nicht gibt, so kann dies nicht durch die massenhafte Einholung von Einverständniserklärungen umgangen werden.

Außerdem bleiben ernstliche Zweifel an der Freiwilligkeit solcher Einverständniserklärungen. Wem steht es denn tatsächlich frei, sich für oder gegen eine solche Maßnahme zu entscheiden, wenn das Unternehmen, bei dem er beschäftigt ist, einen Auftrag an einem der akkreditierungspflichtigen Standorte angenommen hat.

Für einen durchschnittlichen Beschäftigten eines Unternehmens, das in einem der Stadien tätig wurde, oder für einen Journalisten verlief das Akkreditierungsverfahren so, dass er von seinem Arbeitgeber aufgefordert wurde, eine Einverständniserklärung zu unterschreiben und einen Fragebogen auszufüllen. Diese Einverständniserklärung verblieb dann beim Arbeitgeber. Der Arbeitgeber wiederum erklärte gegenüber dem DFB, dass er seinen zur Akkreditierung angemeldeten Beschäftigten die Einverständniserklärung abgenommen hatte. Der DFB übermittelte die Daten dann an das Bundeskriminalamt. Weder der DFB noch das Bundeskriminalamt noch sonstige öffentliche Stellen haben die Einverständniserklärungen der Betroffenen je gesehen. Alle haben sich auf die Zusicherung des Arbeitgebers verlassen. Allein dieser Umstand macht das Verfahren aus Sicht der öffentlichen Stellen datenschutzrechtlich unvertretbar.

Beim Bundeskriminalamt wurden die Daten bereits mit den vorhandenen Datenbeständen abgeglichen und anschließend an die Landeskriminalämter des

Hauptwohnsitzes des Betroffenen und das Bundesamt für Verfassungsschutz weitergeleitet.
Die Landeskriminalämter glichen die Daten mit ihren Beständen ab und gaben ein Votum zur Akkreditierung an das Bundeskriminalamt ab. In den Fällen, in denen ein Abgleich durch das Landeskriminalamt keine Erkenntnisse ergab, wurde der Betroffene gleich als „approved“ - keine Bedenken - an das Bundeskriminalamt zurückgemeldet. Lagen Erkenntnisse vor, wurde die bearbeitende Polizeidienststelle um eine Einschätzung gebeten und anschließend ein Votum gegenüber dem Bundeskriminalamt abgegeben.

Das Bundesamt für Verfassungsschutz bearbeitete die Daten nach dem selben System wie das Bundeskriminalamt. Es glich die Daten in eigenen Dateien ab und verteilte die Daten nach dem Hauptwohnsitzprinzip an die Landesverfassungsschutzbehörden. Diese verfuhren wie die Landeskriminalämter (das VerfSchG-LSA enthält hierzu keine Regelung) und meldeten im Ergebnis ihrer Prüfung ein Votum an das Bundesamt für Verfassungsschutz. Das Bundesamt für Verfassungsschutz bildete aus seinem und dem Votum der jeweiligen Landesverfassungsschutzbehörde ein Votum, dass es an das Bundeskriminalamt weiterleitete.

Beim Bundeskriminalamt lagen nun die Einschätzungen der Polizei und des Verfassungsschutzes vor. Es wurde ein abschließendes Votum gebildet und an den DFB gemeldet. Die Betroffenen und der Arbeitgeber wussten zu diesem Zeitpunkt weder, dass noch welches Votum abgegeben wurde, und vor allem nicht, aufgrund welcher Erkenntnisse. Der Arbeitgeber wurde dann vom DFB insoweit informiert, dass eine Akkreditierung erfolgen kann oder nicht.

Einwände gegen eine nicht erteilte Akkreditierung musste der Betroffene allerdings nicht gegenüber dem die Akkreditierung verweigernden DFB, sondern gegenüber dem jeweiligen Landeskriminalamt geltend machen.

Der Landesbeauftragte hat das Akkreditierungsverfahren, soweit es seiner Kontrolle unterfiel, überprüft und festgestellt, dass sich das Landeskriminalamt des Landes Sachsen-Anhalt an die im Vorhinein bundeseinheitlich vereinbarten Absprachen und Konzepte gehalten hat und insoweit kein Grund für ein Eingreifen bestand. Auch das Sperren der Daten nach Abschluss der Fußball-Weltmeisterschaft und das Löschen der Datenbestände wurde fristgerecht vorgenommen.

Aus datenschutzrechtlicher Sicht dürfen solche Verfahrensweisen nicht für andere Großereignisse Schule machen. Sie beeinträchtigten die Rechte der Betroffenen in erheblichem Maße.

17.4.3 „Public-Viewing“

Alle diejenigen, denen kein Ticket für ein Weltmeisterschaftsspiel zugeteilt worden war, oder denen der Aufwand, eines zu erlangen, einfach zu groß war, konnten die allerorts angebotenen Public-Viewing-Veranstaltungen nutzen, um etwas von der WM-Stimmung mitzunehmen.

Als der Landesbeauftragte aus der Presse davon erfuhr, dass Public-Viewing-Veranstaltungen auch in Sachsen-Anhalt stattfinden würden, fragte er beim Minister des Innern an, wie die nach Presseberichten vom Ministerium des Innern geforderten Mindestanforderungen an die Absicherung dieser Veranstaltungen rechtlich und tatsächlich umgesetzt werden sollen. Zu diesen Mindestanforderungen sollte es nämlich gehören, Public-Viewing-Veranstaltungen per Videokamera zu überwachen und die Bilder an die jeweiligen Polizeidienststellen weiterzuleiten.

Das Ministerium des Innern konnte die Situation allerdings soweit aufklären, dass es zwar Videoüberwachungen geben werde, dies allerdings nicht zwingende Voraussetzung für die Genehmigung von Public-Viewing-Veranstaltungen sei.

Zuständig für die Genehmigung von Public-Viewing-Veranstaltungen waren die Ordnungsbehörden der Städte bzw. Verwaltungsgemeinschaften, in denen Public-Viewing-Veranstaltungen durchgeführt werden sollten. Von den Veranstaltern wurden Anträge gestellt, denen eine Konzeption für die jeweilige Public-Viewing-Veranstaltung beigefügt war. Zur Unterstützung der Ordnungsbehörden und zur Sicherstellung eines landeseinheitlichen Vorgehens erließ das Landesverwaltungsamt als Fachaufsichtsbehörde über die Ordnungsbehörden eine Verfügung, die die Mindestanforderungen an Konzepte und die erforderlichen Sicherungsmaßnahmen beschreibt. U.a. wörtlich: „Unabhängig von der Einhaltung ggf. weitergehender ordnungsbehördlicher Vorgaben sollten folgende Mindeststandards zur Gewährleistung der öffentlichen Sicherheit angestrebt werden (Vorfeldmaßnahmen): ... Einrichtung von Videoüberwachungsanlagen durch den Veranstalter, wenn Örtlichkeit oder Besucheraufkommen dies erfordern.“ Der Verfügungstext ließ durch die Verwendung von Wörtern wie „sollten“, „angestrebt werden“ und „wenn dies erfordern“ genügend Ermessensspielraum für die Ordnungsbehörden, ihre Maßnahmen auf die konkreten Bedingungen vor Ort abzustimmen. Wenn in einer Gemeinde mit 500 Einwohnern eine Public-Viewing-Veranstaltung stattfindet, so ist es nachvollziehbar, dass die Anforderungen dort andere sind, als z.B. beim „WM-Fieber“ in der Landeshauptstadt. Von einer zwingenden Vorgabe, dass Public-Viewing-Veranstaltungen per Videokamera zu überwachen sind, konnte nicht ausgegangen werden. Selbst für das „WM-Fieber“ in Magdeburg stellte die Stadt in ihrer Ordnungsverfügung fest, dass „Art und Umfang der Videoüberwachung ... einer privatrechtlichen Regelung vorbehalten“ bleiben.

Entgegen den Presseverlautbarungen sollten die Bilder der Veranstaltungen, die videoüberwacht würden, auch nicht direkt an die Polizei weitergeleitet werden. Die Polizei hätte auf die Bilder der privaten Veranstalter nur in den Fällen zurückgegriffen, in denen dies gesetzlich zugelassen ist. So wäre es denkbar gewesen, dass die Polizei im Falle von Ausschreitungen oder bei der Verfolgung von Strafanzeigen, Einsicht in die Aufnahmen der Veranstalter nimmt. Ein solches Vorgehen der Polizei hätte von der geltenden Rechtslage gedeckt gewesen sein können (§ 6b BDSG).

Die Public-Viewing-Veranstaltungen in Sachsen-Anhalt sind vor diesem Hintergrund in einem rechtlich - auch datenschutzrechtlich - zulässigen Rahmen durchgeführt worden. Beschwerden von Betroffenen sind beim Landesbeauftragten nicht eingegangen.

17.5 Videoüberwachung öffentlicher Flächen

Über die gesetzlichen Bestimmungen zur Videoüberwachung und Videoaufzeichnung hatte der Landesbeauftragte zuletzt in seinem VII. Tätigkeitsbericht (Ziffn. 14.2 und 17.1.2) berichtet. Am gesetzlichen Rahmen hat sich im Berichtszeitraum nichts geändert. Allerdings erging im Berichtszeitraum eine interessante Entscheidung des Bundesverfassungsgerichtes zur Videoüberwachung eines Kunstwerkes im öffentlichen Raum vom 23. Februar 2007 (1 BvR 2368/06, DVBl. 2007, 497).

Zum Sachverhalt sei zunächst erläutert, dass eine Stadt ein Bodenkunstwerk errichtet und dies der Allgemeinheit übergeben hatte. Danach kam es im Bereich des Kunstwerkes zu mehreren Vorfällen, die die Stadt dazu veranlassten, die Errichtung einer Videoüberwachungsanlage für den Bereich des Kunstwerkes anzustrengen. Ein Einwohner der Stadt, der sich regelmäßig im Bereich des Kunstwerkes aufhielt, erhob vorbeugende Unterlassungsklage gegen die Stadt. Der Beschwerdeführer klagte sich durch die Instanzen bis zum Bundesverfassungsgericht.

Das Bundesverfassungsgericht stellt in seiner Entscheidung fest:

„Die geplante Videoüberwachung greift in das allgemeine Persönlichkeitsrecht des Beschwerdeführers in seiner Ausprägung als Recht der informationellen Selbstbestimmung ein. Dieses Recht umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, und daher grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen (...).

Das durch die Videoüberwachung gewonnene Bildmaterial kann und soll dazu genutzt werden, belastende hoheitliche Maßnahmen gegen Personen vorzubereiten, die in dem von der Überwachung erfassten Bereich bestimmte unerwünschte Verhaltensweisen zeigen. Die offene Videoüberwachung eines öffentlichen Ortes kann und soll zugleich abschreckend wirken und insofern das Verhalten der Betroffenen lenken (...). Durch die Aufzeichnung des gewonnenen Bildmaterials werden die beobachteten Lebensvorgänge technisch fixiert und können in der Folge abgerufen, aufbereitet und ausgewertet sowie mit anderen Daten verknüpft werden. So kann eine Vielzahl von Informationen über bestimmte identifizierbare Betroffene gewonnen werden, die sich im Extremfall zu Profilen des Verhaltens der betroffenen Personen in dem überwachten Raum verdichten lassen.

Der Eingriff in das Grundrecht entfällt nicht dadurch, dass lediglich Verhaltensweisen im öffentlichen Raum erhoben werden. Das allgemeine Persönlichkeitsrecht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen des Einzelnen, der sich in die Öffentlichkeit begibt, Rechnung (...).

Von einer einen Eingriff ausschließenden Einwilligung in die Informationserhebung kann selbst dann nicht generell ausgegangen werden, wenn die Betroffenen aufgrund einer entsprechenden Beschilderung wissen, dass sie im räumlichen Bereich der Begegnungsstätte gefilmt werden. Das Unterlassen eines ausdrücklichen Protests kann nicht stets mit einer Einverständniserklärung gleichgesetzt werden (...)."

Diese deutlichen Worte des Bundesverfassungsgerichtes müssen künftig die Richtschnur sein, an der die Qualität des Eingriffs in das Recht auf informationelle Selbstbestimmung durch eine Videoüberwachung im öffentlichen Raum gemessen werden muss. § 30 DSG-LSA ist im Lichte dieser Entscheidung auszulegen.

17.6 Videoüberwachung - Ein Marktplatz im Visier

Aufgrund von Presseberichten Ende des Jahres 2006 erfuhr der Landesbeauftragte, dass der Marktplatz einer Stadt künftig durch drei Videokameras überwacht werden solle. Grund seien Übergriffe auf Personen und sonstige Straftaten gewesen.

Der Landesbeauftragte wandte sich daraufhin an die zuständige Polizeibehörde, die die Videoüberwachungen initiiert haben sollte. Die Stellungnahme bezeichnete § 16 Abs. 2 Satz 2 SOG LSA als Rechtsgrundlage der Maßnahme und stellte die der Maßnahme vorausgegangenen Straftaten in dem nunmehr videoüberwachten Bereich dar. Insgesamt handelte es sich um 56 registrierte Straftaten in einem Zeitraum von sechs Monaten. Darunter fanden sich Körperverletzungsdelikte, Sachbeschädigungen, schwere Diebstähle und Einbrüche.

Auch wenn die Zulässigkeit einer Videoüberwachung unter diesen Voraussetzungen durch den Landesbeauftragten nicht in Frage gestellt wurde, so machte er sich doch vor Ort ein Bild von der Maßnahme. Insbesondere achtete er dabei auf die ausreichende Beschilderung des zu überwachenden Geländes. Jeder, der sich in diesen Bereich begibt, muss durch ausreichende Hinweisschilder darauf aufmerksam gemacht werden, dass hier eine Videoüberwachung stattfindet. Darüber hinaus ließ sich der Landesbeauftragte informieren, wie die Aufzeichnungen im Polizeirevier aufbewahrt und gelöscht werden.

Die Videoüberwachungsmaßnahme war zunächst zeitlich begrenzt worden. Eine Auswertung sollte zeigen, ob und welche Veränderungen durch eine Videoüberwachung erreicht werden können. Nach Ablauf der zeitlichen Begrenzung wurde die Anweisung zur Videoüberwachung für weitere drei Monate verlängert. Die Auswertung der Deliktszahlen durch die Polizei ergab, „... dass eine gewisse Lageberuhigung eingetreten ist und das Ziel der vorbeugenden Straftatenbekämpfung mit der Maßnahme der Videoüberwachung teilweise erreicht wurde." In den drei Monaten der Videoüberwachung wurden lediglich sechs relevante Delikte in dem überwachten Bereich registriert. Die Polizei geht davon aus, dass die Deliktszahlen wieder steigen würden, wenn die Videoüberwachung eingestellt würde.
Der Landesbeauftragte wird die Maßnahme weiter begleiten.

17.7 Sexualstraftäterdatei

Dass Sexualstraftäter nach ihrer Entlassung aus dem Strafvollzug stärker überwacht werden sollen, wurde in der Vergangenheit bereits mehrfach öffentlich thematisiert. Als Anfang 2006 ein 13-jähriges Mädchen entführt und gefangen gehalten wurde, flammte die Diskussion wieder auf. Gesetzesverschärfungen wurden gefordert. Ende 2006 wurden dann erste Forderungen nach einer öffentlich zugänglichen Datei laut, in der alle Sexualstraftäter mit Anschriften verzeichnet sein sollten. Jeder in der Nachbarschaft sollte so in Erfahrung bringen können, ob in seiner unmittelbaren Umgebung Sexualstraftäter wohnen. Nach heftigen Protesten gegen diesen Vorschlag wurden die Bestrebungen alsbald wieder verworfen.

Der Ruf nach einer effizienteren Überwachung von Sexualstraftätern nach der Haft ist allerdings noch nicht verhallt. Im Grunde besteht darüber auch Konsens. Über das Wie einer solchen „Nachbetreuung“ gehen die Vorstellungen allerdings nach wie vor auseinander. Die Vorstellungen reichen von der Errichtung eines Zentralregisters bis hin zu schlicht erleichtertem Zugriff der Polizei auf Meldedaten. Wohin sich die Diskussion und ggf. auch die Gesetzgebung entwickeln wird, bleibt abzuwarten. Im Bereich der Führungsaufsicht für entlassene Straftäter erließ der Bundesgesetzgeber bereits zusätzliche Regelungen für strengere Auflagen.

Dass eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig wäre, daran besteht aus datenschutzrechtlicher Sicht kein Zweifel. Die Betroffenen würden an eine Art elektronischen Pranger gestellt und infolge solcher öffentlichen Bloßstellung sozial geächtet werden. Die Möglichkeit der Resozialisierung, die den Betroffenen nach unserer Rechtsordnung zusteht, würde den Betroffenen genommen werden. Ihren Standpunkt hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder anlässlich ihrer 73. Tagung im März 2007 in Erfurt durch eine entsprechende Entschließung (**Anlage 21**) verdeutlicht.

17.8 „Erinnerungsmitteilungen“ - Die ungelöschte Datenbank im Kopf

Im Berichtszeitraum hat sich ein Bürger mit der Bitte an den Landesbeauftragten gewandt, eine unübersichtlich gewordene Situation aufzuklären. Im März des Jahres 2004 hatte der Betroffene ein Polizeirevier im Land gebeten, ihm Auskunft über die zu seiner Person gespeicherten Daten zu geben und eventuell vorhandene Daten zu löschen. Von diesem Polizeirevier wurde er an die zuständige Polizeidirektion A verwiesen, welche ihm Ende April 2004 schriftlich mitteilte, dass keine Daten zu seiner Person gespeichert seien.

Im Mai 2005 wandte sich der Betroffene erneut an die Polizeidirektion A. Er schilderte, dass er kürzlich von der Polizei vorgeladen worden sei. Ihm sei in diesem Zusammenhang vorgehalten worden, dass er zu Beginn der 90er Jahre Hausbesetzer gewesen sei und im Jahre 1997 bei einem Ladendiebstahl strafrechtlich in Erscheinung getreten sei. Außerdem sei ihm ein Foto von seiner Person vorgelegt worden. Er bat erneut um Überprüfung, ob und ggf. welche Daten zu seiner Person gespeichert sind.

Eine erneute Überprüfung des Datenbestandes der Polizeidirektion A ergab jedoch wiederum, dass keine Daten zur Person des Betroffenen in Akten oder Dateien vorgehalten werden. Dies wurde dem Betroffenen im Mai 2005 auch nochmals so mitgeteilt.

Daraufhin hat der Betroffene die Polizeidirektion A nochmals angeschrieben und nunmehr mitgeteilt, dass er von einer anderen Polizeidirektion B vorgeladen worden sei. Von den dort ermittlungsführenden Beamten seien ihm die vorstehend genannten Vorhaltungen gemacht wurden. Nach einer ihm in Kopie vorliegenden Mitteilung der Polizeidirektion A habe diese der Polizeidirektion B die Erkenntnisse zu seiner Person mitgeteilt.

Der Landesbeauftragte hat sich nunmehr an die Polizeidirektion A mit der Bitte um Klärung des Sachverhaltes gewandt. Im Ergebnis wurde festgestellt, dass tatsächlich keine polizeilichen Erkenntnisse mehr zur Person des Betroffenen vorgehalten wurden. Aber woher kamen dann die Angaben? Des Rätsels Lösung liegt so nahe, dass man erst einmal darauf kommen muss. Der Beamte der Polizeidirektion A, der die Anfrage zur Person des Betroffenen der Polizeidirektion B bearbeitete, hat die Angaben aus dem Gedächtnis heraus gemacht. Er konnte sich aus seiner Tätigkeit an einzelne Vorkommnisse im Zusammenhang mit der Person des Betroffenen erinnern. Seine Erinnerungen teilte er dann der Polizeidirektion B mit. Der Landebeauftragte konnte gemeinsam mit der Polizeidirektion A die Herkunft der Angaben in der Mitteilung klären.

Rechtmäßig wurden Name, Vorname, Geburtsdatum, Wohnanschrift und ein Lichtbild des Betroffenen übermittelt. Alle diese Angaben entstammen dem Einwohnermelderegister. Die Übermittlung eines Bildes war erforderlich, weil ein Täter anhand einer vorhandenen Videoaufnahme identifiziert werden sollte. Unrechtmäßig wurden die Angaben aus der Vergangenheit des Betroffenen übermittelt. Hierzu wurde die Polizeidirektion A aufgefordert, die Polizeidirektion B entsprechend zu informieren und somit die Verwertung der unzulässig übermittelten Angaben zu verhindern. Gleichzeitig hat die Dienststellenleitung der Polizeidirektion A ihre Beschäftigten nochmals ausdrücklich darauf hingewiesen, dass Mitteilungen aus Erinnerungen heraus zu unterbleiben haben. Mitteilungen an andere Polizeidienststellen dürfen nur Angaben enthalten, die in Akten oder Dateien der Polizei gespeichert sind und deren Mitteilung zulässig ist.

17.9 Elektronisches Polizeirevier

Die Polizei des Landes Sachsen-Anhalt im Internet, das ist nichts Neues. Seit Jahren präsentiert sie sich auch virtuell. Aber am 14. Februar 2005 hat sich die Internetpräsenz der Polizei grundlegend verändert. Denn seit diesem Zeitpunkt dient das Internet der Polizei nicht mehr ausschließlich zur Eigenpräsentation gegenüber den Bürgern. Seit dem 14. Februar 2005 kommuniziert die Polizei auch mit den Bürgern über das Internet. Möglich macht es das elektronische Polizeirevier.

Das elektronische Polizeirevier steht allen Bürgern unter der Internetadresse http://www.polizei.sachsen-anhalt.de zur Verfügung. Neben Informationen zur Polizei des Landes Sachsen-Anhalt, Verkehrsmeldungen, Fahndungsmeldungen usw. können die Bürger hier auch Anzeigen erstatten, Hinweise geben, Fragen stellen, sich beschweren, sich bedanken oder sich bewerben.

Um eine Anzeige zu erstatten, müssen die Bürger ihre persönlichen Daten angeben, den Sachverhalt schildern und das ganze dann über das Internet an die Polizei senden. Um hier ein Höchstmaß an Sicherheit für die Bürger zu gewährleisten, erfolgt die Übertragung zwischenzeitlich verschlüsselt.

Über diese Regelung hinaus nahm der Landesbeauftragte Einfluss auf die zu speichernden Protokolldaten für Zugriffe auf das elektronische Polizeirevier. Ursprünglich beabsichtigte die Polizei nämlich die Speicherung der IP-Adressen aller Besucher. Da es sich bei der IP-Adresse um ein personenbeziehbares Datum handelt und dieses Datum nur erhoben werden darf, wenn es für Abrechnungszwecke erforderlich ist, kam eine Protokollierung aller IP-Adressen unter datenschutzrechtlichen Aspekten nicht in Betracht. Auf Drängen des Landesbeauftragten verzichtete die Polizei gänzlich auf die Protokollierung der IP-Adressen.

18. Rechtspflege

18.1 Gerichtsvollzieher und Medien

Petenten haben sich beim Landesbeauftragten darüber beschwert, dass ein Gerichtsvollzieher unzulässigerweise verschiedene sie betreffende personenbezogene Daten an einen Fernsehsender übermittelt habe. Auch sei diesem Sender die Möglichkeit eingeräumt worden, an einer durch den Gerichtsvollzieher veranlassten Wohnungsöffnung teilzunehmen und dabei zu filmen.
Dem Landesbeauftragten war bereits durch eine fernmündliche Voranfrage beim Ministerium der Justiz bekannt geworden, dass dieses selbst keine Regelung in seinem Geschäftsbereich zum Verhalten von Bediensteten, wie z.B. der Gerichtsvollzieher, gegenüber Presse und anderen Medien getroffen hat. Nachdem das Ministerium der Justiz darüber informiert hatte, dass aufgrund dieses Vorfalls bereits eine Auswertung zu dieser Problematik mit dem Oberlandesgericht erfolgt sei, bat der Landesbeauftragte das Amtsgericht um Angaben zu eventuell dort getroffenen generellen Regelungen.
Der dann folgende Schriftverkehr mit dem zuständigen Amtsgericht nahm einen erstaunlichen Verlauf.
So wurde vom aufsichtsführenden Gericht zunächst berichtet, der Gerichtsvollzieher habe versichert, dass die Betroffenen in Aufnahmen eingewilligt hätten. Nachdem klargestellt war, dass dies nicht den Tatsachen entsprach und die Betroffenen zudem am Tag der Wohnungsöffnung nicht anwesend gewesen waren, wurde in einem neuerlichen Bericht dargestellt, dass das Filmteam nur unter einem „strengen Prozedere“ Aufnahmen hätte machen dürfen. Auf erneute Nachfrage wurde dazu erläutert, dass keine Namensschilder im Film sichtbar sein würden.
Der Landesbeauftragte sah daher die Notwendigkeit, auf die grundsätzlichen Gesichtspunkte dieses Sachverhalts hinzuweisen. So ist bereits die Information an

das Fernsehteam, bei wem vollstreckt werden soll, eine Übermittlung personenbezogener Daten und deswegen problematisch, weil das Fernsehteam, datenschutzrechtlich betrachtet, privater Dritter ist. Die datenschutzrechtlich bedeutsame Übermittlung personenbezogener Daten ist jede ausdrückliche oder konkludente Weitergabe der Information über Betroffene an das Fernsehteam, nicht erst die darauf folgende Weitergabe der durch die Filmaufnahmen erlangten visuellen und anderen Informationen an ein zahlenmäßig unbestimmtes Publikum.

Auf wiederholte Nachfrage hin wurde schließlich eine dienstliche Erklärung des Gerichtsvollziehers vorgelegt, dass er dem anwesenden Fernsehteam weder vor noch während der Vollstreckungshandlungen Hinweise auf die Identität des Schuldners gegeben habe. Wie er die zwangsläufig damit einhergehende Kenntnisnahme der Schuldnerdaten einschätzt, wurde dadurch nicht deutlich. Das um Klärung gebetene Ministerium der Justiz teilte schließlich mit, dass der Gerichtsdirektor den Vorfall mit den Gerichtsvollziehern seines Bezirks unter Berücksichtigung der Rechtsauffassung des Landesbeauftragten, welche geteilt werde, ausgewertet habe. Auch die Leitung der Presse- und Öffentlichkeitsarbeit des Ministeriums der Justiz sei über die besondere Problematik, die sich an diesem Fall der Berichterstattung über die Arbeit der Gerichtsvollzieher exemplarisch zeige, unterrichtet.
In Bezug auf vergleichbare Sachverhalte sei vor der möglichen Dokumentation von hoheitlichen Maßnahmen das Einverständnis der Betroffenen einzuholen. Etwas anderes gelte dann, wenn die Presse aus eigenen Recherchen Kenntnis von bevorstehenden Maßnahmen erlange und diese durch vor Ort gewonnenes Bildmaterial dokumentiere. Dies sieht der Landesbeauftragte ebenso. Ein ähnlicher Vorfall dürfte sich bei Beachtung dieser Vorgaben folglich nicht wiederholen.

Das nach Strafanzeigen der Petenten gegen den Gerichtsvollzieher eingeleitete Strafverfahren ist eingestellt worden, da die Ermittlungen der Staatsanwaltschaft keinen genügenden Anlass zur Erhebung der öffentlichen Klage ergaben.
Letztlich konnte, insbesondere wegen der angemessenen Auswertung des Vorfalls durch den Direktor des Amtsgerichts, auf eine förmliche Beanstandung verzichtet werden.

18.2 Kontrolle bei Staatsanwaltschaften zu Telekommunikationsüberwachungsmaßnahmen (TKÜ); eine Fortsetzung

Im vorherigen VII. Tätigkeitsbericht (Ziff. 18.5) hat der Landesbeauftragte von den Kontrollen dieser verdeckten Maßnahmen berichtet. Nachdem der kontrollierten Behörde die Feststellungen des Landesbeauftragten mit der Bitte um Stellungnahme mitgeteilt worden waren, wurde diese über den Dienstweg von der Generalstaatsanwaltschaft ohne weitere inhaltliche Äußerungen an ihn weitergeleitet. Wenn denn der Bericht dem Landesbeauftragten schon nicht direkt von der verantwortlichen Stelle zugeleitet wird, wäre - zumindest vorliegend - eine grundlegende Äußerung der vorgesetzten Dienststelle zur weiteren Verfahrensweise im Lande vor allem hinsichtlich des Umgangs mit aus einer TKÜ gewonnenen Unterlagen angezeigt gewesen.

Nachdem der Landesbeauftragte hierauf hingewiesen hatte, ging ihm Ende 2005 schließlich eine überwiegend zufriedenstellende Antwort der Generalstaatsanwaltschaft zu.

So sei mit den Leitern der Staatsanwaltschaften und den Zweigstellenleitern erörtert worden, dass die Vernichtungsregelung in § 100b Abs. 6 StPO genauestens zu beachten sei. Insbesondere sei nicht mehr benötigtes Material unverzüglich zu vernichten, gleich um welche Datenträger es sich handele. Der Landesbeauftragte geht daher davon aus, dass dieses künftig zeitgerecht und - wie vorgeschrieben - unter staatsanwaltschaftlicher Aufsicht erfolgt.

In der genannten Besprechung des Generalstaatsanwalts sei auch unter Bezugnahme auf die Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff Einigkeit erzielt worden, dass weder die Antworten auf Vorhalte aus Akten noch solche Angaben aus der TKÜ zu vernichten sind, welche Eingang in die Akten gefunden hätten und sich auf den Verfahrensgegenstand bezögen. Habe ein Datum nichts mit dem Verfahrensgegenstand zu tun, so sei es auch dann zu vernichten, wenn es Aktenbestandteil geworden sei. Der Landesbeauftragte teilt diese Auffassung.

Auch der Äußerung des Generalstaatsanwalts hinsichtlich der Benachrichtigung der in § 101 StPO bezeichneten Personen kann er teilweise zustimmen. In dieser Bestimmung wird festgelegt, dass bestimmte Personen von den getroffenen Maßnahmen, wie z.B. einer TKÜ, im Nachhinein unter bestimmten Voraussetzungen zu benachrichtigen sind. Das Gesetz spricht in § 101 StPO nicht von „Betroffenen“ wie das Datenschutzrecht, sondern von Beteiligten. Der Landesbeauftragte teilt die Auffassung, dass der Gesetzgeber den Begriff des „Beteiligten“ mit Bedacht gewählt hat. Angesichts der Bedeutung des Grundrechts auf informationelle Selbstbestimmung kann jedoch nicht unterstellt werden, dass damit nur derjenige gemeint wäre, gegen den sich die TKÜ richtet. Wesentlicher Beweggrund des Gesetzgebers zur veränderten Begriffswahl war nicht, die Benachrichtigungspflicht ausschließlich auf jene zu beschränken, gegen die sich die TKÜ-Maßnahme aufgrund der vorausgegangenen gerichtlichen oder staatsanwaltschaftlichen Entscheidung schon unmittelbar richtet. Ausschlaggebend war vor allem, dass der bereits vorhandene Eingriff in die Grundrechte weiterer Betroffener durch eine Benachrichtigung nicht noch vertieft werden darf. Dies könnte z.B. geschehen, wenn nur zum Zwecke der Benachrichtigung Ermittlungen durchgeführt werden müssten - etwa um die Anschrift Betroffener zu erlangen.

Der Landesbeauftragte verweist nachdrücklich darauf, dass das Bundesverfassungsgericht immer wieder deutlich gemacht hat, dass die Möglichkeit, Rechtsschutz beanspruchen zu können, zu den wesentlichen grundrechtssichernden Verfahrensschritten gehört (z.B. BVerfGE 100, 313 (361), NJW 2000, 55). Der mit dem Grundrecht auf informationelle Selbstbestimmung verbundene Anspruch auf Rechtsverfolgung ist nicht auf den gerichtlichen Schutz beschränkt, sondern kann sich auch im Recht auf Löschung oder Berichtigung realisieren (Beschluss vom 25. April 2001, 1 BvR 1104/92, Abs. Nr. 63, NJW 2002, 1037).

Diese Optionen können indessen nur genutzt werden, wenn Betroffene eine Information über sie berührende, verdeckt durchgeführte Maßnahmen erhalten. Wenn, wie bei der TKÜ, die Datenerhebung nicht offen erfolgt, ist die Benachrichtigung Betroffener „besonders bedeutsam“ (BVerfG, a.a.O., Abs. Nr. 60). Daher kann der Verzicht auf eine Benachrichtigung nur im Einzelfall und aufgrund einer nachvollziehbaren sowie zu dokumentierenden Begründung akzeptiert werden.

Da im Gesetz nicht vorgesehen ist, u.U. die Grundrechte verschiedener Betroffener gegeneinander abzuwägen, bleibt im Falle einer vermuteten Rechtekollision nur die Prüfung, ob eine Benachrichtigung aus Gründen der Verhältnismäßigkeit unterbleiben muss. Auch dies wäre zu dokumentieren. Ob dafür der Hinweis auf eine unvertretbare Personalbindung, wie von der Generalsstaatsanwaltschaft bemerkt, ausreicht, erscheint angesichts der Grundrechtsbedeutsamkeit fraglich.
Ob die vorgesehene Neuregelung zu verdeckten Maßnahmen nach der StPO auch insoweit Klarstellungen erbringen kann (vgl. Ziff. 18.3), wird ggf. im nächsten Tätigkeitsbericht darzustellen sein.

18.3 Telekommunikations- und andere verdeckte Überwachungsmaßnahmen - Neuregelung und die Absicht heimlicher Online-Durchsuchung

Der Landesbeauftragte hatte bei Kontrollen von Telekommunikationsüberwachungsmaßnahmen Defizite u.a. bei der nachträglichen Benachrichtigung der von solchen Maßnahmen Betroffenen festgestellt. Dies deckte sich mit Feststellungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht in einem Gutachten zur Telekommunikationsüberwachung für das Bundesministerium der Justiz aus dem Jahre 2003 (siehe VII. Tätigkeitsbericht, Anlage 13).

Nachdem das Bundesverfassungsgericht die akustische Wohnraumüberwachung, den sog. Großen Lauschangriff, in weiten Teilen für verfassungswidrig erklärt hatte (vgl. VII. Tätigkeitsbericht, Ziff. 18.2), verabschiedete der Bundestag im Juni 2005 eine Neuregelung (vgl. dazu Beschluss des Bundesverfassungsgerichts vom 11. Mai 2007, 2 BvR 543/06).
Nunmehr darf Wohnraum im Rahmen strafrechtlicher Ermittlungen nur noch überwacht werden, wenn aufgrund tatsächlicher Anhaltpunkte davon auszugehen ist, dass bei der Überwachung Äußerungen, die dem **Kernbereich privater Lebensgestaltung** zuzurechnen sind, nicht erfasst werden. Die Maßnahme ist unverzüglich zu unterbrechen, soweit sich während der Durchführung der Maßnahme doch Anhaltspunkte für Äußerungen aus dem Kernbereich privater Lebensgestaltung ergeben. Daher müssen bei der Überwachung von Privatwohnungen Gespräche regelmäßig live mitgehört werden, damit die gesetzlichen Vorgaben in der Praxis tatsächlich eingehalten werden können.
Wie von den Datenschutzbeauftragten des Bundes und der Länder bereits gefordert, hat der Gesetzgeber außerdem eine Kennzeichnungspflicht für die durch eine strafprozessuale Wohnraumüberwachung erlangten Daten eingeführt. Nur dadurch kann die strikte Zweckbindung der Verwendung dieser Daten und ihre Löschung gesichert werden, sobald sie für das jeweilige Verfahren nicht mehr erforderlich sind.

Am 27. Juli 2005 traf das Bundesverfassungsgericht eine Entscheidung zum präventiven Telekommunikationsangriff nach dem niedersächsischen Polizeigesetz (BVerfGE 113, 348). Wie zuvor in der Entscheidung zur Wohnraumüberwachung, stellte das Gericht auch hier das Fehlen hinreichender Vorkehrungen zur Vermeidung von Eingriffen in den absolut geschützten Kernbereich privater Lebensgestaltung fest. Auch aus diesem Urteil wurde letztlich deutlich, dass eine umfassende Neuregelung verdeckter Maßnahmen im Sicherheitsrecht wie im Strafprozessrecht notwendig ist, welche u.a. verfahrensbezogene Regelungen zur Siche-

rung der Rechte Betroffener enthalten müsste. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dies aufgegriffen und in einer Entschließung zum „Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden“ (**Anlage 5**) eine Neuregelung der entsprechenden gesetzlichen Ermächtigungen gefordert.

In der Koalitionsvereinbarung auf Bundesebene haben die beteiligten Parteien der Großen Koalition im November 2005 festgelegt, dass sie die Regelungen zur Telekommunikationsüberwachung in der Strafprozessordnung im Sinne einer harmonischen Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen überarbeiten wollen.
Nachdem die Datenschutzbeauftragten auf Arbeitsebene schon vorab grundlegende Informationen zu einem entsprechenden Gesetzentwurf erhalten hatten, wurde Ende 2006 ein Referentenentwurf zur Änderung der entsprechenden strafprozessualen Regelungen vorgelegt, der eng an den Entscheidungen des Bundesverfassungsgerichts dessen Vorgaben umzusetzen sucht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich in ihrem Arbeitskreis Justiz mit dem Entwurf befasst und nach abschließender Beratung in der Tagung der Konferenz am 8./9. März 2007 u.a. festgestellt, dass vor allem die vorgesehene Kernbereichsregelung ungenügend ist.
So werde in Kauf genommen, dass regelmäßig kernbereichsrelevante Informationen erfasst werden. Stattdessen sollte grundsätzlich ein Erhebungsverbot gelten. In zweiter Linie müsste dann für dennoch erlangte Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung ein absolutes Verwertungsverbot gelten.
Ein Verwertungsverbot sollte zudem nicht auf Strafverfahren begrenzt bleiben.
Im Gesetz selbst sei zudem festzulegen, wann die Polizei das Abhören abbrechen müsse und in welchen Fällen Informationen zwar gewonnen, aber nicht für die Ermittlungen verwertet werden dürfen.
Im bis zum Ende des Berichtszeitraums bekannten Gesetzentwurf (BR-Drs. 275/07) ist ein Erhebungsverbot nur dann vorgesehen, wenn ein Gespräch absehbar ausschließlich dem Kernbereich privater Lebensgestaltung zuzurechnen ist. In der Praxis bedeutet dies, dass regelmäßig kernbereichsbedeutsame Informationen erfasst werden. Diese Regelung ist mit den Vorgaben des Bundesverfassungsgerichts nicht vereinbar (Entschließung „Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen“, **Anlage 20**; siehe zur Vorratsdatenspeicherung Ziff. 23.1). Entsprechendes gilt im Übrigen für den Entwurf des Zollfahndungsdienstgesetzes (BT-Drs. 16/4663).
Regelungen, durch welche im Gesetz selbst definiert wird, wann Abhörmaßnahmen abzubrechen sind und in welchen Fällen Informationen zwar gewonnen, aber nicht für die Ermittlungen verwertet werden dürfen, müssen für alle verdeckten Maßnahmen geschaffen werden.

Kurz nach Vorlage des Gesetzentwurfs zur Neuregelung strafprozessualer Maßnahmen wurde eine weitere verdeckte Eingriffsmethode in die Diskussion eingebracht. Dieser neueste Angriff auf die Grundrechte der Bürgerinnen und Bürger stellt sich als Absicht der Sicherheitsbehörden dar, staatliches „hacking“, d.h. das

heimliche Eindringen in Computersysteme z.B. mit „Trojanern“, erlauben zu wollen.
Der Bundesgerichtshof hat in seiner Entscheidung vom Januar 2007 (Beschluss vom 31. Januar 2007, StB 18/06, NJW 2007, 930, der den Beschluss des Ermittlungsrichters des BGH vom 25. November 2006, 1 BGs 184/2006, bestätigte) die Auffassung der Datenschutzbeauftragten bestätigt, dass solche **heimlichen Online-Durchsuchungen** im Bereich der Strafverfolgung rechtswidrig sind. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung heimlicher Durchsuchung und Ausforschung privater Computer herangezogen werden. Der Landesbeauftragte wendet sich nachdrücklich gegen die Einführung von Eingriffsgrundlagen, welche solche Maßnahmen erlauben würden – gleichgültig ob im repressiven oder auch im präventiven Bereich. Mit den anderen Datenschutzbeauftragten des Bundes und der Länder unterstreicht er dies in einer Entschließung („Keine heimliche Online-Durchsuchung privater Computer“, **Anlage 19**).
Wie die öffentlichen Äußerungen aus der Politik in der folgenden Zeit deutlich machten, ist zwar das Bundesministerium des Innern der Auffassung, dass die Regelungen in den Gesetzen für die Nachrichtendienste so im BVerfSchG, BNDG, MADG bereits aktuell den Einsatz von „Regierungs-Trojanern“ erlauben. Da diese Auffassung aber umstritten ist, wird auch über eine Verfassungsänderung nachgedacht. Der Landesbeauftragte seinerseits befragte das Ministerium des Innern nach seiner rechtlichen Meinung zur bestehenden Rechtslage beim Verfassungsschutz in Sachsen-Anhalt. Laut dessen Auskunft werden solche Maßnahmen derzeit nicht durchgeführt.

Da von Sicherheitspolitikern so vehement weitergehende „Anpassungen“ der Gesetzeslage gefordert werden, weist der Landesbeauftragte darauf hin, dass das Bundesverfassungsgericht im Beschluss zum IMSI-Catcher (Beschluss vom 22. August 2006, 2 BvR 1345/03; NJW 2007, 351) den Gesetzgeber nicht nur aufgefordert hat, im Zusammenhang mit der Neuregelung verdeckter Maßnahmen zu prüfen, ob verfahrensrechtliche Vorkehrungen wie Benachrichtigungspflichten oder Rechtsschutzmöglichkeiten zu erweitern sind. Es sieht den Gesetzgeber vor allem auch in die Pflicht genommen, sich regelmäßig die Frage zu stellen, ob von neuerlichen Ausdehnungen heimlicher Ermittlungsmethoden, vor allem im Hinblick auf die Grundrechtspositionen unbeteiligter Dritter (also des größten Teils der Bevölkerung), Abstand zu nehmen ist.
Die Beachtung dieser Vorgabe hält der Landesbeauftragte nicht nur in der strafrechtlichen Gesetzgebungskompetenz des Bundes, sondern vor allem im gefahrenabwehrenden Zuständigkeitsbereich des Landesgesetzgebers für unabdingbar.

18.4 Auskunft aus den Dateien der Staatsanwaltschaft

Vor nunmehr über vier Jahren hatte der Landesbeauftragte beim Ministerium der Justiz die Praxis der Auskunftserteilung aus staatsanwaltschaftlichen Informationssystemen erfragt. Erst im Zusammenhang mit Einzelfällen, die sich inhaltlich um die nachträgliche Information von Personen rankten, welche sich von einer verdeckten Maßnahme betroffen glaubten, ging schließlich - nach einigem erneuten Hin und Her - Anfang 2007 eine Antwort des Generalstaatsanwalts ein, wel-

che an Kürze und Prägnanz kaum zu überbieten ist: „Auskunftsanträge werden aufgrund einer Einzelfallentscheidung entschieden."
Zum Hintergrund: Mit dem Strafverfahrensänderungsgesetz 1999 wurden Regelungen für staatsanwaltschaftliche Dateien in die Strafprozessordnung (StPO) eingeführt und den Betroffenen in den §§ 491, 495 StPO ein Auskunftsrecht entsprechend § 19 BDSG gegeben. Mit Gesetz vom 10. September 2004 wurde diese Regelung hinsichtlich des Zeitpunkts, wann innerhalb des Strafverfahrens eine Auskunft an nicht verfahrensbeteiligte Betroffene erteilt werden dürfte, modifiziert. Das grundsätzliche Recht auf Auskunft wurde dadurch jedoch nicht berührt. Die im Gesetz bereits vorgegebenen Begrenzungen zur inhaltlichen Qualität einer solchen Auskunft wurden zudem nicht verändert. Beim Landesbeauftragten war, nach entsprechenden Äußerungen aus dem staatsanwaltschaftlichen Bereich, gleichwohl der Eindruck entstanden, dass inhaltliche Auskünfte prinzipiell nicht erteilt werden.
Gegen eine Verfahrensweise, welche jegliche Auskünfte, eine generelle Ausforschungsabsicht unterstellend, ablehnt, bestehen wesentliche Bedenken.
Eine nicht am Einzelfall orientierte Entscheidung würde dem Gesetz nicht entsprechen, welches den Betroffenen grundsätzlich einen Anspruch auf Auskunft einräumt, sofern dem nicht im Einzelfall die im Gesetz genannten Gründe entgegenstehen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss. Das Vorliegen dieser Voraussetzungen ist in jedem Einzelfall vor einer Auskunftsablehnung zu prüfen. Eine durchgängige Auskunftsverweigerung würde zudem der besonderen Bedeutung des Auskunftsrechts für die individuelle Entfaltung des Einzelnen (vgl. BVerfGE 65, 1 ff., 42 f.) nicht gerecht. Die Auskunftserteilung ist Voraussetzung für eventuelle Ansprüche auf Berichtigung, Löschung oder Schadensersatz, die ohne Kenntnis von einer Speicherung gar nicht wahrgenommen werden könnten. Eine Auskunftsverweigerung ist auch nicht mit der Begründung zu rechtfertigen, in allen zur Auskunftsverweigerung vorgesehenen Fällen müsse generell vom Vorliegen von Ablehnungsgründen ausgegangen werden. Dies gilt vor allem nicht in jenen Fällen, in denen keine Speicherungen vorhanden sind. Dem kann auch nicht in jedem Fall entgegengehalten werden, dass gerade auch die Mitteilung, dass keine Speicherungen vorhanden sind, künftige Ermittlungen gefährden könnte. Das Bundesverfassungsgericht hat es als unzulässig erachtet, dass zur Vermeidung einer Ausforschung die Auskunft schematisch, auch bei Fehlen jeglicher Daten, verweigert wird, um so Rückschlüsse auf eine mögliche Datenspeicherung durch die Differenzierung zwischen Negativauskunft und Auskunftsverweigerung zu vereiteln (vgl. 1 BvR 586/90, Beschluss vom 10. Oktober 2000, Abs. Nr. 12, 15, 17). Die Auskunft dürfe nur aufgrund einer konkreten Einzelfallentscheidung verweigert werden. Die Verweigerung müsse prinzipiell auch begründet werden. Eine bloße Wiederholung des Gesetzestextes oder der pauschale Verweis auf eine Gefährdung des Zwecks des Auskunftsverweigerungsrechts wäre hierbei nicht ausreichend.

Im eingangs erwähnten Schreiben weist der Generalstaatsanwalt abschließend darauf hin, dass ein Grundsatz, wonach inhaltliche Auskunft nicht erteilt werde, als solcher bei den Staatsanwaltschaften nicht bestehe.
Der Landesbeauftragte nimmt dies mit einem gewissen Erstaunen zur Kenntnis. Hatte doch die gleiche Behörde, im Zusammenhang mit den oben erwähnten Ein-

zelfällen bei verdeckten Maßnahmen, über eine von ihr an die nachgeordneten Dienststellen gerichtete Verfügung berichtet, nach der eine grundsätzlich gleichmäßige Handhabung der Antwort an Betroffene zu gewährleisten sei, nämlich: inhaltliche Nichtinformation. Warum sollte dies von den nachgeordneten Dienststellen in Bezug auf Auskunftsersuchen aus staatsanwaltschaftlichen Informationssystemen anders wahrgenommen werden?

Der Landesbeauftragte geht davon aus, dass die vom Generalstaatsanwalt mitgeteilte Verfahrensweise, im Einzelfall über Auskunftsanträge zu entscheiden, unter Berücksichtigung der verfassungsrechtlichen Vorgaben in die Praxis umgesetzt wird.

18.5 Handakten der Staatsanwaltschaft... wie auch anderer Dienststellen

Der Landesbeauftragte bat die Generalstaatsanwaltschaft um Mitteilung, wie mit Anträgen von Betroffenen auf Einsicht in bzw. Auskunft aus staatsanwaltschaftlichen Handakten verfahren wird.
Betroffene können nach seiner Auffassung gem. § 15 DSG-LSA einen Antrag auf Auskunft an die betreffende Staatsanwaltschaft richten, welche unter Berücksichtigung der Vorgaben in § 15 DSG-LSA über dieses Auskunftsersuchen zu entscheiden hat. Als Betroffene kommen vor allem Personen in Betracht, die nicht als Beschuldigte Verfahrensbeteiligte sind; Beschuldigte haben i.d.R. kein Interesse an einer Auskunft aus Handakten, sondern an jenen Akten, welche dem Gericht vorliegen oder im Falle der Anklage diesem vorzulegen wären; § 147 Strafprozessordnung (StPO). Bezüglich dieser Ermittlungsakten gelten die Bestimmungen der StPO. Nur soweit Unterlagen keinen Eingang in die Ermittlungsakten gefunden hätten und noch in einer Handakte vorgehalten würden, wäre auf das DSG-LSA zurückzugreifen, denn in Bezug auf diese „Arbeitsakten“ besteht keine spezielle gesetzliche Regelung.
Da aus dem Antwortschreiben an den Landesbeauftragten entnommen werden konnte, dass mehrfach Auskunftsersuchen zu staatsanwaltschaftlichen Handakten an den Geschäftsbereich des Ministeriums der Justiz herangetragen worden waren, hat er darum gebeten, ihn zur Häufigkeit solcher Anträge und den hierzu getroffenen Entscheidungen der Staatsanwaltschaft zu informieren. Entgegen seiner Erwartung konnten weitere Fälle indessen nicht berichtet werden. Unabhängig hiervon zeigte sich eine Diskrepanz zur Justiz über die rechtliche Grundlage eines Auskunftsanspruchs in Bezug auf Handakten, die sich nach Auffassung des Landesbeauftragten aus § 15 DSG-LSA ergibt. Der Justizbereich ging stattdessen davon aus, dass Auskunftsrechte nur nach den Regeln der StPO geltend gemacht werden könnten. Eine Auskunft aus Handakten sei dort nicht geregelt, ergo nicht möglich. Die Bestimmungen der StPO (z.B. § 475 StPO) zur Akteneinsicht beziehen sich aber nach Auffassung des Landesbeauftragten nur auf die Ermittlungsakten. Dass, bezogen auf diese Akten, die StPO eine abschließende Regelung trifft, sieht der Landesbeauftragte genauso.
Allerdings handelt es sich bei den Handakten gerade nicht um Ermittlungsakten, sondern um sonstige Vorgänge, die personenbezogene Daten enthalten können, aber nicht müssen. Dass sich Kopien aus den Ermittlungsakten in diesen Handakten befinden, ist wahrscheinlich. Dies widerspricht jedoch nicht der Anwendung

der allgemeinen Auskunftsregelungen, da durch Aufnahme dieser Kopien die Handakten nicht zu Ermittlungsakten nach der StPO werden.
Durch die grundsätzliche Akzeptanz des Auskunftsrechts ist eine Umgehung der StPO-Regelungen zur Akteneinsicht - wie von staatsanwaltschaftlicher Seite befürchtet - ebenso wenig zu erwarten, wie die Gefährdung von Rechten Dritter. Denn die handaktenführende Staatsanwaltschaft darf die Auskunft, u.U. auch ohne Begründung, verweigern (§ 15 Abs. 4, 5 DSG-LSA). Auch der als Beleg der eigenen Auffassung vom Ministerium der Justiz herangezogene Beschluss des BGH (vom 27. April 2001, Az: 3 StR 112/01, NStZ 2001, 551) führt in die Irre, weil dieser sich in seiner Begründung letztlich doch nur auf jene Akten bezieht, für die unbestritten die StPO Anwendung findet, nämlich Ermittlungsakten.

Die zu staatsanwaltlichen Handakten geführte Auseinandersetzung hat Bedeutung auch für vergleichbare Datensammlungen anderer Behörden, welche typischerweise als Arbeitsakten der Bearbeitenden geführt werden – gleich ob Justiz-, Polizei- oder Verwaltungspersonal solche Vorgänge anlegt. Die diesen Arbeitsakten beigefügten Papiere mit personenbezogenen Daten unterliegen dem DSG-LSA auch dann, wenn diese Akten keine Aktennummer erhalten und nur im Schreibtisch des Bearbeiters abgelegt sind – es gibt unter Geltung des Rechtsstaatsprinzips keine dienstlichen „Privatakten“. Ganz im Gegenteil: Würden solche Akten quasi sakrosankt, könnten dort unliebsame Blätter aus anderen Vorgängen „gesichert“ werden.
Der Sachverhalt „Handakten“ ist nicht neu und deckt sich weitgehend mit dem Problem der Duplikat-Akten, mit welchem der Landesbeauftragte bereits befasst war (vgl. II. Tätigkeitsbericht, Ziff. 20.11). Auch wenn es sich ausdrücklich so nicht äußert, scheint das Ministerium der Justiz dies jedoch insgesamt ähnlich einzuschätzen, als es bereits zur Problematik der Duplikat-Akten (II. Tätigkeitsbericht, Ziff. 20.11) dargelegt hatte, dass die StPO zum Umgang mit diesen Akten keine Regelung treffe (sic!).

Im abschließenden Schreiben des Ministeriums der Justiz zur Problematik der Handakten wird zwar das in § 15 DSG-LSA geregelte Auskunftsrecht nicht wörtlich in Bezug genommen, aber festgestellt, dass Auskunft ausnahmsweise möglich sei, wenn ein berechtigtes Interesse an der Auskunft dargelegt sei und sonst keine Bedenken bestünden - dies entspricht im Kern dem Regelungsgehalt des Auskunftsrechts nach dem allgemeinen Datenschutzrecht und dem allgemein anerkannten Anspruch von Antragstellern, dass über ein Auskunftsbegehren nach pflichtgemäßem Ermessen zu entscheiden ist. Zudem wird, ohne es zu benennen, eine Entscheidung des Bundesverfassungsgerichts aus neuerer Zeit aufgegriffen. Dieses stellt unter Hinweis darauf, dass nicht alle Daten Bestandteil der dem vorrangigen Auskunftsrecht gem. § 475 StPO unterliegenden Ermittlungsakten werden, fest, dass hinsichtlich unbeteiligter Drittbetroffener ggf. auf den datenschutzrechtlichen Auskunftsanspruch zurückzugreifen ist (Beschluss vom 12. April 2005, 2 BvR 1027/02, Abs. Nr. 130, NJW 2005, 1917).

Der Landesbeauftragte geht davon aus, dass diese Auffassung Eingang auch in die staatsanwaltschaftliche Praxis beim Umgang mit Handakten findet.

18.6 Aktenaufbewahrungsgesetz

Die Datenschutzbeauftragten des Bundes und der Länder fordern seit Jahren (Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich vom 9./10. März 1995, II. Tätigkeitsbericht, Anlage 15) eine gesetzliche Grundlage für die Aufbewahrung, Löschung etc. von Akten und Dateien in der Justiz. Bis heute richtet sich die Justiz nach den sog. Aufbewahrungsbestimmungen, welche nichts anderes sind als Verwaltungsvorschriften. Als Grundlage für z.T. erhebliche Speicherungsfristen sind sie z.B. immer dann nicht ausreichend, wenn eine spezialgesetzliche Regelung fehlt.
Ein Gesetzentwurf des Bundes zu einer einheitlichen Normierung wurde, nachdem das Bundesverfassungsgericht in einem anderen Sachgebiet die Länderzuständigkeit hervorgehoben hatte, wegen möglicherweise vergleichbarer Situation aus kompetenzrechtlichen Gründen zusammengestrichen. Nunmehr verfügt zwar der Bund über ein Gesetz (Schriftgutaufbewahrungsgesetz, Art. 11 des Justizkommunikationsgesetzes, BGBl. 2005 I, S. 837, 852), auch wenn dieses letztlich nur eine Ermächtigung enthält, eine Verordnung über die Aktenaufbewahrung zu erlassen, also wesentliche Bedingungen zur Festlegung von Speicherfristen usw. nicht selbst trifft. Das Land Sachsen-Anhalt hat jedoch nach wie vor nichts Vergleichbares. Zwar wurde von einem Land federführend für die anderen ein Entwurf gefertigt, zu welchem sich der Arbeitskreis Justiz der Datenschutzbeauftragten des Bundes und der Länder auch äußern konnte. Aber dieser Entwurf ist qualitativ nicht umfänglicher als das Bundesgesetz und lässt ebenfalls noch nicht einmal ahnen, wie die inhaltliche Ausgestaltung in einer Rechtsverordnung aussehen könnte. Hinzu kommt, dass nunmehr seit Monaten „Funkstille“ herrscht und bis zum Ende des Berichtszeitraums weder ein auf dem Entwurf basierendes Landesgesetz noch ein adäquater Verordnungsentwurf in Sicht ist. Auch auf Bundesebene gibt es - trotz eines entsprechenden Gesetzes - noch keinen Entwurf einer die Details regelnden Verordnung. Der Landesbeauftragte hat daher die Sorge, dass selbst, wenn denn in absehbarer Zeit vielleicht ein Landesgesetz beschlossen worden sein könnte, trotzdem mit den bereits genannten Verwaltungsvorschriften langfristig „weitergewerkelt“ wird. Er hält es daher für sinnvoll, dass die Landesregierung im Zuge der Diskussion zum Aktenaufbewahrungsgesetz des Landes nicht nur die Grundzüge der vorgesehenen Verordnungsregelungen deutlich werden lässt, sondern Vorbereitungen trifft, dass nach Inkrafttreten des Gesetzes die Verordnung umgehend erlassen werden könnte.

Dass dieses Rechtssetzungsvorhaben angegangen werden muss, bestätigte auch eine Beschwerde beim Landesbeauftragten.
Der Petent hatte darauf hingewiesen, dass seine personenbezogenen Daten, die im Rahmen eines im allgemeinen Register (AR-Register) aufgenommenen Vorgangs im EDV-System EUREKA gespeichert worden waren, weit über den Zeitraum der Erforderlichkeit hinaus noch vorhanden waren. In diesem AR-Register werden Vorgänge wie z.B. Anfragen um Aktenübersendungen von anderen Gerichten zu dort geführten Verfahren digital erfasst. In den bereits genannten Aufbewahrungsbestimmungen sind als Maximalfrist in der Regel zwei Jahre für solche Vorgänge, wie z.B. die genannten Aktenanforderungen von anderen Gerichten, vorgesehen. Allerdings bestand im konkreten Einzelfall, nachdem die Akte

wieder beim versendenden Gericht eingegangen war, keine Notwendigkeit zur Speicherung von personenbezogenen Daten aus dem anderen Verfahren mehr; zumal die Anforderung als solche regelmäßig sowohl in der angeforderten als auch der „anfordernden“ Akte dokumentiert ist. Dass das EDV-System entsprechend seiner Programmierung in einem solchen Fall automatisiert eine Maximalfrist vorgibt, genügt rechtsstaatlichen Ansprüchen nicht. Das Ausschöpfen von Fristen ohne Einzelfallfestlegung ist unzulässig, da die gesetzlichen Regelungen des DSG-LSA Speicherungen von personenbezogenen Daten nur erlauben, solange sie erforderlich sind.

18.7 Schülergerichte

Wie der Landesbeauftragte Zeitungsmeldungen entnehmen konnte, beabsichtigt das Ministerium der Justiz, im Land Teen-Courts, auch Schülergerichte oder Schülergremien genannt, einzuführen. Schülerinnen und Schüler sollen über Gleichaltrige „richten“.
Die Tätigkeit der Gremien ist im staatsanwaltschaftlichen Ermittlungsverfahren angesiedelt. Diese sollen in solchen Fällen von Jugendkriminalität aktiv werden, in denen eine Beendigung eines Strafverfahrens ohne Anklageerhebung bzw. Urteil möglich erscheint. Dabei sollen die Schülergerichte Gespräche mit den strafrechtlich auffälligen Jugendlichen führen und daraufhin Maßnahmen vorschlagen, welchen die Beschuldigten nachkommen müssen.

Aus datenschutzrechtlicher Sicht könnten auf den ersten Blick bereits Zweifel an der Verhältnismäßigkeit eines Schülergerichtsverfahrens begründet sein. Denn als Rechtsgrundlage zur Übermittlung von im Ermittlungsverfahren gewonnen Daten zu Tat, Täter und seiner Persönlichkeit sowie seinen Sozialbezügen soll ausschließlich eine Einverständniserklärung der Beschuldigten und der Erziehungsberechtigten zur Teilnahme am Schülergerichtsverfahren und der Akzeptanz der Entscheidung des Schülergerichts dienen. Auch wenn die Mitglieder des Schülergerichts - wie das Ministerium der Justiz mitteilt - selbst keine Akteneinsicht erhalten sollen, dürften Daten aus den Ermittlungsakten Eingang in das Verfahren finden, da die Akten wohl zum Schülergerichtsverfahren „beigezogen“ werden. Denn die Ermittlungsakten sollen, nachdem der Delinquent die Maßnahme akzeptiert hat, der Staatsanwaltschaft wieder zugeleitet werden, was zunächst bedeutet, dass sie beim Schülergerichtsverfahren genutzt wurden.
Die situativ bedingte relative Freiwilligkeit der Einverständniserklärung zum Verfahren vor den Schülergerichten begründet die Zweifel an ihrer Eignung als alleiniger rechtlicher Handlungsgrundlage. Die Ausgestaltung des Verfahrens und der Inhalt der Einverständniserklärung werden, nachdem detailliertere Informationen vom Ministerium der Justiz vorliegen, daher noch genauer zu betrachten sein.

Zweifel bestehen auch daran, dass die Verschwiegenheit der Schülerrichterinnen und -richter rechtlich verbindlich gewährleistet werden kann. Nicht umsonst sind in rechtlich vergleichbaren Verpflichtungserklärungen, z.B. zur Mitwirkung bei der Feuerwehr oder im Katastrophenschutz, wirksame Willensbekundungen erst mit Eintritt der vollen Geschäftsfähigkeit möglich.
Auch wenn, so das hiesige Ministerium der Justiz, aus Bayern, wo dieses Verfahren bereits modellhaft versucht wird, bestätigt wird, es seien bislang keine Prob-

leme in der praktischen Umsetzung bekannt geworden, so kann dies insbesondere hinsichtlich möglicher Vertraulichkeitsverletzungen nicht ausschlaggebend sein. Dass noch nichts bekannt wurde, gibt keine Rechtfertigung, angemessene rechtliche Bindungen der beteiligten Schülerrichterinnen und Schülerrichter zu unterlassen.

Das Ministerium der Justiz hatte auf Nachfrage umfassende Unterrichtung angekündigt. Über die Ergebnisse wird im nächsten Tätigkeitsbericht zu berichten sein.

18.8 Neuregelung der forensischen DNA-Analyse und erste praktische Konsequenzen

Bereits im vorherigen Tätigkeitsbericht hatte der Landesbeauftragte weitgehende Erläuterungen zur Problematik der DNA-Untersuchung gegeben und auf die bedenkliche Entwicklung hingewiesen, die sich aus einer Gleichsetzung des daktyloskopischen mit dem genetischen „Fingerabdruck“ angesichts der rapide fortschreitenden DNA-Technik ergeben kann (VII. Tätigkeitsbericht, Ziff. 18.3).

Das am 1. November 2005 in Kraft getretene Gesetz zur Novellierung der forensischen DNA-Analyse vom 12. August 2005 (BGBl. I S. 2360) hat den Anwendungsbereich der DNA-Analyse deutlich erweitert. Immerhin blieb der Richtervorbehalt für die Entnahme von Körpersubstanz und deren molekulargenetische Untersuchung grundsätzlich erhalten. Sein Wegfall in Einwilligungs- und Eilfällen begegnet nach wie vor Bedenken. In solchen Fällen entscheidet dann die Staatsanwaltschaft oder die Polizei. Es wird sich erst noch zeigen müssen, wie häufig solche Fälle sein werden, da das Bundesverfassungsgericht die Sicherstellung der Erreichbarkeit richterlichen Personals als staatliche Gewährleistungsaufgabe gefordert hat. Außerdem entfällt der Richtervorbehalt für anonyme Tatortspuren.

Bei DNA-Analysen für Zwecke künftiger Strafverfahren werden durch die Gesetzesänderung die Anforderungen an die konkrete Anlasstat sowie die Negativprognose verringert. Vorher durften DNA-Analysen für Zwecke künftiger Strafverfahren nur erfolgen, wenn eine Straftat von erheblicher Bedeutung oder eine Sexualstraftat begangen worden war und wenn zu erwarten war, dass gegen den Betroffenen künftig Strafverfahren wegen Straftaten von erheblicher Bedeutung zu führen sein werden. Nun kann auch die wiederholte Begehung sonstiger Straftaten im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen. Zugleich wurden die bisherigen Regelbeispiele für eine Straftat von erheblicher Bedeutung gestrichen. Ob dies verfassungsrechtlich Bestand haben wird, kann man bezweifeln. Zwar hält das Bundesverfassungsgericht eine wirksame Strafverfolgung und damit eine möglichst vollständige Wahrheitsermittlung im Strafverfahren für rechtsstaatlich geboten. Eingriffe in das Grundrecht auf informationelle Selbstbestimmung sind jedoch nur insoweit zu rechtfertigen, als nicht gegen das Übermaßverbot verstoßen wird. Das Bundesverfassungsgericht hat in zwei Entscheidungen in 2000 und 2001 (Beschluss vom 14. Dezember 2000, 2 BvR 1741/99, 2 BvR 276/00, 2 BvR 2061/00, NJW 2001, 879; Beschluss vom 15. März 2001, 2 BvR 1841/00, 2 BvR 1876/00, 2 BvR 2132/00, 2 BvR 2307/00, NJW 2001, 2320) den Grundsatz der Verhältnismäßigkeit im Hinblick auf die damaligen Regelungen für die Durchführung einer DNA-Analyse für Zwecke künftiger Strafverfahren nur deshalb als gewahrt angesehen, weil Voraussetzung hierfür das

Vorliegen einer Straftat von erheblicher Bedeutung und die auf bestimmten Tatsachen beruhende Prognose gewesen ist, dass gegen den Betroffenen künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sein werden. Die seit November 2005 geltende Rechtslage lässt als Anlasstaten im Rahmen der Negativprognose die wiederholte Begehung bzw. die zu erwartende wiederholte Begehung jeglicher Straftaten genügen, sofern diese insgesamt in ihrem Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen. Ob es real möglich ist, insbesondere im Rahmen einer Prognose, den geforderten Schweregrad der gesetzlichen Voraussetzungen durch eine Kumulation letztlich fiktiver Taten zu erfüllen, erscheint eher zweifelhaft. Damit hätte der Gesetzgeber erneut einen nicht erfüllbaren Auftrag vergeben. Eine solche Regelungspraxis ist äußerst bedenklich, geht es doch nicht um die Aufklärung bereits erfolgter Straftaten, sondern darum, in welchem Maß Erkenntnisse aus einer DNA-Analyse für die Aufklärung erst noch vermutlich zu begehender Taten verarbeitet und genutzt werden dürfen. Da durch diese Vorratsdatenspeicherung auch solche Personen betroffen sein werden, die später nicht mehr straffällig werden, ist auf die Einhaltung des Erforderlichkeitsprinzips mit besonderem Nachdruck zu achten.

Mit der Neuregelung wurde schließlich eine gesetzliche Regelung zu DNA-Reihengentests eingeführt. Ein Richter darf eine solche Reihenuntersuchung nur anordnen, wenn ein Verbrechen gegen Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung begangen wurde und der betroffene Personenkreis anhand von Prüfungsmerkmalen umschrieben ist. Das Gesetz stellt klar, dass die betroffenen Personen nicht zur Mitwirkung verpflichtet und sie darüber zu belehren sind, dass

- ihre Mitwirkung freiwillig ist,
- die entnommenen Körperzellen nach der Untersuchung unverzüglich zu vernichten sind und
- keine Speicherung in der DNA-Datei des BKA erfolgen darf.

Um die Handhabung insbesondere im Bereich der Polizei zu vereinheitlichen, verfasste das Ministerium des Innern einen Vorentwurf für eine entsprechende Verwaltungsvorschrift. Nach einer erheblichen Abstimmungszeit zwischen den beteiligten Ressorts erging eine umfängliche Anwendungsvorschrift in Form eines gemeinsamen Runderlasses vom Ministerium des Innern und Ministerium der Justiz. Der Landesbeauftragte war beteiligt worden und hatte unter anderem darauf gedrungen, dass bei Betroffenen, welche sich in einer besonderen Zwangssituation befinden, die tatsächliche Freiwilligkeit einer Einwilligung in eine DNA-Untersuchung durch entsprechende Regelungen im Verfahrensablauf in besonderer Weise zu sichern ist. So empfiehlt es sich z.B. bei Strafgefangenen darauf zu achten, dass derartige Erklärungen nicht im Zusammenhang mit anderen haftbezogenen Entscheidungen abverlangt werden.

Auf eine Arbeitshilfe zu DNA-Reihengentests wurde mit der - fernmündlich mitgeteilten - Begründung verzichtet, dass derartige Tests selten vorkämen und keiner Einzelfallregelung bedürften. Inwieweit diese Maßnahme tatsächlich nur als ultima ratio zum Einsatz kommt, werden ggf. entsprechende Kontrollen erweisen.

Wie der Landesbeauftragte ca. ein Jahr später feststellen musste, schien der Runderlass noch nicht in allen zuständigen Dienststellen inhaltlich angekommen zu sein (siehe folgende Ziff. 18.9). Angesichts dieser bekanntgewordenen Fälle, die erfahrungsgemäß nur ein Bruchteil der tatsächlichen durchgeführten Maßnahmen darstellen dürfte, mahnt der Landesbeauftragte erneut (VII. Tätigkeitsbericht, Ziff. 18.3) Maßhalten an.

18.9 Ausgesetzter Säugling - DNA-Analyse sollte helfen, die Mutter zu finden

Im Zusammenhang mit dem Aussetzen eines Säuglings übersandte die Polizei an etliche Frauen im gebärfähigen Alter eine Vorladung zur Abgabe einer Speichelprobe, um die Mutter zu ermitteln. Aus der gleichsam in Befehlsform gehaltenen Aufforderung war weder ein Hinweis auf die Freiwilligkeit einer solchen Maßnahme noch darauf, ob die Betroffenen sich als Beschuldigte oder Zeugen beteiligen sollten, zu entnehmen bzw. nach welchen Merkmalen hier eine Rasterung der vorgeladenen Personen erfolgte. Im Ergebnis vermittelte die Vorladung für die Betroffenen den Eindruck, dass sie verpflichtet sind, bei der Polizei vorzusprechen und eine Speichelprobe abzugeben. Dies mag zwar wirkungsvoll sein. Aufgrund des Rechtsstaatsprinzips ist die öffentliche Hand grundsätzlich zu transparentem Vorgehen verpflichtet - besonders bei Maßnahmen, welche u.U. erheblich in Grundrechte eingreifen.

Nach Mitteilung des Ministeriums des Innern hatte die zuständige Polizeidirektion bereits vor Eingang des Schreibens des Landesbeauftragten Zweifel an der eigenen Verfahrensweise bekommen und die Maßnahme zunächst unterbrochen. Letztlich bestätigte die Polizeidirektion - auch nach Rücksprache zum Verfahren mit der verfahrensleitenden Staatsanwaltschaft - die rechtlichen Bedenken des Landesbeauftragten. Denn die getroffene Maßnahme stellte sich nun auch für die Polizeidirektion als Reihengentest dar, für den nach § 81h StPO eine richterliche Anordnung erforderlich ist.

Auf eine Beanstandung konnte aufgrund der angemessenen Reaktion der Polizeidirektion und auch wegen der Neuheit der Regelungen verzichtet werden. Allerdings regt der Landesbeauftragte an, zu prüfen, ob nicht zumindest ein erläuternder Hinweis zu Reihengentests im Anwendungsrunderlass zu DNA-Untersuchungen aufgenommen werden sollte.

18.10 Ermittlungsgruppe Schulweg - Die Suche nach einem Sexualstraftäter

Ein aktueller Anwendungsfall der DNA-Analyse ist die Suche nach einem Sexualstraftäter in Halle (Saale). Wie Presseberichten im Februar 2007 zu entnehmen war, fahndete die Polizei mittels freiwilliger DNA-Analyse nach einer zwischen 30 und 60 Jahre alten Person männlichen Geschlechts. Die etwa 1000 vorgeladenen Personen sollten alle bereits wegen einschlägiger Vorstrafen polizeibekannt sein.

Es dauerte allerdings nicht lange, bis der Landesbeauftragte auch wieder aus Pressemitteilungen davon Kenntnis erlangte, dass anscheinend nicht nur einschlägig vorbestrafte Personen, sondern auch bisher polizeiunbekannte Personen zur Abgabe einer Speichelprobe aufgefordert worden waren.

Der Landesbeauftragte nahm diese Informationen zum Anlass, bei der ermittlungsleitenden Staatsanwaltschaft zum Sachverhalt und den rechtlichen Grundlagen des Vorgehens von Staatsanwaltschaft und Polizei nachzufragen.

Telefonische Anfragen und schriftliche Eingaben von Betroffenen gingen beim Landesbeauftragten auch bereits im Februar ein. Der Tenor der Anfragen war stets der gleiche. Alle Betroffenen fühlten sich vor allem deshalb unzulässig beeinträchtigt, weil die Presse in aller Regel von einschlägig vorbestraften Personen sprach und die Betroffenen dies aber nicht waren. Trotzdem wurden sie von ihrem Umfeld zunächst so wahrgenommen, weil eine Richtigstellung seitens der Staatsanwaltschaft oder der Polizei nicht erfolgte. Es hätte nach Auffassung des Landesbeauftragten viel Aufregung bei den Betroffenen vermieden werden können, wenn z.B. mittels Presseerklärung richtig gestellt worden wäre, dass aufgrund eines entsprechenden Beschlusses des zuständigen Amtsgerichtes eben nicht nur polizeibekannte Personen vorgeladen werden.

Ein Petent stellte seine Situation so dar, dass er beruflich als Selbstständiger in Halle (Saale) tätig sei und wegen der Vorladung geschäftliche Termine absagen musste. Dass er seinen Geschäftspartnern mitteilen musste, dass er zur Abgabe einer Speichelprobe beim Polizeirevier vorsprechen sollte, wirkte sich nicht förderlich aus. Zu diesem Zeitpunkt ging aufgrund der Presseberichte noch jeder davon aus, dass nur einschlägig vorbestrafte Personen vorgeladen werden. Ein so entstandener Verdacht ist nur schwer auszuräumen und kann die berufliche Existenz gefährden. Vor dem Hintergrund solcher Berichte ist es unverständlich, dass eine öffentliche Richtigstellung nicht angestrebt wurde.

Nach Berichten der ermittlungsleitenden Staatsanwaltschaft habe das Amtsgericht Halle-Saalkreis am 21. Dezember 2006 einen Beschluss gefasst, nachdem „... bei allen männlichen Einwohnern zwischen einem Lebensalter von 30 bis 50 Jahren, welche zur Tatzeit in der Stadt Halle und Saalkreis mit Haupt- oder Nebenwohnsitz wohnten bzw. von dort verzogen oder anderweitig ansässig waren und die durch Straftaten mit sexuellem Hintergrund auffällig waren ...“ eine DNA-Analyse vorgenommen werden sollte. Insoweit entsprach die Berichterstattung zunächst den tatsächlichen Gegebenheiten.
Allerdings erging auf Antrag der Staatsanwaltschaft bereits am 2. Februar 2007 - und damit noch vor dem Aufleben der öffentlichen Diskussion - ein weiterer Beschluss des Amtsgerichtes Halle-Saalkreis. Danach durfte jetzt „... bei allen männlichen Einwohnern zwischen einem Lebensalter von 30 - 50 Jahren, welche zur Tatzeit in der Stadt Halle und Saalkreis mit Haupt- oder Nebenwohnsitz wohnten bzw. von dort verzogen oder anderweitig ansässig waren und von Personen, die durch Straftaten mit sexuellem Hintergrund auffällig waren ...“ eine DNA-Analyse gemacht werden. Im Ergebnis bedeutet das, dass es nunmehr auf irgendeine Verbindung zu Straftaten mit sexuellem Hintergrund nicht mehr ankam. Es konnte jeden treffen.

Die Anfrage des Landesbeauftragten bei der Staatsanwaltschaft veranlasste diese, die Beschlüsse des Amtsgerichtes noch einmal zu prüfen. Im Ergebnis hat die Staatsanwaltschaft festgestellt, dass der „... sehr weit gefasste ...“ Beschluss vom

2. Februar 2007 beim mittlerweile erarbeiteten Stand der Ermittlungen nicht erforderlich sei, um die gesuchte Person ausfindig zu machen. Die Staatsanwaltschaft hat deshalb die Ergänzung und Neufassung (Zusammenfassung) der Beschlüsse des Amtsgerichtes beantragt.

Am 23. Februar 2007 fasste das Amtsgericht daraufhin einen erneuten Beschluss, nach dem

„1. bei allen männlichen Einwohnern zwischen einem Lebensalter von 30 bis 50 Jahren, welche zu den Tatzeiten in der Stadt Halle und Saalkreis mit Haupt- und Nebenwohnsitz wohnten oder dort einer Tätigkeit nachgingen und die durch Straftaten mit sexuellem Hintergrund auffällig waren
sowie darüber hinaus

2. bei allen männlichen Einwohnern zwischen einem Lebensalter von 30 bis 50 Jahren, welche zu den Tatzeiten mit Haupt- und Nebenwohnsitz im Nahbereich des Tatortschwerpunktes ... wohnten bzw. deren Arbeitsstelle sich in diesem Bereich befand, der die Straßenzüge ... umfasst
oder
bei allen männlichen Personen im Alter zwischen 30 bis 50 Jahren, die auf Hinweise aus der Bevölkerung hin als im Nahbereich von ... während der Tatzeiten als aufhältig ermittelt werden konnten..."

DNA-Analysen mit Einwilligung der Betroffenen vorgenommen werden können.

Der Landesbeauftragte hat sich durch die Vorlage entsprechender Unterlagen davon überzeugt, dass auf die Freiwilligkeit der Maßnahme in den Vorladungen an die Betroffenen ausdrücklich hingewiesen wird.

Gegen die Umsetzung der Maßnahme durch die Polizei bestehen derzeit keine Bedenken. Der Landesbeauftragte wird die Maßnahme jedoch weiter begleiten und vor allem die rechtmäßige Löschung der Daten und die Vernichtung des Materials im Rahmen seiner Zuständigkeiten kontrollieren.

18.11 „Mikado"

„Mikado" ist nicht nur ein Gesellschaftsspiel mit Stäbchen. Unter der Bezeichnung „Mikado" hat die Staatsanwaltschaft Halle ein Ermittlungsverfahren gegen Pädophile durchgeführt. In der Presse fand dieses Verfahren ein sehr breites Echo. Nicht nur die lokalen Medien berichteten ausführlich über das Ermittlungsverfahren. Allerdings entsprach nicht jede dieser Darstellungen den tatsächlichen Gegebenheiten. Vom Ablauf des Verfahrens hat sich der Landesbeauftragte von der Staatsanwaltschaft Halle berichten lassen und eine datenschutzrechtliche Bewertung vorgenommen. Im Ergebnis bestehen vor dem Hintergrund des dem Landesbeauftragten Bekannten keine datenschutzrechtlichen Bedenken gegen das Vorgehen der Staatsanwaltschaft Halle.

Durch Pressemitteilungen vom 8. Januar 2007 erlangte der Landesbeauftragte erstmals Kenntnis von der durch die Staatsanwaltschaft Halle und das Landeskriminalamt durchgeführten Ermittlungsmaßnahme „Mikado". An der Vorbereitung und Durchführung der Ermittlungsmaßnahme war der Landesbeauftragte nicht beratend beteiligt.

Nach zunächst telefonischen Rücksprachen mit der Staatsanwaltschaft Halle zum Sachverhalt am 9. Januar 2007 und zwischenzeitlich vorliegenden schriftlichen Stellungnahmen stellt sich der Sachverhalt so dar, dass unter dem 6. Juni 2006 bei der Staatsanwaltschaft Halle durch einen Redakteur eines Nachrichtenmagazins Strafanzeige bezüglich einer Internetseite erstattet wurde. Bereits im Preview-Bereich wurde kinderpornografisches Material angeboten. Die Anpreisungen in englischer Sprache waren eindeutig und ließen keinen Zweifel aufkommen, welches Material im sogenannten Member-Bereich, der gegen die Zahlung von 79,99 $ „betreten“ werden konnte, zu finden ist. Staatsanwaltschaft und Landeskriminalamt sicherten und prüften den Inhalt der Seiten. Es wurde festgestellt, dass es sich im Member-Bereich ausschließlich um strafbewehrtes Material handelte. Beworben wurde das Internetportal mittels „Spam-Mails“.

Am 31. Juli 2006 wurden 13 Kreditkartenserviceunternehmen durch die Staatsanwaltschaft Halle mit der Bitte angeschrieben, zur Namhaftmachung der Nutzer des Internetportals beizutragen. Die Kreditkartenserviceunternehmen wurden in diesem Anschreiben darauf hingewiesen, dass zur Vermeidung einer zeugenschaftlichen Vernehmung eines Mitarbeiters gem. § 161a StPO Fragen beantwortet werden sollen. Erfragt wurden die Kreditkartenkonten, die ab dem 1. März 2006 bis zum Zeitpunkt der Anfrage einen Überweisungsbetrag von 79,99 $ an eine bestimmte Firma aufwiesen. Angegeben war darüber hinaus die Bank, über die die Zahlung mit Master- oder VISA-Card abgewickelt worden sein musste. Als weiteres Suchkriterium wurde eine sogenannte Merchant-ID - Händlernummer - an die Kreditkartenserviceunternehmen übermittelt.

Anfang August 2006 gingen die ersten Daten von Tatverdächtigen bei der Staatsanwaltschaft Halle ein. Durch die Kreditkartenserviceunternehmen wurden im Ergebnis die personenbezogenen Daten zu 322 Tatverdächtigen an die Staatsanwaltschaft Halle übermittelt, die sich auf die Bundesländer wie folgt verteilt:
Nordrhein-Westfalen 68, Bayern 56, Baden-Württemberg 36, Hessen 30, Niedersachsen 27, Rheinland-Pfalz 23, Berlin 17, Sachsen 15, Brandenburg 11, Schleswig-Holstein 8, Saarland 6, Thüringen 5, Bremen 5, Mecklenburg-Vorpommern 3, Sachsen-Anhalt 2.

Den Presseberichten zu „Mikado“ war zu entnehmen, dass das Vorliegen eines Anfangsverdachtes, der die Voraussetzung für das Tätigwerden der Staatsanwaltschaft ist, angezweifelt wurde. Aus Sicht des Landesbeauftragten ist der Anfangsverdacht allerdings aufgrund der Erfahrungen mit entsprechenden Verfahren in der Vergangenheit als gegeben anzusehen.

Wie die Ausführungen der Staatsanwaltschaft Halle nachvollziehbar darlegten, nutzten auch früher schon deutsche Internet-User ihre Kreditkarten zur Freischaltung von Member-Bereichen kinderpornographischer Portale. Frühere bzw. parallele Verfahren zeigten nur allzu deutlich, dass bei internationalen „Werbeaktionen“ für kinderpornographische Portale durch Spam-Mails auch deutsche „Kunden“ gewonnen werden. Diese Beobachtung, dass sich auch Deutsche Zugang zu kinderpornographischem Material verschaffen, sei auch auf dem nicht kommerziellen kinderpornographischen „Markt“ zu machen.

§ 152 Abs. 2 StPO fordert als Voraussetzung für das Einschreiten der Staatsanwaltschaft das Vorliegen zureichender tatsächlicher Anhaltspunkte. Das Wissen, dass nach kriminalistischer Erfahrung eine verfolgbare Straftat gegeben ist, genügt für das Vorliegen eines Anfangsverdachtes. Sprechen jedoch lediglich Vermutungen oder kriminalistische Hypothesen dafür, dass Straftaten begangen worden sind, greift die dienstliche Verfolgungspflicht noch nicht ein. Die Erkenntnisse der Staatsanwaltschaft gingen im vorliegenden Fall allerdings über bloße Vermutungen hinaus; es handelte sich nicht um Ermittlungen „ins Blaue hinein“.

Weiterhin wurde vielfach die Auffassung vertreten, dass es sich bei der Maßnahme der Staatsanwaltschaft Halle um eine Rasterfahndung gehandelt habe, die einer richterlichen Anordnung bedurft hätte. Der Landesbeauftragte geht davon aus, dass es sich bei der Maßnahme der Staatsanwaltschaft Halle nicht um eine Rasterfahndung im Sinne des § 98a StPO gehandelt hat.

Eine Rasterfahndung liegt vor, wenn personenbezogene Daten von Personen, die bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, mit anderen Daten maschinell abgeglichen werden, um Nichtverdächtige auszuschließen oder Personen festzustellen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen. Der Zweck der Rasterfahndung besteht darin, den Kreis möglicher Tatverdächtiger einzugrenzen, um dann weitere personenbezogene Ermittlungen führen zu können. Eine Eingrenzung des Verdächtigenkreises lag aber bei der Maßnahme der Staatsanwaltschaft Halle nicht im Mittelpunkt des Interesses. Vielmehr wurden durch die Maßnahme bereits bestimmbare Tatverdächtige gesucht. Personen, auf die die fünf Kriterien zutrafen, waren Tatverdächtige, gegen die zu ermitteln war. Es handelte sich nicht um mögliche Tatverdächtige, aus deren Kreis noch Tatverdächtige zu ermitteln waren. Das Wesen der Rasterfahndung ist jedoch, dass eine Vielzahl unverdächtiger Grundrechtsträger mit erfasst und dann ebenfalls den Strafverfolgungsbehörden gemeldet werden. Durch die Auswahl der Suchkriterien war die Erfassung Unverdächtiger vorliegend ausgeschlossen. Als unzutreffend erwiesen sich auch Presseverlautbarungen, wonach der Staatsanwaltschaft Halle Daten zu mehr als 20 Millionen Kreditkarteninhabern übermittelt worden seien.

Bedingt wird die direkte Einordnung als Tatverdächtige für alle aufgrund der Maßnahme an die Staatsanwaltschaft Halle übermittelten Daten dadurch, dass sich nach § 184b Abs. 4 S.1 StGB bereits derjenige strafbar macht, der es unternimmt, sich den Besitz von kinderpornographischen Schriften zu verschaffen, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben. Dieser Tatbestand ist bereits dadurch erfüllt, dass jemand den Betrag von 79,99 $ an eine bestimmte Bank zugunsten einer bestimmten Firma in der Absicht überweist, sich den Besitz von kinderpornographischem Material zu verschaffen. Insoweit kann auch nicht von einer Verdachtsschöpfung durch die Maßnahme ausgegangen werden.

Nach Einschätzung des Landesbeauftragten handelt es sich bei der Maßnahme der Staatsanwaltschaft Halle um ein Auskunftsersuchen mit Selektionskriterien, wie sie auch im Bereich der Telekommunikation nach § 113 TKG - ohne richterlichen Beschluss - an die jeweiligen Diensteanbieter gestellt werden können. Aus-

kunftsersuchen werden in der Regel schriftlich an den Zeugen, d.h. an den zuständigen Sachbearbeiter des Unternehmens, gerichtet. Die Zeugenpflicht des Sachbearbeiters umfasst es, sich in Vorbereitung auf die Zeugenvernehmung Kenntnis über die in Rede stehenden Daten zu verschaffen und entsprechende Unterlagen mitzubringen. Diese Zeugenpflicht wurde im vorliegenden Fall dadurch erfüllt, dass die Unternehmen die durch Selektion nach vorgegebenen Kriterien ermittelten Daten schriftlich an die Staatsanwaltschaft übermittelt haben. Das Bankgeheimnis war hier nicht berührt.

Diese Art von Auskunftsersuchen findet ihre Rechtsgrundlage in den §§ 160 ff. StPO. Die Staatsanwaltschaft Halle hat die Ermittlungen im Verfahren „Mikado“ im Rahmen der ihr zustehenden Befugnisse durchgeführt.

Beim zuständigen Amtsgericht Halle wurden zwischenzeitlich mehrere Anträge auf Feststellung der Unzulässigkeit der Maßnahme der Staatsanwaltschaft Halle gestellt. Es finden sich sowohl Anträge von Personen, die nicht zu denen gehören, deren Daten an die Staatsanwaltschaft Halle übermittelt wurden, als auch Anträge von Personen, die eine Verfügung auf ihrem Kreditkartenkonto zu verzeichnen haben, auf die alle fünf Kriterien zutreffen und deren Daten infolge dessen übermittelt wurden.

Aus einem bereits vorliegenden Beschluss des Amtsgerichts Halle-Saalkreis vom 11. März 2007 ist zu entnehmen, „... dass die Datenabfrage der Staatsanwaltschaft Halle bei bundesdeutschen Kreditkarten- und Abrechnungsunternehmen im Rahmen des Ermittlungsverfahrens ‚Mikado’ rechtmäßig war.“ „Der erforderliche Anfangsverdacht im Sinne des § 152 Abs. 2 StPO lag vor.“ „Das Gericht verkennt aber nicht, dass sich die Annahme eines Anfangsverdachts hier auf der niedrigsten Verdachtsstufe bewegt und lediglich ein ‚schmaler Grat’ zwischen Anfangsverdacht und Generalverdacht bzw. einem durch einen Verdachtsgewinnungseingriff produzierten Verdacht besteht.“ „Die beanstandete Ermittlungsmaßnahme ist durch §§ 161, (161a) StPO gedeckt.“ „Es liegt auch keine dem Richtervorbehalt unterfallende Rasterfahndung gemäß § 98a StPO vor, die als spezialgesetzliche Regelung der Anwendung des § 161 StPO vorgehen würde.“ „Schließlich ist die beanstandete Maßnahme auch nicht unverhältnismäßig gewesen.“ „Die Ermittlungshandlung der Staatsanwaltschaft beeinträchtigt den Antragsteller - sowie die übrigen Betroffenen - nicht unzulässig in ihrem Recht auf informationelle Selbstbestimmung.“
Der Antragsteller hat gegen die Entscheidung des Amtsgerichts Beschwerde eingelegt, die das Landgericht Halle/S. am 16. Mai 2007 als unbegründet verworfen hat.

18.12 Probleme im Zusammenhang mit Abrufen aus dem maschinell geführten Grundbuch

Auf der Grundlage eines Verwaltungsabkommens der Länder Brandenburg, Mecklenburg-Vorpommern, Sachsen, Thüringen und Sachsen-Anhalt war 1992 in Barby das Grundbucharchiv als Dienststelle des Ministeriums der Justiz des Landes Sachsen-Anhalt eingerichtet worden. Ursprünglich verwahrte es die geschlossenen Grundbücher aus dem Beitrittsgebiet mit Ausnahme Berlins. Nach-

dem die übrigen beteiligten Länder ihre Bestände übernommen hatten, lagerten in Barby seit Mitte der 90er Jahre nur noch Akten aus Sachsen-Anhalt. Dazu zählten vor allem Grundbücher der Amtsgerichte Sachsen-Anhalts, die vor 1990 geschlossen worden waren, sowie Grundbücher, die anlässlich der Anlegung des maschinell geführten Grundbuches geschlossen wurden. Der mit der ursprünglicher Aufgabe verbundene Geschäftsanfall ging damit stetig zurück.
Das Grundbucharchiv übernahm neue Aufgaben. So befindet sich heute in Barby das Rechenzentrum für das Elektronische Grundbuch.
Das Grundbuch in maschineller Form als automatisierte Datei zu führen, hat die Landesregierung durch die auf Basis von § 126 GBO erlassene Verordnung über das maschinell geführte Grundbuch bestimmt. Damit eröffnet sich gem. § 133 Abs. 1 GBO auch in Sachsen-Anhalt die Möglichkeit, auf diesen zentralen Grundbuch-Datenbestand nicht nur durch die grundbuchführenden Stellen selbst, sondern, nach Genehmigung durch die Landesjustizverwaltung, u.a. auch durch andere Behörden, Notare und die öffentlich bestellten Vermessungsingenieure im Zuge eines automatisierten Verfahrens, das die Übermittlung der Daten durch Abruf ermöglicht, zuzugreifen. Diese Genehmigung gilt, so § 133 Abs. 7 GBO, im ganzen Land Sachsen-Anhalt und, wenn die technischen Voraussetzungen dafür gegeben und festgestellt sind, auch im übrigen Bundesgebiet.
Wer sich jetzt vor Augen hält, dass prinzipiell auch die Angaben der Abteilung III des Grundbuches zum Abruf bereitstehen, die Daten über grundpfandrechtliche Belastungen wie Hypotheken des Grundstückes und damit über die Vermögenssituation des Eigentümers enthalten, wird die datenschutzrechtliche Bedeutsamkeit des Verfahrens erkennen.
Die Genehmigung zur Teilnahme am elektronischen Datenabruf gilt - auch für regional tätige Verfahrensteilnehmer wie Gemeinden oder Zweckverbände - für das Gebiet des ganzen Landes, später möglicherweise für das ganze Bundesgebiet. In der Regel wird eine Gemeinde zur Erfüllung ihrer Aufgaben keinen Bedarf und damit kein berechtigtes Interesse am möglichen Abruf deutschlandweit verfügbarer Grundbuchdaten haben.

Der Bundesgesetzgeber hat zum Schutz des Datenschutzgrundrechts des Einzelnen einige Regelungen getroffen.

- So wird in § 83 GBV festgelegt, dass das Grundbuchamt alle Abrufe zu protokollieren hat. Dies gibt u.a. dem Grundbuchamt die Möglichkeit, festzustellen, ob Abrufberechtigte das in sie gesetzte Vertrauen rechtfertigen. Allerdings muss dafür auch die Protokollierung in einem ordnungsgemäßen Verfahren sichergestellt werden. Anlässlich einer Kontrolle im Grundbucharchiv hat der Landesbeauftragte erhebliche Protokollierungsdefizite festgestellt. Im Rahmen dieser Kontrolle wollte er prüfen, inwieweit von Gemeinden Grundbuchdaten exterritorialer Grundstücke abgerufen worden waren. Die dem Landesbeauftragten zunächst vorgelegten Abruf“protokolle“ waren durch Copy & Paste-Verfahren in einer Standardtextverarbeitungssoftware zusammengestellt worden, fehlerhaft und offenbar beliebig änderbar. Der Landesbeauftragte war im Ergebnis mit dem Ministerium der Justiz zu der Feststellung gekommen, dass die Protokollierung der Grundbuchabrufe so ihren Zweck nicht erfüllen kann. Bei einer weiteren Kontrolle wird er auch hinterfragen, ob in den einzelnen Fällen der abrufenden Stellen die Form der Da-

tenübermittlung durch automatisierten Abruf gem. § 133 Abs. 2 Ziff. 1 GBO unter Berücksichtigung der schutzwürdigen Interessen der betroffenen dinglich Berechtigten wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit überhaupt angemessen ist.

- Eine weitere Schutzfunktion haben Auskunftsrechte Betroffener. Daher hat der Landesbeauftragte in Nachbereitung der Kontrolle - durch entsprechende fernmündliche Testanrufe bei den zuständigen Rechtspflegerinnen und Rechtspflegern - bei etlichen Grundbuchämtern in Erfahrung bringen wollen, wie „er“ als Eigentümer eines Grundstücks oder eines grundstücksgleichen Rechts Auskunft aus dem über die Abrufe zu führenden Protokoll erhalten könne. Das Ergebnis war nicht erfreulich! Bis auf eine Mitarbeiterin eines Amtsgerichts war keiner/keinem anderen wenigstens der Regelungsgehalt der Vorschrift des § 133 Abs. 5 S. 2 GBO, die einen entsprechenden Auskunftsanspruch enthält, bekannt. Erst nach längerem Gespräch wurde einmal der Hinweis auf das Grundbucharchiv Barby gegeben.

- Als generelles Problem ist festzuhalten, dass zur Zeit programmtechnisch keine Möglichkeit besteht, den Zugriff externer Nutzer auf bestimmte Gemeindebereiche oder wenigstens Amtsgerichtsbezirke zu beschränken. Eine solche geografische wirksame Beschränkung einzuführen, hat der Landesbeauftragte im Jahre 2006 als Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gegenüber der Vorsitzenden der Konferenz der Justizministerinnen und Justizminister angeregt. In ihrer abschlägigen Antwort legte diese dar, dass diese regionale Beschränkung der Abrufmöglichkeit rechtlich nicht geboten und eine technische Änderung des Systems daher nicht erforderlich sei. Den datenschutzrechtlichen Belangen werde ihres Erachtens durch die in § 133 Abs. 1 Nr. 2 GBO, § 83 GBV geregelte Abrufprotokollierung, verbunden mit der Pflicht der Aufsichtsbehörden zu stichprobenartigen Kontrollen, ausreichend Rechnung getragen.
  Gerade diese Antwort unterstreicht die Notwendigkeit eines ordentlichen Protokollierungsverfahrens, welches insbesondere eine regelmäßige zumindest stichprobenartige Überprüfung des Protokolls durch die verantwortliche Stelle beinhaltet.

Der Landesbeauftragte geht davon aus, dass das Ministerium der Justiz in diesem Sinne tätig werden wird und es zumindest dafür Sorge tragen wird, dass Auskunftsinteressenten künftig eine brauchbare Antwort erhalten.

18.13 Bundesweites Registerportal unter Beteiligung der Länder

Mit dem Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG) sind die Bundesländer zur bundesweit ausschließlich maschinellen Führung des Handels-, Genossenschafts- und Partnerschaftsregisters verpflichtet worden. Zur Umsetzung dieser Verpflichtung ist ein gemeinsames Registerportal der Länder in Nordrhein-Westfalen eingerichtet worden. Das Land Sachsen-Anhalt hat mittels Staatsvertrag und Verwaltungsvereinbarung Aufgaben nach dem Handelsgesetzbuch auf dieses Land übertragen (GVBl. LSA 2007, S. 130).

Das Ministerium der Justiz hat darüber erst auf Anfrage informiert; beteiligt worden ist der Landesbeauftragte gem. § 14 Abs. 1 Satz 2 DSG-LSA jedoch nicht. Da auch nach diesem Informationsschreiben datenschutzrechtliche Fragen offen blieben, musste er sich an die Kollegin aus Nordrhein-Westfalen wenden. Diese stellte in ihrer Stellungnahme folgendes klar:

„Sinn des bundesweiten Registerportals ist es, im Internet eine zentrale Zugriffs- und Bekanntmachungsmöglichkeit für die Handels-, Genossenschafts- und Partnerschaftsregisterdaten der Amtsgerichte in den Ländern bereitzustellen sowie eine einheitliche Schnittstelle für den Datenaustausch mit anderen elektronischen Informations- und Kommunikationssystemen (z.B. das Unternehmensregister) einzurichten. Dabei werden die Aufgaben der Veröffentlichung sowie des Zugangs zu den Daten über die Internetplattform dem in Nordrhein-Westfalen gelegenen Amtsgericht Hagen übertragen. Datenhaltende Stellen der Registerdaten bleiben nach diesem Konzept die Registergerichte der Länder. Auch bleibt neben dem elektronischen Abruf der Daten über das Registerportal weiterhin eine Auskunftserteilung auf Länderebene möglich. Eine Bündelung der datenschutzrechtlichen Kontrolle kann meiner Ansicht nach nur in dem Umfang stattfinden, wie durch die Staatsverträge hoheitliche Aufgaben auf Stellen des Landes Nordrhein-Westfalen übertragen werden. Dabei geht es im Wesentlichen um Fragen der organisatorischen und technischen Abwicklung, insbesondere der Datensicherheit."

Jetzt wartet der Landesbeauftragte noch auf das Sicherheitskonzept des Projekts, das die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen beim dortigen Justizministerium angefordert hat.

19. Schulen

19.1 Umstellung der Schulstatistik auf Individualdaten mit bundeseinheitlichem Kerndatensatz

Mit Beschluss der Kultusministerkonferenz (KMK) vom 28. Januar 2000 „zur Sicherstellung eines einheitlichen Aufkommens schulstatistischer Daten für überregionale und internationale Zwecke" wurde festgestellt, dass ein aktueller und vergleichbarer Bestand an Schuldaten der Länder unerlässlich sei. Am 30. Januar 2003 beschloss die KMK dann den sog. Kerndatensatz (KDS).
Der KDS enthält verschiedene Merkmalssätze, z.B. zur Schule, zur Klasse, zu den Unterrichtseinheiten, zu den Schülern und zu den Lehrkräften der Schule. Die Merkmalssätze sind untereinander verknüpfbar. Der Merkmalssatz zu den Schülern enthält u.a. Angaben zum Geschlecht, Geburtsmonat und -jahr, Wohnort, Ersteinschulung, Geburtsland, bei nichtdeutschem Geburtsland das Jahr des Zuzugs nach Deutschland, Staatsangehörigkeit, Sprache bei nichtdeutscher Verkehrssprache, Art der Wiederholung, erteilter Unterricht in Unterrichtseinheiten, Förderschwerpunkte, Ganztagsunterricht und angestrebter Beruf. Außerdem erhält jeder Schüler zur Einschulung eine eindeutige Identifikationsnummer (Schüler-ID), die ihn sein gesamtes Schülerleben begleiten soll. Dadurch sollen auch schul- und länderübergreifend Informationen weitergegeben werden können. Diskutiert werden auch Datenerfassungen zu besonderen Problemgruppen (Zuwan-

derer, sozial Benachteiligte), außerdem die Einbeziehung von Kindergartenzeit und Berufsausbildung.

Aus datenschutzrechtlicher Sicht sind u.a. folgende Gesichtspunkte kritisch zu betrachten:

1. Beim KDS handelt es sich um Totalerhebungen. Es wurde bisher nicht ersichtlich, warum anders strukturierte Erhebungen zur Bildungsberichterstattung nicht ausreichen. Verfassungsrechtlich geboten ist es, Totalerhebungen zu vermeiden, wenn das gewünschte Ergebnis auf andere Weise erreichbar ist.

2. Offen ist auch, wie, von wem und unter welchen Vorgaben die Schüler-ID generiert werden soll. Zweifelhaft ist vor allem, ob die ID rechtlich als Hilfsmerkmal oder als Erhebungsmerkmal zu werten ist, da mittels dieser ID die Verknüpfungen mit Daten der Lehrer und der Schule erfolgen sollen. Ebenso unklar ist, inwieweit der Datensatz aufgrund der Vielzahl der gespeicherten Daten nicht mehr pseudonymisiert, sondern personenbezogen ist.

3. Es ist unklar, für welche konkreten Zwecke die Datensätze genutzt werden sollen. Zu beachten ist jedenfalls, dass statistische Daten dem Statistikgeheimnis unterliegen, d.h. die amtliche Statistik muss von Aufgaben des Verwaltungsvollzuges abgeschottet sein.

4. Auch unklar ist, welche Stellen auf Landesebene die Daten zusammenführen sollen bzw. darauf zugreifen und sie nutzen dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder haben anlässlich der Konferenz im Oktober 2006 eine missbilligende Entschließung gefasst (**Anlage 17**). Danach ist das bisherige Konzept datenschutzrechtlich grundsätzlich bedenklich und sollte in dieser Form von der KMK nicht weiter verfolgt werden. Aufgrund einer bisher fehlenden präzisen Zweckbestimmung zur Verarbeitung des KDS und der bereits durchgeführten bzw. geplanten wissenschaftlichen Studien (z.B. PISA) erscheint ein bundesweites zentrales Register nicht erforderlich und stellt damit einen unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht dar.

Beratungen der KMK mit Bildungsexperten, Datenschützern und interessierten Bürgern wurden durchgeführt. So fand z.B. am 5. Dezember 2006 während der Sitzung der Statistikkommission der KMK ein Gespräch u.a. mit dem Landesbeauftragten als Vorsitzenden der Datenschutzkonferenz statt, in der die datenschutzrechtlichen Bedenken erläutert werden konnten. Am 13. Februar 2007 fand ebenfalls zu diesem Thema ein öffentlicher Workshop der KMK statt, bei dem der Landesbeauftragte die Position der Datenschutzkonferenz vortrug.

Mittlerweile wird das bisherige Konzept auch von einigen Kultusverwaltungen kritisch gesehen. So haben die Länder Sachsen, Thüringen und Sachsen-Anhalt vereinbart, dass es keine Zustimmung zu einer gemeinsamen nationalen Daten-

bank geben wird. Die weitere Entwicklung der Schulstatistikumstellung wird vom Landesbeauftragten begleitet. Eine „gläserne Schule“ darf es nicht geben.

Das Kultusministerium hat unabhängig von der vorbeschriebenen Problematik dem Landesbeauftragten zugesichert, diesen vor der Einführung einer Schulverwaltungssoftware, die auch die Schulen von statistischen Aufgaben entlasten könnte, frühzeitig zu beteiligen.

19.2 PISA und IGLU

Im Mai 2006 wurde zum dritten Mal die PISA-Studie in sachsen-anhaltischen Schulen durchgeführt. Zeitgleich wurde, bereits zum zweiten Mal, die IGLU-Studie fortgesetzt.
In beiden Studien wurden Schülerinnen und Schüler getestet und befragt. Eltern und Lehrkräfte wurden ebenfalls zu verschiedenen Themen ihres persönlichen und beruflichen Umfeldes befragt. Das Ziel der Studien ist, die Bildungsadministration mit Informationen zur Qualität des Schulsystems zu versorgen.
Die Einhaltung des Datenschutzes bezüglich der Befragungen der Teilnehmer wurde vom Landesbeauftragten geprüft. Da beide Projekte bereits aus den früheren Zyklen bekannt waren und eine frühzeitige Beteiligung des Landesbeauftragten (bereits im September 2005) erfolgte, konnten seine Hinweise und Anregungen in den Anschreiben und Fragebögen berücksichtigt werden. Auch fand eine Informationsveranstaltung für die Datenschutzbeauftragten und die Ansprechpartner in den Kultusministerien der Länder zu IGLU 2006 und PISA 2006 statt.

In Sachsen-Anhalt besteht insoweit eine Besonderheit bezüglich der Befragungen, da nicht nur die Schülerinnen und Schüler verpflichtet sind, zur Qualitätssicherung schulischer Arbeit an Befragungen, Erhebungen und Unterrichtsbeobachtungen sowie internationalen Schulleistungsuntersuchungen teilzunehmen (§ 84a Abs. 3a Satz 1 SchulG LSA), sondern auch die Erziehungsberechtigten sind zur Qualitätssicherung schulischer Arbeit verpflichtet, bei Befragungen, Erhebungen bzw. internationalen Schulleistungsuntersuchungen die erforderlichen Auskünfte zu erteilen (§ 84a Abs. 3a Satz 2 SchulG LSA).

Je Studie sei ein Problempunkt beispielhaft dargestellt:

Bezüglich der Fragebögen zu PISA 2006 hat der Landesbeauftragte darauf hingewiesen, dass mittels der Schülerfragebögen Daten der Eltern erhoben werden (z.B. berufliche Tätigkeit, Schulabschluss der Eltern). Es gilt allerdings der Grundsatz der Datenerhebung beim Betroffenen. Hiervon abgewichen werden darf nur, wenn die Betroffenen z.B. nicht selbst befragt werden können. In Sachsen-Anhalt besteht jedoch, wie bereits dargestellt, eine gesetzliche Verpflichtung der Eltern zur Auskunft der erforderlichen Angaben. Das mit der Leitung der PISA-Studie beauftragte Institut erläuterte, dass sich die doppelte Datenerhebung bei Schülern und Eltern aufgrund des internationalen Charakters der Studie nicht verhindern lasse. International ist der Elternfragebogen nur eine Option und wird nur in knapp einem Viertel der an PISA beteiligten Länder eingesetzt. Insofern müssen die Fragen aufgrund der Vergleichbarkeit der Ergebnisse im Schülerfragebogen erhoben werden. Der Vorschlag des Landesbeauftragten, dann zumindest die El-

tern im Elternanschreiben über die Themen, zu denen sowohl die Eltern als auch die Schüler befragt werden, zu informieren, wurde übernommen.

Bezüglich der Elternfragebögen zu IGLU 2006 hat der Landesbeauftragte datenschutzrechtliche Bedenken in Bezug auf einzelne Fragen geäußert, da kein schulischer Kontext zu erkennen war, zumal es sich um Abfragen zu personenbezogenen Daten besonderer Art handelte. So wurden z.B. Fragen zu religiösen Überzeugungen („In meinem Leben spielen christliche Wertvorstellungen keine Rolle.“) und politischen Meinungen („Man sollte sich politisch engagieren, um Unterdrückung und Ausbeutung in unserer Gesellschaft zu bekämpfen.“) gestellt. Das mit der Leitung der IGLU-Studie beauftragte Institut hat daraufhin die kritischen Fragen aus dem Elternfragebogen gestrichen.

19.3 TIMSS und Übergangsstudie

Im Berichtszeitraum fand in den Grundschulen Sachsen-Anhalts auch die TIMSS-Studie (TIMSS - Trends in International Mathematics and Science Study) statt. TIMSS 2007 wird von einem Hochschulinstitut koordiniert und erhebt Leistungen von Schülern der vierten Jahrgangsstufe in den Bereichen Mathematik und Naturwissenschaften im internationalen Vergleich. Im Rahmen dieser Studie wird ebenfalls der Übergang von der Grundschule in die weiterführenden Schulen untersucht. Diese ergänzende nationale Studie, die sog. Übergangsstudie, wird von einem anderen Hochschulinstitut durchgeführt.
Die Übergangsstudie findet in drei Phasen statt, wobei erst die dritte Phase im Rahmen von TIMSS durchgeführt wird.
Beide Forschungseinrichtungen wurden aus datenschutzrechtlicher Sicht beraten. Hinweise und Anmerkungen fanden Berücksichtigung.

19.4 Prüfung von Schulen

Im Berichtszeitraum hat der Landesbeauftragte in Grund- und Sekundarschulen vor Ort die Einhaltung der datenschutzrechtlichen Vorschriften überprüft.
Insgesamt ist hervorzuheben, dass in allen Schulen aus datenschutzrechtlicher Sicht eine ähnliche Sachlage festzustellen war.

19.4.1 Datenverarbeitung durch Schulen

Einige Schulleiter haben bisher die Regelungen des § 84a Abs. 2 SchulG LSA i.V.m. § 14a DSG-LSA übersehen. Obwohl die Frist für die Einsetzung eines behördlichen Datenschutzbeauftragten bereits zum 31. Januar 2002 (§ 32 Abs. 2 DSG-LSA) verstrichen war, gab es keine behördlichen Datenschutzbeauftragten. Die Schulen, die automatisierte Schülerverwaltungssoftware verwenden, haben unverzüglich einen behördlichen Datenschutzbeauftragten bestellt, sodass von einer formalen Beanstandung abgesehen werden konnte.

Schulen dürfen gem. § 84a Abs. 3 Satz 1 SchulG LSA nur die Daten der Schülerinnen und Schüler erheben, die zur Aufgabenerfüllung der Schule erforderlich sind. Bei Schuleintritt wird daher für jeden Schüler ein Schülerstammblatt angelegt. Das Kultusministerium hat mit einem RdErl. Richtlinien zum Schülerstamm-

blatt erlassen. Schülerdaten, die in diesem RdErl. vorgesehen sind, werden also vom Kultusministerium für erforderlich für die Aufgabenerfüllung von Schulen erachtet. Die von den Schulen verwendeten Vordrucke zum Schülerstammblatt beinhalteten allerdings oftmals Datenerhebungen, die im RdErl. zum Schülerstammblatt nicht vorgesehen sind. Die Erforderlichkeit dieser Daten für die Aufgabenerfüllung der Schulen ist damit grundsätzlich nicht gegeben. Diese Daten werden von den Schulen zukünftig nicht mehr erhoben. Beispielhaft seien Daten wie Nationalität, Anzahl der Geschwister und Geburtskreis genannt.

Bei Anmeldung des Kindes in den Schulen werden die Eltern gebeten, Vordrucke auszufüllen, die Daten der Kinder enthalten, die nicht im Schülerstammblatt vorgesehen sind, aber dennoch zur Erfüllung des Erziehungs- und Bildungsauftrages oder der Fürsorgeaufgaben nach § 84a Abs. Satz 1 SchulG LSA erforderlich sind. So werden aber auch z.B. die Daten „Religionszugehörigkeit“ oder die „Telefonnummer für den Notfall“ von den Eltern erhoben. Bezüglich des Datums „Religionszugehörigkeit“ hat der Landesbeauftragte darauf hingewiesen, dass diese Datenerhebung für die Erfüllung des Erziehungs- und Bildungsauftrages nicht unerlässlich sein kann, da die Fachwahl der Schüler zwischen (evangelischem und katholischem) Religions- bzw. Ethikunterricht nicht von der Zugehörigkeit zu einer der Religionsgemeinschaften abhängig ist, sondern hiervon frei erfolgen kann. Bei der Abfrage des Datums „Telefonnummer für den Notfall“ hat der Landesbeauftragte empfohlen, die Eltern im Vordruck schriftlich auf die Freiwilligkeit der Datenangabe hinzuweisen. Eine Not-/Erstversorgung des Schülers durch den Arzt ist immer zu gewährleisten, auch wenn die Telefonnummer der Eltern nicht vorliegen würde. Da die meisten Eltern wohl eine Information bei Eintritt eines Notfalls wünschen werden, sollte die Telefonnummer freiwillig erhoben werden. Die Vordrucke werden entsprechend den Hinweisen überarbeitet. Im Übrigen hat der Landesbeauftragte in den Grundschulen darauf hingewiesen, dass die Erforderlichkeit bzw. Nützlichkeit der Datenerhebungen ebenfalls im zeitlichen Kontext zu betrachten sind. So ist die Datenerhebung der „Telefonnummer für den Notfall“ vor der Feststellung des Schulleiters über die Einschulung des Kindes in diese Grundschule weder erforderlich noch nützlich. Diese Daten sollten daher erst nach dieser Entscheidung erhoben werden. Dagegen stehen die ebenfalls mit diesem Vordruck erhobenen Daten zum Kindergartenbesuch des Kindes sehr wohl im direkten Zusammenhang mit der Schulfähigkeitsentscheidung. Wenn die Entscheidung der Schulleitung zur Schulfähigkeit durch Informationen des Kindergartens begründeter wird, ist eine Abfrage vor der Aufnahmeentscheidung gerechtfertigt. Der Schulleiter hat daher veranlasst, die Datenerhebungen mittels zweier Vordrucke zu den jeweiligen Zeitpunkten durchzuführen.

In den Grundschulen hat der Landesbeauftragte festgestellt, dass die Aufbewahrungsfristen für den Datenbestand an Schulen entsprechend einem RdErl. des Kultusministeriums nicht überwacht werden. So befanden sich in einer Schule sämtliche Schülerakten seit 1993 im Schulleiterbüro und alle Klassenbücher seit 1993 zum Teil im Keller und im Schulleiterbüro. In einer anderen Schule wurden alle Schülerakten und Klassenbücher sogar seit 1990 im Keller aufbewahrt. Die im RdErl. festgelegten Aufbewahrungsfristen bestimmen jedoch, dass Schülerstammblätter zehn Jahre nach der Schulentlassung und Klassenbücher bereits ein Jahr nach Ende des Schuljahres datenschutzgerecht zu vernichten sind. Die

Schulleiter sicherten eine unverzügliche Kontrolle und datenschutzgerechte Vernichtung der Datenbestände zu.

Weiterhin war festzustellen, dass private Lehrer-PC dienstlich genutzt werden. Gemäß RdErl. des Kultusministeriums ist diese Nutzung zuvor von der Schulleitung zu genehmigen. Dies war in den Schulen nicht erfolgt. Der Landesbeauftragte hat den Schulleitern daher empfohlen, die Lehrkräfte aufzufordern, entsprechend dem Runderlass zu verfahren.

19.4.2 Zusammenarbeit mit Kindertagesstätten

Die geprüften Grundschulen arbeiten bezüglich der einzuschulenden Kinder mit jeweils einer Kindertagesstätte zusammen. Unter anderem finden in diesem Rahmen sog. „Bienchen- bzw. Schnupperstunden“ statt, in denen sich die Kinder mit der Schule und dem zukünftigen Klassenlehrer und dem pädagogischen Mitarbeiter bekannt machen können. Die Kinder werden entweder vom Schulleiter von der Kindertagesstätte abgeholt oder von den Erzieherinnen der Kindertagesstätte zur Schule gebracht. Die Schulleiter konnten nicht ausschließen, dass bei sog. „Kann-Kindern“ oder bei Verhaltensauffälligkeiten einzelner Kinder Gespräche zwischen den Erzieherinnen und den Klassenlehrern bzw. dem Schulleiter stattfinden. Für die Gespräche zwischen den Erzieherinnen und den Klassenlehrern wurden von den Schulen keine Einwilligungserklärung der Erziehungsberechtigten eingeholt, da die Schulen annahmen, dass diese von den Kindertagesstätten eingeholt wurden. Der Landesbeauftragte hat die Schulleiter darauf hingewiesen, dass die Erhebung personenbezogener Daten aufgrund von Gesprächen zwischen Lehrern der Grundschule und Erzieherinnen der Kindertagesstätte ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung und eine Datenerhebung ist, die einer Rechtsgrundlage bedarf. § 84a Abs. 3 SchulG greift hier nicht, da es sich bei den Kindern der Kindertagesstätte noch nicht um Schüler handelt. Zulässig wäre eine Datenerhebung daher nur auf der Grundlage der Einwilligung der Erziehungsberechtigten des betroffenen Kindes. Diese Einwilligung muss allerdings den Voraussetzungen des § 4 Abs. 2 DSG-LSA entsprechen. Die Schulleiter sicherten zu, zukünftig erst nach der Erklärung des Einverständnisses der Erziehungsberechtigten, Gespräche mit den Erzieherinnen der Kindertagesstätten durchzuführen (vgl. Ziff. 20.21).

19.5 Umstellung der Datenerhebung bei den Schulen

Bisher übermittelten die Schulen die für die Verwaltungsaufgaben notwendigen Schüler- und Lehrerdaten in Papierform an die zuständige Stelle im Landesverwaltungsamt (LVwA). Dies sollte durch eine webbasierte Anwendung vereinfacht werden. Dazu sollte nach Vorstellung des Kultusministeriums, das den Landesbeauftragten frühzeitig beteiligte, auf einem WWW-Server pro Schule eine verschlüsselte Datei zur Verfügung gestellt werden, die die Grunddaten der jeweiligen Schule enthält. Diese Datei konnten nur durch genau zwei Stellen entschlüsselt werden, die Schule selbst und das LVwA. Um ihre Daten einzugeben, sollte sich die Schule über einen Web-Browser an dem WWW-Server anmelden, um die generierten HTML-Seiten SSL-verschlüsselt auf den Schul-PC herunterzuladen. Die eingegebenen Daten würden wieder SSL-verschlüsselt an den WWW-Server

übertragen. Hier sollte eine Konsistenzprüfung erfolgen. Beim Auftreten von Fehlern wäre die Schule zur Überprüfung und Neueingabe aufgefordert worden. Erfolgreich geprüfte Daten wären verschlüsselt auf dem WWW-Server abgelegt worden. Das LVwA hätte die Dateien dann verschlüsselt heruntergeladen und zuständigkeitshalber verarbeitet und genutzt. Auf dem WWW-Server wären die Daten nach dem Herunterladen gelöscht worden.

Das dargestellte Verfahren begegnete bei Berücksichtigung einiger Hinweise keinen durchgreifenden datenschutzrechtlichen Bedenken.

Die bei der webbasierten Datenerhebung geplanten technisch-organisatorischen Maßnahmen waren - auch für die Erhebung von Individualdaten - grundsätzlich dem Schutzzweck angemessen. Ergänzend wurde ein serverseitiges SSL-Zertifikat angeregt, damit die Schulen überprüfen können, dass sie sich tatsächlich auf dem WWW-Server des LVwA befinden.
Die Daten würden auf dem WWW-Server verschlüsselt abgelegt, d.h. der externe Anbieter hat zu diesem Zeitpunkt keine Möglichkeit, Kenntnis von diesen Daten zu erlangen. Lediglich während der Konsistenzprüfung sind die Daten unverschlüsselt im Hauptspeicher des Rechners vorhanden. Die Gefahr eines Zugriffs durch Unbefugte während dieser Zeit erschien im konkreten Fall jedoch als sehr unwahrscheinlich und damit im Sinne des Verhältnismäßigkeitsprinzips akzeptabel.

Datenschutzrelevante Vorgänge nach § 2 Abs. 4 und 5 DSG-LSA i.V.m. § 84a Abs. 2 SchulG LSA lagen damit nicht vor:

Das Erheben (vgl. § 2 Abs. 4 DSG-LSA) ist das zielgerichtete, bewusste und gewollte Beschaffen bzw. Entgegennehmen personenbezogener Informationen. Soweit lediglich Rechenkapazität im Hauptspeicher zur Verfügung gestellt wird, ohne dass ein Interesse am Inhalt der Daten durch den Serverbetreiber besteht und ein Missbrauch - abgesehen von einem ggf. vertretbaren Restrisiko - ausgeschlossen ist, liegt keine zielgerichtete Datenbeschaffung vor. Es wäre allenfalls das Niveau einer „beiläufigen Wahrnehmung“ erreicht.

In Betracht kam ein Speichern (vgl. § 2 Abs. 5 Nr. 1 DSG-LSA) des Serverbetreibers als Erfassen oder Aufnehmen personenbezogener Informationen auf einem Datenträger. Diese Merkmale decken alle Formen der Verkörperung, unabhängig von der Art der Fixierung, der Sprache und dem physikalischen Trägermedium ab. Datenträger können grundsätzlich jegliche Medien sein, auf denen Daten lesbar festgehalten werden.
Ob aber ein Haupt- bzw. Arbeitsspeicher einer EDV-Anlage bzw. eines Webservers in Folge der „Kurzlebigkeit“ der dort vorhandenen Information noch als Datenträger im Sinne dieser Vorschrift angesehen werden kann, erschien fraglich. Es fehlte hier an der nachlesbaren Fixierung. Der Zweck weiterer Verarbeitung oder Nutzung als Voraussetzung des Speicherungsbegriffs war nicht gegeben. Die Vorschrift zur Speicherung stellt dem Sinn und Zweck nach darauf ab, dass die Belange der Betroffenen tangiert werden, indem die in den Daten verkörperten Informationen verwendet werden. Es sollte jedoch lediglich eine einer Funktionsprüfung ähnliche Konsistenzprüfung im Sinne der Prüfung der Plausibilität und

Vollständigkeit durch das Programm im Arbeitsspeicher erfolgen. Diese Verwendung zielte ausschließlich in Richtung der die Daten selbst eingebenden Schule. Die Verwendung der Informationen erfolgt daher inhaltlich betrachtet innerhalb der Schule, soweit die Verbindung zu dem extern handelnden Arbeitsspeicher des Webservers sicher ist. Ist die technische Sicherheit gewährleistet, sind die Belange der Betroffenen daher nicht tangiert.

Auch lag kein Verändern (vgl. § 2 Abs. 5 Nr. 2 DSG-LSA) durch inhaltliches Umgestalten gespeicherter personenbezogener Daten vor. Dies würde eine Veränderung des Informationsgehaltes voraussetzen. Zwar sehen die vorhandenen Informationen physikalisch nach der Verschlüsselung anders aus, so dass zunächst ein Umgestalten nahe lag. Betrachtet man jedoch den Absender der Information (Schule) und den Adressaten (Landesverwaltungsamt), der den Schlüssel hat, liegt lediglich eine Reduktion der Lesbarkeit des unveränderten Informationsinhalts für unbefugte Dritte vor.

20. Sozialwesen

Allgemeines

20.1 Elektronischer Einkommensnachweis

Bei dem Projekt „Elektronischer Einkommensnachweis“ („ELENA“, früher „JobCard“) handelt es sich um ein Fachverfahren unter Einsatz einer Signaturkarte. Die Daten sollen jedoch nicht auf der Karte, sondern auf zentralen Servern gespeichert werden. Ziel ist es z.B., Bescheinigungen der Arbeitgeber durch automatisierte Verfahren zu ersetzen. Alle Arbeitgeber übermitteln auf elektronischem Wege die zu bescheinigenden Daten der Arbeitnehmer (z.B. Höhe der Entgeltzahlungen) an die Zentrale Speicherstelle. Dort werden die Daten gespeichert und stehen im Bedarfsfall für sozialrechtliche Leistungsverfahren zur Verfügung. Dadurch entsteht eine zentrale Datensammlung auf Vorrat. Für den einzelnen Betroffenen erhält diese Sammlung nur dann Bedeutung, wenn ein Antrag auf Sozialleistungen gestellt wird. Es bestehen daher grundsätzliche Bedenken an der Verhältnismäßigkeit und Zulässigkeit des Verfahrens. Die 73. Konferenz der Datenschutzbeauftragten hat am 8./9. März 2007 eine entsprechende Entschließung gefasst, in der u.a. der Nachweis der Erforderlichkeit und Verhältnismäßigkeit des Registers gefordert wird (**Anlage 22**).

Der Landesbeauftragte wird die Entwicklung des ELENA-Verfahrens weiterhin kritisch begleiten.

20.2 Empfehlungen zur Vorlage von Kontoauszügen bei der Beantragung von Sozialleistungen

Aufgrund aktueller Fälle und Anlässe, insbesondere bei der Beantragung von Arbeitslosengeld II und Sozialhilfe und der Frage der Verfahrensweise zur Überprüfung von Einkommen und Vermögen nach den Vorschriften des SGB II und SGB XII unter Berücksichtigung von Kontoauszügen, haben mehrere Landesbeauftrag-

te gemeinsam Empfehlungen zur Vorlage von Kontoauszügen bei der Beantragung von Sozialleistungen entwickelt.

Die Erhebung personenbezogener Daten durch den Sozialleistungsträger ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Artikel 6 Abs. 1 der Landesverfassung).
Dieser ist auf der Grundlage des § 67a Abs. 1 Satz 1 SGB X nur zulässig, wenn er gesetzlich speziell vorgesehen oder zur Aufgabenerfüllung erforderlich ist. Maßgeblich ist daher nicht, ob der Sozialleistungsträger eine Datenerhebung für geboten hält. Vielmehr gestattet der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit lediglich unerlässliche Datenerhebungen.

Nach dem Sozialgesetzbuch sind alle, die Sozialleistungen beantragen, zur Mitwirkung verpflichtet. Klare gesetzliche Vorgaben, ob und in welchem Umfang der Leistungsträger in diesem Zusammenhang die Vorlage von Kontoauszügen verlangen darf und welche Angaben geschwärzt werden dürfen, enthalten diese Vorschriften jedoch nicht. Eine pauschale Anforderung von Kontoauszügen ist datenschutzrechtlich nicht zulässig. Dies gilt insbesondere dann, wenn den Betroffenen generell untersagt wird, einzelne Buchungen zu schwärzen.

Um sowohl dem Recht auf informationelle Selbstbestimmung der Betroffenen als auch den Interessen des Sozialleistungsträgers an einer Prüfung der Anspruchsvoraussetzungen angemessen Rechnung tragen zu können, haben die Landesbeauftragten entsprechende Hinweise entwickelt, die über die Homepage des Landesbeauftragten unter Service/Sonstige Infos abgerufen werden können.

SGB II

20.3 Arbeitslosengeld II

Auch in diesem Berichtszeitraum hat der Landesbeauftragte gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Landesbeauftragten für den Datenschutz die Verbesserung gesetzlicher Regelungen (vgl. Ziff. 20.4) und die Gestaltung der Vordrucke begleitet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte im Oktober 2005 in einer Entschließung „Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen“ (Anlage 6), allen Betroffenen nicht nur schnellstmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den überarbeiteten Ausfüllhinweisen zur Verfügung zu stellen.
Die Umsetzung wurde durch die Bundesagentur für Arbeit (BA) jedoch erst im Juli 2006 vollzogen. Nunmehr sind die überarbeiteten und aktualisierten Antragsvordrucke einschließlich der Ausfüllhinweise im Internet unter http://www.arbeitsagentur.de abrufbar.

Die Umsetzung der von der BA vorgegebenen Software A2LL für die Leistungsberechnung beschäftigt den Landesbeauftragten auch über den VII. Tätigkeitsbericht hinaus. Zwar liegt nunmehr ein Zugriffsberechtigungskonzept vor und auch

eine Protokollierung der Zugriffe wird vorgenommen, jedoch beklagen die Datenschützer weiterhin den bundesweiten Zugriff auf die Daten der Hilfesuchenden.

Im Jahr 2006 begann die BA die flächendeckende Einführung des IT-Verfahren VAM/VerBIS (Virtueller Arbeitsmarkt/Vermittlungs- Beratungs- und Informationssystem) in den Arbeitsgemeinschaften (ARGEn).

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit steht diesbezüglich mit der BA im Gespräch. Hinsichtlich des Umfangs der Zugriffsberechtigungen sieht der Bundesbeauftragte noch Diskussionsbedarf. Als Teil des Zugriffsberechtigungskonzeptes liegt das Protokollierungskonzept bislang nicht vor.

20.4 Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende

Die öffentliche Diskussion über die Kostenexplosion bei „Hartz IV“ und ihre Ursachen sowie die anhaltenden datenschutzrechtlichen Probleme begleiten den Landesbeauftragten bereits seit Mitte 2004 (siehe VI. Tätigkeitsbericht, Ziff. 20.1).

Einige Politiker sahen für die vielschichtigen Kostensteigerungen die Ursache im Missbrauch von Leistungen. Um den Kostensteigerungen Herr zu werden und damit den Missbrauch einzugrenzen, fand im Sommer 2005 eine Telefonbefragung der BA statt.
Spürbar nahmen auch die Hausbesuche zu, die ebenfalls als geeignetes Mittel dargestellt wurden, der Missbrauchsquote Einhalt zu gebieten. Dies mag sicherlich in Einzelfällen auch begründet gewesen sein. Als Ultima Ratio konnten auch diese Maßnahmen nicht ausschließlich den gewünschten Erfolg erbringen.

Anfang August 2006 trat dann das Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende in Kraft (BGBl. I S. 1706).

In einer gemeinsamen Erklärung "Arbeitsuchende unter Generalverdacht" rügten die Datenschutzbeauftragten eine exzessive Datenerhebung, die mit der eingeführten Beweislastumkehr bei eheähnlichen Gemeinschaften ins Haus stehe. Betroffene müssten alle möglichen sensiblen Daten ihrer Mitbewohner preisgeben, um beweisen zu können, dass keine eheähnliche Gemeinschaft existiert.

Außerdem kritisierten sie, dass das Fortentwicklungsgesetz die Rechte der Betroffenen nicht deutlich genug herausgestellt habe, so etwa dass die Teilnahme an Telefonbefragungen durch private Call Center zur Feststellung des Leistungsmissbrauchs freiwillig sei. Hierzu hatten die Landesbeauftragten für den Datenschutz bereits im Oktober 2005 in einer Entschließung gefordert, die Sach- und Rechtslage klarzustellen und die Datenschützer rechtzeitig bei Veränderungen zu beteiligen (**Anlage 7**).

Zudem müsse bei der Überprüfung durch Hausbesuche eines Außendienstes eindeutig auf das grundgesetzlich geschützte Recht der Unverletzlichkeit der Wohnung hingewiesen werden.

Letztendlich wurde beanstandet, dass auch das Fortentwicklungsgesetz nicht eindeutig kläre, wer für die Kontrolle der Datenflüsse von Leistungsempfängern nach dem SGB II in den ARGEn zuständig ist (siehe Ziff. 20.5).

Die Diskussion zu diesem Gesetz entwickelte sich weiter zu Forderungen nach einer Generalrevision oder zumindest gravierenden Änderungen bei Hartz IV. Die Kostenexplosion in diesem Bereich, insbesondere bei der Grundsicherung für Arbeitsuchende, geht, wie etwa auch der Bericht des Bundesrechnungshofes und des Ombudsrates oder Auswertungen der BA feststellten, nur zu einem geringen Teil auf Missbrauchsfälle zurück. Nicht nur die Datenschützer hatten sich gegen einen Generalverdacht gegen Arbeitsuchende gewandt. Wenn Arbeitslose die gesetzlichen Möglichkeiten nutzen, dann kann man nicht von Missbrauch reden.

20.5 Zuständigkeit der ARGEn nach dem SGB II

Umsetzung der Datenschutzkontrolle

Bereits mit Einführung des SGB II wurde die Zuständigkeit der Landesbeauftragten für den Datenschutz in der Ausübung ihrer Datenschutzaufsicht durch die BA in Frage gestellt. Es entsprach jedoch einhelliger Meinung, dass die ARGEn als gemäß § 44b Abs. 3 Satz 4 SGB II der Aufsicht der zuständigen obersten Landesbehörden unterstehende Stellen, die nicht über den Bereich eines Landes hinaus tätig werden, unter der Datenschutzaufsicht der Landesbeauftragten für den Datenschutz stehen (vgl. § 81 Abs. 1 Nr. 2, Abs. 3 SGB X). Um Abgrenzungsdifferenzen mit den Zuständigkeiten des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu vermeiden, hatten sich die Datenschützer darauf verständigt, dass dessen Zuständigkeit dann begründet ist, sofern die BA zentrale EDV-Programme den ARGEn zur Verfügung stellt oder generelle Vorgaben trifft.
Die Prüfung im Einzelfall und dementsprechend die vollumfänglichen Datenschutzkontrolle in den ARGEn obliegt den Landesbeauftragten für den Datenschutz.

Die Datenschutzkontrolle der Landesbeauftragten für den Datenschutz wurde jedoch zum Teil dadurch behindert, dass den Landesbeauftragten bei der Wahrnehmung ihrer Aufgaben auf Weisung der BA keine datenschutzrechtlichen Auskünfte durch die ARGEn erteilt wurden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte im März 2006 in einer Entschließung „Keine kontrollfreien Räume bei der Leistung von ALG II“ die Bundesregierung auf, umgehend einen rechtskonformen Zustand herzustellen (siehe **Anlage 13**).

Die erforderliche und einheitliche Aufsichtszuständigkeit der Datenschützer für die ARGEn wurde durch das Gesetz zur Fortentwicklung der Grundsicherung für Arbeitssuchende (Fortentwicklungsgesetz) (siehe auch Ziff. 20.4) nicht bestätigt.
Die neue Zuständigkeitsregelung in § 50 Abs. 2 SGB II sieht nunmehr vor, dass die BA verantwortliche Stelle nach § 67 Abs. 9 SGB X ist, soweit die ARGEn die Aufgaben der Agenturen für Arbeit nach § 44b Abs. 3 Satz1 SGB II wahrnehmen.

Die Landesbeauftragten für den Datenschutz vertraten überwiegend die Auffassung, dass durch die Rechtsänderung eine Zuständigkeit der BA vorliege - also eine öffentliche Stelle des Bundes -, deren Datenschutzkontrolle ausschließlich durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit begründet wird.
Eine unsichere Rechtslage ergibt sich, wenn man § 44b Abs. 3 Satz 1 SGB II der Regelung in § 50 Abs. 2 SGB II entgegenstellt. Danach übernehmen die ARGEn die Aufgaben der BA als Leistungsträger.

In der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2006 bestätigte man ein zwischen den Datenschutzbeauftragten, der BA und dem Bundesministerium für Arbeit und Soziales vorläufig abgestimmtes Verfahren der Umsetzung der Datenschutzkontrolle in den ARGEn gemäß der o.a. Abgrenzung für generelle Vorgaben und Einzelfälle. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wurde gebeten, auf eine zeitnahe gesetzgeberische Klarstellung hinzuwirken. Die ARGEn wurden inzwischen aufgefordert, eine entsprechende Datenschutzkontrolle zuzulassen.

Kreisreform in Sachsen-Anhalt - unterschiedliche Zuständigkeiten beim ALG II

Die zum 1. Juli 2007 in Kraft tretende Kreisreform wird in Teilen Sachsen-Anhalts für die Antragsteller und Empfänger von ALG II Veränderungen mit sich bringen.
Die Zusammenlegung von Landkreisen und die Zuordnung von Gemeinden in Landkreise wird dazu führen, dass Betroffene in ihrem „neuen“ Landkreis von unterschiedlichen Behörden betreut werden. Je nachdem, wo sie leben, werden sie beispielsweise durch die ARGE des bisherigen Landkreises betreut. Bei der Beantragung von weiteren Leistungen wird die neue Kreisverwaltung zuständig sein.
Veränderungen scheinen wohl erst Anfang 2008 in Sicht, wenn ARGEn innerhalb eines Landkreises fusionieren. Ob dann eine Übertragung des Modells der Optionskommune auf den „neuen“ Landkreis möglich ist, erscheint fraglich. Die Bundesregierung lehnt die Ausweitung des Optionsmodells auf einen neuen größeren Landkreis aus Rechtsgründen ab und verweist auf die ausstehende Evaluierung.

20.6 Kontrollbesuch bei einer Optionskommune

In 69 Kommunen Deutschlands sind für die Bezieher des ab Anfang 2005 bestehenden ALG II nicht die BA und die Kommunen gemeinsam in Form der ARGEn zuständig, sondern nach dem Optionsmodell ausschließlich Städte oder Gemeinden. Dieses wurde auf sechs Jahre befristet. Danach sind die Wirkungen des Modellversuches zu überprüfen.

Der Landesbeauftragte hatte Mitte 2006 eine Optionskommune in Sachsen-Anhalt überprüft. Offensichtliche Mängel wurden während der Überprüfung nicht festgestellt. Zu begrüßen ist, dass die Optionskommune in vielen Einzelbereichen verfahrensrechtliche als auch datenschutzrechtliche Regelungen getroffen hatte, die dem Umgang mit Sozialdaten besonders gerecht werden.
Nur in einigen Bereichen hat der Landesbeauftragte auf Schwachstellen hingewiesen und um Abhilfe gebeten. So sind u.a. die Antragsvordrucke regelmäßig auf ihre Aktualität zu überprüfen und der Gesetzeslage anzupassen.

Neben der Angabe der Personalnummer und der Ausweisart im Hauptantrag wird regelmäßig eine Kopie des Ausweisdokumentes zu den Akten genommen. Der Landesbeauftragte hat vorgeschlagen, dass es zur Legitimierung grundsätzlich ausreicht, den Personalausweis oder Reisepass vorzulegen und in einem Vermerk bzw. im Antragsvordruck schriftlich auf die Vorlage der Ausweisunterlagen hinzuweisen (Handzeichen Sachbearbeiter). Eine Umstellung des Verfahrens ist anzustreben, insbesondere unter der Tatsache, dass die Antragsteller für die verschiedensten Bereiche (z.B. Mehrbedarfsprüfung bei Schwangerschaft) Nachweise vorlegen sollen.

Unter der Rubrik Familienverhältnisse sind sowohl Angaben zu den Mitgliedern, die in der Bedarfsgemeinschaft leben, als auch zu den Mitgliedern der Haushaltsgemeinschaft zu machen. Die Ausfüllhilfe der Optionskommune gibt Hinweise dazu, dass zu den Mitgliedern der Haushaltsgemeinschaft nur Name, Vorname, Geburtsdatum und Verwandtschaftsverhältnis erforderlich sind. Diese Angaben werden u. a. für die Berechnung der Kosten der Unterkunft benötigt.
Im Hinblick auf die unterschiedliche rechtliche Behandlung von Mitgliedern der Bedarfsgemeinschaft und der Haushaltsgemeinschaft und zur Vermeidung versehentlich zu umfänglicher Angaben ist eine differenzierte Erhebung geboten.
Die Vermutungsregelung in § 9 Abs. 5 SGB II sieht vor, dass Hilfebedürftige, die in Haushaltsgemeinschaft mit Verwandten oder Verschwägerten leben, von diesen Leistungen erhalten, soweit dies nach deren Einkommen und Vermögen erwartet werden kann. Wird dies verneint, sind weitere Erkundungen grundsätzlich obsolet. Erhält der Hilfebedürftige Leistungen von den Verwandten/Verschwägerten, die mit ihm in einer Haushaltsgemeinschaft leben, hat der Hilfebedürftige Angaben zu Name, Vorname, Geburtsdatum und des Verwandtschaftsverhältnisses zu machen.
Für die Berechnung lediglich der Kosten der Unterkunft werden diese Angaben nicht benötigt. Dazu reicht es grundsätzlich aus, die Anzahl der in der Wohnung lebenden Personen anzugeben.

Die „pauschale“ Befreiung vom Bankgeheimnis und die Ermächtigung, Kontostände und Kontobewegungen abfragen zu können, begegnet datenschutzrechtlichen Bedenken. Gemäß § 67a Abs. 2 Satz 1 SGB X sind Sozialdaten beim Betroffenen zu erheben. Ohne weiteres können Kontostände und Kontobewegungen beispielsweise durch Vorlage von Kontoauszügen für einen bestimmten Zeitraum dazu dienen, den Leistungsbezug zur Sicherung des Lebensunterhaltes zu prüfen. Dazu reicht es grundsätzlich aus, dass die Betroffenen entsprechende Nachweise vorlegen.
Hinsichtlich der Zulässigkeit und der einhergehenden Anforderung von Kontoauszügen siehe Ziff. 20.2.

Ein weiterer Überprüfungspunkt war die Installation einer Videokamera oberhalb eines Kassenautomaten, den ca. 250 Leistungsempfänger, die über kein Konto verfügen, zur Auszahlung von Leistungen nach dem SGB II nutzen. Sobald Betroffene ihren Auszahlungschip in den Kassenautomaten führen, werden sie mittels der Videokamera von hinten gefilmt, deren Aufnahmen für drei Monate aufbewahrt werden. Ein Hinweisschild ist am Kassenautomaten angebracht.

Diese Verfahrensweise soll einen Leistungsmissbrauch verhindern. Der Landesbeauftragte hielt es für angebracht, die Erforderlichkeit der Aufzeichnungen zu überprüfen. Es erschien fraglich, wie der Auszahlungsvorgang dokumentiert wird, wenn die Aufnahme von hinten erfolgt. Zudem könnten der Kassenbestand und interne Protokollierungen die tatsächliche Auszahlung dokumentieren. Unter Berücksichtigung, dass die Videobilder wegen eines möglichen Leistungsmissbrauchs aufgezeichnet werden, wurde die Optionskommune gebeten, kürzere Speicherungsfristen vorzusehen und das Bildmaterial danach zu löschen.

20.7 Beantragung von Leistungen zur Grundsicherung für Arbeitsuchende in einer Optionskommune

Eine Petentin beklagte sich darüber, dass sie bei der Antragstellung von Leistungen nach der Grundsicherung für Arbeitsuchende umfangreiche Unterlagen vorlegen sollte, die ihres Erachtens nicht bzw. nur in eingeschränktem Maße für die Leistungsgewährung erforderlich seien.

So musste die Petentin beispielsweise eine Kopie des vollständigen Mutterpasses sowie eine Haushaltsbescheinigung übergeben. Mit der Haushaltsbescheinigung bestätigte die ausstellende Gemeinde, dass die Betroffene unter der angegebenen Wohnanschrift auch tatsächlich wohnt. Darüber hinaus musste die Petentin die Einsichtnahme in den Personalausweis ermöglichen und Bank-, Kranken- und Arbeitsamtskundenkarten aller Haushaltsmitglieder der Optionskommune vorlegen, die dann als Kopie der Leistungsakte zugeführt wurden.

Die Optionskommune hat aufgrund der Intervention des Landesbeauftragten die aus datenschutzrechtlicher Sicht aufgetretenen Fehler erkannt und beseitigt. Durch das komplizierte Regelwerk des SGB II sei es zu den Schwachstellen innerhalb der Behörde gekommen.

Eine Doppelerhebung von Sozialdaten in Form der Haushaltsbescheinigung und des Personalausweises erfolgt künftig nicht mehr. Der Mutterpass wird nunmehr im Antragsverfahren vorgelegt. Eine Kopie wird nicht mehr zur Akte genommen.

Die Vorlage von Bank-, Kranken- und Arbeitsamtkundenkarten aller Haushaltsmitglieder wurde eingestellt.

20.8 Leistungen für Unterkunft und Heizung

Eine Eingabe nahm der Landesbeauftragte zum Anlass, das Sozialamt eines Landkreises zu beraten, der weder zugelassener kommunaler Träger (Optionskommune) nach § 6b SGB II war noch gem. § 44b Abs. 3 Satz 2 seine Aufgaben nach dem SGB II auf eine Arbeitsgemeinschaft übertragen hat. Das Sozialamt hatte für die Datenerhebung zu Kosten der Unterkunft und Heizung nach dem SGB II einen eigenen Vordruck entwickelt. Dabei fiel u.a. auf, dass die Antragsteller u.a. zu den zum Haushalt gehörenden Personen Namen und Vornamen, Geburtsdatum und Geburtsort, Familienstand, Staatsangehörigkeit, Tätigkeit/Beruf und Verwandtschaftsverhältnis zum Antragsteller angeben sollten. Ergänzend

wurden Angaben zu den Verwandten ersten Grades des Hilfebedürftigen erfragt, die nicht zur Bedarfsgemeinschaft gehören. Weiterhin wurde um Vorlage des Mietvertrages und entsprechender Nachweise gebeten. Ergänzend sollten Angaben zu Mieten, Betriebskosten und Heizkosten erfolgen. Zudem sollte eine Bescheinigung vorrangig durch den Vermieter vollständig ausgefüllt werden.

Mit dem Landkreis wurde ausführlich erörtert, dass nur die Daten formularmäßig erhoben werden dürfen, die für die Aufgabenerfüllung unerlässlich sind.

Bezüglich der abgefragten Staatsangehörigkeit wurde darauf hingewiesen, dass nach den Regelungen des SGB II die konkrete Staatsangehörigkeit nicht Entscheidungskriterium ist. Maßgeblich ist lediglich die Ausländereigenschaft im Zusammenhang mit der Leistungsberechtigung nach § 1 Asylbewerberleistungsgesetz bzw. dem Zweck der Arbeitssuche als Grundlage des Aufenthaltsrechtes (§ 7 Abs. 1 Satz 2 SGB II). Weiterhin ist die Ausländereigenschaft von Bedeutung für die Prüfung der Erlaubnis zur Aufnahme einer Beschäftigung (§ 8 Abs. 2 SGB II).
Hinsichtlich der Verwendung des Begriffs „Haushalt“ wurde der Landkreis darauf hingewiesen, dass eine Differenzierung zwischen der Bedarfsgemeinschaft, der Haushaltsgemeinschaft sowie der Wohngemeinschaft erforderlich ist. Auf die Erläuterung der Begriffe, ggf. auch durch Ausfüllhinweise, wurde hingewirkt. Weiterhin wurde dargelegt, dass die Abfrage von „Tätigkeit/Beruf“ dazu verleitet, Angaben zu machen, die für die Bearbeitung der konkret anstehenden Fragen nicht von Bedeutung sind. Nach Darstellung des Sozialamtes ging es nämlich gerade nicht darum, den einmal erlernten Beruf bzw. die aktuell ausgeübte Tätigkeit zu erfragen. Vielmehr ging es nach dem Amtsermittlungsgrundsatz um die Ermittlung vorrangiger Leistungspflichten, beispielsweise aus dem Bundesausbildungsförderungsgesetz. Die Förderungsfähigkeit einer Ausbildung ist daher konkret zu erfragen (§ 7 Abs. 5 und 6 SGB II).

Kritisch erschien auch die Frage nach dem „Verwandtschaftsverhältnis zum Antragsteller“. Soweit es darum ging, den Übergang von Ansprüchen nach § 33 SGB II und damit die Verpflichtungen anderer Personen zu prüfen, wären auch hier die konkret benötigten Informationen gesondert zu erfragen. Die hier ggf. interessierenden Unterhaltspflichtigen gehören nicht notwendig zum „Haushalt“.

Auch weitere ggf. erforderliche Informationen, beispielsweise im Hinblick auf eine Unterbringung bzw. eine Rente wegen Alters (§ 7 Abs. 4 SGB II), sollten ebenfalls konkret erfragt werden.

Ergänzend wurde angeregt, auf die namentliche Erfassung der Haushaltsangehörigen jedenfalls insoweit zu verzichten, als es um die Individualisierung der Kosten der Unterkunft geht. Hierfür ist grundsätzlich nur die Kenntnis der Anzahl der Angehörigen zur Aufteilung der Gesamtkosten erforderlich.

Kritisch zu beurteilen war weiterhin die Anforderung von „Mietvertrag und entsprechenden Nachweisen“. Die Erhebung und insbesondere die Speicherung von Nachweisen (Kopien in der Akte) ist auf das unerlässliche Maß zu begrenzen. Zudem ist auch auf Nachweisalternativen hinzuweisen (Mietüberweisungsbelege,

letztes Mieterhöhungsschreiben). Gegebenenfalls kann auch mit Sachbearbeiterhandzeichen dokumentiert werden, dass der Nachweis vorgelegen hat.
Erheblichen Bedenken begegnete auch das Verlangen nach einer ergänzenden, vom Vermieter auszustellenden Bescheinigung. Dies erschien nicht erforderlich.

Das Sozialamt hat dann zunächst seine Datenerhebungen mittels eines neuen Vordruckes angepasst. Bald darauf hat es jedoch mitgeteilt, es sei zwischenzeitlich erforderlich geworden, ein Zusatzblatt herauszugeben. Dort waren u.a. für weitere Angehörige der Haushaltsgemeinschaft neben dem Namen das Geburtsdatum, der Erwerbsstatus, die Staatsangehörigkeit und der Familienstand abgefragt. Zur Begründung wurde darauf verwiesen, dass man als kommunaler Träger nach § 51b Abs. 1 Satz 2 sowie Abs. 5 SGB II gehalten sei, personenbezogene Datensätze zu erstellen und der BA zu übermitteln, wie sie von dort anhand eines vorgegebenen Datenformates abgefordert werden. Der Landesbeauftragte hat sich daraufhin an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gewandt, der die Angelegenheit mit der BA erörtert hat. Danach ergab sich, dass zwar grundsätzlich die Verpflichtung besteht, nach § 51b SGB II Einzeldaten über das von der BA geregelte Verfahren zu liefern. Dieses Verfahren ist im Internetangebot für Statistik der BA beschrieben. Leider sind dabei auch einzelne Informationen zu Zwecken der Identifizierung und Zusammenführung sowie zur Vermeidung von Doppelzählungen aufzunehmen, die eigentlich bereits bei der BA bekannt sind. Über das Datenaustauschverfahren werden allerdings ausschließlich Individualdaten von Bedarfsgemeinschaftsmitgliedern abgefragt. Die Zahl der Mitglieder des Haushaltes unter Einschluss ggf. weiterer Personen der Haushaltsgemeinschaft wird lediglich als Aggregat im Zusammenhang mit den Daten zur Bedarfsgemeinschaft abgefragt. Die Übermittlung von Individualdaten zu Personen, die nicht Bedarfsgemeinschaftsmitglied sind und lediglich der Hausgemeinschaft angehören, ist im Datenaustauschverfahren nicht vorgesehen und wird von der BA nicht gefordert. Der Landesbeauftragte hat demgemäß den Landkreis gebeten, das Formular an die Rechtslage anzupassen.

20.9 Vermieterbescheinigung zu Kosten der Unterkunft

In einer Beratung eines Landkreises zur formularmäßigen Datenerhebung der Unterkunftskosten (§§ 6 Abs. 1 Satz 1 Nr. 2, 22 SGB II) wurde der Landesbeauftragte auf ein Schreiben eines Verbandes der Wohnungswirtschaft aufmerksam. In diesem wurde angeregt, von Antragstellern regelmäßig eine aktuelle Bescheinigung des Vermieters zu verlangen. Dies hätte neben aktuellen Mietangaben den positiven Effekt, dass die Vermieter davon Kenntnis erhalten, wenn ein Antrag auf Arbeitslosengeld II gestellt worden ist. Durch die Transparenz zum Wohle aller könne man mit dem Leistungsträger zusammen arbeiten, auf die Vermeidung unnötiger Mietschulden hinwirken und die Betroffenen zum Arbeitslosengeld II beraten.
Der Landkreis hatte dieses Schreiben zum Anlass genommen, als Nachweis für die Angaben zu den Kosten der Unterkunft nicht nur den Mietvertrag und weitere Nachweise, sondern darüber hinaus formularmäßig zwingend auch die Abgabe einer Vermieterbescheinigung zu fordern. Das Formular der Vermieterbescheinigung enthielt in der Überschrift das Sozialamt als Adressaten. Der Landesbeauf-

tragte sah sich daraufhin veranlasst, die Landkreise und kreisfreien Städte als Sozialleistungsträger nach § 6 SGB II auf Folgendes hinzuweisen:

Die Sozialleistungsträger sind zwar gehalten, die Leistungsvoraussetzungen zu prüfen. Die Antragsteller trifft auch eine Mitwirkungspflicht nach §§ 60 ff. SGB I, wonach sie die Leistungsvoraussetzungen darzulegen und ggf. nachzuweisen haben. Auch bei der Anforderung von Nachweisen ist jedoch der Grundsatz der Verhältnismäßigkeit zu beachten. Maßstab der Aufgabenerfüllung ist der geringst mögliche Eingriff in das Persönlichkeitsrecht des Betroffenen. Demgemäß ist es zunächst dem Antragsteller zu überlassen, in welcher Form er der Nachweispflicht hinsichtlich der von ihm gemachten Angaben nachkommt. Lediglich wenn er einzelne Nachweise nicht erbringen kann oder im begründeten Einzelfall der Verdacht besteht, dass Angaben unrichtig oder unvollständig sind, können weitere, den Betroffenen ggf. stärker beeinträchtigende Nachweise verlangt werden.

Des Weiteren ist zu berücksichtigen, dass durch die Verwendung eines Formulars mit der Kennzeichnung des Sozialamtes als Adressaten der Bescheinigung die Tatsache der Antragstellung bzw. des Sozialleistungsbezuges gegenüber dem Vermieter offenbart wird. Damit würde die Übermittlung von Sozialdaten veranlasst. Dies verstößt grundsätzlich gegen das Sozialgeheimnis (§ 35 Abs. 1 Satz 1 SGB I). Die Übermittlung von Sozialdaten ist nur zulässig, soweit dies nach den Vorschriften der §§ 67c ff. SGB X oder einer anderen Regelung des SGB erlaubt ist oder der Betroffene in die Datenübermittlung eingewilligt hat (§ 67b Abs. 1 Satz 1 SGB X).
Soweit im Einzelfall eine Vermieterbescheinigung ausnahmsweise erforderlich sein sollte, ist sie derart zu gestalten, dass der Vermieter nicht erkennen kann, von wem der Vordruck stammt und bei wem er vorgelegt werden soll. Dies hilft zu vermeiden, dass dem Vermieter unzulässig Sozialdaten bekannt werden.

Lediglich im Fall des § 22 Abs. 4 SGB II ist vorgesehen, dass die Kosten der Unterkunft direkt an den Vermieter oder andere Empfangsberechtigte bezahlt werden können. Dies setzt voraus, dass die zweckentsprechende Verwendung durch den Hilfebedürftigen nicht sichergestellt ist. Die Feststellung dieser tatbestandlichen Voraussetzung ist jeweils im Einzelfall anhand eines konkreten Sachverhaltes zu treffen.

Darüber hinaus kann eine direkte Zahlung an den Vermieter bzw. an den Betreuer des Mietverhältnisses durch den Sozialleistungsträger lediglich auf freiwilliger Basis und auf der Rechtsgrundlage der Einwilligung des Betroffenen erfolgen. Die Voraussetzungen einer wirksamen Einwilligung des Betroffenen nach § 67b Abs. 2 SGB X sind zu beachten (u.a. freie Entscheidung, detaillierte Information). Diese Informationspflicht eröffnet auch die Möglichkeit der Beratung der Antragsteller über die einzelnen Verfahrensweisen, von der einfachen Zahlung auf die Mietschuld bis hin zur Kooperation mit dem Vermieter. Dem Betroffenen muss dabei deutlich werden, dass es sich nur um ein Angebot (Freiwilligkeit) handelt und dem Vermieter die Eigenschaft als Sozialleistungsempfänger bekannt wird.

SGB V

20.10 Genehmigung häuslicher Krankenpflege

Verbände von Pflegedienstleistern haben den Landesbeauftragten darauf hingewiesen, dass die AOK die ärztlichen Verordnungen von Pflegeleistungen in Frage stelle. Die AOK verlange von den Pflegediensten Unterlagen mit medizinischem Inhalt zur Überprüfung der Verordnung. Es stelle sich daher die Frage, ob der Sachbearbeiter der AOK die ärztliche Anordnung negieren und Daten bei den Pflegediensten bzw. den Pflegebedürftigen erheben dürfe.

Demgegenüber verwies die AOK zunächst darauf, dass die praktischen Erfahrungen es leider erforderlich machen würden, in bestimmten Bereichen mit besonderen Auffälligkeiten die Notwendigkeit der Verordnung zu überprüfen. Dazu sei die AOK u.a. auch deshalb befugt, weil § 284 Abs. 1 Satz 1 Nr. 4 SGB V die Datenerhebung zum Zweck der Prüfung der Leistungspflicht gestatte. Zudem sei die Erhebung mit einem Arzt des MDK zuvor abgestimmt. Für medizinische Bewertungen würden die gesammelten Informationen dann auch an den MDK weitergeleitet.

Der Landesbeauftragte hat die AOK in Beratungsgesprächen auf Folgendes hingewiesen:

Zur Erfüllung der Aufgaben der AOK gewähren § 284 Abs. 1 Satz 1 Nr. 4 und Nr. 7 SGB V grundsätzlich die Befugnis zur Datenerhebung. Die Anforderung von medizinischen Informationen aus Pflegedokumentationen von Pflegedienstleistenden durch die AOK im Rahmen der Genehmigung häuslicher Krankenpflege ist jedoch unzulässig. Auch für den Bereich der Überprüfung medizinischer Bewertungen zur häuslichen Krankenpflege nach § 37 SGB V ist die Einschaltung des MDK nach Maßgabe des § 275 Abs. 1 Nr. 1 SGB V notwendig.

Bei der Feststellung der Genehmigungsfähigkeit der beantragten Leistung besteht zwar abgesehen von § 275 Abs. 2 Nr. 4 SGB V keine Verpflichtung zur Beteiligung des MDK. Die Krankenkasse kann auf die Einschaltung des MDK verzichten, wenn dies nach dem Krankheitsverlauf nach ihrer Einschätzung nicht erforderlich erscheint. Bedarf jedoch die Überprüfung der Genehmigungsvoraussetzungen einer medizinischen Bewertung anhand zu erhebender medizinischer Informationen, ist hierfür der MDK zuständig. Das Bundessozialgericht (Urteil vom 30. März 2000, Az: B 3 KR 23/99 R) stellte dazu fest, dass die Krankenkasse, die einzelne vom Arzt verordnete Maßnahmen der Behandlungspflege aus medizinischen Gründen nicht für erforderlich hält, hierüber im Regelfall gem. § 275 Abs. 1 Nr. 1 SGB V in Ermangelung einer eigenen Sachkompetenz in medizinischen Fragen eine gutachterliche Stellungnahme des MDK einzuholen hat.

Auch die Richtlinien des Bundesausschusses der Ärzte und Krankenkassen über die Verordnung häuslicher Krankenpflege sehen unter III. Nr. 10 vor, dass der Arzt lediglich die verordnungsrelevanten Diagnosen als medizinische Begründung für die häusliche Krankenpflege mitzuteilen hat. Die Übermittlung weiterer medizinischer Informationen an die Krankenkasse ist nach der Richtlinie nicht vorgese-

hen. Weitere medizinische Informationen erfragt dann ggf. der MDK, sei es vom Patienten, vom Arzt bzw. vom Pflegedienst. Letztere sind gemäß § 276 Abs. 2 Satz 1 2. Halbsatz SGB V verpflichtet, die erforderlichen Sozialdaten unmittelbar an den MDK zu übermitteln. Hierbei ist - durch den insoweit datenschutzrechtlich verantwortlichen MDK - der Erforderlichkeitsgrundsatz zu beachten.

Die AOK hat nunmehr ihr Verfahren umgestellt. Soweit über die Diagnose hinausgehende medizinische Unterlagen zur Prüfung der Leistungsverpflichtung erforderlich sind, gehen diese den datenschutzrechtlichen Anforderungen entsprechend direkt an den MDK.

20.11 Abrechnungsprüfung bei häuslicher Krankenpflege

Die Einsichtnahme in Pflegedokumentationen war auch Schwerpunkt der Erörterungen des Landesbeauftragten mit der AOK im Hinblick auf die Prüfung von Abrechnungen im Bereich der häuslichen Krankenpflege nach den Vorschriften des SGB V. Dazu wies die AOK darauf hin, dass jede Kasse selbst Einzelverträge nach § 132a Abs.2 Satz 1 SGB V im Rahmen der Richtlinien nach § 92 SGB V und der Rahmenempfehlungen nach § 132a Abs. 1 SGB V mit den Leistungserbringern abschließe. Dabei seien grundsätzlich auch Abrechnungsprüfungen vorgesehen, die aber von den Leistungserbringern in datenschutzrechtlicher Hinsicht als kritisch angesehen würden. Auch hier sei es - wie im Bereich der Pflegeversicherung - erforderlich, in das in der Pflegedokumentation vorhandene Durchführungsblatt Einsicht zu nehmen.

Der Landesbeauftragte hat die AOK darauf hingewiesen, dass die Grundsätze für die Genehmigung der häuslichen Krankenpflege auch für die Prüfung der Abrechnungen zur häuslichen Krankenpflege nach dem SGB V gelten, soweit die Leistungen nicht nach § 114 Abs. 3 Satz 1 und 2 SGB XI in das dortige Prüfverfahren einbezogen sind (vgl. Ziff. 20.24). Demnach gewährleistet zwar die Regelung des § 284 Abs. 1 Nr. 8 SGB V grundsätzlich die Erhebungsbefugnis der Krankenkasse zu Zwecken der Prüfung der Abrechnung. Es besteht jedoch die Notwendigkeit der Einschaltung des MDK für die Bewertung medizinischer Daten nach § 275 ff. SGB V.

Nach umfänglichen Erörterungen unter Einbeziehung von Vertretern von Verbänden der Pflegedienstleister konnten auch hier sachgerechte und datenschutzkonforme Lösungen gefunden werden. Anhand eines Musters eines Durchführungsblattes konnte festgestellt werden, dass dort keine schützenswerten sensiblen Informationen verzeichnet waren. Über die Notiz zur durchgeführten Pflegemaßnahme und das Handzeichen des Sachbearbeiters hinaus sind keine medizinischen Informationen zum Betroffenen enthalten, die der Krankenkasse nicht bereits anderweitig bekannt sind. Gegen die Kenntnisnahme eines derart gestalteten Durchführungsblattes im Einzelfall zur Abrechnungsprüfung wurden daher keine datenschutzrechtlichen Bedenken geltend gemacht. Dies setzt allerdings ein Verfahren voraus, dass der Krankenkasse die Kenntnisnahme der weiteren Bestandteile der Pflegedokumentation mit den dort enthaltenen sensiblen medizinischen Informationen (z.B. zur Ansprechbarkeit, zu Schmerzen, zu Essgewohnheiten oder Miktionsstörung) vorenthält.

20.12 „Task Force“ nach § 197a SGB V

Der Landesbeauftragte erörterte mit der AOK die Einsicht in Pflegedokumente im Rahmen der Prüfung der häuslichen Krankenpflege nach § 37 SGB V. Auf die Frage nach der Rechtsgrundlage für die Prüfungen im Bereich des SGB V wurde seitens der AOK darauf verwiesen, dass nach § 197a SGB V Stellen zur Bekämpfung von Fehlverhalten im Gesundheitswesen eingerichtet worden seien. Sie nähmen nach § 197a Abs. 1 Satz 2 SGB V Kontrollbefugnisse nach § 67c Abs. 3 SGB X wahr. Eine Prüfung sei auch in § 132a Abs. 1 Satz 4 Nr. 5 SGB V vorgesehen. Insgesamt würde deutlich, dass eine externe Kontrollbefugnis auch im Hinblick auf Pflegedokumente bestünde (siehe auch Ziff. 20.24).

Der Landesbeauftragte hat dazu dargelegt, dass die Rechtsgrundlage für die Datenerhebung zur Prüfung von Abrechnungen zu Leistungen der häuslichen Krankenpflege in § 284 Abs. 1 Satz 1 Nr. 8 SGB V gegeben ist. Es sind dabei jedoch die Vorschriften der §§ 275 ff SGB V zu berücksichtigen, wonach für die Bewertung medizinischer Fragen die Einschaltung des MDK notwendig ist.

Aus § 197a SGB V ergibt sich dagegen keine Befugnis für die AOK zur Erhebung von Informationen aus Pflegedokumenten. § 197a SGB V sieht zwar die Schaffung einer organisatorischen Einheit bei der Krankenkasse vor, die Fällen und Sachverhalten im Zusammenhang mit der Nutzung der Finanzmittel nachgeht. Die Einheit nimmt Kontrollbefugnisse nach § 67c Abs. 3 SGB X wahr. § 67c Abs. 3 SGB X enthält aber lediglich die Fiktion, dass eine Speicherung, Veränderung oder Nutzung von Sozialdaten für bestimmte Verwaltungsmaßnahmen, u.a. für Kontrollen für die verantwortliche Stelle, keine Zweckänderung darstellen. Das bedeutet, dass die in der AOK vorhandenen Sozialdaten für die dort genannten Zwecke, hier also die Kontrolle durch die Einheit nach § 197a SGB V, genutzt werden können. Datenerhebungen regelt § 67c SGB X nicht. Erst recht bewirkt er keine über die Spezialregelungen der §§ 284, 275ff SGB V hinausgehenden Erhebungsbefugnisse gegenüber Dritten.

§ 132a Abs. 1 Satz 4 Nr. 5 SGB V sieht zwar vor, dass die Rahmenempfehlungen der Spitzenverbände und -organisationen zur Versorgung mit häuslicher Krankenpflege die Grundsätze der Wirtschaftlichkeit „einschließlich deren Prüfung“ regelt. Eine Prüfung ist daher grundsätzlich vorgesehen. Es können abstrakte Regeln zum Prüfungsverfahren festgelegt werden. Rahmenempfehlungen führen jedoch nicht zu konkreten Eingriffsbefugnissen. Ihnen fehlt die Rechtsverbindlichkeit.

Selbst im Rahmen der Zusammenarbeit nach § 197a Abs. 3 dürfen personenbezogene Daten nicht übermittelt werden. Lediglich die innerhalb der Organisation vorhandenen personenbezogenen Daten dürfen für die Kontrollzwecke des Abs. 1 verwendet werden, es liegt dann keine Zweckänderung vor, die einer Rechtsgrundlage bedürfte. Die Daten müssen jedoch auf anderer Grundlage, wie z.B. § 284 Abs. 1 Satz 1 Nr. 8 SGB V unter Berücksichtigung von §§ 275 ff SGB V, gewonnen worden sein.

20.13 Selbstauskunft eines Versicherten gegenüber der Krankenkasse

Ein Arzt beklagte sich darüber, dass bei längeren Arbeitsunfähigkeiten eine Krankenkasse Selbstauskünfte von Versicherten in Form von Fragebögen abforderte. Neben dem Namen und der Krankenversichertennummer sollte der Betroffene u.a. vorhandene Beschwerden angeben. Der Versicherte hatte in dem Fragebogen auch Angaben zu seinen Angehörigen und deren gesetzlicher Krankenversicherung vorzunehmen. Letztendlich sollte er der Krankenkasse mitteilen, wann eine Arbeitsaufnahme bzw. Meldung bei der Agentur für Arbeit voraussichtlich möglich werde und bei welchen Ärzten er wöchentlich/monatlich in Behandlung sei. Als Rechtsgrundlage für die Datenerhebung gab die Krankenkasse § 35 SGB I i.V.m. § 67a SGB X an. Der Versicherte sollte nach den §§ 60 ff. SGB I zur Abgabe des Vordrucks verpflichtet werden. Die Krankenkasse gab an, die Sozialdaten für den MDK im Rahmen einer Begutachtung zu erheben.

Der Landesbeauftragte wies darauf hin, dass Sozialdaten für eine Begutachtung nach § 275 SGB V grundsätzlich nur durch den MDK angefordert werden dürfen. Nur dieser kann beurteilen, welche Sozialdaten für die gutachterliche Stellungnahme und Prüfung erforderlich sind.
Die Krankenkassen dürfen nur das Ergebnis der Begutachtung erhalten (§ 277 Abs. 1 Satz 1 SGB V). Daraus folgt, dass die Krankenkassen gerade nicht die Sozialdaten erhalten dürfen, die der MDK für die Beratung und Begutachtung benötigt.

Durch den Landesbeauftragten wurde die datenschutzrechtliche Überarbeitung des bisher verwendeten Fragebogens erreicht. So wurde u.a. die Angabe der Angehörigen und deren gesetzliche Krankenversicherung ersatzlos gestrichen.

Nunmehr wird der Selbstauskunftsbogen nur im Einzelfall auf Vorschlag des MDK an die Versicherten mit der Bitte gesandt, den Selbstauskunftsbogen in einem beigefügten, zu verschließenden Umschlag mit der Aufschrift „Nur vom MDK zu öffnen“ zurückzuschicken.

20.14 Fehlbelegungsprüfungen durch den MDK in Krankenhäusern

Bereits im IV. Tätigkeitsbericht (Ziff. 23.8) und im V. Tätigkeitsbericht (Ziff. 18.5) hat sich der Landesbeauftragte zu Fehlbelegungsprüfungen durch den MDK geäußert. Weitere Eingaben zur Anforderung von Kopien aus patientenbezogenen Unterlagen waren Anlass, sich erneut mit dem MDK in Verbindung zu setzen.
Jährlich werden ca. 50.000 Prüfungen durchgeführt, wobei die Gutachter des MDK in ca. 4.500 Überprüfungen vor Ort in den Krankenhäusern tätig werden. Lediglich bei einigen Prüfungen werden Auszüge aus den Krankenakten abgefordert, da diese in der Regel ausreichen, die Abrechnung zu überprüfen. Nur in ca. 200 Fällen jährlich seien komplette Krankenakten als Kopie abgefordert worden. Dies seien bestimmte Fälle, die inhaltlich eine umfassende Würdigung des Vorgangs erforderlich machen, wie insbesondere neurologische Fälle, Widerspruchsverfahren oder Einzelfälle, in denen Auszüge (Epikrisen, OP-Berichte) kein vollständiges Bild ergeben. Die Anforderung von Unterlagen zur Versendung an den MDK erfolgt vornehmlich aus Effizienzgesichtspunkten, um die kostbare Ressour-

ce ärztlicher Prüfungstätigkeit durch Vermeidung unangemessener Reisetätigkeit sinnvoll einzusetzen. Hierbei werden insbesondere zur Vermeidung des Verlustes von Originalunterlagen Kopien übersandt.

Das Verfahren des MDK entsprach im Wesentlichen der Rechtslage:
Rechtsgrundlage für die Übermittlung personenbezogener Informationen durch das Krankenhaus an den MDK ist § 17c Abs. 2 Satz 4 Krankenhausgesetz Sachsen-Anhalt (KHG LSA), wonach das Krankenhaus die erforderlichen Unterlagen, einschließlich der Krankenunterlagen, „zur Verfügung zu stellen“ und die erforderlichen Auskünfte zu erteilen hat. Grundsätzlich ergibt sich zunächst, dass dem MDK die personenbezogenen Informationen zustehen, die unter strenger Berücksichtigung des Verhältnismäßigkeitsgrundsatzes für die Durchführung der Prüfung unerlässlich sind. In welcher Form der MDK Zugang zu den Informationen hat, ist jedoch offen gelassen. § 17c Abs. 2 Satz 5 KHG LSA geht davon aus, dass der MDK die Prüfung grundsätzlich in den Räumen des Krankenhauses durchführt.

Doch hat der Gesetzgeber auch nicht ausgeschlossen, dass der MDK über Kopien mit Sozialdaten verfügen kann. Dies ergibt sich schon aus § 17c Abs. 2 Satz 7, wonach die gespeicherten Sozialdaten zu löschen sind, sobald ihre Kenntnis für die Zweckerfüllung nicht mehr erforderlich ist.

Den datenschutzrechtlichen Anforderungen dürfte nur ein Verfahren gerecht werden, in dem die Prüfung der Unterlagen grundsätzlich vor Ort stattfindet und die Mitnahme von Kopien für die Dokumentation der Verwaltungsvorgänge des MDK und die Erarbeitung der Stellungnahme auf das Unverzichtbare reduziert wird. Die Anforderung kompletter Unterlagen in Kopie zur Prüfung in der Geschäftsstelle des MDK kann daher zur Wahrung eines rechtskonformen Verfahrens lediglich ausnahmsweise in begründeten Einzelfällen vorgenommen werden.

Hierfür sprechen auch die gemeinsamen Empfehlungen zum Prüfungsverfahren nach § 17c KHG LSA der Deutschen Krankenhausgesellschaft und der Spitzenverbände der Krankenkassen vom 6. April 2004. Die dortige Regelung des Prüfverfahrens favorisiert ebenfalls den Verbleib der Patientenakten im Krankenhaus.

20.15 Einsichtnahme in vollständige Behandlungsunterlagen bei der Verfolgung von Schadenersatzansprüchen nach § 66 SGB V und § 116 SGB X

Die Ärztekammer des Landes Sachsen-Anhalt bat den Landesbeauftragten um Unterstützung wegen der durch Krankenkassen an Ärzte gerichteten Aufforderungen, vollständige Patientenunterlagen bzw. ergänzende Auskünfte bei der Prüfung von Behandlungsfehlern nach § 66 SGB V bzw. nach Schadenersatzübergängen gem. § 116 SGB X zu übergeben.

Im ersten Fall bat eine Krankenkasse im Rahmen der Unterstützung der Versicherten bei Behandlungsfehlern und bei Schadensübergängen um Übersendung der vollständigen Behandlungsunterlagen. Die Einwilligungserklärung des Versicherten zur Schweigepflichtsentbindung und Einsichtnahme in die Behandlungsunterlagen lag vor.

Der Landesbeauftragte wies darauf hin, dass zur Erfüllung der Aufgaben nach § 66 SGB V die Krankenkasse nach § 284 Abs. 1 Nr. 5 SGB V zur Erhebung und Speicherung von Daten befugt sei. Rechtsgrundlage für die Übermittlung durch den Arzt ist die Einwilligungserklärung und Entbindung von der Schweigepflicht durch den Versicherten. Dies setzt allerdings voraus, dass das Angebot so ausgerichtet ist, dass die **Initiative** zur Unterstützung vom **Versicherten** ausgehen muss. Zudem müssten die Unterlagen im Zusammenhang mit dem vermuteten Behandlungsfehler stehen (konkrete Schadensvermutung). Dies ist nach den Umständen des Einzelfalls zu prüfen.

Weiterhin wurde dem Landesbeauftragten berichtet, dass eine Krankenkasse beabsichtigte, übergegangene Schadenersatzansprüche nach § 116 SGB X geltend zu machen, und zur Sachverhaltsaufklärung einen entsprechenden Fragebogen verwendete.

Der Landesbeauftragte hat die Ärztekammer Sachsen-Anhalt darauf hingewiesen, dass grundsätzlich erforderliche Daten an die Krankenkasse zu übermitteln sind, sofern Hinweise auf drittverursachte Gesundheitsschäden vorliegen (§ 294a SGB V).

In Anbetracht der Tatsache, dass der Vertragsarzt die erforderlichen Daten, einschließlich der Angaben über Ursachen, nach § 294a SGB V der Krankenkasse mitzuteilen hat, hielt der Landesbeauftragte es für vertretbar, die Abfrage mittels eines konkretisierten inhaltlich begrenzten Fragebogens vorzunehmen. Er wies darauf hin, dass § 294a SGB V eine bereichsspezifische Übermittlungsgrundlage darstellt, die ein zusätzliches Einverständnis des Patienten nicht erfordert.

20.16 Einsichtnahme in Patientenakten zur externen Qualitätssicherung

In Sachsen-Anhalt haben die Landesverbände der Krankenkassen und privaten Krankenversicherungen, die Krankenhausgesellschaft und die Ärztekammer einen Lenkungsausschuss Qualitätssicherung eingerichtet. Zur Wahrnehmung der koordinierenden, organisatorischen und inhaltlichen Aufgaben für die Qualitätssicherungsverfahren hat der Lenkungsausschuss eine Projektgeschäftsstelle Qualitätssicherung installiert. Die Geschäftsführung der Projektgeschäftsstelle wurde der Ärztekammer Sachsen-Anhalt übertragen.

Die Ärztekammer Sachsen-Anhalt bat den Landesbeauftragten zu prüfen, ob zu Zwecken der Qualitätssicherung die Einsicht in Patientenakten eines Krankenhauses durch Vertreter der Projektgeschäftsstelle zulässig ist. Insbesondere war zu klären, ob die Qualitätssicherung gem. § 137 SGB V unter das Tatbestandsmerkmal des § 26 Abs. 1 Nr. 8 DSG-LSA „Zweck der Gesundheitsversorgung“ subsumiert werden kann.

Im Ergebnis stellte der Landesbeauftragte fest, dass die Einsichtnahme in Patientenakten eines Krankenhauses durch Mitarbeiter der Projektgeschäftsstelle nicht möglich ist. Die Projektgeschäftsstelle ist keine verantwortliche Stelle im Sinne des § 2 Abs. 8 DSG-LSA. Sie unterliegt nicht dem Anwendungsbereich des § 3 Abs. 1 DSG-LSA. Denn neben den Verbänden der Krankenkassen und der Ärzte-

kammer sind auch die privaten Krankenversicherungen und die Krankenhausgesellschaft Vertragspartner für die bei der Ärztekammer Sachsen-Anhalt eingerichtete Projektgeschäftsstelle Qualitätssicherung.

Unter diesem Gesichtspunkt konnte auch § 26 Abs. 1 Nr. 8 DSG-LSA keine Anwendung finden. Auch das KHG LSA sieht - anders als in einigen anderen Bundesländern - keine bereichsspezifischen Regelungen vor, die eine Einsichtnahme in Patientenakten im Rahmen der Prüfung zulassen.

Der Ärztekammer wurde mitgeteilt, dass nur ein Datenabgleich aufgrund anonymisierter Dokumente aus der Patientenakte - wie bisher auch - möglich sei.

SGB VII

20.17 Anforderung von Patientenunterlagen durch Berufsgenossenschaften zur Abrechnungsprüfung

Die Krankenhausgesellschaft Sachsen-Anhalt e.V. hatte die Auffassung des Landesbeauftragten erfragt, ob Berufsgenossenschaften zu Zwecken der Abrechungsprüfung Patientenunterlagen anfordern dürften und ob eine Übermittlung zulässig sei.

Die Frage der Rechtsgrundlage der Übermittlung von personenbezogenen Informationen durch Ärzte bzw. auch durch Krankenhäuser (vgl. § 100 Abs. 1 Satz 3 SGB X) an Berufsgenossenschaften zum Zweck der Abrechnungsprüfung ist im Berichtszeitraum im Kreis der Datenschutzbeauftragten des Bundes und der Länder intensiv erörtert worden. Gegen eine pauschale Anforderung von Krankenhausentlassungsberichten bestanden datenschutzrechtliche Bedenken. Andererseits war das Anliegen einer sachgerechten Abrechnungsprüfung nachvollziehbar. Im Ergebnis konnte der Landesbeauftragte Folgendes darlegen:

§ 201 SGB VII stellt grundsätzlich keine Rechtsgrundlage für die pauschale Anforderung von Krankenhausentlassungs- bzw. OP-Berichten durch Berufsgenossenschaften dar.

Im Einzelfall und insbesondere unter strenger Berücksichtigung des Erforderlichkeitsgrundsatzes ist es den Berufsgenossenschaften jedoch auf der Grundlage des § 199 Abs. 1 Satz 1, Satz 2 Nr. 2 SGB VII gestattet, für notwendige Abrechnungsprüfungen die erforderlichen Informationen zu erheben. § 199 SGB VII zählt zwar Aufgaben inhaltlich auf, enthält aber keine abschließenden Regelungen. Demgemäß ist auch eine Aufgabenzuweisung durch einen festgestellten Sachzusammenhang im Rahmen der gesetzlichen Aufzählung denkbar. Zur Leistungserbringung gehört sachnotwendig auch die entsprechende Abrechnung der Leistung.

Bestehen daher im konkreten Einzelfall Anhaltspunkte für die Notwendigkeit einer Abrechnungsüberprüfung, können seitens des Unfallversicherungsträgers weitere - erforderliche - Informationen zur Abrechnungsprüfung erhoben werden. Der Um-

fang ist auf das unerlässliche Maß zu begrenzen. Anhaltspunkte dürften sich in der Regel aus dem Katalog des § 301 SGB V ergeben.

Rechtsgrundlage für die Übermittlung der insoweit notwendigen Informationen kann § 201 Abs. 1 Satz 1, 2 SGB VII sein. Der Rückgriff auf diese Rechtsgrundlage ist insbesondere dann möglich, wenn keine anderweitige spezialgesetzliche Grundlage, wie in Sachsen-Anhalt, gegeben ist.
Hierfür spricht zunächst die Systematik der korrespondierenden Regelungen zur Datenerhebung durch die Sozialleistungsträger und der Datenübermittlung durch die Leistungserbringer, die sich auch in anderen Büchern des SGB findet. Es wäre nicht eingängig, dass der Gesetzgeber in § 199 SGB VII die Erhebungsbefugnis für die genannten Daten vorsieht, die Übermittlungsbefugnis aber und damit letztendlich eine sachdienliche Abrechnungsprüfung von landesgesetzlichen Zufälligkeiten abhängig machen wollte. Zudem bestehen keine Prüfungsalternativen, wie etwa durch den MDK.

Im Ergebnis wird daher stets im Einzelfall abzugrenzen sein, inwieweit auf den genannten Rechtsgrundlagen ein Ausgleich zwischen dem legitimen Interesse der Berufsgenossenschaft an einer sachdienlichen Abrechnungsprüfung einerseits und den notwendigen Verschwiegenheitsinteressen des Krankenhauses und der Ärzte in Bezug auf die Patientenunterlagen andererseits gefunden werden kann.

20.18 Zuständigkeit für den Regionalträger der Deutschen Rentenversicherung Mitteldeutschland

Zur Verbesserung der Wirtschaftlichkeit bzw. Leistungsfähigkeit können sich Regionalträger der Deutschen Rentenversicherung auf Beschluss ihrer Vertreterversammlung zu einem Regionalträger vereinigen, sofern sich der Zuständigkeitsbereich des neuen Regionalträgers nicht über mehr als drei Bundesländer erstreckt, er also landesunmittelbar bleibt.
Hierzu haben sich die bisherigen Landesversicherungsanstalten Thüringen, Sachsen und Sachsen-Anhalt entschlossen. Der neue Regionalträger Deutsche Rentenversicherung Mitteldeutschland hat seinen Hauptsitz in Leipzig.

Entsprechend Artikel 87 Abs. 2 Satz 2 GG haben die Beteiligten Sachsen als aufsichtsführendes Land bestimmt. Die somit bestehende Aufsichtszuständigkeit des Landes Sachsen für die Deutsche Rentenversicherung Mitteldeutschland ist mit der Landeszugehörigkeit im Sinne des § 81 Abs. 2 Satz 2 SGB X gleichzusetzen. Daraus folgt, dass die Kontrollzuständigkeit des Sächsischen Landesbeauftragten für den Datenschutz gegeben ist. Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt hat diese Rechtsauffassung bestätigt.

SGB VIII

20.19 Schutzauftrag bei Kindeswohlgefährdung - Einführung des § 8a SGB VIII

Aufgrund gravierender Fälle von Kindeswohlgefährdung hat der Gesetzgeber bereits durch das „Gesetz zur Weiterentwicklung der Kinder- und Jugendhilfe“ vom 8. September 2005 (Kinder- und Jugendhilfeentwicklungsgesetz - KICK, BGBl. I

S. 2729) den § 8a SGB VIII neu eingeführt. Außerdem wurden die §§ 42 (Inobhutnahme durch Jugendamt) und 72a SGB VIII (Führungszeugnis für Beschäftigte in der Jugendhilfe) neu geregelt. Ziel des Gesetzgebers war es, den staatlichen Schutzauftrag der Kinder- und Jugendhilfe bei Kindeswohlgefährdungen zu konkretisieren.
Doch auch nach Inkrafttreten dieser neuen Regelungen kam es wieder zu Todesfällen bei Kindern, leider auch in Sachsen-Anhalt.

Infolge dessen wird nunmehr in der Öffentlichkeit erneut eine Diskussion über Kindeswohlgefährdungen und Möglichkeiten der Behörden zum Eingreifen sowie über Frühwarnsysteme und verpflichtende Vorsorgeuntersuchungen geführt.
Im November 2006 nahm der Landesbeauftragte an einem vom Präsidenten des Landgerichtes Stendal veranstalteten Kolloquium „Kommunikatives Netzwerk Kindeswohl“ teil. Der Landesbeauftragte hat dabei seine Position zur Zusammenarbeit der Behörden mit den Jugendämtern, zu Rechtsgrundlagen und der Praxis der Präventions- und Interventionsmaßnahmen dahingehend dargelegt, dass die bisher gültigen Rechtsgrundlagen ausreichend erscheinen. Ein „Mehr an Staat“ kann leicht zu einer „Familienpolizei“ führen und macht alle Eltern potenziell zu Personen, die ihre Kinder vernachlässigen. Künftige politische und gesetzgeberische Entscheidungen sollten daher im Hinblick auf Überregulierung und Überwachung genauestens abgewogen werden. Im Rahmen eines vom Landesbeauftragten initiierten Erfahrungsaustauschs in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde festgestellt, dass Datenschutz und Kindesschutz kein Gegensatz sind; dies belegen viele Kooperationsprojekte in den Ländern.

Sachsen-Anhalt plant, die Früherkennungsuntersuchungen verbindlicher zu gestalten und hat dafür gemeinsam mit Hamburg eine Entschließung im Bundesrat erwirkt. Danach sollen die Krankenkassen schriftlich zu den Untersuchungen einladen. Im Falle der Nichtbefolgung durch die Eltern sollen die Krankenkassen die Daten an das Gesundheits- und Jugendamt weitergeben können. Das Jugendamt soll nach einer zweiten verstrichenen Einladung im Elternhaus nachschauen dürfen.

Die Bundesregierung steht solchen Überlegungen bislang eher skeptisch gegenüber; das Bundesjustizministerium plant eine Initiative zur Stärkung der Befugnisse der Familiengerichte (§ 1666 BGB) und zu Möglichkeiten z.B. der Schulen, sich ohne Umweg über das Jugendamt direkt ans Gericht wenden zu können.

Eine angedachte landesgesetzliche Regelung eines Datenabgleichs mit Meldepflichten zur Durchsetzung von Früherkennungsuntersuchungen hätte nicht nur die staatliche Wächterfunktion (Art. 6 Abs. 2 Satz 2 GG, Art. 11 Abs. 1 Satz 2 Landesverfassung) zu berücksichtigen, sondern u.a. auch den Grundsatz der Verhältnismäßigkeit, wie er in § 8a SGB VIII zum Ausdruck kommt. Auch wurde im Dezember 2006 z.B. ein Expertenrat aus Jugend-, Sozial- und Gesundheitsamt, Beratungsstellen, Ärzten, Hebammen, Kindertagesstätten, Schulen, Justiz und Polizei unter dem Titel „Allianz für Kinder in Sachsen-Anhalt“ eingesetzt. Ein weiterer Baustein soll das Familienhebammen-Projekt sein. Der Landesbeauftrag-

te wurde bei der Überarbeitung eines Leitfadens für Ärzte „Gewalt gegen Kinder und Jugendliche“ beteiligt.

20.20 Fragebogen für künftige Pflegeeltern

Durch die Anfrage eines Landkreises wurde der Landesbeauftragte auf einen Fragebogen zur Aufnahme eines Pflegekindes aufmerksam, der im Rahmen eines durch das Landesjugendamt geförderten Projektes entstanden war. Die Abfragen richteten sich auf spezifische Angaben in teilweise sensiblen Bereichen. Der Fragebogen bezog sich auf Unterbringungen im Rahmen von Hilfe zur Erziehung in Vollzeitpflege gem. §§ 27, 33 SGB VIII. Dabei müssen die Pflegepersonen besonderen fachlichen Ansprüchen genügen. Ihre Eignung für die Betreuung schwieriger, traumatisierter Kinder ist im Vorfeld der Unterbringung durch das zuständige Jugendamt festzustellen.

Im Rahmen der Beratung des Landesjugendamtes wurden einzelne Aspekte des Fragebogens aufgegriffen. Oberstes Gebot ist zweifellos die Wahrung des Kindeswohles. Darüber hinaus ist jedoch auch im Bereich des SGB VIII auf die Einhaltung der verfassungsrechtlichen Rahmenbedingungen der Erforderlichkeit und Verhältnismäßigkeit Acht zu geben.
Der Landesbeauftragte hat daher zu einzelnen konkreten Fragen angeregt, die Erforderlichkeit kritisch zu prüfen. Zu anderen Fragestellungen konnte er deutlich machen, dass eine zu pauschale Fragestellung eine den gewünschten Erkenntnissen nicht angemessene und über das Ziel hinausgehende Datenübermittlung verursachen könnte. Dies wäre mit den Geboten der Datensparsamkeit und Datenvermeidung nicht zu vereinbaren. Insgesamt bat daher der Landesbeauftragte darum, die Möglichkeit einer Reduzierung, Präzisierung und Konkretisierung der Datenerhebung zu überprüfen.

20.21 Prüfung von Kindertagesstätten

Im Berichtszeitraum hat der Landesbeauftragte auch in Kindertagesstätten vor Ort die Einhaltung der datenschutzrechtlichen Vorschriften überprüft. Insgesamt ist hier hervorzuheben, dass in den Kindertagesstätten aus datenschutzrechtlicher Sicht sehr verschiedene Sachlagen festzustellen waren.

In einer Kindertagesstätte werden die Eltern während des Aufnahmegespräches gebeten, eine Karteikarte zu persönlichen Angaben des Kindes auszufüllen. Neben den Personalien und der Adresse des Kindes werden ebenfalls die private Telefonnummer, die Arbeitsstelle und dienstliche Telefonnummer beider Elternteile, der Hausarzt, die Krankenkasse und der Impfstatus des Kindes und die abholberechtigten Personen abgefragt. Gemäß § 62 Abs. 1 SGB VIII dürfen Sozialdaten nur erhoben werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. Alle Daten (außer abholberechtigte Personen) werden für den Notfall erhoben. Außerdem werden die Daten Hausarzt, Krankenkasse und Impfstatus an den jeweiligen Notarzt für eine schnellere Behandlung übermittelt. Der Landesbeauftragte hat darauf hingewiesen, dass eine Notversorgung des Kindes durch den Arzt immer zu gewährleisten ist, auch wenn die o.g. Daten nicht vorliegen würden. Da aber die meisten Eltern wohl eine Information bei Eintritt eines

Notfalles wünschen werden, hat der Landesbeauftragte empfohlen, die Datenerhebung der dienstlichen und privaten Telefonnummern auf dem Vordruck mit dem schriftlichen Hinweis auf freiwillige Angabe und auf den Erhebungsgrund zu versehen. Da die Angabe der Arbeitsstelle der Eltern jedoch nicht erforderlich ist, hat der Landesbeauftragte angeregt, diese Daten nicht weiter zu erheben. Außerdem hat der Landesbeauftragte empfohlen, die Erforderlichkeit der Datenerhebung Hausarzt, Krankenkasse und Impfstatus erneut zu überdenken und, soweit diese zumindest nützlich sein sollten, diese Abfragen jedenfalls auch mit einem Freiwilligkeitshinweis und der Einholung der Einwilligungserklärung der Erziehungsberechtigten zur Datenübermittlung an den Notarzt zu verbinden. Der Vordruck wurde daraufhin von der Kindertagesstättenleiterin entsprechend den dargestellten Hinweisen überarbeitet.

In einer anderen Kindertagesstätte hat der Landesbeauftragte festgestellt, dass ärztliche Bescheinigungen über die gesundheitliche Eignung von Kindern, die gem. § 18 Abs. 1 Kinderförderungsgesetz des Landes Sachsen-Anhalt (KiFöG) nach jeder Krankheit eines Kindes in der Kindertagesstätte vorzulegen sind, seit ca. zehn Monaten noch immer im Gruppenbuch aufbewahrt werden. Die Erhebung erfolgt zur Sicherstellung, dass kranke Kinder in der Kindertagesstätte keine weiteren Kinder anstecken können und ggf. zur Nachprüfung bei Ansteckungen. Eine kurzfristige Aufbewahrung dieser Bescheinigungen ist daher vertretbar. Aufgrund der überschaubaren Inkubationszeiten von Krankheiten ist eine zehnmonatige Aufbewahrung eher nicht notwendig. Der Landesbeauftragte hat daher unter Hinweis auf § 84 SGB X angeregt, die tatsächlich erforderlichen Aufbewahrungszeiten zu ermitteln und festzulegen und die entsprechenden Bescheinigungen datenschutzgerecht zu vernichten.

Die Kindertagesstätten arbeiten jeweils mit einer Grundschule bezüglich der einzuschulenden Kinder im Rahmen von „Schnupperstunden“ zusammen. Vereinzelt finden dann auch Gespräche zwischen Erzieherinnen und zukünftigen Klassenleitern oder dem Schulleiter statt. Die Kindertagesstätten haben für diese Gespräche bisher keine Einwilligungserklärungen der Erziehungsberechtigten eingeholt und verwiesen auf die zugehörige Schule. Dort wurde allerdings mit dem Hinweis auf die in der Kindereinrichtung vorliegenden Einwilligungserklärung ebenfalls keine Einwilligung eingeholt. Bei diesen Gesprächen handelt es sich aber um Datenerhebungen gem. § 84a Abs. 3 SchulG LSA durch die Schule und um Datenübermittlungen von der Kindertagesstätte an die Schule (§ 67 Abs. 6 Satz 2 Nr. 3 SGB X). Die Übermittlung personenbezogener Daten ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung, hier in Gestalt des Sozialgeheimnisses (§ 35 Abs. 1 SGB I). Sie ist gem. § 67b Abs. 1 Satz 1 SGB X nur zulässig, wenn das SGB sie erlaubt oder der Betroffene bzw. seine Erziehungsberechtigten eingewilligt haben. Die Regelungen des SchulG LSA und des DSG-LSA sind auf Übermittlungen von Kindertagesstätten an Schulen im Rahmen der Zusammenarbeit nicht anwendbar. Zulässig wäre eine Datenübermittlung daher nur auf der Grundlage der Einwilligung der Erziehungsberechtigten des betroffenen Kindes. Diese Einwilligung muss allerdings den Voraussetzungen des § 67b Abs. 2 SGB X entsprechen, insbesondere aufgrund hinreichender Informationen zu Zweckbestimmungen, Identität der verantwortlichen Stelle und Empfängern erfolgen. Der Landesbeauftragte hat daher den Kindertagesstätten empfohlen, bei Gesprächs-

bedarf im Einzelfall zuvor die Einwilligung der Erziehungsberechtigten einzuholen. Dieses datenschutzrechtlich korrekte Verfahren aus schulischer Sicht wird in Ziff. 19.4.2 dargestellt.

20.22 Ärztliche Untersuchungen in Kindertagesstätten

Kindertagesstätten sind gelegentlich unsicher, ob die Teilnahme der Kinder an den regelmäßig stattfindenden ärztlichen und zahnärztlichen Untersuchungen gem. § 18 Abs. 2 KiFöG der vorherigen Einwilligung der Eltern bedarf. Der Landesbeauftragte vertritt, ebenso wie das Ministerium für Gesundheit und Soziales des Landes Sachsen-Anhalt, die Auffassung, dass die Teilnahme der Kinder an den Untersuchungen freiwillig ist, so dass folgerichtig die Eltern zuvor in die Untersuchung eingewilligt haben müssen. Zum Einen wird eine Teilnahmepflicht, wie in § 38 Abs. 2 SchulG LSA verankert, nicht explizit im KiFöG geregelt. Zum Anderen besteht nach § 36 Abs. 1 SchulG LSA die Schulpflicht, während der Besuch einer Kindertagesstätte nach § 2 Abs. 1 KiFöG jedoch freiwillig ist.

SGB IX

20.23 Klientenverwaltungssystem für Integrationsfachdienste

Der Landesbeauftragte hatte im Januar 2006 erfahren, dass in Sachsen-Anhalt das Programm Klientenverwaltungssystem für Integrationsfachdienste (KLIFD) eingesetzt wird. Hierbei handelt es sich um ein Programm, dass in den auf der Grundlage der §§ 109 ff SGB IX tätigen Integrationsfachdiensten (IFD) die interne Dokumentation sicherstellen soll. Außerdem sollen dort alle Daten zur Verfügung stehen, die dem Integrationsamt (IA) zu übermitteln sind. KLIFD wurde in Sachsen-Anhalt bereits im Februar 2005 aufgrund eines Beschlusses der Bundesarbeitsgemeinschaft der Integrationsämter und Hauptfürsorgestellen eingeführt. Eine Beteiligung des Landesbeauftragten vor Einführung dieses Verfahrens erfolgte nicht.

Aufgrund der sodann erfolgten Abstimmung mit dem Landesverwaltungsamt konnte der Landesbeauftragte zwar feststellen, dass die Anwendung von KLIFD nicht auf grundlegende datenschutzrechtliche Bedenken stößt. Im Einzelnen waren jedoch Änderungen vorzunehmen, um den datenschutzrechtlichen Anforderungen zu genügen. Diese waren z.B.:

Gelöschte Datensätze in der Datenbank des IFD werden als solche lediglich gekennzeichnet, nicht jedoch physisch aus dem Datenbestand entfernt. In dieser Form werden sie bei der nächsten Datenübertragung an das IA gesendet.

Da die Datenbanken mittels Texteditor manipulierbar sind, ist nicht erkennbar, wer wann eine Änderung veranlasst hat. Die Integrität der gespeicherten Daten ist zu gewährleisten. Zur Zeit stehen die administrativen Funktionen allen Softwarenutzern in den IFD zur Verfügung.

Die unterschiedlichen Phasen der Unterstützung der Klienten (Kontaktaufnahme, Beratung, Betreuung) werden nicht durch verschiedene Masken abgebildet. In

den IFD entscheidet jeder Mitarbeiter selbst, welche Eingaben erforderlich sind. Eine Unterscheidung sollte jedoch im Hinblick auf den Erforderlichkeitsgrundsatz bereits durch die Software unterstützt werden. Dies würde die Gefahr mindern, dass mehr personenbezogene Daten der Klienten als erforderlich erhoben und gespeichert werden.

Eine Unterscheidung zwischen Pflicht- und freiwilligen Angaben findet z.Zt. nicht statt. Erst eine Plausibilitätskontrolle bei der Speicherung zeigt fehlende Einträge. Die Software sollte derart geändert werden, dass verpflichtende und freiwillige Angaben unterschieden werden können.

In KLIFD sind Kontaktpersonen bei Kooperationspartnern als Datensätze in einer eigenen Kontaktpersonendatenbank gespeichert. In den Klientendatensätzen wird ein Verweis auf die Kontaktpersonendatenbank angelegt. Eine Löschung der Einträge in der Kontaktpersonendatenbank ist nicht möglich, da der Verweis beim Klienten sonst in Leere ginge. Im Laufe der Jahre kommt es zu einer Datensammlung zu früheren Mitarbeitern bei Behörden oder Institutionen, die als Ansprechpartner nicht mehr zur Verfügung stehen. Diese Funktion muss aufgrund des Grundsatzes der Datensparsamkeit und Datenvermeidung grundsätzlich überdacht werden.

Das Landesverwaltungsamt hat diese Hinweise umgehend an die Arbeitsgruppe zur Programmpflege und Entwicklung von KLIFD weitergegeben. Im Ergebnis soll zunächst die Löschung von Klientendaten gewährleistet werden. Ob und inwieweit die weiteren Maßgaben umgesetzt werden, wird der Landesbeauftragte weiterhin beobachten.

SGB XI

20.24 Einsichtnahme in Pflegedokumente in der Pflegeversicherung

Auf der Grundlage der §§ 36 ff SGB XI werden durch die Pflegekassen häusliche Pflegeleistungen gewährt. Nach § 80 SGB XI regeln Vereinbarungen der Spitzenverbände die Grundsätze und Maßstäbe zu Qualität und Qualitätssicherung in der ambulanten Pflege. Versorgungsverträge der Pflegekassen mit den Pflegeeinrichtungen nach § 72 SGB XI beziehen die qualitätsbezogenen Verpflichtungen ein. Nach §§ 112 ff SGB XI erfolgt die Überprüfung u.a. der Qualität der Leistung, der Versorgungsabläufe und auch der Abrechnung.

Die Verbände der Pflegedienstleister beklagten hierzu gegenüber dem Landesbeauftragten, dass die Mitarbeiter der AOK als Pflegekasse im Rahmen von Prüfungen der häuslichen Pflege vor Ort Ablichtungen aus Pflegedokumentationen zum Zweck der Abrechnungsprüfung fordern bzw. selbst erstellen und mitnehmen würden.

Die AOK ging davon aus, dass die Regelungen zur Prüfung nach §§ 112 ff SGB XI den Pflegekassen die Abrechnungsprüfung gestatten. Die Pflegedokumentation sei zur Abrechnungsprüfung erforderlich, da in ihr das sog. Durchführungsblatt enthalten sei. Allein dort könne man ersehen, ob eine Leistung - wie abgerech-

net - durchgeführt sei, insbesondere auch durch eine ausreichend qualifizierte Fachkraft. Die Einsichtnahme sei unstreitig zulässig und damit auch die Mitnahme von Kopien.

Die datenschutzgerechte Lösung liegt in der Mitte. Die Unterlagen der Pflegedokumentation stellen keine Abrechnungsunterlagen dar. Zusammengefasst dient die Pflegedokumentation dem Zweck, die ordnungsgemäße Durchführung der Pflege zu gewährleisten. Sie enthält umfängliche medizinische pflegerelevante Daten über den Pflegebedürftigen, wird von allen an der Pflegeleistung Beteiligten geführt und steht im Eigentum des Pflegedienstes. Demgegenüber ist die Befugnis der Pflegekasse zur Erhebung von Daten zu Abrechnungszwecken nach § 94 Abs. 1 Nr. 5 i.V.m. § 105 Abs. 1 Satz 1 Nr. 1 SGB XI auf Unterlagen begrenzt, die die Leistung der Pflegedienste in dem dort genannten Rahmen nachweisen (Art, Menge, Preis usw.). Diese Unterlagen sind von Pflegeunterlagen mit sensiblen medizinischen Daten zu unterscheiden.

Zudem werden Prüfungen vor Ort nach § 114 SGB XI durch den MDK vorgenommen. Allerdings ist ein Vertreter der betroffenen Pflegekasse auf Verlangen nach § 114 Abs. 6 Satz 1 SGB XI an der Prüfung zu beteiligen. Ein Vertreter der Pflegekasse kann damit im Rahmen einer Prüfung des MDK rein faktisch Einsicht in die Pflegedokumentationen nehmen. Datenschutzrechtlich verantwortlich bleibt jedoch der MDK, der die Prüfung durchführt. Ein eigenes Prüfungsrecht oder gar das Recht, selbst Kopien anzufertigen und mitzunehmen, besteht für die AOK nicht. Ein Mitnehmen von Kopien und Einheften in die eigenen Vorgänge würde die Tatbestände des Erhebens und Speicherns erfüllen. § 114 Abs. 6 SGB XI gibt hierfür keine Rechtsgrundlage. Die Berechtigungen des § 114 SGB XI beziehen sich auf den MDK. Die Beteiligung der Vertreter der Pflegekassen nach Abs. 6 erfolgt wegen der Sachnähe zur Abrechnung lediglich durch „Hinzuziehen“ (Begründung zum Entwurf des Pflegequalitätssicherungsgesetzes, BT-Drs. 14/5395 S. 40 zu § 112 Abs. 3 und S. 43 zu § 114 Abs. 6).

Soweit daher seitens der AOK im Einzelfall die Prüfung durch Einsichtnahme in die Durchführungsbögen der Pflegedokumentation für notwendig erachtet wird, hat dies im Rahmen der gesetzlich dafür vorgesehenen Verfahren (§§ 112 ff SGB XI) - durch den MDK - stattzufinden. Der MDK muss nach der durch den Vertreter der Pflegekasse unterstützten Prüfung in eigener Verantwortung entscheiden, ob und welche Informationen an die Pflegekasse nach § 115 Abs. 1 Satz 1 SGB XI weiterzuleiten sind. Bei häuslicher Pflege ist das Ergebnis der Qualitätsprüfung einschließlich der dabei gewonnen Daten und Informationen den zuständigen Pflegekassen zum Zweck der Erfüllung ihrer Aufgaben zu übermitteln. Die Aufgabenerfüllung der AOK ist daher auch bei Beachtung der dargestellten datenschutzrechtlichen Vorgaben nicht beeinträchtigt.

SGB XII

20.25 Erhebung medizinischer Informationen für die Eingliederungshilfe

Das Sozialamt einer Stadt hatte einen Petenten zu seinem Antrag auf Eingliederungshilfe Ambulant Betreutes Wohnen aufgefordert, Befunde und/oder Berichte

von ärztlichen Behandlungen im ambulanten oder stationären Bereich in Bezug auf seine Erkrankung einzureichen. Der Landesbeauftragte wies das Sozialamt darauf hin, dass die Prüfung der Voraussetzungen für die Eingliederungshilfe nach §§ 53, 54 Abs. 1 SGB XII i.V.m. §§ 55 Abs. 1 SGB IX vornehmlich auf die Behinderung im Sinne von § 2 Abs. 1 Satz 1 SGB IX gerichtet ist, die Wesentlichkeit der Behinderung im Sinne des § 53 Abs. 1 SGB XII sowie die Aussicht, dass die Aufgabe der Eingliederungshilfe erfüllt werden kann. Inhaltlich sind daher vornehmlich medizinische Bewertungen vorzunehmen, die ärztlicher Kompetenz bedürfen, die lediglich beim amtsärztlichen Dienst vorliegt.

Das Sozialamt teilte daraufhin mit, dass die medizinische Bewertung tatsächlich Aufgabe des amtsärztlichen Dienstes sei, wohin die Unterlagen weitergeleitet würden. Die Anforderung schon durch das Sozialamt sei jedoch erforderlich, da nach bisherigen Erfahrungen die meisten Antragsteller trotz entsprechender Aufforderung keinerlei Unterlagen zur amtsärztlichen Untersuchung mitgebracht hätten. Das Sozialamt wollte die Informationen nicht selbst bewerten, sondern nur rechtzeitig dem ärztlichen Dienst vorlegen. Erforderlich aus Sicht des Sozialamtes war daher das Gutachten des ärztlichen Dienstes, nicht aber alles, was der Petent vorsorglich an Informationen dem Gutachter zur Berücksichtigung zur Verfügung stellt. Die Unterlagen sollten künftig in einem verschlossenen Kuvert beigebracht werden.

Der Landesbeauftragte hat eine Ergänzung des Verfahrens durch dienstliche Maßnahmen angeregt, die sicherstellen, dass eine Kenntnisnahme der Daten durch das Sozialamt verhindert wird. Die Antragsteller sollten durch hervorgehobenen Fettdruck schriftlich auf die Verwendung eines verschlossenen Kuverts hingewiesen werden und ggf. vorgedruckte Kuverts erhalten, auf denen vermerkt ist, dass es sich um ärztliche Unterlagen handelt, die nur vom amtsärztlichen Dienst zu öffnen sind.

Die Sozialagentur hat von der Auffassung des Landesbeauftragten Kenntnis bekommen und den herangezogenen Gebietskörperschaften vorgegeben, dass im Rahmen der Sachverhaltsaufklärung alle erheblichen Tatsachen festzustellen sind. Hierzu können auch ärztliche Gutachten und die darin dargestellten Informationen gehören, die dann in das medizinische Beiheft übernommen werden.

Dazu konnte der Landesbeauftragte eine weitgehende Übereinstimmung feststellen. Der Erforderlichkeitsgrundsatz ist allerdings stets zu beachten. Die Anspruchsvoraussetzungen können zwar mit der notwendigen Gewissheit festgestellt werden. Die Vorschriften des Sozialdatenschutzes gehen aber den Pflichten des Leistungsträgers zur Amtsermittlung und Beweiserhebung nach §§ 20, 21 SGB X nach dem eindeutigen Wortlaut des § 37 Satz 3 SGB I vor, d.h. sie geben den gesetzlichen Rahmen zulässiger Amtsermittlung.

Ist der Sachbearbeiter danach mangels entsprechender Ausbildung nicht in der Lage, selbst die medizinische Bewertung für das Vorliegen des Tatbestandsmerkmals vorzunehmen (wie beispielsweise zur wesentlichen Behinderung im Rahmen der Eingliederungshilfe), kann er einen ärztlichen Gutachter beauftragen. Welche medizinischen Informationen dieser benötigt, um seine medizinische Be-

wertung gemäß dem Auftrag des Sachbearbeiters durchzuführen, obliegt aber grundsätzlich seiner ärztlichen Verantwortung. So wäre beispielsweise die Erhebung der Körpergröße durch den Sachbearbeiter der Fachverwaltung allein deshalb, weil nach seiner laienhaften Einschätzung dieses Datum zur Anamnese gehört, nicht erforderlich, wenn der beauftragte Arzt nach seiner Fachkenntnis diese Information für die Bewertung der geistigen Gesundheit im Sinne von § 53 Abs. 1 Satz 1 SGB XII i.V.m. § 2 Abs. 1 S.1 SGB IX nicht benötigt.
Der Landesbeauftragte geht davon aus, dass die herangezogenen Gebietskörperschaften auch weiterhin unter Berücksichtigung der sozialdatenschutzrechtlichen Rahmenbedingungen verfahren.

20.26 Ersuchen eines Sozialamtes nach § 45 Abs. 1 Satz 1 SGB XII i.V.m. § 109a Abs. 2 SGB VI beim Träger der Rentenversicherung

Im Rahmen einer Kontrolle eines Sozialamtes wurde dem Landesbeauftragten bekannt, dass das Sozialamt vor Gewährung von Grundsicherung wegen dauerhafter Erwerbsminderung infolge eines Ersuchens des Rentenversicherungsträgers die Übersendung von Untersuchungsbefunden einiger Krankenhäuser erbeten hatte. Das Sozialamt sah sich veranlasst, unter Einschaltung des Gesundheitsamtes und der Hausärzte medizinische Informationen und damit Sozialdaten besonderer Art (§ 67 Abs. 12 SGB X) des Betroffenen abzufordern. Der Landesbeauftragte hält dieses Verfahren für bedenklich.

Ausschließlich und abschließend sollen die Rentenversicherungsträger die medizinische Begutachtung zur Feststellung der genannten Voraussetzungen durchführen und die erforderlichen Daten über die Betroffenen erheben. Insbesondere durch die Regelungen des § 45 Abs. 1 Satz 2 SGB XII hat der Gesetzgeber verbindlich klargestellt, dass die Entscheidung des Trägers der Rentenversicherung für den ersuchenden Träger der Sozialhilfe bindend ist.

Als Rechtsgrundlage für die Datenerhebungen zur Durchführung dieser Aufgaben nach § 109a Abs. 2 SGB VI kommt nach Auffassung des Landesbeauftragten lediglich die Regelung des § 67a SGB X in Betracht. Nach § 67a Abs. 2 SGB X müsste der Rentenversicherungsträger die erforderlichen Daten grundsätzlich beim Betroffenen, hier dem Antragsteller, erheben. Der Rentenversicherungsträger könnte demnach Angaben von behandelnden Ärzten mit einer Erklärung des Betroffenen zur Entbindung von der Schweigepflicht im Rahmen der Erforderlichkeit direkt abfordern.

Die in § 67a Abs. 2 SGB X genannten Voraussetzungen der Datenerhebung ohne Mitwirkung des Betroffenen dürften nicht erfüllt sein. Die Erhebung beim Betroffenen erfordert keinen unverhältnismäßigen Aufwand, da der Rentenversicherungsträger zunächst selbst den Umfang der Erhebung bestimmen muss. Die Zwischenschaltung weiterer Stellen würde das Verfahren gerade verzögern.

Insbesondere aber scheint das Sozialamt nicht im Sinne des 67a Abs. 2 Satz 2 Nr. 1 a) SGB X zur Übermittlung an den Rentenversicherungsträger befugt gewesen zu sein. Zwar dürfte sich die Befugnis zur Übermittlung der zum Zeitpunkt des Ersuchens beim Sozialamt bereits vorhandenen Sozialdaten in erforderlichem

Umfang an den Rentenversicherungsträger aus § 69 Abs.1 Nr. 1 SGB X ergeben. Diese grundsätzliche Befugnis zur Übermittlung vorhandener Informationen an den Rentenversicherungsträger begründet jedoch keine Befugnis zur Durchführung eigener Ermittlungen in Bezug auf Daten, die das Sozialamt selbst für die Erfüllung der eigenen Aufgaben nicht benötigt. Die angeforderten Epikrisen benötigt das Sozialamt selbst nicht.

Eine Rechtsgrundlage für die Datenerhebung durch das Sozialamt dürfte sich auch nicht aus § 109a Abs. 2 Satz 3 SGB VI i.V.m. der Vereinbarung zwischen dem Deutschen Landkreistag, Deutschen Städtetag, Deutschen Städte- und Gemeindebund und dem Verband Deutscher Rentenversicherungsträger zur Regelung des Verfahrens und der Kostenerstattung ergeben. Nach § 109a Abs. 2 Satz 3 SGB VI können in einer solchen Vereinbarung zwar Verfahrensregelungen getroffen werden. Die Vereinbarung hat jedoch nicht die Rechtsnormqualität, die erforderlich wäre, um als Rechtsgrundlage einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen. Vielmehr muss das in der Vereinbarung geregelte Verfahren die sozialdatenschutzrechtlichen Rahmenbedingungen berücksichtigen. Eine Unterstützung für den Rentenversicherungsträger durch das Sozialamt in der Weise, dass das Sozialamt zunächst selbst medizinische Daten erhebt, erscheint daher nicht zulässig.

Die durch Umstrukturierungsmaßnahmen jetzt zuständige Deutsche Rentenversicherung Mitteldeutschland hat diese Auffassung bestätigt. Das Verfahren wurde entsprechend der Rechtslage angepasst.

20.27 Grundsicherung im Alter und bei Erwerbsminderung

Die Mutter und Betreuerin ihres behinderten Sohnes teilte dem Landesbeauftragten mit, dass ein Grundsicherungsträger um Abgabe einer sog. „Offenbarungserklärung zum Datenschutz“ gebeten habe, um den Antrag auf Grundsicherungsrente prüfen zu können. Die Petentin konnte sich nicht erklären, warum der Landkreis als Grundsicherungsträger Angaben von Ärzten einholen möchte. Die Offenbarungserklärung umfasste Übermittlungen von zum Teil auch sensiblen Daten. So waren nicht nur andere Sozialleistungsträger, wie z.B. die Arbeitsämter oder Krankenkassen, sondern auch Finanzämter, Wohnungs- und Energieversorgungsunternehmen und Banken in der Offenbarungserklärung aufgeführt. Nachdem trotz zweifacher Aufforderung keine schriftliche Stellungnahme vom Landkreis einging, wurde vor Ort ein Beratungsgespräch durchgeführt.

Zwei Problemkreise waren hier zu thematisieren: das Verfahren zur Prüfung von Anträgen auf Grundsicherungsrente und die Einholung von Einwilligungserklärungen.
Grundsicherungsrente kann u. a. dann gewährt werden, wenn Personen, die das 18. Lebensjahr vollendet haben, dauerhaft voll erwerbsgemindert sind (§ 41 Abs. 1 Nr. 2 SGB XII). Die Feststellung der dauerhaften vollen Erwerbsminderung erfolgt in Verantwortung des Sozialhilfeträgers. Die medizinischen Prüfungen werden allerdings auf Ersuchen des Sozialhilfeträgers ausschließlich durch die Träger der Rentenversicherung vorgenommen und der Sozialhilfeträger ist an die dort getroffene Feststellung gebunden (§ 45 Abs. 1 SGB XII). Ein Ersuchen findet

nur bei Vorliegen der Voraussetzungen des § 45 Abs. 1 Satz 3 SGB XII nicht statt.
Da der betroffene behinderte Sohn eine Werkstatt für behinderte Menschen besucht und der Fachausschuss bereits eine entsprechende Stellungnahme abgegeben hat, erfolgt ein Ersuchen an den Rentenversicherungsträger nach § 45 Abs. 1 Satz 3 Nr. 2 SGB XII nicht. Die Einholung eines Einverständnisses zur Übermittlung von medizinischen Unterlagen des Arztes war damit unnötig.

Darüber hinaus handelt es sich bei der Offenbarungserklärung um eine Blanko-Ermächtigung. Der Landkreis wurde auf die Grundsätze der Datensparsamkeit und Verhältnismäßigkeit aufmerksam gemacht. Der Antragsteller muss auf den Zweck der vorgesehenen Übermittlung hingewiesen werden, d.h. die Erklärung muss einzelfallbezogen und inhaltlich bestimmt sein. Blanko-Erklärungen sind demnach unwirksam.
Der Landkreis sicherte zu, den Vordruck nicht mehr zu verwenden und für zukünftige Übermittlungen im Einzelfall eine datenschutzgerechte Einwilligung einzuholen.

20.28 Datenerhebungen für die Sozialhilfe zu und bei Dritten

Ein Petent hat im Rahmen von Gerichtsverfahren Einsicht in die ihn betreffenden Unterlagen des Sozialamtes zur Gewährung von Sozialhilfe nehmen können (vgl. Ziff. 3.4). Er wandte sich an den Landesbeauftragten, da er die dort vorgefundenen umfänglichen Datensammlungen für bedenklich hielt. Der Landesbeauftragte hat das Vorgehen überprüft und konnte dem Sozialamt umfängliche Hinweise im Hinblick auf die Datenerhebungen für die Sozialhilfe geben.

Erste Hinweise ergingen zum Einsatz von Sozialhilfeermittlern. Im Ergebnis war der Einsatz von Sozialhilfeermittlern zwar grundsätzlich gerechtfertigt, da das Sozialamt konkreten Anlass hatte, den Angaben des Antragstellers nachzugehen. Der Lebensstil des Antragstellers mit einer luxuriösen Mietwohnung schien die Verhältnisse eines Sozialhilfeempfängers zu übersteigen. Im Hinblick auf die detaillierte Begründung des Einsatzes von Sozialhilfeermittlern und den konkreten Auftrag zu Datenerhebungen an die Sozialhilfeermittler waren jedoch Defizite zu erkennen. Hierauf musste der Landesbeauftragte unter Bezugnahme auf seine Darlegungen im VI. Tätigkeitsbericht (Ziff. 20.4) hinweisen.

Weiterhin hatte das Sozialamt bei der Zulassungsstelle Angaben zur Eigenschaft als Kfz-Halter abgefragt und die entsprechenden Ergebnisse in den Sozialhilfeakten dokumentiert. Die Unterlagen bezogen sich jedoch nicht nur auf den Petenten selbst. Die Datensammlungen bezogen sich auch auf eine Person, von der angenommen wurde, dass sie - zumindest zeitweise - Mitbewohner des Petenten und im Hinblick auf ein Kraftfahrzeug Versicherungsnehmer sei. Weiterhin war vermerkt, dass der Vater des Petenten im Hinblick auf ein Kraftfahrzeug Halter gewesen ist. Die Abfrage der Eigenschaft als Kfz-Halter war jedoch nur in Bezug auf diejenigen Personen zulässig, die die Leistungen beziehen, hier also den Petenten selbst. Auch bezieht sich die Abfrage lediglich auf die Eigenschaft als Kfz-Halter, weitere Angaben zur Eigenschaft als Versicherungsnehmer bzw. zu Art

und Alter des betroffenen Kraftfahrzeuges waren von der Abfragebefugnis nicht gedeckt.

Auch unter dem Aspekt der persönlichen Beziehung war eine Abfrage zum potentiellen Mitbewohner nicht zulässig. Eine eheähnliche Gemeinschaft, die ggf. hätte Berücksichtigung finden können, konnte nicht vorliegen. Eine bereichsspezifische Regelung für eingetragene bzw. nicht eingetragene gleichgeschlechtliche Lebenspartnerschaften war bisher nicht in die Regelungen über die Sozialhilfe aufgenommen worden. Demgemäß war es nicht gestattet, bis zu einer gesetzlichen Regelung gleichgeschlechtliche Partner in einer nicht eingetragenen Lebensgemeinschaft in den Anwendungsbereich der Vorschrift einzubeziehen, die eheähnliche Gemeinschaften hinsichtlich Voraussetzungen und Umfang der Sozialhilfe Ehegatten gleichstellt.

Der Petent hatte wiederholt Anlass zu Zweifeln an seinen Angaben gegeben, u.a. weil die nachträglich eingereichten Nachweise - wie beispielsweise inhaltlich unterschiedliche Mietverträge - die zuvor gemachten Angaben nicht bestätigten. Aufgrund dessen und der Mitteilungen der Sozialhilfeermittler hegte das Sozialamt den Verdacht auf eine missbräuchliche Inanspruchnahme von Sozialhilfemitteln. Diesbezüglich erfolgte eine Rücksprache mit dem zuständigen Polizeirevier. Es wurden Auskünfte zum Petenten und seine potentiellen Mitbewohner erbeten. Im Ergebnis waren Informationen zur kriminellen Laufbahn der Betroffenen in den Akten enthalten.

Hierzu wies der Landesbeauftragte darauf hin, dass es der Stadt unbenommen bleibt, anhand vorliegender Tatsachen zu erwägen, ob eine Strafanzeige erstattet wird. Eine Rechtsgrundlage für Datenerhebungen durch Rücksprache mit der Polizei, um erst die Voraussetzungen für eine Anzeige abzuklären, war jedoch nicht ersichtlich. Insbesondere bestand auch keine Rechtsgrundlage, Daten über die Straffälligkeit des potentiellen Mitbewohners in den Akten zu speichern. Im Übrigen hätte die Mitteilung des Polizeireviers am Ausgang des Sozialhilfeverfahrens des Petenten nichts geändert. Sofern ein Anspruch auf Sozialhilfe besteht, ist dieser unabhängig davon zu erfüllen, ob der Petent kriminalpolizeilich bekannt war oder nicht.
Der Landesbeauftragte hat auf die Verpflichtung zur Löschung unzulässig gespeicherter bzw. nicht mehr zur Aufgabenerfüllung erforderlicher Daten nach § 84 Abs. 2 SGB X hingewiesen.

Heimrecht

20.29 Mitarbeiterdatenüberprüfung durch die Heimaufsicht

Ein Verband privater Heime beklagte sich über die Praxis der Heimaufsichtsbehörden, bei Prüfungen Namenslisten von Mitarbeitern mitzunehmen und in den Unterlagen der Heimaufsichtsbehörde zu speichern. Dies sei mit § 15 Abs. 2 Heimgesetz (HeimG) und der dazu ergangenen Rechtsprechung nicht vereinbar, wonach die Aufsichtsbehörde grundsätzlich nur ein Einsichtsrecht, aber keinen Anspruch auf schriftliche Auskünfte habe.

Die Heimaufsichtsbehörde teilte hierzu mit, dass lediglich unter Berücksichtigung der Umstände im Einzelfall (z.B. große Einrichtungen mit entsprechend großer Beschäftigtenzahl, anderer Prüfungsschwerpunkt, Zeitpunkt der letzten Änderungsanzeige nach § 12 Abs. 3 HeimG) entschieden werde, ob eine Einsichtnahme in die Personalliste vor Ort genüge oder darüber hinaus eine Kopie zur Prüfung in der Dienststelle der Heimaufsichtsbehörde erforderlich sei. Gegen diese angemessene Datenerhebung auf der Grundlage des § 9 Abs. 1 DSG-LSA bestanden keine datenschutzrechtlichen Bedenken.

Bereits in der Gesetzesbegründung (BT-Drs. 14/5399, S. 30) wird erwähnt, dass der Träger der Heimaufsichtsbehörde Fotokopien der Geschäftsunterlagen zur Verfügung stellen soll. Auch wenn nach obergerichtlicher Rechtsprechung im Hinblick auf den Gesetzeswortlaut kein genereller Anspruch auf schriftliche Auskünfte gegeben ist, besteht dennoch die Verpflichtung des Heimträgers über seine Aufzeichnungs-, Aufbewahrungs- und Duldungspflichten im Sinne von §§ 13, 15 Abs. 2 Satz 2 HeimG, Unterlagen in Ablichtung zur Verfügung zu stellen, soweit dies zur Durchführung des Heimgesetzes erforderlich ist und die sonstigen Befugnisse der Aufsichtsbehörde, wie etwa das Einsichtsrecht, nicht ausreichen.

21. Statistik

21.1 EU-weiter Zensus 2011

Aus zwei Gründen wird den Bürgerinnen und Bürgern in Deutschland voraussichtlich im Jahre 2011 eine Volkszählung (Zensus) ins Haus stehen: Der Zensus ist durch die EU geplant und wird wohl für die Mitgliedsstaaten per EU-Verordnung zur Pflicht gemacht werden. Außerdem sei, so die politischen Planer bei Bund, Ländern und Gemeinden seit Jahren unisono, ein tragfähiges Datenfundament zu Bevölkerung, Erwerbstätigkeit und Wohnsituation in Deutschland nicht wirklich vorhanden, da die letzte Volkszählung im Gebiet der ehemaligen DDR 1981 und in den alten Bundesländern 1987 stattfand. Der Zensus wird - wieder aus zwei Gründen - voraussichtlich nicht als traditionelle Volkszählung durch Befragung aller Bürgerinnen und Bürger durch schätzungsweise eine Million Erhebungsbeauftragte durchgeführt werden, obgleich die EU den Mitgliedsstaaten bei der Wahl der Datenquellen keine Vorschriften machen wird. Diese Erhebungsart würde, so eine Schätzung des Statistischen Bundesamtes, mit Kosten von ca. 1,4 Milliarden Euro zu Buche schlagen. Außerdem hatte das Bundesverfassungsgericht in seinem Volkszählungsurteil verlangt, dass sich der Gesetzgeber vor künftigen Zensen mit der statistischen Methodendiskussion auseinandersetzt. Dies ist erfolgt und hatte den registergestützten Zensus zum Ergebnis. Es werden also nicht die Bürgerinnen und Bürger gezählt, sondern die Einträge über sie in den Verwaltungsregistern.
Mit der Umsetzung einer Empfehlung der EU, ab dem Jahre 2001 eine Volkszählung in den Mitgliedsländern durchzuführen, wurde in Deutschland erprobt, ob ein solcher Registerzensus überhaupt verwendbare Ergebnisse haben kann. Dafür wurde mit dem Zensustestgesetz als Artikel 1 des Zensusvorbereitungsgesetzes vom 27. Juli 2001 eine Rechtsgrundlage geschaffen. Der Zensustest bewies die grundsätzliche Geeignetheit des Verfahrens, er brachte aber auch zu erwartende Schwierigkeiten ans Licht. So wurde die durchschnittliche Fehlerquote der deut-

schen Melderegister mit ca. 5 % ermittelt, die Register in Berlin, Hamburg und dem Saarland wiesen ca. 10 % Fehler auf. Eine Zählung in den Melderegistern wird also mit weiteren Maßnahmen untersetzt werden müssen, um planungssichere Ergebnisse erzielen zu können. Solche Maßnahmen, deren Kern die Verknüpfung der Daten weiterer Register der Bundesagentur für Arbeit und der Vermessungsbehörden mit den Einwohnermeldedaten sein wird, finden sich in dem Entwurf eines Zensusvorbereitungsgesetzes wieder, zu dem der Landesbeauftragte zum Ende des Berichtszeitraumes Stellung genommen hat, da der Entwurf eine Fülle datenschutzrechtlich bedenklicher Sachverhalte enthielt.
So soll für die Vorbereitung des eigentlichen Zensus beim Statistischen Bundesamt ein zentrales Adress- und Gebäuderegister betrieben werden, das von ihm selbst, aber auch von den Statistischen Ämtern der Länder mit aufgebaut, gepflegt und genutzt werden soll. Die Frage, in wessen Verantwortlichkeit das Register betrieben wird und wer folglich für die datenschutzrechtliche Kontrolle zuständig wäre, ist in dem Gesetzentwurf nicht geregelt.
Die Adress- und Gebäuderegisterdaten sollen mit geodätischen Koordinatenwerten versehen werden (Georeferenzierung). Ziel soll sein, die von der Politik geforderten kleinräumigen Auswertungen zu ermöglichen. Dem Gesetzgeber ist wohl bewusst, dass durch diese kleinräumigen Auswertungen die Anonymität der hinter den Adressen stehenden natürlichen Personen bedroht wäre. Allerdings wird mit seiner Intention, durch Nutzung des georeferenzierten Registers Verfahren zu entwickeln, die die Anonymität der Ergebnisse gewährleisten, das Pferd von der falschen Seite aufgezäumt. Der Landesbeauftragte hält es für nicht ausgeschlossen, dass solche Verfahren ihr Ziel verfehlen. Der Gesetzentwurf genügt wegen dieses möglichen übermäßigen Eingriffs in das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger den verfassungsrechtlichen Vorgaben nicht.
Ferner sieht der Gesetzentwurf vor, dass die Meldebehörden adressenscharf die Familiennamen aller Einwohner und deren exakten Geburtsdaten an die Statistischen Ämter der Länder übermitteln. Der Familienname sei, so die Gesetzesbegründung, erforderlich, um die Zahl der Haushalte an einer Adresse zu ermitteln, und das Geburtsdatum diene dazu, das Alter der Bewohner zu errechnen. Beide Angaben könnten die Einwohnermeldeämter aber selbst ermitteln.

Für besonders problematisch, und dies hat er dem Ministerium des Innern so mitgeteilt, hält er jedoch die vom Gesetzentwurf vorgesehene Rückübermittlung von Daten aus der Statistik zurück in den Verwaltungsvollzug an die Meldebehörden, um dort „zu klären“, ob die Daten zu bestimmten monierten Adressbereichen unvollständig oder fehlerbehaftet sind. Dass die Melderegister fehlerbehaftet sind, ist oben erwähnt. Ihre Konditionierung kann allerdings nicht durch Aufhebung des strikten Trennungsgebotes von Statistik und Verwaltungsvollzug bewerkstelligt werden. Hier verfassungsrechtlich saubere Lösungen zu suchen und zu finden, ist der Gesetzgeber gefordert, wenn er eine Konditionierung denn für erforderlich hält. Die im dem Landesbeauftragten vorliegenden neuesten Entwurf des Zensusvorbereitungsgesetzes und seiner Begründung (BR-Drs. 222/07) aufgenommene Formulierung, die oben genannte Fehlerklärung in den Meldeämtern solle "anhand der vorhandenen Daten", ohne Einzelprüfungen vor Ort erfolgen, vermochte seine Bedenken schon nicht zu zerstreuen. Zu allem Überfluss empfahlen die vom Bundesrat beteiligten Ausschüsse diesem, in seiner Stellungnahme ge-

nau jene Formulierung wieder streichen zu lassen und damit die Meldeämter zu Einzelprüfungen zu verpflichten. Der Bundesrat folgte dieser Empfehlung in seinem Beschluss vom 11. Mai 2007 (BR-Drs. 222/07 - Beschluss). Der Landesbeauftragte weist im Übrigen auf seinen bereits in seinem III. Tätigkeitsbericht (Ziff. 25.2) zur Trennung zwischen Statistik und Verwaltungsvollzug bei der Gebäude- und Wohnungszählung vertretenen Standpunkt hin.

21.2 Eine Bürgerbefragung - nicht ganz datenschutzgerecht

Viele Gemeinden in Sachsen-Anhalt leiden an einem beständigen Bevölkerungsverlust. Um in dieser Situation eine lebenswerte Stadt mit ausreichenden Wohnangeboten, attraktiven Freiflächen und den notwendigen Versorgungseinrichtungen für die Zukunft planen zu können, sollte in einer Stadt ein integriertes Stadtentwicklungskonzept erarbeitet werden. Grundlage dieser Arbeit sollte eine Bürgerbefragung sein, in der die Wohn- und Lebensverhältnisse der Bewohner, ihre Wünsche und Kritikpunkte gegenüber ihrer Stadt sowie zu ihrem Wohngebiet untersucht werden sollten. Die Stadt versprach, diese Informationen in die zukünftigen Planungen einzubeziehen.

Ein Mitglied des Landtages trug dem Landesbeauftragten die Bedenken einer Bürgerin seines Wahlkreises vor, die zur Teilnahme an dieser kommunalen Bürgerbefragung ausgewählt worden war, die im Auftrag der Stadt von einem Stadtforschungsinstitut durchgeführt werden sollte.
Die daraufhin von der Stadt angeforderten Erhebungs- und Vertragsunterlagen enthielten so viele Probleme, dass sich zunächst für den Datenschutz ein unklares Szenario abzeichnete, auch wenn in dem Anschreiben der Stadt erklärt wurde, die Teilnahme an dem Projekt sei freiwillig.
Beispielsweise wurde den Bürgerinnen und Bürgern im Anschreiben in fetter Schrift versichert, die Antworten würden anonym ausgewertet. Jedoch: In der ersten Zeile des Fragebogens sollten Straße und Hausnummer der Wohnung angegeben werden, die, so das Hinweisblatt zum Fragebogen, erforderlich seien, um die Zuordnung zu einem Wohngebiet zu ermöglich. Datenschutz- bzw. statistikrechtlich heißt das nichts anderes, als die eben noch postulierte Anonymität, zumindest im Fall von Einfamilien- oder Reihenhäusern, wieder aufzugeben. Der Landesbeauftragte ist schon der Meinung, dass die Befragungsteilnehmer in der Lage gewesen wären, ihr Wohngebiet selbst anzugeben.
Wenn das Hinweisblatt in diesem Zusammenhang, also gleich zu Beginn, noch einmal den im Anschreiben in kleiner Schrift gegebenen Hinweis auf die Freiwilligkeit der Teilnahme oder besser noch auf die Freiwilligkeit der Beantwortung der einzelnen Fragen drucktechnisch hervorgehoben enthalten hätte, wäre die Akzeptanz bei den Befragten sicherlich größer gewesen. Dass dies möglich gewesen wäre, zeigt die Tatsache, dass eben dieser Hinweis bei der Frage nach dem Netto-Haushaltseinkommen auftaucht. Der von der Stadt gegangene Weg war datenschutzrechtlich ungeschickt, auch weil er einen Verstoß gegen das Gebot der Datensparsamkeit aus § 1 Abs. 2 DSG-LSA darstellt.

Da die Stadt die Befragung nicht selbst durchführte, sondern sich eines Dritten bediente, untersuchte der Landesbeauftragte auch die Vertrags- und ergänzenden Unterlagen.

Aus denen ging z.B. hervor, dass das Zufallsverfahren, nach dem die beteiligten Haushalte ausgewählt würden, darin bestand, bei kleinen Stadtteilen alle Haushalte, bei mittleren ca. 50 % und bei größeren Stadtteilen 33 % der Haushalte einzubeziehen, alles in allem ca. 10.000 ausgewählte Haushalte.
Der Auftragnehmer, der das integrierte Stadtentwicklungskonzept erstellen sollte, hatte laut Vertrag und Leistungsbeschreibung die „Datenbestände der Meldeämter (...) so auszuwerten, dass ein möglichst kleinräumiger Entwicklungsverlauf sichtbar wird“ und Bestand und Prognose für Bevölkerung, Haushalte und Migration zu ermitteln. All das deutete darauf hin, dass man ihm die Einwohnermeldedaten, zumindest teilweise, überlassen hatte, was, als Datenverarbeitung im Auftrag gem. § 8 DSG-LSA vertraglich vereinbart, datenschutzrechtlich zulässig darstellbar gewesen wäre. Doch in dem gesamten Vertragswerk tauchte das Wort „Datenschutz“ nicht ein einziges Mal auf!
Allerdings konnte der Landesbeauftragte sehr schnell feststellen, dass, zumindest in Bezug auf die Einwohnermeldedaten, doch korrekt gearbeitet wurde. So wurde die Stichprobenauswahl der zu beteiligenden Haushalte durch Werbemittelverteiler bewerkstelligt, die anonyme Briefumschläge mit den Fragebögen entweder in jeden, in jeden zweiten oder in jeden dritten Hausbriefkasten einwarfen. Nicht gerade repräsentativ, aber datenschutzgerecht.
Die Auswertung der Melderegister selbst erledigten die Meldeämter, die die erforderlichen anonymisierten Ergebnistabellen an den Auftragnehmer übersandten. Dieser hatte, so wurde dem Landesbeauftragten versichert, niemals Zugang zu Einzeldaten der Meldeämter.

Damit blieb für den Landesbeauftragten nur noch, die Stadt aufzufordern, sich die restlose Vernichtung der zurückgelaufenen Erhebungsbögen und die Löschung aller im Zusammenhang mit der Bürgerbefragung erhobenen personenbezogenen Daten vom Auftragnehmer quittieren zu lassen, was auch erfolgte.

22. Strafvollzug

22.1 Datenschutz und ein großes Investitionsprojekt: PPP-Burg

Im Jahr 2006 hatte das Land Bau und Betrieb einer Justizvollzugsanstalt (JVA) im Rahmen eines sog. public-private-partnership-Projekts (PPP) ausgeschrieben. Da nur wenige hoheitliche Tätigkeiten öffentlicher Stellen existieren, welche in gleicher Art und Intensität in die Rechte von Menschen eingreifen, wie die Befassung des Staates mit Strafgefangenen, hatte sich der Landesbeauftragte an das Ministerium der Justiz mit der Bitte gewandt, ihn über die datenschutzrechtlich bedeutsamen Gesichtspunkte dieses Vorhabens zu informieren. Auf diese Anfrage hin hatte das Ministerium umfassende Information angekündigt. Leider entwickelte sich in der Folge das Informationsverhalten seiner Mitarbeiter, wie auch jener Mitarbeiter des Ministeriums für Landesentwicklung und Verkehr, welches das Ausschreibungsverfahren im Wesentlichen betreibt, gegenteilig. So sollten nur nach Abgabe einer gesonderten Schweigeverpflichtungserklärung durch den Landesbeauftragten und seine Mitarbeiter die Bieterkonzepte zum Datenschutzreglement übersandt werden - obwohl deren Zusendung bereits vorab angekündigt worden war.

Der Landesbeauftragte sieht in dieser Bedingung einen Verstoß gegen § 23 Abs. 1 DSG-LSA, der die Unabhängigkeit der Amtsausübung des Landesbeauftragten beeinträchtigt. Dass diese Antwort dann auch noch von einem Mitarbeiter einer nicht angefragten öffentlichen Stelle (Ministerium für Landesentwicklung und Verkehr) gegeben wurde, erschien ihm zudem bemerkenswert. Den Vogel abgeschossen hat indessen der pauschale Hinweis, der Landesbeauftragte möge sich mit dem zum PPP-Projekt beratenden Anwaltsbüro auseinandersetzen. Dies entspricht schon nicht dem Amtsverständnis in der Funktion des Landesbeauftragten. Es verwundert auch deshalb, weil für die Erfüllung der Auskunftspflicht gegenüber dem Landesbeauftragten nach den gesetzlichen Regelungen des DSG-LSA die zuständige öffentliche Stelle eigenständig Verantwortung trägt.
Da das vorgelegte Schweigeverpflichtungsformular entsprechende Formulierungen enthielt, wies der Landesbeauftragte noch klarstellend darauf hin, dass er selbstverständlich nicht Beteiligter im Vergabeprozess ist. Sein Interesse bezog und bezieht sich ausschließlich auf die datenschutzgrundrechtlichen Aspekte dieses Vorgangs. Folglich war die umfassende Vorlage aller Unterlagen weder erbeten worden, noch aus seiner Sicht sinnvoll.

Unabhängig von den verfassungs-/datenschutzrechtlichen Fragen im Zusammenhang mit dem konkreten Projekt, hat der Landesbeauftragte daher das Ministerium der Justiz um Stellungnahme zu dem nicht akzeptablen Versuch, die unabhängige Amtsausübung des Landesbeauftragten zu beeinträchtigen, gebeten. Da PPP-Projekte, welche regelmäßig u.a. datenschutzrechtliche Fragen aufwerfen, künftig in unterschiedlichen Bereichen der staatlichen und kommunalen Verwaltungen vermehrt in Angriff genommen werden dürften, hat er auf eine Klarstellung der rechtlichen Position Wert gelegt.
Zwar wurden die erbetenen Informationen auch nach dem mahnenden Schreiben nicht umgehend zur Verfügung gestellt, aber die Staatssekretäre der beteiligten Ministerien verabredeten kurzfristig einen persönlichen Informationsaustausch mit dem Landesbeauftragten, in welchem sie darlegten, dass Ursache der nicht angemessenen Unterrichtung des Landesbeauftragten ein Missverständnis gewesen sei. Man sei davon ausgegangen, dass nicht allein das Datenschutzkonzept Gegenstand der Anfrage des Landesbeauftragten gewesen sei. Diese Erklärung konnte der Landesbeauftragte schon angesichts seiner gesetzlich eindeutig geregelten Zuständigkeit nicht nachvollziehen. Abgesehen davon läge auch eine unbegrenzte Anforderung von Unterlagen ausschließlich in der Entscheidungskompetenz des Landesbeauftragten. Denn in manchen Fällen kann nur nach Sichtung der vollständigen Unterlagen das datenschutzrechtlich Wesentliche herausgefiltert werden. Auf eine Beanstandung konnte jedoch verzichtet werden, da deutlich wurde, dass eine Beeinträchtigung der Unabhängigkeit des Amtes im Konkreten nicht beabsichtigt war.

Gegen Ende des Berichtszeitraums dieses Tätigkeitsberichts wurde nunmehr u.a. ein Datenträger mit Vertragsentwürfen zum PPP-Projekt der neuen JVA in Burg übersandt. Eine angemessene Auswertung nimmt geraume Zeit in Anspruch, sodass ggf. im folgenden Tätigkeitsbericht über die weitere Entwicklung der datenschutzrechtlichen Absicherung des PPP-Projekts zu berichten sein wird. Inhaltlich geht es u.a. um die Zulässigkeit der Abgabe hoheitlicher Aufgaben an private Drit-

te und entsprechende Datenflüsse wie auch die Sicherstellung von deren Vertraulichkeit.

22.2 Kontrollen in Justizvollzugsanstalten

Im Berichtszeitraum wurden in zwei JVA datenschutzrechtliche Kontrollen und Informationsbesuche durchgeführt. Diese ergaben hinsichtlich des alltäglichen Umgangs des dort beschäftigten Personals mit Daten von Insassen und Dritten keine datenschutzrechtlich gravierenden Verstöße.
Problemhinweise wurden in der Regel weitgehend akzeptiert. Allerdings wurde öfter mit dem Verweis zu beantworten versucht, dass die jeweilige JVA hinsichtlich festgestellter technisch-organisatorischer Mängel nichts tun könne, da sie keinen eigenen Administrator habe. Der Landesbeauftragte legt daher Wert auf die Feststellung, dass dieses keine geeignete Reaktion bleiben kann, da die rechtliche Zuständigkeit als verantwortliche Stelle im Sinne des Datenschutzrechts (vgl. § 3 Abs. 7 BDSG) nicht abgegeben werden kann. Die jeweilige JVA hat sich daher selbst um die Behebung der Defizite unter Inanspruchnahme geeigneter Hilfe zu kümmern.

Bei der Prüfung von Gefangenenpersonalakten (GPA) wurde u.a. festgestellt, dass, neben konkreten Eignungsmitteilungen als deren Ergebnis, verschiedentlich Auswertungs- und Ergebnisbogen von Intelligenz- und Befähigungstests bzw. Psychotests offen eingeheftet waren. Die daraus ersichtlichen Daten und Auswertungen ergaben ein die Persönlichkeit des Gefangenen umfassend bewertendes Bild. Das offene Abheften in der GPA erscheint dem Landesbeauftragten mit §§ 182, 183 StVollzG nicht vereinbar und daher datenschutzrechtlich fragwürdig. Die Praxis, so weitgehende Informationen unverschlossen in den GPA einzuheften, wird nach seiner Einschätzung noch dadurch verschärft, dass eine nachträgliche Kontrolle der Zulässigkeit erfolgter Einsichtnahmen in die GPA nicht möglich ist. Aus den Akten war nicht ersichtlich, weder durch einzelne Vermerke, noch etwa durch ein entsprechendes vorgeheftetes Dokumentations-Blatt, wer zu welchem Zweck Einsicht in die GPA erhalten hat. Die Erforderlichkeit von Einsichtnahmen kann damit nicht belegt werden. Der Vorschlag der JVA, künftig nur noch die Eignungsmitteilung als solche zu den GPA zu nehmen, erscheint nur auf den ersten Blick sinnvoll. Dann wäre jedoch zu klären, was mit den so entstehenden Nebenvorgängen geschieht; u.a. müsste in der GPA ein Hinweis auf diese Nebenakten aufgenommen werden, um u.a. die zeitgleiche Löschung dieser Vorgänge sicherstellen zu können.
Dem Schutz des Grundrechts der Gefangenen wie auch der Verwaltungspraktikabilität wird es eher entsprechen, das Ergebnis offen, die Beurteilungsgrundlage dagegen verschlossen (mit Zugriffsbefugnis nur für einen begrenzten Personenkreis) in der GPA einzuheften. Vergleichbar ist die gängige Praxis, in Personalakten Aktenteile mit besonders schützenswerten Daten in dieser Art zu sichern. Der Schutz solcher Daten innerhalb der Akten wurde bereits oberstgerichtlich für notwendig erachtet und zur Lösung beispielhaft auf eingeheftete geschlossene Umschläge verwiesen (Bundesarbeitsgericht, Urteil vom 12.9.2006 – 9 AZR 271/06). Der Landesbeauftragte hält diesen Weg für praktisch vertretbar und erwartet, dass diese Verfahrensweise Beachtung findet.

Die kontrollierten JVA stellen den Insassen ein Gefangenen-Telefonsystem (TELIO) zur Verfügung, mit dessen Hilfe Gefangene über ein Guthabenkonto telefonieren können. Wie letztlich per Nachfrage bei einem Gefangenen geklärt werden konnte, wird durch den Dienstleister TELIO bei jedem Telefonat ein Hinweis an beide Teilnehmer des Gesprächs eingespielt, dass eine Überwachung des Telefonats erfolgen könnte. Dass ein solcher Dauerhinweis im TELIO-System den Gesprächsteilnehmern eine unbelastete Kommunikation verwehrt, sei nur erwähnt. Nach dem Wortlaut von § 32 S. 3, 4 StVollzG ist der dort geforderte Hinweis nur hinsichtlich eines tatsächlich zu überwachenden Gesprächs vorgesehen. Neben rechtlichen Zweifeln an dieser Praxis erscheint zweifelhaft, ob eine JVA mit dieser Verfahrensweise auch rechtlich der ihr obliegenden Informationspflicht genügen kann. Bei dem regelmäßigen Hinweis dürfte es sich eher um einen „Informationsservice“ der Fa. TELIO handeln. Die gesetzlich begründete hoheitliche Verpflichtung, im Einzelfall zu informieren, dürfte dadurch nicht substituiert werden.

Für die Entsorgung dienstlichen Schriftgutes in größeren Mengen wird auf verschließbare Container eines Aktenvernichtungsunternehmens zurückgegriffen. Mit dem Unternehmen besteht ein Aktenvernichtungsvertrag. Bei diesem Auftragnehmer handelt es sich um eine GmbH. Auf sie wären, da es sich um eine sog. nicht-öffentliche Stelle handelt, die Vorschriften des DSG-LSA zunächst nicht anwendbar. Üblicherweise wird dies landesrechtlich dadurch „korrigiert“, dass nach § 8 Abs. 6 DSG-LSA die JVA als Auftraggeberin im Vertrag sicherstellen muss, dass der Auftragnehmer die Bestimmungen des DSG-LSA befolgt und sich der Kontrolle durch den Landesbeauftragten entsprechend den §§ 22 bis 24 DSG-LSA unterwirft. Im Weiteren hätten vertraglich die in § 8 Abs. 2 DSG-LSA vorgesehenen technischen und organisatorischen Maßnahmen festlegt werden müssen. Schließlich hätte der Landesbeauftragte über die Beauftragung unterrichtet werden müssen. All das ließ sich vor Ort nicht feststellen.
Allerdings ist bereits im Grundsatz zweifelhaft, dass die JVA rechtlich befugt war, die Aktenvernichtung im Wege einer Datenverarbeitung im Auftrag zu vergeben. Das StVollzG selbst enthält keine Regelung hinsichtlich einer Datenverarbeitung im Auftrag. Auch die Verweise in § 187 StVollzG auf die Geltung des BDSG sowie auf das Landesrecht hinsichtlich der Kontrollbefugnisse des Landesbeauftragten enthalten keinen Bezug zu einer der Regelungen über die Auftragsdatenverarbeitung. Da diese Regelung den abschließenden Charakter der StVollzG-Bestimmungen beim Umgang mit personenbezogenen Daten deutlich macht (so BT-Drs. 13/10245 an mehreren Stellen), fehlt eine gesetzliche Grundlage für jegliche Datenverarbeitung im Auftrag im Bereich des Justizvollzugs. Somit dürfte die Vernichtung von Unterlagen mit personenbezogenem Inhalt nur in Eigenregie zu erfolgen.
Da dies Auswirkungen auch hinsichtlich anderer Auftragsvergaben von JVA haben könnte, fragte der Landesbeauftragte das Ministerium der Justiz nach seiner Auffassung. Es antwortete, dass die fehlende ausdrückliche Bestimmung im Wege der Analogie zu ergänzen sei.
Eine Analogie ist zulässig, wenn das Gesetz eine planwidrige Regelungslücke enthält und der zu beurteilende Sachverhalt in rechtlicher Hinsicht so weit mit dem Tatbestand vergleichbar ist, den der Gesetzgeber geregelt hat, dass angenommen werden kann, der Gesetzgeber wäre bei einer Interessenabwägung, bei der

er sich von den gleichen Grundsätzen hätte leiten lassen, wie bei dem Erlass der herangezogenen Gesetzesvorschrift, zu dem gleichen Abwägungsergebnis gekommen. Auch wenn man von parallelen Bestimmungen im DSG-LSA ausgeht, dürfte die weitere Voraussetzung keineswegs gegeben sein. Schon die im StVollzG bestehende Verweisklausel zur Anwendung des BDSG nimmt die dortige Norm zur Auftragsdatenverarbeitung nicht in Bezug. Von daher ist es eher unwahrscheinlich, dass der Gesetzgeber die Problematik übersehen haben sollte. Dafür spricht gerade auch der vom Ministerium der Justiz zur Begründung des Gegenteils herangezogene § 155 StVollzG. Danach können Aufgaben „aus besonderen Gründen auch nebenamtlichen oder vertraglich verpflichteten Personen übertragen werden“. Die Festlegung auf besondere Gründe sprechen gegen regelmäßige Übertragungen von Aufgaben und dokumentieren zudem, dass der Gesetzgeber schon lange vor 1983 (vom 15. Dezember 1983 datiert das Volkszählungsurteil des Bundesverfassungsgerichts) gesehen hat, dass im Strafvollzug nur in einem sehr begrenzten Umfang Tätigkeiten von Außenstehenden wahrgenommen werden dürfen. Dadurch wird der Wille des Gesetzgebers unterstrichen, keine Aufweichungen in diesem besonders grundrechtsinvasiven Bereich staatlicher Hoheitsgewalt zulassen zu wollen; die Nichtregelung der Auftragsdatenverarbeitung wird daher als eine bewusste Entscheidung des Gesetzgebers hingenommen werden müssen. Ganz abgesehen davon, dass Analogien zu Lasten der Grundrechte Betroffener rechtsstaatlich schwer zu begründen sein dürften. Von einer planwidrigen Regelungslücke dürfte folglich nicht auszugehen sein.

In seiner Stellungnahme hat das Ministerium der Justiz darauf hingewiesen, dass es ein großes Interesse an Rechtsklarheit und Rechtssicherheit habe und folglich u.a. eine Regelung zur Auftragsdatenverarbeitung in den kurzfristig zu erarbeitenden Gesetzen zum Strafvollzug (vgl. Ziff. 22.3) treffen will. Ob eine weite Öffnung für Auftragsdatenverarbeitung - etwa durch eine die Strafvollzugsbestimmungen umfassend ergänzende Bezugnahme auf die Normen des DSG-LSA - der Weisheit letzter Schluss sein darf, wird das Ministerium der Justiz, unter Berücksichtigung der hohen Eingriffsintensität des Justizvollzugs insgesamt, noch zu prüfen haben.

22.3 Neuregelung für den Jugendstrafvollzug

In einer neueren Entscheidung (Urteil vom 31. Mai 2006, 2 BvR 1673/04, 2 BvR 2402/04, NJW 2006, 2093) hat das Bundesverfassungsgericht festgestellt, dass die verfassungsrechtlich erforderlichen und auf die besonderen Anforderungen des Strafvollzuges an Jugendlichen angepassten gesetzlichen Grundlagen fehlen. Für eine begrenzte Übergangszeit bis zum Inkrafttreten der erforderlichen gesetzlichen Regelungen müssen eingreifende Maßnahmen im Jugendstrafvollzug indessen hingenommen werden, soweit dies zur Aufrechterhaltung eines geordneten Vollzuges unerlässlich ist. Das Bundesverfassungsgericht räumt dem Gesetzgeber eine Übergangsfrist bis Ablauf des Jahres 2007 ein. Gemäß dieser Entscheidung hatte, trotz Fehlens der unumgänglichen gesetzlichen Grundlagen, die Verfassungsbeschwerde eines Beschwerdeführers aus dem Jugendstrafvollzug, der sich gegen die Anordnung einer allgemeinen Kontrolle seiner Post sowie gegen eine Disziplinarmaßnahme gewandt hatte, lediglich in Bezug auf seinen kon-

kreten Einzelfall keinen Erfolg. Denn die angeordneten Maßnahmen waren zur Aufrechterhaltung eines geordneten Jugendstrafvollzuges unerlässlich.

Da die Gesetzgebungsbefugnis für den Strafvollzug seit dem Inkrafttreten der Föderalismusreform I am 1. September 2006 den Ländern zusteht, wurde ein gemeinsamer Vorentwurf eines Jugendstrafvollzugsgesetzes von neun Ländern erstellt, der dann von den einzelnen Ländern auf die landesrechtliche Rechtslage anzupassen war.

Während z.B. die bremische Bürgerschaft bereits den Entwurf eines Bremischen Jugendstrafvollzugsgesetzes im Februar 2007 in erster Lesung beschlossen und an den Rechtsausschuss zur weiteren Beratung und Berichterstattung überwiesen hatte, lag in Sachsen-Anhalt erst ein Referentenentwurf vor, welcher jedoch erst zum Ende des Berichtszeitraums dieses Tätigkeitsberichtes dem Kabinett vorgelegt worden war, sodass über das Ergebnis des Gesetzgebungsverfahrens im nächsten Tätigkeitsbericht zu berichten sein wird. Der Landesbeauftragte wird sich beratend beteiligen.

23. Telekommunikations- und Medienrecht

23.1 Vorratsdatenspeicherung

Die geplante Vorratsdatenspeicherung, über die der Landesbeauftragte in seinem letzten Tätigkeitsbericht (Ziff. 23.2) berichtet hat, wird nun offensichtlich auch in Deutschland traurige Realität werden. Die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG ist in Kraft getreten und muss in den einzelnen Mitgliedsstaaten in nationales Recht umgesetzt werden. Aus diesem Grund hat das Bundeskabinett am 18. April 2007 einen Entwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG beschlossen (vgl. Ziff. 18.3).

Darin ist vorgesehen, dass Anbieter von Telekommunikationsdiensten künftig sechs Monate lang auf Vorrat speichern müssen, wer wann mit wem per Festnetz, Mobilfunk oder E-Mail kommuniziert hat, wer sich mit welcher IP-Adresse im Internet bewegt hat und in welcher Funkzelle sich Mobilfunknutzer zu Beginn einer Verbindung aufgehalten haben. Dabei handelt es sich um die sog. Verkehrsdaten der Telekommunikation, aber auch um Standortdaten. Die Inhalte der Kommunikation dürfen nicht gespeichert werden. Der Speicherungszweck ist nicht mehr, wie ursprünglich geplant, die Verfolgung schwerer Straftaten (z.B. Terrorismus oder organisierte Kriminalität), sondern der Zugriff auf diese Daten soll bereits zur Verfolgung von Straftaten von erheblicher Bedeutung sowie von mittels Telekommunikation begangener Straftaten ermöglicht werden.

Die Richtlinie 2006/24/EG ist bis zum 15. September 2007 in nationales Recht umzusetzen. Allerdings darf die Frist für die Dienste Internetzugang, Internet-

Telefonie und E-Mail bis längstens zum 15. März 2009 aufgeschoben werden. Hierzu ist eine besondere Erklärung der Mitgliedsstaaten notwendig. Eine solche Erklärung haben 16 der 25 Mitgliedsstaaten abgegeben, darunter Deutschland und Österreich. Trotzdem sieht der Gesetzentwurf auch für diese Dienste ein Inkrafttreten für den 1. Januar 2008 vor.

Der Umsetzung der Richtlinie in nationales Recht stehen erhebliche verfassungsrechtliche Bedenken gegenüber. Grundsätzlich dürfen personenbezogene Daten nur gespeichert werden, wenn dies zu einem gesetzlich festgelegten Zweck erforderlich ist. Eine verdachtsunabhängige Speicherung auf Vorrat widerspricht dem Grundsatz der Verhältnismäßigkeit. Auch der wissenschaftliche Dienst des Deutschen Bundestages hat in seiner Ausarbeitung zur Zulässigkeit der anlass- und verdachtslosen Vorratsdatenspeicherung Zweifel an der Verfassungsmäßigkeit der Richtlinie und ihrer möglichen Umsetzung in innerdeutsches Recht geäußert. Weitere Zweifel bestehen hinsichtlich der Vereinbarkeit mit dem Europarecht. Dies betrifft zum einen die Wahl der Rechtsgrundlage, zum anderen aber auch die Vereinbarkeit mit den im Gemeinschaftsrecht anerkannten Grundrechten. Zwei Mitgliedstaaten der Europäischen Union haben bereits den Europäischen Gerichtshof angerufen, um die Richtlinie überprüfen zu lassen.

Sowohl auf der 70. als auch auf der 73. Datenschutzkonferenz haben die Datenschutzbeauftragten des Bundes und der Länder Entschließungen verabschiedet (**Anlagen 4** und **20**), in denen sie die anlasslose Speicherung personenbezogener Daten auf Vorrat ablehnen. Die freie Kommunikation als Teil des Fundaments einer freien demokratischen Gesellschaft ist in Gefahr.

23.2 Speicherung von IP-Adressen

Das Urteil des Landgerichtes Darmstadt vom 07.12.2005, Az.: 25 S 118/2005, wonach Access-Provider bei einem Flatrate-Tarif verpflichtet sind, die dem Kunden jeweils zugeordnete dynamische IP-Adresse nach Beendigung der Verbindung zu löschen, wurde durch den Beschluss des Bundesgerichtshofes (BGH) vom 26.10.2006, Az.: III ZR 40/06 rechtskräftig. Das Landgericht Darmstadt hatte ausgeführt, dass insbesondere eine Speicherung nach § 97 Abs. 2 Telekommunikationsgesetz (TKG) nicht in Betracht kommt, da die IP-Adresse weder für die Entgeltermittlung noch für die Entgeltabrechnung erforderlich ist.

Allerdings gelten sowohl das Urteil des Landgerichtes als auch der Beschluss des BGH nur für den Vertrag zwischen T-Online und dem Kläger. Wird die geplante Vorratsdatenspeicherung (siehe Ziff. 23.1) umgesetzt, könnte die bisherige Praxis von T-Online außerdem verpflichtend werden. Dann müssten alle Verkehrsdaten - also auch die IP-Adresse - mindestens sechs Monate gespeichert werden.

Das Amtsgericht Darmstadt hatte in erster Instanz im Juli 2005 entschieden (Az.: 300 C 397/04), dass die Speicherung der IP-Adressen bis 80 Tage nach Rechnungsstellung den datenschutzrechtlichen Vorgaben des TKG widerspreche. Allerdings hielt es das Amtsgericht für vertretbar, dass die Daten erst nach mehreren Tagen gelöscht werden.

Dieser Argumentation hat sich mittlerweile auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit angeschlossen, der die derzeitig von der T-Com (technischer Dienstleister für T-Online) praktizierte einwöchige Vorhaltung von Verkehrsdaten bei Flatrates für gesetzeskonform und datenschutzverträglich hält. Dabei bezieht er sich auf die in § 100 TKG erlaubte Verwendung von Verkehrsdaten zur Missbrauchseingrenzung und die in § 109 TKG festgelegte Verpflichtung der Telekommunikationsanbieter, angemessene Maßnahmen zum Schutz ihrer Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe bzw. äußere Angriffe zu treffen.

Problematisch ist jedoch nicht nur die IP-Adressenspeicherung bei Access-Providern wie T-Online, sondern auch bei den sog. Content-Providern, die als Anbieter von Telemedien (früher: Tele- bzw. Mediendiensten) beim Besuch ihres Internetangebots ebenfalls die IP-Adressen der Nutzer protokollieren. Allerdings sieht auch das neue Telemediengesetz (TMG, siehe Ziff. 23.3) eine Speicherung von Nutzungsdaten über das Ende der Verbindung hinaus nur für Zwecke der Abrechnung vor. Das heißt, dass bei kostenlosen Internetangeboten die Nutzungsdaten und damit auch die IP-Adresse nach Ende der Verbindung gelöscht werden müssten.

Dieses Problem bestand auch bei der beabsichtigten statistischen Auswertung der Zugriffe auf das hiesige Landesportal. Anhand der IP-Adresse sollte ausgewertet werden, woher die jeweiligen Nutzer kommen und welchen „Weg“ sie durch das Landesportal „gehen“. Aufgrund der technischen Realisierung im Landesinformationszentrum (LIZ) war eine solche Auswertung allerdings gar nicht möglich, da die Zugriffe auf das Landesportal zunächst über einen Proxy geleitet werden. Der Webserver des Landesportals „sieht“ als Nutzer nur die IP-Adresse des Proxys, wodurch eine nutzerbezogene Auswertung nicht mehr möglich ist.

Allerdings werden die IP-Adressen der Landesportalnutzer auf dem Proxy mitprotokolliert, wobei die Protokolldaten nach fünf Tagen gelöscht bzw. überschrieben werden. Obwohl das TMG keine Regelungen zur Missbrauchsbekämpfung und zu technischen Schutzmaßnahmen enthält, wie sie im TKG vorgesehen sind, akzeptiert der Landesbeauftragte einstweilen diese Protokollierung zur Sicherstellung eines ordnungsgemäßen Betriebes (vgl. § 10 Abs. 4 DSG-LSA). Der Landesbeauftragte ist mit dem LIZ darüber im Gespräch, ob diese Protokollierung tatsächlich für die o.g. Zwecke genutzt werden konnte und damit weiterhin erforderlich ist.

23.3 Fortentwicklung der Medienordnung

Der Bundesrat hat im Februar 2007 die vom Bundestag verabschiedete Neuordnung des Medienrechts durch das Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz (ElGVG) passieren lassen, dessen Kernstück das neue Telemediengesetz (TMG) bildet (BGBl. I S. 179).

Die wesentliche Änderung besteht darin, dass künftig nicht mehr zwischen Tele- und Mediendiensten unterschieden wird. Teledienste sind bislang bundesrechtlich im Teledienstegesetz (TDG) geregelt. Dabei handelt es sich vor allem um Waren-

und Dienstleistungsangebote, die im Internet abgerufen werden können. Mediendienste, die bisher im Mediendienste-Staatsvertrag (MDStV) geregelt sind, sind alle meinungsrelevanten Abrufdienste, wie beispielsweise die redaktionell gestalteten Online-Angebote von Nachrichtenmagazinen und Zeitungen sowie die Verteildienste.

Diese Unterscheidung hat in der Praxis zu Abgrenzungsproblemen und auch zu zahlreichen Doppelregulierungen geführt, die in Zukunft entfallen. Unter dem Begriff "Telemedien" werden künftig "Tele- und Mediendienste" zusammengeführt. Die wirtschaftsbezogenen Anforderungen an Telemedien (z.B. Verantwortlichkeitsregelungen, Herkunftslandsprinzip) werden im Telemediengesetz für alle Angebote einheitlich geregelt, während die inhaltsbezogenen Vorschriften (wie journalistische Sorgfaltspflichten, Gegendarstellungsrecht) in einem neuen Kapitel des Staatsvertrages für Rundfunk und Telemedien konzentriert werden. Die datenschutzrechtlichen Vorschriften, die bisher für Teledienste im Teledienstedatenschutzgesetz (TDDSG) und für Mediendienste im MDStV geregelt waren, werden ebenfalls in das TMG überführt.

Allerdings wird es auch weiterhin Abgrenzungsprobleme zwischen den verschiedenen elektronischen Medien geben, da Telekommunikationsdienste und Rundfunk nicht unter dieses Gesetz fallen. Mit einem PC kann jedoch nicht nur im Internet gesurft, sondern auch telefoniert, E-Mail versendet, ferngesehen oder Radio gehört werden, so dass Telemedien, Telekommunikation und Rundfunk unter Umständen durch einen einzigen Diensteanbieter erbracht werden. Obwohl die Unterscheidung zwischen Tele- und Mediendiensten entfällt, muss nun eine Unterscheidung zwischen Telemedien, Telekommunikation und Rundfunk getroffen werden. Das neue TMG bringt keine Klarheit, welche verschiedenen datenschutzrechtlichen Regelungen durch die Diensteanbieter zu beachten sind und welche Aufsichtsbehörde jeweils für die Datenschutzkontrolle zuständig ist.

Die notwendigen Änderungen im bisherigen Rundfunkstaatsvertrag - unter anderem die neue Bezeichnung „Staatsvertrag für Rundfunk und Telemedien“ - haben die Länder in der Ministerpräsidentenkonferenz am 22. Juni 2006 mit dem 9. Rundfunkänderungsstaatsvertrag beschlossen. Dieser ist zeitgleich mit dem TMG am 1. März 2007 in Kraft getreten (GVBl. LSA S. 18).

23.4 Urheberrecht vs. Fernmeldegeheimnis

Am 24. Januar 2007 hat das Bundeskabinett den Entwurf eines Gesetzes zur Durchsetzung der Rechte des geistigen Eigentums beschlossen (BR-Drs. 64/07). Hiermit soll die Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 umgesetzt werden. Die Frist zur Umsetzung der Richtlinie ist bereits am 29. April 2006 abgelaufen.

Der Gesetzentwurf sieht unter anderem vor, dass Rechteinhaber künftig auch gegenüber unbeteiligten Dritten wie Internet-Providern, die selbst keine Urheberrechtsverletzung begangen haben, Auskunftsansprüche geltend machen können. So sollen diese Auskunft über - dem Fernmeldegeheimnis unterliegende - Ver-

kehrsdaten ihrer Nutzer erteilen, wenn den Nutzern eine Urheberrechtsverletzung vorgeworfen wird.

Diese Auskunft darf zwar nur erteilt werden, wenn vorher eine richterliche Anordnung erwirkt wurde, allerdings hat sich der Bundesrat am 9. März 2007 für eine Streichung des Richtervorbehalts ausgesprochen. Zwar würde für die Auskunft auf Verkehrsdaten zugegriffen, die dem Fernmeldegeheimnis unterliegen, allerdings beziehe sich die eigentliche Auskunft auf reine Bestandsdaten, da es darum gehe, welcher Person zu der fraglichen Zeit welche IP-Adresse zugewiesen wurde. In der Gegenäußerung der Bundesregierung (BT-Drs. 16/5048) wird diesem Antrag jedoch nicht gefolgt.
Die Frage, ob ein Auskunftsanspruch nur besteht, wenn die Rechtsverletzung im geschäftlichen Verkehr erfolgt ist, wird von der Bundesregierung noch geprüft. Der Bundesrat lehnt dies ab, da ansonsten z.B. Teilnehmer an Internet-Tauschbörsen, bei denen die meisten Urheberrechtsverletzungen auftreten, nicht erfasst wären.

In einer Entschließung anlässlich der 71. Konferenz (**Anlage 12**) warnen die Datenschutzbeauftragten des Bundes und der Länder ausdrücklich davor, dass erstmals das Fernmeldegeheimnis auch zugunsten privater wirtschaftlicher Interessen eingeschränkt werden soll. Es sei zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer Interessengruppen geweckt werden könnten. Deshalb fordern die Datenschutzbeauftragten des Bundes und der Länder die Bundesregierung und den Gesetzgeber auf, auf eine weitere Einschränkung des Fernmeldegeheimnisses zu verzichten. Die Musik- und Filmindustrie müsse dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßige Nutzungen verhindert werden.

Im Übrigen ist der Auskunftsanspruch auch im neuen Telemediengesetz (TMG) verankert (vgl. Ziff. 23.3). Nach der bisherigen Gesetzeslage war die Herausgabe von Bestandsdaten nur an Strafverfolgungsbehörden und Gerichte zum Zweck der Strafverfolgung zulässig. In § 14 Abs. 2 TMG wurde dieser Kreis nun um die Verfassungsschutzbehörden des Bundes und der Länder, den Bundesnachrichtendienst und den Militärischen Abschirmdienst erweitert. Außerdem ist die Auskunft auch zu erteilen, wenn dies zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.

23.5 E-Mail und Internet am Arbeitsplatz - Spamfilterung bei privater E-Mail-Nutzung

Zur Nutzung von E-Mail und Internet am Arbeitsplatz hat sich der Landesbeauftragte bereits in seinem VI. Tätigkeitsbericht (Ziff. 23.2) und in seinem VII. Tätigkeitsbericht (Ziff. 23.3) geäußert. Grund für die neuerliche Befassung mit diesem Thema ist die Problematik der Spam-Filterung, die durch das hohe Aufkommen an Spam mittlerweile unverzichtbar geworden ist. Allerdings gibt es hierbei wiederum Probleme, wenn die private E-Mail-Nutzung gestattet ist, da der Arbeitgeber gegenüber seinem Mitarbeiter dann zum Telekommunikationsdiensteanbieter wird und zur Einhaltung des Fernmeldegeheimnisses verpflichtet ist.

Gemäß § 206 Abs. 2 Nr. 2 Strafgesetzbuch (StGB) wird nämlich bestraft, wer unbefugt einem solchen Unternehmen (welches geschäftsmäßig TK-Dienste erbringt, also hier das Land Sachsen-Anhalt als Arbeitgeber) zur Übermittlung anvertraute Sendungen unterdrückt.

Seit Dezember 2005 erfolgt auch im Landesinformationszentrum (LIZ) eine zentrale Spamfilterung aller eingehenden E-Mails. Das Innenministerium informierte in einem Schreiben an die Mitglieder des IT-KA über diese Maßnahme und wies darauf hin, dass die Ressorts sowie deren nachgeordnete Bereiche bei Gestattung privater E-Mail-Nutzung eine Einwilligung der Bediensteten in diese Spamfilterung einholen müssen. Gleichzeitig wurde die Überarbeitung der Musterdienstanweisung über die Bereitstellung und Nutzung von Internet-Zugängen in Aussicht gestellt.

Leider liegt dem Landesbeauftragten die überarbeitete Musterdienstanweisung trotz mehrmaliger Nachfragen noch nicht vor. Die Zuständigkeit wurde vom IT-KA auf den IMA-Org übertragen. Der zwischenzeitlich im IT-KA diskutierte Vorschlag, die private Internet- und E-Mail-Nutzung zu untersagen, um so auf eine Einwilligung der Mitarbeiter verzichten zu können, wurde mehrheitlich abgelehnt. Vielmehr bestand Einigkeit darüber, die Musterdienstanweisung hinsichtlich der Einwilligungserklärung so zu ergänzen, dass der Mitarbeiter in die Spam-Filterung und mögliche Unterdrückung an ihn adressierter E-Mails einwilligt.

Zur Zeit wird im LIZ ein Großteil der Spam-Mails durch Verfahren wie z.B. Greylisting abgewehrt. Der Begriff Greylisting bezeichnet eine Form der Spam-Bekämpfung, bei dem E-Mails von unbekannten Absendern temporär abgewiesen und erst nach einem zweiten Zustellversuch angenommen werden. Die trotz Greylisting angenommenen restlichen Spam-Mails sowie E-Mails mit unzulässigen Dateianhängen (unzulässiges Dateiformat, zu langer Dateiname) werden in einer Quarantäne-Datenbank gespeichert und nach 30 Tagen gelöscht. Dabei ist ein Großteil der Spam-Mails außerdem an unbekannte Empfänger gerichtet, die in der Domäne lsa-net.de bzw. sachsen-anhalt.de gar nicht existieren.

Bei der derzeitigen Verfahrensweise werden nur Empfänger von E-Mails mit unzulässigen Dateianhängen darüber informiert, dass ihre E-Mail in der Quarantäne-Datenbank zwischengespeichert wurde. Um ein für alle Nutzer transparentes Verfahren einzuführen, das auch dem bei privater Nutzung zu beachtenden Fernmeldegeheimnis Rechnung trägt, sollen die Spam-Mails zukünftig nicht zwischengespeichert, sondern markiert und an die Empfänger weitergeleitet werden. Dazu ist es jedoch erforderlich, das Spam-Aufkommen und damit die Menge weitergeleiteter E-Mails erheblich zu reduzieren. Dazu soll weiterhin die bewährte Methode des Greylisting zum Einsatz kommen und zusätzlich ein Abgleich mit dem zentralen Adressverzeichnis erfolgen, wodurch alle aufgrund unbekanntem Empfänger nicht zustellbaren E-Mails abgewiesen werden.

Der Landesbeauftragte weist darauf hin, dass unabhängig von der Änderung der Musterdienstanweisung jede öffentliche Stelle, die ihren Mitarbeitern die private Nutzung der dienstlichen E-Mail-Adresse gestattet, von jedem Mitarbeiter eine

Einwilligung in die Spam-Filterung und mögliche Unterdrückung der E-Mails einholen muss.

23.6 Anonyme Nutzung des Rundfunks

Seit einiger Zeit konkretisieren sich die Pläne privater Fernsehanbieter, ihre Programme ähnlich wie beim Pay-TV nur noch verschlüsselt über Satellit, Kabel und DVB-T zu übertragen. Das hätte zur Folge, dass der Fernsehempfang nur durch Entschlüsselung der Signale mittels einer Set-Top-Box und einer entsprechenden Smartcard möglich wäre. Dabei sind die Unternehmen offensichtlich daran interessiert, ausschließlich personalisierte Smartcards herauszugeben, um so die Nutzung bestimmter Angebote personenbezogen auswerten zu können.

Gemäß § 47 Rundfunkstaatsvertrag i.V.m. § 13 Abs. 6 Telemediengesetz ist die Nutzung und Bezahlung von Rundfunk anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Da auch datenschutzfreundliche Varianten wie z. B. Prepaid-Karten für die Abrechnung zur Verfügung stehen, fordern die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung anlässlich der 73. Konferenz (**Anlage 24**), auch in Zukunft die anonyme Nutzung von Rundfunkprogrammen sicherzustellen. Außerdem wird an die Forderung erinnert, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

24. Verfassungsschutz

24.1 Terrorismusbekämpfungsergänzungsgesetz

Zum Unwort des Jahres werden seit 1991 „sprachliche Missgriffe in der öffentlichen Kommunikation“ gekürt, „...die sachlich grob unangemessen sind...“. So ist es auf den Internetseiten des Dudens nachzulesen. Vielleicht hat der Begriff „Terrorismusbekämpfungsergänzungsgesetz“ nicht das Zeug zum Unwort des Jahres, weil er sachlich nicht grob unangemessen ist. Ein „Wortungetüm“ ist es allemal. Und was sich inhaltlich hinter diesem Begriff verbirgt, ist zumindest datenschutzrechtlich in Teilen unangemessen.

Das Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl. I S. 2) besteht aus 16 einzelnen Artikeln, von denen 13 bestehende Gesetze, im Hinblick auf eine bessere Bekämpfung terroristischer Bestrebungen, ändern.

Artikel	Änderung
1	Bundesverfassungsschutzgesetz
2	Terrorismusbekämpfungsgesetz
3	Gesetz über den militärischen Abschirmdienst
4	Bundesnachrichtendienstgesetz
5	Artikel 10-Gesetz
6	Sicherheitsüberprüfungsfeststellungsverordnung
7	Gesetz zum Schengener Übereinkommen vom 19. Juni 1990
7a	Vereinsgesetz
7b	Passgesetz
8	Zollverwaltungsgesetz
9	Straßenverkehrsgesetz
9a	Luftsicherheitsgesetz
10	Weitere Änderungen zum 10. Januar 2012

An der Änderung von Gesetzen wie dem Vereinsgesetz oder dem Straßen-

verkehrsgesetz lässt sich ersehen, in welche Bereiche des Lebens die Terrorismusbekämpfung zwischenzeitlich schon vorgedrungen ist. Nun wird nicht jedes Vereinsmitglied mit dem Eintritt in einen Verein oder jedes zugelassene Fahrzeug zur Terrorismusbekämpfung an den Verfassungsschutz gemeldet. Aber im Straßenverkehrsgesetz gibt es durch das Terrorismusbekämpfungsergänzungsgesetz eine Vorschrift, die es den Straßenverkehrsbehörden erlaubt, Daten an die Verfassungsschutzbehörden, den Militärischen Abschirmdienst und den Bundesnachrichtendienst zu übermitteln. Natürlich erfolgen diese Übermittlungen nur zur Erfüllung der diesen Einrichtungen durch Gesetz übertragenen Aufgaben. Aber das Aufgabenspektrum dieser Einrichtungen ist erweiterbar und wurde bereits erweitert. Bisher gab es diese Ermächtigung zur Datenübermittlung nicht.

Aus Sicht der Freiheitsrechte geht es letztlich nicht darum, eine spezielle Regelung im Straßenverkehrsgesetz als datenschutzrechtlich unzulässig zu kennzeichnen. Entscheidend ist es, die Tendenz zu verdeutlichen: Die Tendenz zu immer ausgedehnteren Befugnissen im Namen der Terrorismusbekämpfung, die sich nicht mehr nur auf Terrorverdächtige beschränken. Das Verhältnis zwischen Freiheit und Sicherheit ist aus dem Gleichgewicht geraten. Die Bürgerinnen und Bürger bezahlen einen vermeintlichen Zugewinn an Sicherheit mit überproportional großen Einbußen bei ihren Freiheitsrechten.
Dieses Missverhältnis zwischen Sicherheit und Freiheit greift die Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter dem Titel „Das Gewicht der Freiheit beim Kampf gegen den Terrorismus“ auf: „Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit.“ (**Anlage 15**)

In Artikel 11 des Terrorismusbekämpfungsergänzungsgesetzes wird - wie bereits beim Terrorismusbekämpfungsgesetz - eine Evaluierung der geänderten Vorschriften vor dem 10. Januar 2012 unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt werden muss, festgeschrieben. Die Datenschutzbeauftragten des Bundes und der Länder mussten hinsichtlich der Evaluation des Terrorismusbekämpfungsgesetzes in ihrer Entschließung feststellen: „Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der ‚Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes’ ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.“

24.2 GIAZ

Das GIAZ - was ist das? Es ist das Gemeinsame Informations- und Auswertungszentrum islamistischer Terrorismus. Es ist eine Einrichtung des Landes Sachsen-Anhalt, installiert im Landeskriminalamt. Es ist eine Schnittstelle von Polizei und Verfassungsschutz. Und genau darin liegt die Brisanz seiner Existenz.

Im GIAZ arbeiten sowohl Polizisten als auch Mitarbeiter der Verfassungsschutzbehörde. Nach Mitteilung des Ministeriums des Innern sollte jeder Mitarbeiter nur den Aufgaben nachgehen, die er auch in seiner eigenen Dienststelle wahrnehmen dürfte. Die Polizisten erledigen polizeiliche Aufgaben im Rahmen der für die Polizei geltenden Rechtsvorschriften. Die Mitarbeiter der Verfassungsschutzbehörde nehmen nur Aufgaben des Verfassungsschutzes und nach den für diese Aufgaben geltenden Vorschriften wahr. Polizisten und Verfassungsschützer sind in unterschiedlichen Räumen untergebracht und sollen ausschließlich den Weisungen ihrer jeweiligen polizeilichen bzw. Verfassungsschutz-Vorgesetzten unterliegen. Im Grunde soll jeder das tun, was er rechtlich gesehen auch sonst darf. Mehrmals die Woche treffe man sich zu gemeinsamen Dienstberatungen. Dann werden Erkenntnisse ausgetauscht; natürlich im Rahmen der geltenden Übermittlungsvorschriften.
Wenn sich alles im Rahmen der Gesetze bewegt, fragt man sich, warum wurde in den vergangenen zwei Jahren soviel über das GIAZ geschrieben und gesprochen?

Grundsätzlich dürfen Polizei und Verfassungsschutz Informationen untereinander austauschen. Allerdings gibt es dafür strikte gesetzliche Vorgaben. Nicht jede Information des einen darf beim anderen ankommen. Die Zusammenarbeit von Polizei und Geheimdiensten wird durch das **Trennungsgebot** begrenzt.
Das Trennungsgebot geht auf einen Brief der drei Westalliierten an den Parlamentarischen Rat vom 14. April 1949 zurück, in dem die künftige Struktur der deutschen Sicherheitsbehörden festgelegt wurde. Dieser „Polizeibrief“ enthält u.a. die Vorgabe, dass der künftige Geheimdienst „keine Polizeibefugnisse“ haben und „keine Bundespolizeibehörde ... Befehlsgewalt über Landes- oder Ortspolizeibehörden besitzen“ dürfe. Hintergrund dieser Vorgaben waren die Erinnerungen an den zentralisierten Macht- und Terrorapparat des Nazistaates. Im Lichte dieser Beweggründe ist das Trennungsgebot von Polizei und Nachrichtendiensten bis heute von Bedeutung (siehe §§ 2 Abs. 2, 7 Abs. 5 VerfSchG-LSA) und darf auch in Zeiten von erhöhter Terrorgefahr nicht umgangen werden. Es hat, wie auch eine Entscheidung des Sächsischen Verfassungsgerichtshofes vom 21. Juli 2005 (Az. Vf.67-II-04, NVwZ 2005, 1310) belegt, verfassungsrechtliche Relevanz.

Die Einrichtung und der Betrieb des GIAZ gemäß Vorerlass vom Dezember 2004 und Erlass vom Dezember 2005 haben im Berichtszeitraum zu einem umfangreichen Schriftwechsel zwischen dem Landesbeauftragten und dem dafür zuständigen Ministerium des Innern des Landes Sachsen-Anhalt geführt. Kernpunkt war und ist es, die Organisation und Arbeitsweise des GIAZ so auszurichten, dass trotz Zusammenarbeit von Polizei und Verfassungsschutz das Trennungsgebot gewahrt bleibt. Es muss verhindert werden, dass Polizei und Verfassungsschutz sich über das gesetzlich vorgesehene Maß des Datenaustausches hinaus personenbezogene Daten wechselseitig übermitteln.

Dazu bedarf es eindeutiger organisatorischer Regelungen. So wurde ausdrücklich verfügt, dass sowohl Polizisten als auch Verfassungsschützer, die im GIAZ arbeiten, nur ihren jeweiligen Weisungssträngen unterworfen sind. Da das GIAZ derzeit von einem Polizeibediensteten geleitet wird, musste ausdrücklich festgelegt werden, dass die Mitarbeiter der Verfassungsschutzbehörde nicht der Weisungs-

befugnis des Leiters des GIAZ unterstehen. Auch die Zugangsberechtigungen zu Büroräumen und IT-Technik mussten geregelt werden. Die Polizisten dürfen die Räume des Verfassungsschutzes nicht betreten. Umgekehrt gilt das Gleiche. Natürlich dürfen Datenbestände vom jeweils anderen nicht bzw. nur im Rahmen des Antiterrordateigesetzes (siehe Ziff. 24.3) genutzt werden.

Doch selbst wenn organisatorisch einiges dafür getan wurde, die Trennung von Polizei und Verfassungsschutz sicherzustellen, so ist doch die Möglichkeit nicht von der Hand zu weisen, dass im GIAZ mehr besprochen wird, als es nach Recht und Gesetz zulässig ist. Dass diese Befürchtung nicht absolut abwegig ist, zeigt die Lebenserfahrung. Wenn Menschen einander täglich begegnen und miteinander arbeiten, kann die gebotene Distanz schnell schwinden. Obwohl keine gemeinsame Dienststelle geschaffen werden sollte, hält das Ministerium des Innern an der organisationsrechtlichen Festlegung eines Gemeinsamen Zentrums fest. Besonders problematisch ist der Umstand, dass die Verfassungsschützer am Gewinnen repressiver Ermittlungsansätze im Sinne gemeinsamer Ermittlungsgruppen mitwirken, was die funktionelle Trennung in Frage stellt.

Im Sommer 2006 wurde seitens des Ministeriums versichert, das GIAZ zum Jahresende 2006 zu evaluieren. Bis zum Ende des Berichtszeitraums wurde dem Landesbeauftragten nicht bekannt, dass eine Evaluierung stattgefunden hat. Eine Stellungnahme des Ministeriums des Innern auf eine entsprechende Anfrage des Landesbeauftragten stellte Anfang Mai 2007 fest, dass das GIAZ wie bisher weitergeführt werde. Der Landesbeauftragte wird die Entwicklung rund um das GIAZ weiter aufmerksam verfolgen.

24.3 Antiterrordatei - Mit dem Trennungsgebot noch vereinbar?

Mit dem im Dezember 2006 erlassenen Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz, BGBl. I, S. 3409) hat der Bundesgesetzgeber den Weg hin zu mehr automatisiertem Datenaustausch freigemacht. Zum Einen wurde mit dem Gemeinsame-Dateien-Gesetz das Antiterrordateigesetz erlassen. Zum Anderen wurden in verschiedenen Gesetzen - Bundesverfassungsschutzgesetz, BND-Gesetz, Bundeskriminalamtgesetz - die gesetzlichen Voraussetzungen dafür geschaffen, dass diese Einrichtungen an der Antiterrordatei mitwirken können.

Im Ergebnis wurde mit den Regelungen zur Antiterrordatei ein Ausmaß an Datenaustausch ermöglicht, der verfassungsrechtliche Bedenken hervorruft. Ganz grundlegend bleibt festzustellen, dass das Trennungsgebot - zu dem bereits unter Ziff. 24.2 ausgeführt wurde - hier nicht mehr gewahrt erscheint. Anlässlich der 72. Tagung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2006 in Naumburg haben sich diese mit dem Antiterrordateigesetz auseinandergesetzt. Im Ergebnis ihrer Beratungen wurde eine Entschließung gefasst, deren gesamter Wortlaut in **Anlage 16** zu diesem Tätigkeitsbericht abgedruckt ist und deren zentrale Forderungen nachfolgend dargestellt sind:

„... Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden

Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.

Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.

In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.

Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.

Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.“

Diese Erwartungen, die die Datenschutzbeauftragten formuliert haben, bezogen sich zu diesem Zeitpunkt zwar auf den Entwurf des Gemeinsame-Dateien-Gesetzes. Weil der Gesetzgeber die Hinweise der Datenschutzbeauftragten nicht aufgenommen hat, bleiben sie auch nach Erlass des Gesetzes aufrecht erhalten.

Für Sachsen-Anhalt wirkt sich das Antiterrordateigesetz so aus, dass das Landeskriminalamt und die Verfassungsschutzbehörde des Landes an die Antiterror-

datei angebunden wurden. Im ersten Quartal 2007 wurde jeweils eine begrenzte Anzahl von Mitarbeitern für den Zugriff auf die Antiterrordatei freigeschaltet. Durch die Länder und den Bund wird die Datei nun entsprechend einem Stufenplan mit Daten bestückt.

Aus Anlass der Inbetriebnahme der Antiterrordatei gab das Ministerium des Innern am 29. März 2007 eine Presseerklärung ab: „Die neue Datei stellt gewissermaßen den Schlüssel für die weitere Kommunikation der Behörden dar.“ Der Landesbeauftragte wird auch in Zukunft sein Augenmerk darauf legen, dass dieser „Schlüssel“ die Tür zur Datenwelt der Terrorismusbekämpfung nur in den gesetzlich vorgesehenen Fällen und nach sorgsamer Abwägung öffnet.

24.4 Änderung des Verfassungsschutzgesetzes

Am 2. Februar 2006 trat das Gesetz zur Änderung verfassungsschutzrechtlicher Vorschriften und zur Stärkung des Verfassungsschutzes in Kraft (GVBl. LSA S. 12). Allein aus der Bezeichnung vermag jeder die Grundtendenz der darin enthaltenen Gesetzesänderungen zu erkennen. Mit diesem Gesetz wurden sowohl das Gesetz zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt (VerfSchG-LSA) als auch das Sicherheitsüberprüfungs- und Geheimschutzgesetz (SÜG-LSA) verkündet (siehe zum SÜG-LSA Ziff. 24.6).

Im Rahmen des Gesetzgebungsverfahrens zum VerfSchG-LSA wurde der Landesbeauftragte beteiligt. Trotz wiederholter Stellungnahmen zu datenschutzrechtlich bedenklichen Regelungen konnte sich der Landesbeauftragte nicht in allen Punkten durchsetzen.

In seiner ersten Stellungnahme zum Gesetzentwurf vom März 2005 hat der Landesbeauftragte seine Kritikpunkte gegenüber dem Ministerium des Innern des Landes Sachsen-Anhalt deutlich gemacht. Insbesondere richtete sich seine Kritik gegen die Neuregelung der § 10 - Speicherbefugnis für Personen zwischen dem 14. und 16. Lebensjahr -, § 11 - Verlängerung der Löschungsfristen - und § 17a - Berichtspflicht des Innenministeriums gegenüber der parlamentarischen Kontrollkommission - sowie die fehlende Evaluierungsklausel für neu eingeführte Instrumente.

Mit der Änderung des § 10 VerfSchG-LSA wurde die Befugnis der Verfassungsschutzbehörde, personenbezogene Daten zu Minderjährigen zu speichern, auf Personen ab dem 14. Lebensjahr ausgeweitet. Bisher durften erst über Personen ab dem 16. Lebensjahr Daten gespeichert werden. Aus Sicht des Landesbeauftragten wahrt die neue Regelung den Grundsatz der Verhältnismäßigkeit nicht. Von einer solchen Überwachungsregelung geht ein hoher Anpassungsdruck auf das sich noch entwickelnde politische und soziale Bewusstsein von Jugendlichen aus. Nur wegen vereinzelter Fälle, in denen verfassungsschutzrelevante Belange durch Jugendliche berührt werden, erscheint die neue Regelung nicht zu rechtfertigen.

In § 11 VerfSchG-LSA wurde die Löschungsfrist für personenbezogene Daten von 10 auf 15 Jahre erhöht. Außerdem entfiel die ausdrücklich formulierte Begrün-

dungspflicht für die Fälle, in denen eine ausnahmsweise längere Speicherung erfolgt. In der Begründung zum Gesetzentwurf wurde die Auffassung vertreten, dass sich Personen über einen Zeitraum von zehn Jahren hinweg bewusst so konspirativ verhalten könnten, sodass neue Erkenntnisse erst nach mehr als zehn Jahren vorliegen; dann wären aber die alten vorher bereits gelöscht. Vor dem Hintergrund der äußerst niedrigen Verdachtsschwelle, bei der die Verfassungsschutzbehörde tätig werden darf, erscheint es allerdings wenig wahrscheinlich, dass sich eine Person bewusst zehn Jahre lang so untätig verhalten kann, dass sie aus dem Informationssystem des Verfassungsschutzes gelöscht würde. Im Rahmen der Gesetzesbegründung konnten noch nicht einmal Fälle dieser Art zahlenmäßig, geschweige denn sachverhaltlich benannt werden. Der Wegfall der bisher ausdrücklich formulierten Begründungspflicht bringt im Ergebnis keine Arbeitserleichterung für die Verfassungsschutzbehörde. Aus rechtsstaatlichen Gründen kann auf eine Begründung solcher Einzelfallentscheidungen nicht verzichtet werden.

§ 17a VerfSchG-LSA regelt die Übermittlung von besonderen Informationen an die Verfassungsschutzbehörde. Absatz 1 der Vorschrift verweist auf das Verfassungsschutzgesetz des Bundes und gesteht den Landesverfassungsschutzbehörden dieselben Rechte zu. Im Einzelnen darf die Verfassungsschutzbehörde des Landes Sachsen-Anhalt u.a. Auskünfte von Kreditinstituten, Postdienstleistern, Luftfahrtunternehmen und Telekommunikationsanbietern einholen. Auch § 17a Abs. 6 VerfSchG-LSA führte im Rahmen der parlamentarischen Beratungen wiederholt zu Diskussionen. Er ermächtigt die Verfassungsschutzbehörden dazu, durch technische Mittel den Standort eines aktiv geschalteten Mobilfunkendgerätes sowie dessen Geräte- und Kartennummer zu ermitteln, mittels des sog. IMSI-Catchers (vgl. Ziff. 18.3). Mit § 17a VerfSchG-LSA wurde eine Berichtspflicht der Verfassungsschutzbehörde an die Parlamentarische Kontrollkommission vorgesehen. Auch wenn das dem Grunde nach zu begrüßen ist, so hätte es der Festschreibung von Mindestanforderungen an diese Berichte bedurft. Zu diesen Mindestanforderungen gehören nach Auffassung des Landesbeauftragten Zahlenangaben über die Betroffenen, Mitbetroffenen, eingesetzten Mitarbeiter und die Maßnahmedauer ebenso wie Qualitätsangaben zu Übermittlungsfakten, zur vorgesehenen Weiternutzung von Daten, zur Kombination mit anderen Eingriffsformen sowie Erfolgs- und Misserfolgsdaten.

Eine Evaluationsklausel hat der Landesbeauftragte vor dem Hintergrund der umfassenden Änderungen für notwendig erachtet, um die Effektivität der neuen Instrumente festzustellen und so ggf. auf deren Änderung oder Abschaffung hinzuwirken. Eine entsprechende Klausel hat der Gesetzgeber bis auf die Regelung zum IMSI-Catcher nicht vorgesehen.

Im Rahmen der Ausschuss- und Plenumsberatungen hat der Landesbeauftragte immer wieder auf seine Bedenken hingewiesen und auch - erfolgreich - auf eine rechtskonforme Ausgestaltung der Vorschrift zum Zitiergebot wegen der Einschränkung von Grundrechten - § 30a VerfSchG-LSA - hingewirkt. Im Ergebnis muss aber festgestellt werden, dass die Mehrzahl seiner Anregungen keinen Eingang in den Gesetzestext gefunden hat. Auch auf die fehlenden Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung wurde wiederholt aufmerk-

sam gemacht. Da die Änderung des VerfSchG-LSA der Entscheidung des Bundesverfassungsgerichts zum Kernbereichsschutz zeitlich nachgelagert war, hätten die Regelungen des VerfSchG-LSA an diese Rechtsprechung bereits angepasst werden können (vgl. Ziff. 17.1).

Das Gesetz enthält im Übrigen keine Bestimmung zur heimlichen Online-Durchsuchung. Dabei sollte es bleiben (siehe Ziff. 18.3 und **Anlage 19**). Gegen eine Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen, wonach Befugnisse zum verdeckten Zugriff u.a. auf Festplatten geschaffen wurden, ist Verfassungsbeschwerde eingelegt worden.

24.5 Beobachtung von Demonstranten

Infolge einer Erörterung im Arbeitskreis Sicherheit der Datenschutzkonferenz hat der Landesbeauftragte im Sommer 2005 bei der Verfassungsschutzbehörde zur Praxis der Videoaufzeichnung anlässlich von Demonstrationen nachgefragt. Nach § 7 Abs. 3 VerfSchG-LSA darf die Verfassungsschutzbehörde mit nachrichtendienstlichen Mitteln, insbesondere durch den Einsatz von Bild- und Tonaufzeichnungen, verdeckt ermitteln.

Aus Sicht des Landesbeauftragten greift die Verfassungsschutzbehörde durch das Aufzeichnen von Demonstrationen mittels Videokamera in das Grundrecht auf Versammlungsfreiheit nach Art. 8 GG und Art. 12 Landesverfassung ein. Ein solcher Grundrechtseingriff ist nur zulässig, wenn die Vorschrift, aufgrund derer er vorgenommen wird, den verfassungsrechtlichen Anforderungen u.a. des Zitiergebots entspricht. In § 30a VerfSchG-LSA - Einschränkung von Grundrechten – findet sich ein Hinweis darauf, dass das Grundrecht auf Versammlungsfreiheit durch das VerfSchG-LSA eingeschränkt wird, nicht.
Durch die Videoaufzeichnung bei Demonstrationen erfolgt bereits per Gesetz eine Einflussnahme auf die Teilnahmebereitschaft an einer Demonstration und ergo ein entsprechender abstrakter Grundrechtseingriff. Konsequenterweise hätte das betroffene Grundrecht bezeichnet werden müssen. Im Rahmen der Überarbeitung des VerfSchG-LSA wurden die Bestimmungen nicht in § 30a VerfSchG-LSA aufgenommen.

Aus Sicht der Verfassungsschutzbehörde besteht zur Aufnahme der Art. 8 GG und 12 Landesverfassung keine Veranlassung. Nach Auffassung der Verfassungsschutzbehörde stellt das Videografieren von Demonstranten deshalb keinen Grundrechtseingriff dar, weil die Ermächtigung der Verfassungsschutzbehörde für solche Maßnahmen für jedermann im VerfSchG LSA nachlesbar sei. Deshalb müsse derjenige, der an Versammlungen teilnimmt, bei denen extremistische Inhalte transportiert werden, ohnehin davon ausgehen, dass eine solche Veranstaltung beobachtet wird. Die Umstände, die zu einer Beobachtung führen, seien für den Grundrechtsträger damit nachvollziehbar.

Dieser Auffassung vermag sich der Landesbeauftragte nicht anzuschließen. Durch das Wissen um die Möglichkeit einer Beobachtung wird ein Anpassungsdruck ausgeübt, der Eingriffsqualität hat.

24.6 SÜG-LSA - Geheimschutz und Sicherheitsüberprüfungen stehen endlich auf gesetzlichen Füßen

Wie bereits in Ziff. 24.4 dargestellt, trat am 2. Februar 2006 das Gesetz zur Änderung verfassungsschutzrechtlicher Vorschriften und zur Stärkung des Verfassungsschutzes in Kraft. Neben der Änderung des VerfSchG LSA wurde mit Art. 2 dieses Gesetzes auch das Sicherheitsüberprüfungs- und Geheimschutzgesetz des Landes Sachsen-Anhalt (SÜG-LSA) erlassen.

Zweck des SÜG-LSA ist es zum Einen, im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse vor der Kenntnisnahme durch Unbefugte zu schützen und den Zugang von Personen zu verhindern, bei denen ein Sicherheitsrisiko nicht ausgeschlossen werden kann. Zum Anderen soll die Beschäftigung von Personen, bei denen ein Sicherheitsrisiko nicht ausgeschlossen werden kann, an sicherheitsempfindlichen Stellen von lebens- und verteidigungswichtigen Einrichtungen verhindert werden.
Dazu regelt das SÜG-LSA die Voraussetzungen und das Verfahren zur Überprüfung von Personen, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen. In der Vergangenheit wurden diese Sicherheitsüberprüfungen auf der Grundlage eines entsprechenden Erlasses des Ministeriums des Innern durchgeführt. Die Sicherheitsüberprüfungen stellen jedoch einen erheblichen Eingriff in die Rechte der Betroffenen dar, so dass die Schaffung einer gesetzlichen Grundlage für die Durchführung der Sicherheitsüberprüfungen überfällig war.
Voraussetzung für eine Sicherheitsüberprüfung ist zwar nach § 8 Abs. 2 SÜG-LSA die Einwilligung des Betroffenen. Als freiwillig wird die Sicherheitsüberprüfung trotzdem häufig nicht empfunden werden, da sie überwiegend aufgrund der beruflichen Beschäftigung mit sicherheitsempfindlichen Erkenntnissen erforderlich sein wird. Wer dienstlich mit Fragen des Zivilschutzes befasst ist oder wer beim Verfassungsschutz tätig sein will, muss sich einem Sicherheitsüberprüfungsverfahren unterziehen.

Am Gesetzentwurf bemängelte der Landesbeauftragte, dass der Umfang der Unterrichtung der Betroffenen hinsichtlich der Verarbeitung der im Rahmen einer Sicherheitsüberprüfung erhobenen Daten wesentlich verringert werden sollte. Die entsprechende Regelung des § 8 SÜG-LSA war auf eine Einschränkung ausgerichtet. Der Landesbeauftragte wies allerdings darauf hin, dass das DSG-LSA ergänzend zum SÜG-LSA anzuwenden ist, weil das SÜG-LSA in diesem Punkt keine abschließende Regelung trifft. Nach § 4 Abs. 2 DSG-LSA ist der Betroffene auf die Bedeutung der Einwilligung, den Zweck der Erhebung, Verarbeitung und Nutzung sowie auf sein Recht und die Folgen der Verweigerung der Einwilligung hinzuweisen. Diese Regelung des DSG-LSA fängt die Schlechterstellung der Betroffenen aus dem SÜG-LSA heraus auf.

Nach § 23 Abs. 1 Nr. 2 SÜG-LSA dürfen die im Rahmen der Sicherheitsüberprüfung gespeicherten personenbezogenen Daten für Zwecke der Abwehr erheblicher Gefahren für die öffentliche Sicherheit verwendet und nach § 23 Abs. 2, 3 übermittelt werden. Unter Zugrundelegung des ordnungsrechtlichen Gefahrenbegriffes ist es bei dieser Formulierung u.a. denkbar, dass die im Rahmen einer Sicherheitsüberprüfung erlangten Daten, z.B. wegen einer groben Umweltver-

schmutzung, übermittelt werden. Dadurch wird nach Auffassung des Landesbeauftragten, der Grundsatz, dass Daten nur für den Zweck verwendet werden sollen, für den sie erhoben wurden, unverhältnismäßig durchbrochen.

Auch die Regelungen des § 24 SÜG-LSA sind in ihrer Erforderlichkeit nicht nachvollziehbar begründet. Die festgelegten Löschfristen unterscheiden nach der zuständigen Stelle und der mitwirkenden Behörde. Zuständige Stelle ist die, bei der die sicherheitsempfindliche Tätigkeit ausgeübt wird, bei der also die sicherheitsüberprüfte Person beschäftigt ist. Mitwirkende Behörde ist die Verfassungsschutzbehörde des Landes Sachsen-Anhalt.
Es wurde nicht plausibel dargelegt, warum die im Rahmen der Sicherheitsüberprüfung erhobenen personenbezogenen Daten bei der mitwirkenden Behörde wesentlich später gelöscht werden sollen als bei der zuständigen Stelle. Nachvollziehbar erläutert wurde nur, warum die Daten bei der zuständigen Stelle bis zu fünf Jahre nach dem Ausscheiden des Betroffenen aus der sicherheitsempfindlichen Tätigkeit vorgehalten werden sollen. Eine Begründung, warum die Verfassungsschutzbehörde als mitwirkende Behörde diese Daten nach dem Löschungszeitpunkt bei der zuständigen Stelle noch weitere zehn Jahre vorhalten darf, fehlt.

Eine Sicherheitsüberprüfung dient nach § 1 Abs. 1 SÜG-LSA dazu, Personen, bei denen ein Sicherheitsrisiko vorliegt, von der Beschäftigung an sicherheitsempfindlichen Stellen auszuschließen und ihren Zugang zu geheimhaltungsbedürftigen Informationen zu verhindern. Diesem Interesse wird in der Regel bereits dadurch Rechnung getragen, dass Personen mit Sicherheitsrisiko für derartige Aufgaben nicht zugelassen werden. Aber auch dann, wenn die Betroffenen keine sicherheitsempfindliche Tätigkeit aufnehmen, dürfen die erhobenen personenbezogenen Daten für elf Jahre bei der Verfassungsschutzbehörde vorgehalten werden. Das Interesse bei der Durchführung von Sicherheitsüberprüfungen kann nicht in der Gewinnung von Daten für den Verfassungsschutz liegen. Zumal nicht jedwede sicherheitserheblichen Erkenntnisse (siehe § 22 Abs. 2 Nr. 3 SÜG-LSA) den Aufgaben des Verfassungsschutzes zuzuordnen sein müssen. Diese Zweckdurchbrechung ist vor allem unter Berücksichtigung der langen Speicherdauer unverhältnismäßig.

Nach § 25 Abs. 2 SÜG-LSA erstreckt sich die grundsätzlich bestehende Auskunftsverpflichtung gegenüber dem Betroffenen nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen. Wenn die Regelung hinsichtlich der Herkunft der Daten noch einsichtig ist, so erschließt sich die Auskunftsverweigerung bezüglich der Empfänger von Übermittlungen nicht. Den Betroffenen ist es so nicht möglich, das Ausmaß der Verbreitung ihrer Daten zu übersehen und ggf. dagegen zu intervenieren. Sie sind damit schlechter gestellt als verurteilte Straftäter.
Als Korrektiv, um die Sicherheitsinteressen des Staates im Verhältnis zur Auskunftspflicht zu wahren, reicht die bestehende Regelung in § 25 Abs. 3 SÜG-LSA völlig aus. Wann der Gesetzgeber mit der Festlegung in Abs. 2 eine mögliche Entscheidung zugunsten eines Auskunftsberechtigten unterbinden wollte, ist nicht nachvollziehbar. Da das Bundesverfassungsgericht die Information Betroffener auch aus Gründen des rechtsstaatlichen Verfahrensanspruchs hoch einschätzt

(vgl. Ziffn. 18.4, 18.5), erscheint die Verfassungsmäßigkeit dieser Regelung zweifelhaft.

Die geäußerten Bedenken und Anregungen des Landesbeauftragten fanden im beschlossenen Gesetzestext keinen Widerhall.

24.7 Geheimschutzbeauftragter - Keine Aufgabe für einen Verfassungsschützer

Der Landesbeauftragte wurde auf die Problematik des Geheimschutzbeauftragten im Ministerium des Innern des Landes Sachsen-Anhalt aufmerksam. Der Geheimschutzbeauftragte des Ministeriums des Innern war gleichzeitig stellvertretender Leiter der Verfassungsschutzbehörde. In dieser Aufgabenkombination sieht der Landesbeauftragte eine Interessenkollision.

Vor diesem Hintergrund teilte der Landesbeauftragte dem Ministerium des Innern seine Rechtsauffassung mit. Nach der Verschlusssachenanweisung für das Land Sachsen-Anhalt (VSA) stellt der Geheimschutzbeauftragte in Fällen der vermuteten Durchbrechung des Geheimschutzes den Sachverhalt fest. Die dann erforderlichen Maßnahmen hat der Geheimschutzbeauftragte zu treffen. Nur in Fällen, in denen ein nachrichtendienstlicher Hintergrund oder eine Verratstätigkeit anderer Art nicht auszuschließen ist, beteiligt der Geheimschutzbeauftragte die Verfassungsschutzbehörde. Hieraus folgt eine klare Trennung zwischen Geheimschutz einerseits und Einschaltung der Verfassungsschutzbehörde andererseits. Die gleichzeitige Wahrnehmung beider Aufgaben durch eine Person steht damit im Widerspruch zu den einschlägigen Regularien in der VSA; im Übrigen unterscheidet auch das SÜG-LSA zwischen zuständiger Stelle und mitwirkender Behörde (siehe Ziff. 24.6).

Sicherlich kann es Sachverhalte geben, welche Geheimschutzinteressen verletzen und gleichzeitig den Verfassungsschutz in seinem Aufgabenspektrum tangieren. Jedoch dürften Verstöße gegen die VSA aus dem Grunde, dass der Umgang mit VS-Sachen vergleichsweise kompliziert ausgestaltet ist, wie auch, dass Fehler aus Nachlässigkeit bzw. Unwissenheit entstehen, im Vergleich zu jenen Fällen, in denen der inkorrekte Umgang mit vertraulichen Unterlagen zugleich verfassungsschutzrelevantes Fehlverhalten der betreffenden Bediensteten darstellt, deutlich überwiegen.

Wenn indessen der Geheimschutzbeauftragte des Ministeriums des Innern zugleich die Funktion des stellvertretenden Leiters der Verfassungsschutzbehörde inne hat, so werden die Übermittlungsvoraussetzungen nach der VSA - nachrichtendienstlicher Hintergrund oder andere Verratstätigkeit, unter denen ein Geheimschutzbeauftragter die Verfassungsschutzbehörde zu beteiligen hat - unterlaufen. Der Grundsatz der informationellen Gewaltenteilung ist dadurch faktisch negiert. Informationen, die der Amtsinhaber in seiner Funktion als Geheimschutzbeauftragter erlangt, nimmt er zugleich in der Funktion als stellvertretender Leiter der Verfassungsschutzbehörde zur Kenntnis.

Das Ministerium des Innern teilte die Rechtsauffassung des Landesbeauftragten zunächst nicht und wollte an seiner Praxis, den stellvertretenden Leiter der Ver-

fassungsschutzbehörde zum Geheimschutzbeauftragten zu berufen, nichts ändern. Es bedurfte eines wiederholten Austausches der Argumente, um letztlich zu bewirken, dass im Juli 2006 eine personelle und organisatorische Trennung der Funktion des stellvertretenden Leiters der Verfassungsschutzbehörde und des Geheimschutzbeauftragten des Ministeriums des Innern erfolgte.

25. Verkehr

25.1 Kfz-Zulassungsvoraussetzungsgesetz

Zu einem Gesetzentwurf der Landesregierung über die Einforderung rückständiger Gebühren und Auslagen bei der Zulassung von Fahrzeugen - Kfz-Zulassungsvoraussetzungsgesetz (LT-Drs. 5/287 vom 11.10.2006) wandte sich der Landesbeauftragte im November 2006 an die Vorsitzende des federführenden Ausschusses für Finanzen im Landtag im Hinblick auf die Behandlung im dortigen Ausschuss. Der zu diesem Zeitpunkt vorliegende Gesetzentwurf vom 11. Oktober 2006 war nicht mehr identisch mit dem Gesetzentwurf des Ministeriums für Landesentwicklung und Verkehr, zu dem der Landesbeauftragte seine Stellungnahme im April 2006 abgegeben hatte.

Der damalige Gesetzentwurf ging von einer Verweigerung der Zulassung von Fahrzeugen bei rückständigen Gebühren und Auslagen eines Fahrzeughalters im **eigenen** Zuständigkeitsbereich der Zulassungsbehörde aus und begegnete damit keinen datenschutzrechtlichen Bedenken, denn er diente der Umsetzung des § 6a Abs. 8 Straßenverkehrsgesetz (StVG).

Der normale Zulassungsvorgang in der Zulassungsbehörde als „Zug-um-Zug-Geschäft“ stellt nicht das Problem dar, denn nach geltendem Gebührenrecht kann die Zulassungsbehörde im gebührenpflichtigen Zulassungsverfahren die Zulassung eines Kraftfahrzeuges von der vorherigen Entrichtung der Verwaltungsgebühr abhängig machen. Das eigentliche Problem liegt bei den vom Fahrzeughalter verursachten nicht antragsgebundenen aber gebührenpflichtigen Amtshandlungen, bei der diese vorherige Entrichtung der Gebühr für eine Zwangsmaßnahme nicht gefordert werden kann. Dies betrifft insbesondere behördliche Zwangsmaßnahmen zur Außerbetriebsetzung von Kraftfahrzeugen, die Mängel aufweisen, die nicht haftpflichtversichert sind oder für die keine Kfz-Steuer entrichtet wurde.
Der Zulassungsbehörde sind diese aus ihrem eigenen Zuständigkeitsbereich bestehenden Rückstände aus durchgeführten gebührenpflichtigen Zwangsmaßnahmen gegen Fahrzeughalter bekannt, und der daraus abgeleitete eventuell notwendige Informationsgewinn über die tatsächliche Höhe der aufgelaufenen Gebührenschulden eines Fahrzeughalters aus dem Bereich des eigenen Kassenwesens stellt keine Zweckänderung bei der Nutzung dieser Informationen dar und war damit von § 10 Abs. 1 DSG-LSA gedeckt.

Im Verlauf des Gesetzgebungsverfahrens wurde der Landesbeauftragte allerdings vom Ministerium für Landesentwicklung und Verkehr nicht mehr beteiligt, obwohl § 40 der Gemeinsamen Geschäftsordnung der Ministerien - Allgemeiner Teil - dies so festlegt.

Die Kritik des Landesbeauftragten richtet sich gegen die im Gesetzentwurf der Landesregierung vorgenommene Änderung zu § 1 Abs. 1 durch das Hinzufügen der Sätze 2 und 3. Insbesondere die Gesetzesbegründung zu § 1 Abs. 1 des Gesetzentwurfes - zur Prüfung von Rückständen bei Zuzug aus einem anderen Zulassungsbezirk - begegnet erheblichen datenschutzrechtlichen Bedenken.
Diese Prüfung sollte der Begründung nach „nur“ erfolgen, „wenn die Behörde - auf welchem Weg auch immer - positiv Kenntnis über bestehende Rückstände erlangt hat“ (Zitat aus der Begründung). Diese Formulierung ist rechtstechnisch, vor allem aber allgemein rechtsstaatlich und insbesondere datenschutzrechtlich nicht akzeptabel.
Damit werden die Zulassungsbehörden per Gesetz aufgefordert, sich rechtswidrig Daten von anderen Zulassungsbehörden oder den Kassen der Landkreise zu beschaffen, um Rückstände „aufzuspüren“.

Das geltende Zulassungsverfahren ist bundesgesetzlich geregelt. Dieses Bundesrecht wird durch die Länder (Zulassungsbehörden) ausgeführt. Die bis zum 28. Februar 2007 geltende Fahrzeugregisterverordnung (FRV) regelte in den §§ 2 und 3 die Erhebung und Speicherung von Halter- und Fahrzeugdaten sowie in § 7 FRV die Übermittlung bestimmter Daten der Zulassungsbehörde an andere Zulassungsbehörden abschließend. Weder die Erhebung von Gebührenrückständen für das örtliche Fahrzeugregister noch deren Speicherung und schon gar nicht deren Übermittlung an andere Zulassungsbehörden ließen sich der FRV entnehmen.
Nach § 7 Abs. 1 FRV erfuhr die bisherige Zulassungsbehörde, bei der eventuell Gebühren- und Kostenrückstände des verzogenen Fahrzeughalters bestehen, erst nach der Erteilung eines neuen amtlichen Kennzeichens durch die andere, nunmehr zuständige Zulassungsbehörde von diesem Umstand, mehr aber auch nicht. Eine Rückfrage der anderen Zulassungsbehörde bei der bisherigen Zulassungsbehörde war in der FRV bisher nicht vorgesehen und wäre datenschutzrechtlich unzulässig. Der mit dem Kfz-Zulassungsvoraussetzungsgesetz des Landes beabsichtigte sofortige Abbau der bereits bestehenden ca. vier Millionen Euro Gebührenrückstände ließ sich so nicht erreichen.
Auch die seit dem 1. März 2007 geltende Verordnung über die Zulassung von Fahrzeugen zum Straßenverkehr - Fahrzeug-Zulassungsverordnung - FZV vom 25. April 2006 (BGBl. I S. 988), welche die alte FRV abgelöst hat, verändert die Gesetzeslage nicht. Die Übermittlungsregelungen der neuen Fahrzeug-Zulassungsverordnung in § 34 FZV wurden, was die zu übermittelnden Daten betrifft, unverändert aus § 7 FRV übernommen.
Der Bundesgesetzgeber hat zwar in § 6a Abs. 1 StVG die Erhebung von Kosten (Gebühren und Auslagen) geregelt, gerade aber für das Gebührenrecht in Bezug auf die Zulassung von Kraftfahrzeugen keine entsprechenden Regelungen für die Speicherung und Übermittlung in der FRV und auch nicht in der seit 1. März 2007 in Kraft getreten FZV getroffen.

Der Landesbeauftragte hat deshalb empfohlen, durch Streichung der Sätze 2 und 3 in § 1 Abs. 1 des Gesetzentwurfes darauf Einfluss zu nehmen, dass im weiteren Gesetzgebungsverfahren die gesetzliche Regelung im § 1 Abs. 1 Kfz-Zulassungsvoraussetzungsgesetz auf die Prüfung von Rückständen im eigenen Zuständigkeitsbereich der jeweiligen Zulassungsbehörde beschränkt bleibt. Denn nur so er-

gibt sich sowohl für die Zulassungsbehörde als auch für den Betroffenen eine normenklare und transparente Regelung.

Darüber hinaus hat der Landesbeauftragte angeregt, dass seitens des Ministeriums für Landesentwicklung und Verkehr überprüft werden sollte, ob nicht analog wie in § 3 Abs. 2 Nummer 21 FRV (Vermerk, dass den Vorschriften über die Kraftfahrzeugsteuer nicht genügt ist) die FRV in gleicher Weise um einen Vermerk, dass Gebührenrückstände in einer bestimmten Höhe bestehen, ergänzt werden könnte.
In der jetzt geltenden FZV sind diese Regelungen über Kfz-Steuerverstöße im Abschnitt 6 (Fahrzeugregister) für das zentrale Fahrzeugregister in § 30 Abs. 1 Nr. 21 Buchstabe f (Verstöße gegen die Vorschriften über die Kraftfahrzeugsteuer) und für das örtliche Fahrzeugregister in § 31 Abs. 1 Nr. 21 Buchstabe f (Verstöße gegen die Vorschriften über die Kraftfahrzeugsteuer) enthalten.
Analog könnte die jetzt geltende FZV in den besagten §§ 30 und 31 um ein Datum, z.B. unter Nr. 21 Buchstaben g (Höhe der Gebührenrückstände), in gleicher Weise ergänzt werden. Durch diese Aufnahme bereits bestehender Gebührenrückstände als neues Datum in die FZV wären damit auch bei länderübergreifenden Umzügen von Fahrzeughaltern deren bestehenden Gebührenrückstände ermittelbar, allerdings auf einer für die Zulassungsbehörde und für den Betroffenen normenklaren Rechtsgrundlage.

Die Schaffung einer Verknüpfung des Zulassungsrechts mit dem Gebührenrecht, analog wie es bereits zwischen dem Zulassungsrecht- und dem Kraftfahrzeugsteuerrecht erfolgt ist (vgl. Begründung in BT-Drs. 15/4921 vom 22. Februar 2005), ist mit § 6a Abs. 8 StVG nicht gelungen.
Die Zweckbestimmung der Fahrzeugregister ist im Hinblick auf das Kraftfahrzeugsteuerrecht in § 32 Abs. 1 Nr. 3 StVG (Nr. 3.: für Maßnahmen zur Durchführung des Kfz-Steuerrechts) normenklar geregelt. Eine Zweckbestimmung in den Fahrzeugregistern für „Maßnahmen des Gebührenrechts“ sucht man in § 32 StVG vergebens.

Der Landesbeauftragte hat seine kritische Wertung vom November 2006 auch nachrichtlich dem Ministerium für Landesentwicklung und Verkehr zugesandt. Eine Reaktion erfolgte aber bisher nicht.

25.2 Auskünfte aus dem Fahrzeugregister

Eine Bürgerin beschwerte sich beim Landesbeauftragten darüber, dass das Straßenverkehrsamt eines Landkreises einem Rechtsanwalt Auskunft über das Kraftfahrzeug erteilt habe, dessen Halterin sie sei.
Eine solche Halterauskunft, in aller Regel nach § 39 Abs. 1 StVG „zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße“, ist nichts ungewöhnliches. Die Dinge im Fall der Bürgerin lagen jedoch anders.

Der Rechtsanwalt des Gegners der Bürgerin in einem Streit um zivil- und familienrechtliche Ansprüche beabsichtigte, sich mit der begehrten Halterauskunft ein möglichst vollständiges Bild der Vermögenssituation der Petentin zu verschaffen; den Streitgrund hatte er im Auskunftsersuchen dem Straßenverkehrsamt auch mitgeteilt.
Bekanntermaßen ist es so, dass zur Erhebung und Verarbeitung personenbezogener Daten, zu der auch die Übermittlung zählt, dann eine Rechtsgrundlage erforderlich ist, wenn der Betroffene nicht eingewilligt hat. Diese Rechtsgrundlage ist im Fall der Übermittlung von Daten aus dem Fahrzeugregister zur Verfolgung von Rechtsansprüchen der bereits genannte § 39 StVG. Anhand dessen hätte das Straßenverkehrsamt zu prüfen gehabt, ob die Auskunft statthaft war. Wie bereits dargelegt, regelt § 39 Abs. 1 StVG, darüber hinaus auch Abs. 2, die Datenübermittlung im Fall von Ereignissen, die mit dem Straßenverkehr im ursächlichen oder wenigstens im weiteren Zusammenhang stehen, was hier nicht der Fall war. § 39 Abs. 3 StVG regelt hingegen Auskünfte in Fällen, die nicht mit dem Straßenverkehr im Zusammenhang stehen. Das kann die Geltendmachung, Sicherung oder Vollstreckung von öffentlich-rechtlichen Ansprüchen oder übergegangenen Ansprüchen nach dem Unterhaltsvorschussgesetz oder dem Zweiten oder Zwölften Buch Sozialgesetzbuch sein. All das traf im Fall der Petentin jedoch nicht zu. Das Straßenverkehrsamt hätte zwangsläufig zu dem Ergebnis kommen müssen, dass eine Auskunftserteilung zu unterbleiben hatte.

25.3 Luftsicherheitsgesetz

Nach den Textzeilen eines Liedes soll die Freiheit über den Wolken grenzenlos sein. Heute würde aber wohl niemand mehr solches behaupten. Ganz im Gegenteil wurde der Luftraum nach den Ereignissen des 11. September 2001 doch Stück für Stück zu einer gut überwachten und damit vermeintlich sicheren Zone.

Das Luftsicherheitsgesetz (LuftSiG) trat im Januar 2005 in Kraft (BGBl. I, S. 78). Zurück geht das Gesetz auf die Verordnung Nr. 2320/2002 des Europäischen Parlaments und des Rates vom Dezember 2002. Im November 2003 stand dann der Entwurf der Bundesregierung. Das LuftSiG geht in seinen Regelungen allerdings über die Verordnung Nr. 2320/2002 hinaus. Zulässig ist dies allemal. Nach Art. 6 der Verordnung steht es den Mitgliedstaaten frei, Maßnahmen anzuwenden, die unter Einhaltung des Gemeinschaftsrechts strenger sind als die Maßnahmen in der Verordnung selbst. Im Namen der Sicherheit hat die Bundesrepublik Deutschland davon Gebrauch gemacht. So sind bei Sicherheitsüberprüfungen nach § 7 LuftSiG die Wohnsitze der vergangenen zehn Jahre anzugeben und die Wiederholungsprüfungen erfolgen nach jeweils drei Jahren. Die Verordnung Nr. 2320/2002 sieht eine Überprüfung von Personen für mindestens die vergangenen fünf Jahre und Wiederholungsprüfungen nach spätestens fünf Jahren vor.

Zum Gesetzentwurf der Bundesregierung wird das Folgende als Zielsetzung des LuftSiG definiert: „Der vorliegende Entwurf enthält die für einen wirksamen Schutz des Luftverkehrs gegen Flugzeugentführungen, Sabotageakte und sonstige gefährliche Eingriffe erforderlichen Regelungen in einem eigenen Gesetz. ... Ferner wird der Einsatz der Streitkräfte in den Fällen, in denen die Polizeibehörden der Länder nicht über die personelle und technische Ausstattung zum Handeln verfü-

gen, ausdrücklich geregelt. Dies dient der Rechtssicherheit und der Rechtsklarheit."

Klar ist zwischenzeitlich, dass die sog. „Abschussbefugnis" für Flugzeuge, die eine ggf. terroristische Bedrohung darstellen, verfassungswidrig ist. Nach § 14 Abs. 3 LuftSiG ist die unmittelbare Einwirkung mit Waffengewalt nur zulässig, wenn nach den Umständen davon auszugehen ist, dass das Luftfahrzeug gegen das Leben von Menschen eingesetzt werden soll, und sie das einzige Mittel zur Abwehr dieser gegenwärtigen Gefahr ist. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 15. Februar 2006 die Verfassungswidrigkeit dieser Regelung festgestellt (1 BvR 357/05, NJW 2006, 751).

Zum Einen sieht das Gericht den Rahmen von Art. 35 Abs. 2 und 3 GG im Hinblick auf die Rechtsfolge aus der Regelung des LuftSiG überschritten. Art. 35 GG regelt das Maß der Unterstützung der Polizeien der Länder durch die Bundespolizei und die Streitkräfte bei Naturkatastrophen und schweren Unglücksfällen. Zum Anderen ist die Regelung des LuftSiG nicht mit Art. 2 Abs. 2 Satz 1 GG - Recht auf Leben - und Art. 1 Abs. 1 GG - Menschenwürde - vereinbar. Das Gericht hebt den besonderen Menschenwürdegehalt des Art. 2 Abs. 2 GG dadurch hervor, indem das Recht auf Leben als „vitale Basis der Menschenwürdegarantie" begriffen wird. Die betroffenen Passagiere und Besatzungsmitglieder werden „verdinglicht und zugleich entrechtlicht; indem über ihr Leben von Staats wegen einseitig verfügt wird, wird den als Opfern selbst schutzbedürftigen Flugzeuginsassen der Wert abgesprochen, der dem Menschen um seiner selbst willen zukommt."
Anders sieht es das Gericht für Fälle, in denen Luftfahrzeuge unbemannt oder ausschließlich mit Entführern besetzt sind. Entsprechend der Rechtfertigung des polizeilichen Todesschusses zur Rettung einer Geisel wird die Tötung von für die Gefahr Verantwortlichen als mit Art. 2 Abs. 2 und Art. 1 Abs. 1 GG vereinbar angesehen.

Alle sonstigen Regelungen des LuftSiG haben bisher Bestand. Das bedeutet aber nicht, dass nicht dagegen auch rechtliche Bedenken vorgetragen werden. So war der Presse wiederholt zu entnehmen, dass die Luftfahrer Bedenken gegen den § 7 des LuftSiG geäußert haben.

§ 7 LuftSiG regelt das Verfahren der Zuverlässigkeitsüberprüfungen von Personen, die nicht nur gelegentlich Zugang zu nicht allgemein zugänglichen Bereichen von Flughäfen haben, die bei Flugplatz- und Luftfahrtunternehmen beschäftigt sind, die Luftfahrzeuge führen und sogar die Mitglieder flugplatzansässiger Vereine oder Schülerpraktikanten sind. § 7 LuftSiG verlangt allen Beteiligten viel ab, nicht nur den Luftfahrern und sonstigen Beschäftigten, auch den zuständigen Luftsicherheitsbehörden. Der Paragraf hat elf Absätze und zieht sich über drei Seiten im Bundesgesetzblatt.

Im Januar 2005 traf der Erlass des LuftSiG die Luftsicherheitsbehörde des Landes Sachsen-Anhalt ziemlich unvorbereitet. Das lag aber nicht in erster Linie an der Behörde selbst. Dem Landesverwaltungsamt war zum Zeitpunkt des Inkrafttretens des LuftSiG die Zuständigkeit als Luftsicherheitsbehörde noch nicht einmal übertragen. Entsprechende Regelungen musste der Verordnungsgeber erst

schaffen. Zwischenzeitlich ist die Zuständigkeitsübertragung natürlich längst erfolgt, in den Anfangstagen bildete allerdings nur ein Erlass die Grundlage dafür, dass das Landesverwaltungsamt Zuverlässigkeitsüberprüfungen vornahm, die einen erheblichen Eingriff auch in das Recht auf informationelle Selbstbestimmung darstellen. Ohne formell einwandfreie Zuständigkeitsübertragung immerhin ein Zustand, der datenschutzrechtlich zumindest nicht zu begrüßen war.

Eine Zuverlässigkeitsüberprüfung erfolgt nach § 7 Abs. 2 LuftSiG nur auf Antrag des Betroffenen. Man könnte also meinen, dass es im Ermessen der Betroffenen steht, ob sie sich einer Überprüfung unterziehen. Dem ist natürlich bei der ganz überwiegenden Zahl der zu überprüfenden Personen nicht so. Wer seine Fluglizenz beruflich benötigt oder bei einem Flugplatz- bzw. Luftfahrtunternehmen beschäftigt ist, hat hier keine Wahl. Er muss sich, will er seinen Arbeitsplatz behalten, einer Zuverlässigkeitsüberprüfung unterziehen. Denn nach § 7 Abs. 6 LuftSiG darf dem Betroffenen ohne eine abgeschlossene Zuverlässigkeitsüberprüfung, bei der keine Zweifel an der Zuverlässigkeit des Betroffenen verbleiben, kein Zugang zu nicht allgemein zugänglichen Bereichen gewährt werden oder er darf seine Tätigkeiten nicht aufnehmen.

Bei der Antragstellung ist der Betroffene über die zuständige Luftsicherheitsbehörde, den Zweck der Datenerhebung, -verarbeitung und -nutzung, die Stellen, deren Beteiligung in Betracht kommt, und die Empfänger von Übermittlungen durch die Luftsicherheitsbehörde zu unterrichten.

Zur Überprüfung der Zuverlässigkeit darf die Luftsicherheitsbehörde nach § 7 Abs. 3 LuftSiG bei den Polizeivollzugs- und Verfassungsschutzbehörden der Länder sowie, soweit im Einzelfall erforderlich, dem Bundeskriminalamt, dem Zollkriminalamt, dem Bundesamt für Verfassungsschutz, dem Militärischen Abschirmdienst und der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der Deutschen Demokratischen Republik Anfragen stellen. Zudem darf die Luftsicherheitsbehörde unbeschränkte Auskünfte aus dem Bundeszentralregister und bei ausländischen Betroffenen auch aus dem Ausländerzentralregister einholen. Kommt die Luftsicherheitsbehörde nach Auswertung all dieser Unterlagen zu der Auffassung, dass Zweifel an der Zuverlässigkeit bestehen, gibt sie dem Betroffenen die Gelegenheit, sich zu den eingeholten Auskünften zu äußern. Nach Abschluss der Zuverlässigkeitsüberprüfung unterrichtet die Luftsicherheitsbehörde den Betroffenen, dessen gegenwärtigen Arbeitgeber, das Flugplatz-, Luftfahrt- oder Flugsicherungsunternehmen sowie die beteiligten Polizei- und Verfassungsschutzbehörden des Bundes und der Länder über das Ergebnis der Überprüfung. Eine Information des Arbeitgebers ist datenschutzrechtlich nicht zu beanstanden, wenn es sich um Personen handelt, die bei Flugplatz-, Luftfahrt- oder Flugsicherungsunternehmen beschäftigt sind. Bei „Hobbypiloten“ ist die Erforderlichkeit einer solchen Information für den Arbeitgeber nicht erkennbar. Die Anwendung der Vorschrift ist folglich mit Blick auf die Grundrechte Betroffener verfassungsgemäß zu begrenzen.

Werden den beteiligten Bundesbehörden bzw. den Flugplatzbetreibern und Luftfahrtunternehmen im Nachhinein zur Zuverlässigkeitsüberprüfung Informationen bekannt, die für die Beurteilung der Zuverlässigkeit von Bedeutung sind, sind die-

se Stellen verpflichtet, die Luftsicherheitsbehörde über die ihnen vorliegenden Erkenntnisse zu informieren.

Gelöscht werden die im Rahmen einer Zuverlässigkeitsüberprüfung gespeicherten personenbezogenen Daten bei der Luftsicherheitsbehörde innerhalb eines Jahres, wenn der Betroffene keine Tätigkeit aufnimmt, die eine Zuverlässigkeitsüberprüfung erfordert bzw. nach Ablauf von drei Jahren, nachdem der Betroffene aus einer entsprechenden Tätigkeit ausgeschieden ist, es sei denn, er hat zwischenzeitlich erneut eine entsprechende Tätigkeit aufgenommen.

Soweit die Theorie; zur Praxis hat sich der Landesbeauftragte Mitte 2005 an das Landesverwaltungsamt gewandt und um Auskunft darüber gebeten, welche personenbezogenen Daten wie erhoben, verarbeitet und genutzt werden und um Überlassung ggf. verwendeter Formblätter gebeten. Der daraufhin vorgelegte Bericht veranlasste den Landesbeauftragten, sich eingehender mit der Problematik auseinander zu setzen. Mit der geltenden Rechtslage war zu diesem Zeitpunkt in der Praxis auch nur schwerlich umzugehen. Nach § 17 Abs. 2 LuftSiG regelt das Bundesinnenministerium durch Rechtsverordnung die Einzelheiten der Zuverlässigkeitsüberprüfung nach § 7. Eine entsprechende Rechtsverordnung war noch nicht erlassen; Zuverlässigkeitsüberprüfungen mussten die Luftsicherheitsbehörden allerdings schon durchführen (siehe aber jetzt Verordnung vom 23. Mai 2007, BGBl. I S. 947).

Insbesondere bei Fragen des technisch-organisatorischen Datenschutzes und der Gestaltung der verwendeten Antragsformulare und Merkblätter bestand Handlungsbedarf. Aufgrund von entsprechenden Hinweisen durch den Landesbeauftragten konnten die Antragsformulare und Merkblätter in Zusammenarbeit mit dem Landesverwaltungsamt so überarbeitet werden, dass sie datenschutzrechtlichen Anforderungen gerecht werden. Vor allem auf eine umfassende Aufklärung der Betroffenen zum Umfang der Zuverlässigkeitsüberprüfung wurde Wert gelegt.

25.4 Mautdaten zur Terrorabwehr

Der letzte Beitrag in diesem VIII. Tätigkeitsbericht führt zu den Anfangsüberlegungen zum Verhältnis von Freiheit und Sicherheit zurück. Das Autobahnmautgesetz sieht eine Datenverarbeitung der Maut- und Kontrolldaten ausschließlich zu Abrechnungszwecken vor. Infolge von einigen einzelnen gravierenden Delikten fordert das Bundesministerium des Innern seit längerem eine Zweckdurchbrechung zugunsten der Verfolgung schwerer Straftaten, jedenfalls für den Zugriff auf bereits gespeicherte Daten. Der Bundesrat zog sogar eine Verbindung der Mautdatennutzung zur Terrorismusbekämpfung insgesamt (BR-Drs. 672/06 – Beschluss zum Gemeinsame-Dateien-Gesetz). Doch der Generalbundesanwalt wollte schon zuvor die Mautdatennutzung auch auf Verkehrsdelikte erstreckt sehen. Dann ist man nicht mehr weit weg von Bewegungsprofilen der Autobahnnutzer, und zwar über den gewerblichen Verkehr hinaus letztlich für jeden privaten Autofahrer, und damit vom „gläsernen Autofahrer“. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte dies schon in Entschließungen in den Jahren 1995 und 2001 kritisch kommentiert (siehe II. Tätigkeitsbericht, Anlage 17, und VI. Tätigkeitsbericht, Anlage 8). Der Landesbeauftragte nimmt die ak-

tuelle Diskussion auch vor dem Hintergrund befürwortender Äußerungen aus dem Ministerium des Innern zum Anlass, auch hier vor der Aufgabe rechtsstaatlicher Freiheitsprinzipien zu warnen. Das Mautdatensystem darf nicht zu einem weiteren Datenvorratsregister werden.

Anlage 1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. Juni 2005:

Einführung biometrischer Ausweisdokumente

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützter Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

- dass die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,
- dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,
- dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,
- dass vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,
- dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

Anlage 2

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005:

Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische **Informationsgesellschaft** unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden **Modernisierung des Datenschutzrechtes**. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der **Ausforschung ihrer Lebensgewohnheiten** und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.
Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen **Evaluierung durch unabhängige Stellen** unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der **Leistungs- und Finanzkontrolle** die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im **Gesundheitswesen**, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u.a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte **Arbeitnehmerdatenschutzgesetz** muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

Die **Datenschutzkontrolle** hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend.. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher **Datenschutz in der Europäischen Union** gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

Anlage 3

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005:

Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.

Anlage 4

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005:

Keine Vorratsdatenspeicherung in der Telekommunikation

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internet-Nutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z. B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dammbruch zulasten des Datenschutzes unverdächtiger Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner und –partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzelnen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z.B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden.
Mit einem Quick-freeze Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommunikation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen. Dieselben – unzutreffenden – Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

Anlage 5

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005:

Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber auf Grund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes – insbesondere die Angemessenheit der Datenerhebung – und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der – zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten – Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u.a. bei der Novellierung der §§ 100a und 100b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

Anlage 6

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005:

Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Datenerhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.
Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt, noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und -empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.
Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z.B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS beachtet werden.
Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisherigen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung“).
Es handelt sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für Datenschutz unterliegen. Dies haben die Bundesanstalt und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.
Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems A2LL wegen der offenbar nicht zu beseiti-

genden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

Anlage 7

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005:

Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privaten Callcentern durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

Anlage 8

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005:

Telefonieren mit Internettechnologie (Voice over IP - VoIP)

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internet-Technologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internettelefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

- angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,
- Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,

- Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,
- auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offenzulegen,
- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und
- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

Anlage 9

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. Dezember 2005:

Sicherheit bei eGovernment durch Nutzung des Standards OSCI

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.
Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheits-Standard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.
Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von sogenannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.
Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.
Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

Anlage 10

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006:

Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Auf europäischer Ebene wird verstärkt über die Ausweitung des grenzüberschreitenden Informationsaustauschs für Zwecke der Polizei und Justiz mit dem Ziel diskutiert, einen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen. Der Austausch personenbezogener Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten setzt ein hohes und gleichwertiges Datenschutzniveau bei allen beteiligten Stellen voraus.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die EU-Kommission einen Rahmenbeschluss zur Harmonisierung und zum Ausbau des Datenschutzes bei den Polizei- und Justizbehörden vorgelegt hat[*]. Sie betonen, dass die Regelungen in enger Anlehnung an die allgemeine Datenschutzrichtlinie (95/46/EG) erfolgen müssen, damit der Datenschutz in der EU auf einem einheitlich hohen Niveau gewährleistet wird.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen die Forderungen der Europäischen Datenschutzkonferenz in ihrem Beschluss vom 24. Januar 2006. Auch sie treten dafür ein, den Datenschutz im Zusammenarbeitsbereich der sog. „Dritten Säule“ der EU im Sinne der EU-Grundrechte-Charta zu gestalten.

Dies bedeutet u.a., dass Eingriffe in Freiheitsrechte nur im überwiegenden öffentlichen Interesse und im Rahmen der Verhältnismäßigkeit zulässig sind. Die Rahmenrichtlinie muss die Voraussetzungen der Datenverarbeitung und -übermittlung nach den jeweiligen Rollen der Verfahrensbeteiligten (Beschuldigte, Verdächtigte, Zeugen und Zeuginnen, Opfer) normenklar und differenziert regeln. Zudem müssen die Rechte der Betroffenen auf Auskunft, Berichtigung und Löschung gewährleistet werden. Die Datenverarbeitung muss umfassend durch unabhängige Datenschutzbehörden kontrolliert werden können. Die Datenschutzkontrollrechte müssen – unter Beachtung der richterlichen Unabhängigkeit – gewahrt werden. Sie dürfen nicht mit der Begründung eingeschränkt werden, dass ein laufendes Verfahren vorliege oder die Gefahrenabwehr bzw. die Strafverfolgung behindert werde. Einheitliche Datenschutzregelungen müssen zudem alle Formen der Datenverarbeitung – auch sofern sie in Akten erfolgt - einbeziehen.

Daten von europäischen Polizei- und Justizbehörden dürfen an Drittstaaten außerhalb der EU nur übermittelt werden, wenn ihre Verarbeitung im Zielland nach rechtsstaatlichen Grundsätzen erfolgt und ein angemessener Datenschutz sichergestellt ist. Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen muss ferner der Grundsatz der Zweckbindung beachtet werden. Abweichungen des ersuchenden Staates vom angegebenen Ver-

[*] KOM (2005) 475 vom 4. Oktober 2005

wendungszweck müssen auf Ausnahmefälle von besonderem Gewicht beschränkt bleiben. Die Ausnahmen müssen für den ersuchten Staat umfassend und zeitnah kontrollierbar sein.

Zur Schaffung eines hohen und einheitlichen Datenschutzstandards in der Dritten Säule der EU gibt es keine Alternative. Es darf nicht dazu kommen, dass auf europäischer Ebene weitere Eingriffsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass gleichzeitig die Freiheitsrechte der hier lebenden Bürgerinnen und Bürger gestärkt und geschützt werden. Aus diesem Grund hält es die Konferenz für dringend erforderlich, entsprechende Datenschutzbestimmungen zügig zu verabschieden und umzusetzen, bevor der Datenaustausch weiter ausgebaut wird.

Anlage 11

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006:

Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige

In den vergangenen Monaten sind die vom Sanktionsausschuss der Vereinten Nationen (VN) erstellten Listen über terrorverdächtige Personen und Organisationen, die von der Europäischen Gemeinschaft durch entsprechende Verordnungen umgesetzt worden sind, in den Blickpunkt der Öffentlichkeit gerückt. Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen.

Ein Eintrag in den genannten Listen greift in das informationelle Selbstbestimmungsrecht der betreffenden Personen ein und kann darüber hinaus gravierende existentielle Folgen haben, die z.B. die Verweigerung von Sozialleistungen umfassen können. Vielfach sind diese Personen nicht eindeutig bezeichnet. Auch in Deutschland lebende Personen sind von entsprechenden Maßnahmen betroffen. In jüngster Zeit gab es Verwechslungen mit schwer wiegenden Folgen für völlig unverdächtige Personen. Besonders kritisch ist zu werten, dass gegen die Aufnahme in die Listen kein Rechtsschutz besteht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Bundesregierung auf, bei den Vereinten Nationen und in der Europäischen Union auf die Einhaltung der rechtsstaatlich gebotenen Standards zu dringen. Dazu gehören insbesondere ein transparentes Listing-Verfahren, Entscheidungen auf einer gesicherten Tatsachenbasis, ein zweifelsfreier Identitätsnachweis und effektiver Rechtsschutz.

Anlage 12

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006:

Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über – durch das Fernmeldegeheimnis geschützte - Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses - erstmals zur Durchsetzung wirtschaftlicher Interessen - zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristi-

scher Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

Anlage 13

Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006:

Keine kontrollfreien Räume bei der Leistung von ALG II

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung“ vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

Anlage 14

Entschließung der Konferenz der Datenschutzbeauftragen des Bundes und der Länder vom 11. Oktober 2006
(bei Enthaltung von Schleswig-Holstein)

Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (BR-Drs. 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.
Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.
Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.
Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.
Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Einsatz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.
Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

Anlage 15

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006:

Das Gewicht der Freiheit beim Kampf gegen den Terrorismus

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der ”Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes” kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der ”Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes” ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

Anlage 16

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006:

Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz-BT-Drs. 16/2950) – verschärft durch Forderungen aus dem Bundesrat - sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem - in einigen Landesverfassungen ausdrücklich genannten - Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.

- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.

- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z.B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.

- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.

- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.

Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

Anlage 17

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006:

Keine Schülerstatistik ohne Datenschutz

Seit einigen Jahren arbeitet die Kultusministerkonferenz an der Einführung eines bundesweit einheitlichen Schulstatistiksystems, in dem weit über das bisherige Maß hinaus Daten aus dem Schulbereich personenbezogen verarbeitet werden sollen. Es soll auf Landesebene in einer Datei für jede Schülerin und jeden Schüler sowie für jede Lehrerin und jeden Lehrer für das gesamte "Schulleben" ein umfangreicher Datensatz angelegt werden. Hierzu erhält jede Person eine Identifikationsnummer, was auf ein pseudonymisiertes Register hinausläuft. Die Länderdateien sollen überdies zu einer bundesweiten Datenbank zusammengefasst werden. Die spätere Ergänzung des Schülerdatensatzes mit so genannten sozialökonomischen Daten über das Elternhaus sowie eine Einbeziehung der Kindergarten- und Hochschulzeit ist beabsichtigt. Eine präzise und einheitliche Zweckbestimmung lässt sich den bisherigen Äußerungen der Kultusministerkonferenz nicht entnehmen.

In datenschutzrechtlicher Hinsicht sind folgende Vorgaben zu beachten:
Wie das Bundesverfassungsgericht festgestellt hat, ist eine Totalerhebung nur zulässig, wenn der gleiche Erfolg nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Im Hinblick auf die bereits gewonnenen Ergebnisse aus stichprobenartigen und weitgehend auf Freiwilligkeit beruhenden wissenschaftlichen Untersuchungen (wie PISA, IGLU oder TIMSS) erscheint die Notwendigkeit der geplanten Einrichtung eines bundesweiten zentralen schüler- bzw. lehrerbezogenen "Bildungsregisters" nicht dargetan. Ein solches Register wäre ein nicht erforderlicher und damit unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht.

Deshalb fordern die Datenschutzbeauftragten von der Kultusministerkonferenz bei diesem Vorhaben nachdrücklich den Verzicht auf eine ID-Nummer. Jede Möglichkeit einer Reidentifizierung von Individualdatensätzen ist durch geeignete Verfahren auszuschließen (kein schüler- oder lehrerbeziehbares Bildungsregister!).

Im übrigen sind folgende verfassungsrechtliche Vorgaben und Grenzen unabdingbar:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.

- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit zu beachten.

- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass Schulministerien in mehreren Ländern das bisherige, datenschutzrechtlich bedenkliche Konzept nicht mehr weiter verfolgen, und strebt dies auch als Gesamtergebnis der mit der Kultusministerkonferenz zu führenden Gespräche und des angekündigten Workshops an.

Anlage 18

Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006:

Verbindliche Regelungen für den Einsatz von RFID-Technologien

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen - zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

- Transparenz
  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.

- Kennzeichnungspflicht
  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.

- Keine heimliche Profilbildung
  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

- Vermeidung der unbefugten Kenntnisnahme
  Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.

- Deaktivierung
  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Anlage 19

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007:

Keine heimliche Online-Durchsuchung privater Computer

Bisher ist nur die offene Durchsuchung privater Computer gesetzlich geregelt. Trotzdem wollen staatliche Behörden auch heimliche Online-Durchsuchungen durchführen. Bei einer Online-Durchsuchung dringen Sicherheitsbehörden mittels sog. „Trojaner“ heimlich in den Rechner ein und verschaffen sich Zugriff auf alle gespeicherten Daten.

Der Bundesgerichtshof hat in seinem Beschluss vom 31. Januar 2007 (StB 18/06) die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt, dass eine heimliche Online-Durchsuchung im Bereich der Strafverfolgung rechtswidrig ist. Weder die Bestimmungen zur Wohnungsdurchsuchung noch zur Telekommunikationsüberwachung können zur Rechtfertigung der heimlichen Durchsuchung und Ausforschung privater Computer herangezogen werden.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Einführung entsprechender Eingriffsgrundlagen sowohl im repressiven als auch im präventiven Bereich. Sie appellieren an die Gesetzgeber, es beim bisherigen Rechtszustand des „offenen Visiers“ zu belassen. Der Staat darf nicht jede neue technische Möglichkeit ungeachtet ihrer Eingriffstiefe zur Ausforschung einsetzen. Dies gilt auch dann, wenn wichtige Belange, wie z.B. die Strafverfolgung, betroffen sind. Hier ist ein Umdenken erforderlich. Es muss ein Raum der Privatsphäre bleiben, der nicht durch heimliche staatliche Überwachungsmaßnahmen ausgehöhlt werden darf.

Eine heimliche Online-Durchsuchung greift tief in die Privatsphäre ein. Die auf einem Computer gespeicherten Daten können aufgrund ihrer Vielzahl und besonderen Sensibilität Einblick in die Persönlichkeit der Betroffenen geben. Der Schutz des Kernbereichs privater Lebensgestaltung wird gefährdet, wenn der Staat heimlich und fortdauernd in private Computer eindringt, um dort personenbezogene Daten auszuspähen. Dies gilt umso mehr, wenn Nachrichtendienste die Möglichkeit heimlichen Zugriffs auf diese Informationen erhalten, obwohl ihnen nicht einmal die offene Erlangung durch eine Beschlagnahme gestattet ist.

Es ist Aufgabe des Staates dafür Sorge zu tragen, dass den Einzelnen die Möglichkeit zur Entfaltung ihrer Persönlichkeit bleibt. Diese Möglichkeit würde unvertretbar eingeschränkt, wenn Durchsuchungsmaßnahmen zugelassen würden, bei denen aufgrund ihrer Heimlichkeit keine Person wissen kann, ob, wann und in welchem Umfang sie von ihnen bereits betroffen ist oder in Zukunft betroffen sein wird. Der Gesetzgeber sollte deshalb davon absehen, derartige neue Eingriffsbefugnisse zu schaffen, nur weil sie ihm technisch möglich erscheinen und ihre Zweckmäßigkeit behauptet wird. Die technische Entwicklung allein kann nicht der Maßstab für die Rechtfertigung von Eingriffen sein.

Die Konferenz befürchtet massive Sicherheitseinbußen, weil zu erwarten ist, dass sich Computernutzer vor staatlicher Ausforschung zu schützen versuchen, indem sie etwa Soft-

waredownloads unterlassen. Somit werden aber auch die sicherheitstechnisch wichtigen Software-Updates verhindert und Computer anfälliger gegen Angriffe Krimineller. Die Einführung von Befugnissen zur Online-Durchsuchung würde das Ansehen des Rechtsstaats und das Vertrauen in die Sicherheit von Informationstechnik, insbesondere von E-Government und E-Commerce, massiv beschädigen. Schließlich würden die hohen Aufwendungen für IT-Sicherheit in Staat und Wirtschaft konterkariert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert deshalb an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung derartiger Befugnisnormen zu verzichten.

Anlage 20

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007:

Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen

Die gesetzlichen Regelungen der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sollen nach der Ankündigung der Bundesregierung unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts einer umfassenden Neuregelung unterzogen werden. Die Bundesregierung will in diesem Zusammenhang auch die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten umsetzen. Das Bundesministerium der Justiz hat zwischenzeitlich einen Referentenentwurf vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont erneut, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widersprechen würde. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz fordert die Bundesregierung auf, die Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung zumindest solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Die geplante Ausweitung der Vorratsdatenspeicherung geht weit über die europarechtliche Umsetzungsverpflichtung hinaus und wäre ein zusätzlicher unverhältnismäßiger Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger. So sollen die Daten auch zur Verfolgung von Straftaten von erheblicher Bedeutung sowie mittels Telekommunikation begangener Straftaten genutzt werden. Zudem soll die Möglichkeit zur anonymen E-Mail-Kommunikation abgeschafft und die Nutzenden öffentlich zugänglicher E-Mail-Dienste sollen zur Angabe ihres Namens und ihrer Adresse verpflichtet werden. Diese Angaben sollen außerdem einer Vielzahl von Behörden zum Online-Abruf zur Verfügung gestellt werden, darunter der Polizei, den Staatsanwaltschaften, den Nachrichtendiensten, dem Zoll und der Bundesanstalt für Finanzdienstleistungsaufsicht. Auch dies begegnet erheblichen datenschutzrechtlichen Bedenken.

Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtsstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

- Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen

Reduzierung kritisch überprüft werden. Es sollten nur Straftaten aufgenommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z.B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.

- Die vorgesehene Kernbereichsregelung ist ungenügend. Sie nimmt in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst werden. Für solche Informationen muss stattdessen grundsätzlich ein Erhebungsverbot gelten. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt werden, müssen zudem einem absoluten Verwertungsverbot unterliegen, nicht nur für Strafverfahren.

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht nur in den Bereichen der Wohnraum- und Telekommunikationsüberwachung zu gewährleisten. Auch für alle anderen verdeckten Ermittlungsmaßnahmen ist eine Regelung zum Schutz des Kernbereichs zu treffen.

- Für die Kommunikation mit Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern sollte ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und Berufshelfer gelten. Die im Entwurf enthaltene Differenzierung zwischen bestimmten Gruppen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern ist sachlich nicht gerechtfertigt.

- Für Angehörige i.S.v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i.S.v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

- Für die sog. Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.

- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

Anlage 21

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007:

Pläne für eine öffentlich zugängliche Sexualstraftäterdatei verfassungswidrig

In der aktuellen Diskussion um einen verbesserten Schutz von Kindern vor Sexualstraftätern wird u.a. die Einrichtung einer öffentlich zugänglichen Sexualstraftäterdatei mit Wohnsitzangaben gefordert. Es wird vorgeschlagen, die Namen und Adressen von verurteilten Sexualstraftätern z.B. über das Internet zu veröffentlichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont, dass an Kindern begangene Sexualstraftaten mit allen zur Verfügung stehenden rechtsstaatlichen Mitteln bekämpft werden müssen. Dies schließt jedoch die Anwendung eindeutig rechtsstaatswidriger Mittel aus. Um ein solches verfassungswidriges Mittel würde es sich aber bei einer solchen Datei handeln. Dadurch würden die Betroffenen an eine Art elektronischen Pranger gestellt. Sie würden durch die öffentliche Bloßstellung sozial geächtet. Tätern würde die Möglichkeit der Resozialisierung genommen, die ihnen nach unserer Rechtsordnung zusteht.

Der Vorschlag ist lediglich dazu geeignet, Misstrauen und Selbstjustiz zu fördern. Die Betroffenen könnten damit eher zu einem erhöhten Gefahrenpotenzial werden. Er sollte deshalb nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder nicht weiter verfolgt werden.

Anlage 22

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007:

Elektronischer Einkommensnachweis muss in der Verfügungsmacht der Betroffenen bleiben

Mit dem Verfahren ELENA (elektronische Einkommensnachweise) sollen die Einkommensdaten sämtlicher abhängig Beschäftigter in einem bundesweiten Register gespeichert werden. Dieses Verfahren ist angesichts der Sensibilität und des Umfangs der dabei erfassten personenbezogenen Daten von erheblicher datenschutzrechtlicher Brisanz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass ein derartiges Register nur dann eingerichtet werden darf, wenn die verfassungsrechtlichen Voraussetzungen erfüllt und die gesetzlichen und technisch-organisatorischen Vorkehrungen zum Schutz der dort gespeicherten Daten getroffen werden.

Zu den wesentlichen verfassungsrechtlichen Voraussetzungen für die Einrichtung des Registers gehören der Nachweis der Erforderlichkeit und die Verhältnismäßigkeit. Angesichts bestehender Zweifel daran, dass diese Voraussetzungen gegeben sind, muss belastbar dargelegt werden, dass die Daten für die jeweiligen Zwecke tatsächlich benötigt werden und dass der angestrebte Zweck nicht mit einem geringeren Eingriff in das Recht auf informationelle Selbstbestimmung erreicht werden kann.

Im Hinblick auf den vom Bundesministerium für Wirtschaft und Technologie erarbeiteten Referentenentwurf sieht die Konferenz darüber hinaus in den folgenden Punkten Klärungsbedarf:

- Es muss gesetzlich festgelegt werden, dass die Daten aus der Datenbank nur mit Mitwirkung der Teilnehmerinnen und Teilnehmer des Verfahrens zu entschlüsseln sind.
- Das Verfahren muss so ausgestaltet werden, dass die Ver- und Entschlüsselung der Daten ohne Vorliegen der Signaturkarte des Betroffenen nur in klar definierten Ausnahmefällen durch eine unabhängige Treuhänderstelle möglich ist.
- Sämtliche im Rahmen des Verfahrens verarbeiteten Daten müssen einem gesetzlichen Beschlagnahmeschutz unterworfen sein.
- Die technischen Komponenten müssen auf der Basis einer unabhängigen Prüfung zertifiziert werden.

Anlage 23

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007:

GUTE ARBEIT in Europa nur mit gutem Datenschutz

Die Ministerinnen und Minister für Beschäftigung und Soziales in Europa haben am 19. Januar 2007 neun Schlussfolgerungen für GUTE ARBEIT aufgestellt: GUTE ARBEIT bedeute Arbeitnehmerrechte und Teilhabe, faire Löhne, Sicherheit und Gesundheitsschutz bei der Arbeit sowie eine familienfreundliche Arbeitsorganisation. Gute und faire Arbeitsbedingungen sowie angemessener sozialer Schutz seien unabdingbar für die Akzeptanz der Europäischen Union bei den Bürgerinnen und Bürgern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt diese Initiative zum Anlass und fordert dazu auf, auch den Beschäftigtendatenschutz zu stärken. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.
Deshalb fordert die Konferenz seit langem ein Arbeitnehmerdatenschutzgesetz. Bereits 2003 hat sie darauf hingewiesen, dass Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht sind, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.

Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.

Anlage 24

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2007:

Anonyme Nutzung des Fernsehens erhalten!

Seit einiger Zeit werden in der Öffentlichkeit Pläne der großen privaten Fernsehveranstalter diskutiert, gemeinsam mit den Betreibern von Übertragungskapazitäten (Satellit, Kabel und DVB-T) ihre Programme nur noch verschlüsselt zu übertragen. Dabei werden vorrangig solche Geschäftsmodelle favorisiert, bei denen die kostenpflichtige Entschlüsselung des Signals nur mit personenbezogenen Smartcards möglich sein soll.

Die Datenschutzbeauftragten des Bundes und der Länder betrachten diese Entwicklung mit Sorge. Nachdem vor allem durch zahlreiche staatliche Eingriffe die verfassungsrechtlich gebotene unbeobachtete Nutzung von Telekommunikation und Internet kaum noch möglich ist, steht nun auch der seit jeher selbstverständliche anonyme und nicht registrierte Empfang von Rundfunkprogrammen auf dem Spiel. Gerade durch die Vermarktung individuell zugeschnittener Programmpakete im digitalen Rundfunk kann bei personenbezogener Abrechnung nachvollzogen werden, wer welche Angebote nutzt. Die entstehenden technischen Infrastrukturen werden zudem auch Möglichkeiten bieten, die konkrete Nutzung einzelner Sendungen zu registrieren. Damit wird die allgegenwärtige Bildung von Persönlichkeitsprofilen um detaillierte Kenntnisse über den Rundfunkkonsum ergänzt.

Die bisher bekannt gewordenen Pläne der Unternehmen widersprechen dem im Rundfunkstaatsvertrag geregelten Gebot, die Inanspruchnahme von Rundfunk und deren Abrechnung anonym zu ermöglichen und verstoßen gegen das Prinzip der Datenvermeidung. Dies wäre nicht akzeptabel, zumal datenschutzfreundliche Varianten der Abrechnung – beispielsweise durch den Einsatz von vorbezahlten Karten – ohne wirtschaftliche Einbußen zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb die Länder auf, die Einhaltung der datenschutzrechtlichen Anforderungen des Rundfunkstaatsvertrages gegenüber den Veranstaltern durchzusetzen, und eine anonyme Nutzung von Rundfunkprogrammen auch in Zukunft sicherzustellen.

Angesichts der immer umfassenderen Individualisierung und Registrierbarkeit des Mediennutzungsverhaltens erinnert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an ihre Forderung, das grundgesetzlich geschützte Fernmeldegeheimnis zu einem allgemeinen Mediennutzungsgeheimnis weiterzuentwickeln.

Anlage 25

Beschluss der obersten Aufsichtsbehörden für den
Datenschutz im nicht öffentlichen Bereich
am 8./9. November 2006 in Bremen

Empfehlung der obersten Aufsichtsbehörden für den Datenschutz
im nicht-öffentlichen Bereich:

Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten!

Die gegenwärtige Entwicklung der RFID-Technologie (Radio Frequency Identification) und ihr Einsatz im Handel und im Dienstleistungssektor kann Kosteneinsparungspotenziale beispielsweise im Rahmen von Logistik- und Produktionsprozessen eröffnen. Sie birgt allerdings auch erhebliche Risiken für das Persönlichkeitsrecht von Verbraucherinnen und Verbrauchern. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es deswegen für erforderlich, dass die RFID-Technologie datenschutzkonform entwickelt und eingesetzt wird. Bereits jetzt sollten Hersteller und Anwender im Handel und im Dienstleistungssektor die Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie nutzen.

RFID ist eine Technik, um Daten mit Hilfe von Funkwellen auf einem Chip berührungslos und ohne Sichtkontakt lesen, speichern und gegebenenfalls verarbeiten zu können. Mit RFID-Chips gekennzeichnete Gegenstände können mit einem Lesegerät abhängig von der Reichweite bzw. Sendestärke identifiziert und lokalisiert werden. Ungeachtet der zahlreichen Vorteile des Einsatzes von RFID-Chips ist zu befürchten, dass zukünftig massenhaft personenbezogene Daten verarbeitet werden, indem nahezu alle Gegenstände des täglichen Lebens (einschließlich Kleidung, Lebensmittel- und andere Verpackungen, Medikamente usw.) über Hintergrundsysteme dauerhaft den Betroffenen zugeordnet werden können. RFID ermöglicht damit technisch die von den Verbraucherinnen und Verbrauchern unbemerkte Ausforschung ihrer Lebensgewohnheiten und ihres Konsumverhaltens etwa zu kommerziellen Zwecken.

Diese technologische Entwicklung stellt den Datenschutz vor neue Herausforderungen. Ob auf RFID-Chips gespeicherte Daten einen Personenbezug aufweisen, wird häufig von den konkreten Umständen des Einzelfalls abhängen. Selbst Informationen, die zunächst keinen Personenbezug haben, weil sie allein ein Produkt kennzeichnen, könnten über die Lebensdauer des Chips gesehen - zum Beispiel mit Hilfe von Hintergrundsystemen - später einer konkreten Person zugeordnet werden. Damit würden rückwirkend alle gespeicherten Daten über einen mit einem RFID-Chip gekennzeichneten Gegenstand zu personenbezogenen Daten. Ein datenschutzkonformer Einsatz der RFID-Technologie wird deshalb immer schwerer kontrollierbar sein. Die Ausübung der verfassungsrechtlich begründeten, datenschutzrechtlich unabdingbaren Rechte der Verbraucherinnen und Verbraucher auf Auskunft sowie auf Löschung und Berichtigung von unrichtigen personenbezogenen Daten wird - insbesondere wegen der geringen Größe der RFID-Chips - künftig erheblich erschwert.

Angesichts dieses Gefährdungspotenzials der RFID-Technologie erscheint es fraglich, ob die bestehenden gesetzlichen Regelungen ausreichen, den wirksamen Schutz der Persönlichkeitsrechte der Betroffenen zu gewährleisten.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es für erforderlich, dass bereits bei der technologischen Ausgestaltung von RFID das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt wird. Dazu gehört vor allem, dass Verbraucherinnen und Verbrauchern nach dem Kauf von Produkten die RFID-Chips auf einfache Weise unbrauchbar machen können. Daneben sind auch die Datenschutzrechte der betroffenen Arbeitnehmerinnen und Arbeitnehmer im Produktions- und Logistikprozess zu wahren. Zugleich sind unter anderem der Handel und der Dienstleistungssektor und insbesondere die entsprechenden Verbände aufgerufen, umfassende, verbindliche und nachprüfbare Selbstverpflichtungen für eine datenschutzfreundliche Ausgestaltung der RFID-Technologie abzugeben.

Für den Schutz der Persönlichkeitsrechte der betroffenen Verbraucherinnen und Verbraucher sind dabei folgende Regeln unabdingbar:

Transparenz / Benachrichtigungspflicht
Die Verbraucherinnen und Verbraucher müssen wegen des möglichen Personenbezugs der auf RFID-Chips gespeicherten Daten umfassend über den Einsatz, Verarbeitungs- und Verwendungszweck und Inhalt von RFID-Chips informiert werden. Werden durch ihren Einsatz personenbezogene Daten gespeichert, sind die Betroffenen hiervon zu benachrichtigen.

Kennzeichnungspflicht
Nicht nur die eingesetzten RFID-Chips selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips, Lesegeräte bzw. dazugehörige Hintergrundsysteme ausgelöst werden, müssen für die Verbraucherinnen und Verbraucher transparent und leicht zu erkennen sein. Eine heimliche Anwendung „hinter dem Rücken“ der Betroffenen darf es nicht geben.

Deaktivierung
Den betroffenen Verbrauchern muss ab dem Kauf von mit RFID-Chips versehenen Produkten die Möglichkeit eröffnet werden, die RFID-Chips jederzeit dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die ursprünglichen Speicherzwecke nicht mehr erforderlich sind. Dieses Recht darf nicht durch Gewährleistungsbeschränkungen in Allgemeinen Geschäftsbedingungen beeinträchtigt werden.

Datensicherheit
Die Vertraulichkeit der gespeicherten und der übertragenen Daten ist durch Sicherstellen der Authentizität der beteiligten Geräte (Peripherie) und durch Verschlüsselung zu gewährleisten. Das unbefugte Auslesen der gespeicherten Daten muss wirksam verhindert werden.

Keine heimliche Profilbildung
Daten von RFID-Chips aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Einwilligung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist,

muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Chips verzichtet werden.

Oberste Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich, 8./9. 11. 2006

Anlage 26

Beschluss der obersten Aufsichtsbehörden für den
Datenschutz im nicht öffentlichen Bereich
am 8./9. November 2006 in Bremen

SWIFT: Datenübermittlung im SWIFT-Verfahren in die USA

Es wird festgestellt, dass die gegenwärtige Spiegelung von Datensätzen im SWIFT-Rechenzentrum in den USA und die anschließende Herausgabe von dort gespeicherten Daten an US-amerikanische Behörden wegen fehlender Rechtsgrundlage sowohl nach deutschem Recht als auch nach EG-Datenschutzrecht unzulässig ist. Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau im Sinne des Artikel 25 Abs. 1 und Abs. 2 der EG-Datenschutzrichtlinie. Rechtlich verantwortlich für die Übermittlung der Daten in die USA sind sowohl die in Belgien ansässige SWIFT, als auch die deutschen Banken, die sich trotz des Zugriffs der amerikanischen Behörden auf die bei SWIFT/USA gespeicherten Datensätze auch weiterhin der Dienstleistungen von SWIFT bedienen.

Die Banken werden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist. Eine Möglichkeit besteht nach Ansicht der Aufsichtsbehörden in der Verlagerung des zur Zeit in den USA gelegenen Servers in einen Staat mit einem angemessenen Datenschutzniveau. Eine weitere Möglichkeit besteht in einer wirksamen Verschlüsselung der in die USA übermittelten Zahlungsverkehrsinformationen. Es muss ausgeschlossen sein, dass die US-amerikanischen Behörden in die Lage versetzt sind, die auf dem dortigen Server gespeicherten Datensätze zu dechiffrieren. Die Aufsichtsbehörden erwarten eine ernsthafte Auseinandersetzung der Banken mit den aufgezeigten Möglichkeiten. Allgemeine Hinweise auf eine faktische oder ökonomische Unmöglichkeit sind nicht akzeptabel. Der Verweis auf einen in der Zukunft liegenden und noch keinesfalls feststehenden Abschluss eines völkerrechtlichen Abkommens zwischen dem EU-Rat und der US-Regierung vermag nicht den gegenwärtigen Handlungsbedarf zu beseitigen.

Unabhängig davon müssen die Banken gemäß § 4 Abs. 3 Bundesdatenschutzgesetz ihre Kundinnen und Kunden darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze auch an ein in den USA ansässiges SWIFT Operating Center übermittelt werden. Dabei bleibt es den Banken überlassen, ob sie alle Kundinnen und Kunden über die Übermittlung der Datensätze an SWIFT/USA informieren oder nur diejenigen, für die die Dienste von SWIFT genutzt werden. Die Unterrichtung der Kundinnen und Kunden ist eine notwendige, wenn auch nicht hinreichende Mindestvoraussetzung für die Zulässigkeit der Übermittlung der Daten an SWIFT/USA. Sie ist unverzüglich umzusetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich nehmen das Anliegen der deutschen Banken zur Kenntnis, aus Gründen des Wettbewerbs eine europaweit einheitliche Lösung zu erreichen. Es soll in Zusammenarbeit mit den übrigen europäischen Datenschutz-Aufsichtsbehörden eine einheitliche Handhabung angestrebt werden.

Oberste Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich, 8./9. 11. 2006

Anlage 27

Der Bundesbeauftragte
für den Datenschutz
und die Informationsfreiheit

Bonn, den 18. Dezember 2006

Zehn Thesen für eine datenschutzfreundliche Informationstechnik

Informationstechnologien beeinflussen immer weitere Bereiche der Wirtschaft, der Verwaltung und des privaten Lebens. Deshalb ist es unverzichtbar, die Bedingungen und die Folgen ihres Einsatzes zu diskutieren. Dabei müssen sowohl Chancen als auch Risiken ausgelotet und entsprechende Schlussfolgerungen gezogen werden. Alle Beteiligten müssen dabei ihrer Verantwortung gerecht werden: Politische Entscheidungsträger, Wissenschaft und Wirtschaft. Im Mittelpunkt muss bei allen Fragen der Mensch stehen, als Bürger, Kunde und als Betroffener. Sein Recht auf Selbstbestimmung muss in einer immer stärker durch Informationstechnik geprägten Umwelt gewahrt und gestärkt werden.

1. Informationstechnik transparent gestalten

Die Entwickler und Anwender von Informationssystemen müssen dafür sorgen, dass ihre Auswirkungen für den Einzelnen und für die Gesellschaft nachvollziehbar sind. Nur wenn die Betroffenen wissen, welche Konsequenzen neue technische Hilfsmittel haben, können sie souverän damit umgehen. Transparenz schafft zugleich Vertrauen in neue IT-Vorhaben und Technologien. Umfassende Aufklärung, Beratung und Information tragen dazu bei, dass datenschutzfreundliche Technologien sich auf dem Markt durchsetzen können. Das gesetzlich bereits seit langem vorgeschriebene Auskunftsrecht des Betroffenen über die gespeicherten personenbezogenen Daten sollte weiterentwickelt werden und generell auch die Herkunft der Daten umfassen und auch dann greifen, wenn die Daten nur temporär zusammengeführt und zur individuellen Bewertung verwendet werden (Scoring). Soweit IT-Systeme mit dem Zweck der späteren Personalisierung betrieben werden (etwa bei RFID-Chips im Handel), sollten die Betroffenen frühzeitig auf ihre Verwendung hingewiesen werden. Ferner sollten technische Systeme so konzipiert werden, dass sie den Nutzern signalisieren, wenn sie aktiviert werden, damit eine heimliche Datenerhebung vermieden wird. Die Anbieter von elektronischen Produkten und Dienstleistungen müssen die Nutzer darüber informieren, wie sie durch ihr Verhalten Datenschutzgefahren vermeiden können und welche Restrisiken jeweils bestehen. Schließlich sollten die für die Verarbeitung verantwortlichen Stellen dazu verpflichtet werden, die Betroffenen über Datenschutzverstöße zu informieren, wie dies bereits in den meisten US-Bundesstaaten vorgeschrieben ist.

2. Entscheidungsfreiheit des Betroffenen stärken

IT-gestützte Verfahren müssen so ausgestaltet werden, dass sie den Nutzerinnen und Nutzern umfassende Wahlrechte hinsichtlich des Umgangs mit ihren Daten bieten. Gegebenenfalls sollte die Möglichkeit erhalten bleiben, private und öffentliche Dienstleistungen auch ohne Nutzung elektronischer Systeme in Anspruch zu nehmen. Die Erhebung von Daten sollte so weit wie möglich an die informierte Einwilligung der Betroffenen gebunden werden. Der Zugriff auf sensible Daten (etwa medizinische Angaben) sollte grundsätzlich nur mit Zu-

stimmung der Betroffenen möglich sein. Echte Freiwilligkeit ist nur dann gegeben, wenn es wirkliche Alternativen gibt. So sollten z.B. bei kommerziellen Diensten verschiedene Bezahlmöglichkeiten angeboten werden, etwa auch datenschutzfreundliche Prepaid- Lösungen. Im Handel verwendete RFID-Chips müssen vom Nutzer deaktivierbar sein, ohne die Funktionalität des Produkts zu beeinträchtigen. Die Betroffenen müssen darüber informiert werden, welche Konsequenzen sich aus ihren Entscheidungen ergeben. Schließlich muss der Einzelne grundsätzlich die Möglichkeit haben, seine Entscheidung nachträglich zu korrigieren und Einwilligungen zu widerrufen.

3. Datenschutzanforderungen frühzeitig berücksichtigen

Datenschutz sollte bereits in das System-Design der IT eingebunden werden. Nachträglich aufgepfropfter Datenschutz ist oftmals schlechter und teurer. Deshalb sollte es eine Selbstverständlichkeit sein, dass Konzepte von IT-Verfahren und Geräten möglichen Gefährdungen des Datenschutzes Rechnung tragen. Je sensibler der Anwendungsbereich und die Daten, desto höher sind auch die Anforderungen an Schutzvorkehrungen gegen einen Missbrauch. Die Gewährleistung dieser Anforderungen darf nicht allein dem Anwender überlassen bleiben, sondern sie muss auch durch die Hersteller ermöglicht werden. Nur wenn das Produkt bzw. IT-Verfahren einen datenschutzkonformen Betrieb ermöglicht (etwa durch Zugriffsschutz-, Protokollierungs- und Verschlüsselungsfunktionen), können es die Anwender datenschutzgerecht verwenden.

4. Datenvermeidung und Datensparsamkeit

Datenvermeidung und Datensparsamkeit sind Grundprinzipien eines zeitgemäßen Datenschutzes. Verfahren müssen so ausgestaltet werden, dass möglichst wenig personenbezogene Daten erfasst werden. Dieser Grundsatz muss bereits bei der Gestaltung der Technik und ihrer Einsatzbedingungen berücksichtigt werden. Dies gilt vor allem für Prozess- und Verkehrsdaten, die beim Betrieb von IT-Systemen beiläufig anfallen und denen beim Übergang zum Ubiquitous Computing zunehmende Bedeutung zukommt. Diese Daten sollten auf ein Mindestmaß beschränkt und so früh wie möglich gelöscht werden. Elektronische Dienste sollten so gestaltet werden, dass auch hierbei so wenig wie möglich personenbezogene Daten verarbeitet werden. Hierzu können anonyme Nutzungsmöglichkeiten einen wichtigen Beitrag leisten. Soweit eine Individualisierung von Dienstleistungen, Statistiken und wissenschaftlichen Forschungsvorhaben erforderlich ist, sollten soweit wie möglich Pseudonyme verwendet werden. Die in § 3a des Bundesdatenschutzgesetzes enthaltenen Vorgaben Datensparsamkeit müssen mit Leben gefüllt werden.

5. Nachprüfbarer Datenschutz

Sowohl Anwender als auch Betroffene müssen prüfen können, ob ein Produkt, eine Dienstleistung oder ein Verfahren datenschutzgerecht ist. Um datenschutzkonforme Lösungen zu erhalten, muss die mit der Umsetzung vertraute Institution den Rahmen vorgeben und nicht der Technik "hinterherlaufen". Schutzprofile, in denen die Anforderungen des Datenschutzes technikspezifisch konkretisiert werden, können den Grundstein für datenschutzgerechte Lösungen bieten. Soweit Schutzprofile auf einer internationalen Norm basieren, können sie die Gültigkeit der Anforderungen über Grenzen hinweg sicherstellen und einen Wettbewerbsvorteil auf dem internationalen Markt bringen. Datenschutzfreundliche Verfahren können durch Auditverfahren zertifiziert werden. Um die Qualität der Auditierung zu gewährleisten, sollten

die qualitativen Anforderungen und das Verfahren zur Vergabe von Datenschutzgütesiegeln wie im Bundesdatenschutzgesetz vorgesehen - gesetzlich vorgegeben werden. Datenschutzgütesiegel können es den Verbrauchern erleichtern, aus der Vielzahl der Angebote solche auszusuchen, bei denen sie sicher sein können, dass mit ihren Daten sorgfältig umgegangen wird.

6. Voreingestellte Sicherheit

Viele Sicherheits- und Datenschutzprobleme bei IT-Produkten sind auf unsichere Grundeinstellungen der Systeme zurückzuführen. So werden Netzwerke häufig ohne Verschlüsselungsfunktion ausgeliefert und dem Normalanwender ist es nur unter Schwierigkeiten oder überhaupt nicht möglich, einen sicheren Betrieb zu gewährleisten. Damit wird dem Datenmissbrach durch Hacking, Abhörmaßnahmen und Datenmanipulation Vorschub geleistet. Die Hersteller und die für den Betrieb der Systeme verantwortlichen Unternehmen, Forschungseinrichtungen und Hochschulen müssen für sichere Grundeinstellungen sorgen. Verständliche Benutzungshinweise und einfach zu bedienende Hard- und Software müssen es den Anwendern ermöglichen, bei den Produkten eine angemessene Datenschutzstufe einzustellen. Beim professionellen Einsatz von IT muss Datenschutzrisiken durch geeignete Sicherheitskonzepte begegnet werden, bei denen der jeweilige Schutzbedarf der Daten berücksichtigt wird. Es muss gewährleistet sein, dass insbesondere sensible Daten stets angemessen geschützt werden.

7. Vertraulichkeit der Kommunikation stärken

Das Vertrauen in den Schutz der Privatsphäre und die Vertraulichkeit von Kommunikationsvorgängen ist eine wichtige Grundlage für den Erfolg elektronischer Dienste. Das traditionelle Fernmeldegeheimnis schützt lediglich die Nachrichtenübermittlung mittels Telekommunikationseinrichtungen. Im Zeitalter des Internet, in denen neben die Individualkommunikation vielfältige andere Formen der elektronischen Kommunikation treten, muss das Fernmeldegeheimnis zu einem umfassenden Mediennutzungsgeheimnis ausgebaut werden. Nur wenn der einzelne sicher sein kann, dass sein individuelles Nutzungsverhalten weder durch private noch durch öffentliche Stellen überwacht wird, wird er sich im virtuellen Raum frei bewegen. Neben politischen Entscheidungen und rechtlichen Regelungen zur Weiterentwicklung des Kommunikationsgeheimnisses müssen sichere Konzepte und Produkte der Kommunikationstechnik dazu beitragen, dass die Vertraulichkeit gewahrt wird. Hierzu gehören auch Möglichkeiten zur verschlüsselten Datenübertragung und zur anonymen bzw. pseudonymen Nutzung elektronischer Dienste.

8. Datenschutz-Werkzeuge

In einer zunehmend technisch geprägten Umwelt lässt sich die Komplexität von IT-Systemen und elektronischen Dienstleistungen für den Einzelnen immer schwerer beherrschen. Deshalb sollten den Nutzern einfach zu bedienende Instrumente an die Hand gegeben werden, mit denen sie ihre Daten wirksam schützen und den Umgang mit ihnen kontrollieren können. Derartige Werkzeuge - etwa zur Verwendung von Pseudonymen, zur Erzeugung von sicheren Passworten, zum Auslesen des Inhalts von persönlichen Datenspeichern und zur automatischen Bewertung des Datenschutz-Niveaus - müssen entwickelt und kostengünstig bereitgestellt werden. Hierbei können auch Programme zum Identitätsmanagement hilfreich sein, die den Betroffenen dabei unterstützen, selbst darüber zu entscheiden, wem gegen-

über er welche persönlichen Daten offenbart. Solche Werkzeuge können einen wichtigen Beitrag zu einem wirksamen Datenselbstschutz leisten.

9. Keine Persönlichkeitsprofile

Vielfältig sind heute die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten: So werden Cookies oder Web Bugs verwendet, um das Nutzungsverhalten von Internetnutzern zu registrieren. In Mobiltelefonen werden fortlaufend Lokalisierungsdaten erzeugt und zunehmend durch Location Based Services ausgewertet. Im Handel erfolgt eine individuelle Registrierung des Kaufverhaltens mittels Verbindung von Produkt- und Käuferdaten. Verkehrsdaten der Telekommunikation geben Auskunft darüber, wer wann mit wem telefoniert hat. Die RFID-Technik erlaubt das heimliche Auslesen von Daten mittels Funk. Beim Geomarketing werden Wohn- und Aufenthaltsorte mit allen möglichen Sekundärinformationen verknüpft, vom Durchschnittseinkommen über das Alter bis zur Kaufkraft. Die Zusammenführung dieser Daten zu Profilen birgt erhebliche Gefahren für das informationelle Selbstbestimmungsrecht. Diesen Gefahren muss wirksam begegnet werden. Die Verantwortlichen haben dafür zu sorgen, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile - wenn überhaupt - nur mit Wissen und Zustimmung der Betroffenen erstellt werden, sich auf konkret definierte Sachverhalte und Zwecke beschränken und unter Kontrolle der Betroffenen bleiben. Umfassende Persönlichkeitsprofile, in denen alle möglichen privaten und öffentlichen Daten zusammengeführt werden, darf es auch und gerade unter den Bedingungen einer immer leistungsfähigeren Informationstechnik nicht geben.

10. Informationelle Selbstbegrenzung von Staat und Wirtschaft

Die Informationstechnik bietet das Potenzial einer Totalüberwachung. Politik und Wirtschaft sind deshalb aufgerufen, mit diesen Möglichkeiten verantwortungsbewusst umzugehen und sich selbst zu begrenzen. Nicht alles, was irgendwie sinnvoll erscheint, darf auch realisiert werden. Stets müssen bei Entscheidungen über den Einsatz von IT-Systemen auch die Wirkungen auf das individuelle Selbstbestimmungsrecht bedacht werden. Die Grundsätze der Menschenwürde und der Verhältnismäßigkeit sind verfassungsrechtlich verankert. Ihre Beachtung ist für eine demokratische Informationsgesellschaft von entscheidender Bedeutung. Daraus ergibt sich, dass es eine Rundumüberwachung genauso wenig geben darf wie eine Kontrolle des Kernbereichs der Privatsphäre. Diese Grundsätze sind nicht nur bei der Erhebung von Daten bedeutsam, sondern auch bei ihrer weiteren Nutzung. Insbesondere Daten, die bei der Verwendung von IT-Systemen automatisch generiert werden, können vielfältig miteinander verknüpft werden. Eine Mehrfachnutzung von Daten mag wirtschaftlich oder auch politisch sinnvoll erscheinen. Zweckänderungen bedürfen jedoch auch unter veränderten technologischen Bedingungen grundsätzlich der Zustimmung des Betroffenen oder einer ausdrücklichen gesetzlichen Erlaubnis. IT-Systeme müssen so gestaltet werden, dass die Zusammenführung für unterschiedliche Zwecke gespeicherter Datenbestände nur unter klar definierten und kontrollierten Bedingungen erfolgen kann.

Peter Schaar

Anlage 28

Europäische Konferenz der Datenschutzbeauftragten vom 25. - 26. April 2005 in Krakau (Polen)

Stellungnahme zu Strafverfolgung und Informationsaustausch in der EU

Einführung
Die Frühjahrskonferenz der Europäischen Datenschutzbehörden hat die folgende Stellungnahme verabschiedet:

Entwurf eines Rahmenbeschlusses vom 4. Juni 2004 (10215/04) zur Vereinfachung des Informations- und Erkenntnisaustauschs zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, insbesondere hinsichtlich schwerer Straftaten einschließlich terroristischer Handlungen.

Sachstand
Unter Bezugnahme auf die Erklärung des Europäischen Rates zur Bekämpfung des Terrorismus vom 25. März 2004, in der der Rat aufgefordert wird, den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten zu verbessern und zu vereinfachen, hat das Königreich Schweden einen Entwurf für einen Rahmenbeschluss mit dem Ziel vorbereitet, einen "gemeinsamen und vereinfachten Rahmen für den Austausch von Informationen und Erkenntnissen zwischen den zuständigen Strafverfolgungsbehörden der Mitgliedstaaten" zu schaffen.

Der Rahmenbeschluss
Im Erläuterungsprotokoll wird festgestellt, dass bestehende Unterschiede in den einzelstaatlichen Rechtsvorschriften und Verwaltungsstrukturen der Mitgliedstaaten die größten Hindernisse für den Informations- und Erkenntnisaustausch innerhalb der EU darstellen und dass ein Rahmenbeschluss die beste Methode darstellt, diese Probleme anzugehen. Es folgt eine kurze Zusammenfassung der entsprechenden Bestimmungen des Entwurfs des Rahmenbeschlusses.

Der geplante Rahmenbeschluss würde von den Strafverfolgungsbehörden in den Mitgliedstaaten verlangen, den Strafverfolgungsbehörden in anderen Mitgliedstaaten auf Anfrage bestimmte Informationen und Erkenntnisse zur Verfügung zu stellen. Im Speziellen sollen durch den Beschluss Regelungen festgelegt werden, nach denen die Strafverfolgungsbehörden der Mitgliedstaaten ... vorhandene Informationen und Erkenntnisse zur Durchführung strafrechtlicher Ermittlungen oder kriminalpolizeilicher Einsätze austauschen können (Artikel 1 Absatz 1).

Diese Informationen müssten unverzüglich und vorzugsweise innerhalb des erbetenen Zeitrahmens (Artikel 4 Absatz 3) bereitgestellt werden, und die Strafverfolgungsbehörden dürften eine Informationsanfrage nur dann ablehnen, wenn sie sich auf eine der Ausnahmeregelungen berufen können, die ihnen im Beschluss eingeräumt werden (Artikel 11).

Alle Strafbestände, die mit einer Höchststrafe von 12 Monaten oder mehr geahndet werden, wären von dem Beschluss erfasst (Artikel 3). Der Rahmenbeschlussentwurf enthält darüber

hinaus ein Verzeichnis der Straftaten, die als schwerer eingestuft werden, und bei denen es deshalb erforderlich wäre, dass Informationen binnen höchstens 12 Stunden nach einer Anfrage zur Verfügung gestellt werden (Artikel 4 Buchstabe a Absatz 2).

Daten können ausgetauscht werden über die Personen, die verdächtigt werden, eine in Artikel 3 (Artikel 6 Absatz 1 Buchstabe a) erfasste Straftat begangen zu haben, über die Personen, die nach kriminalpolizeilichen Erkenntnissen oder anderen beweiserheblichen Umständen eine derartige Straftat begehen könnten (Artikel 6 Absatz 1 Buchstabe b) oder über diejenigen Personen, die unter keine dieser Kategorien fallen, aber tatsächliche Gründe für die Annahme sprechen, dass ein Informations- und Erkenntnisaustausch zur Aufdeckung, Verhütung oder Ermittlung einer Straftat beitragen könnte, bei denen eine der unter Artikel 4 Absatz a des Beschlusses (Artikel 6 Absatz 1 Buchstabe c) genannte Straftat begangen wurde.

In Artikel 7 Absatz 1 ist geregelt, dass das SIRENE-Büro oder EUROPOL oder "eine beliebige andere Vorkehrung auf bilateraler oder multilateraler Ebene unter den Mitgliedstaaten" genutzt werden kann, um Informationen und Erkenntnisse nach diesem Beschluss auszutauschen.

Artikel 9 sieht vor, dass in dem Fall, dass vorhandene Kommunikationskanäle genutzt werden, die Datenschutzregelungen, die für diese Kanäle gelten - wie jene, die in der Europolkonvention enthalten sind - auch auf die Austauschvorgänge anzuwenden sind, die von diesem Beschluss erfasst werden.

Artikel 9 sieht vor, dass "gleichwertige Standards des Datenschutzes" gelten sollten, wenn andere Kanäle genutzt werden.

Allgemeine Bemerkungen
Falls dieser Rahmenbeschluss umgesetzt wird, würde damit ein bewährter Standard in der EU-Politik in diesem Bereich fortgeführt. Die Zusammenarbeit zwischen den Strafverfolgungsbehörden wird als ein wichtiger, wenn nicht sogar entscheidender Aspekt in der Bekämpfung von Kriminalität und Terrorismus angesehen. Kulturelle, organisatorische und rechtliche Hindernisse, die einen Datenschutz \u2013 Dokumente der Europäischen DSB-Konferenz 31 Datenaustausch verhindern, müssen angegangen werden. Viele Initiativen, einschließlich dieses Rahmenbeschlussentwurfs, führen zu einem deutlichen Anstieg des Austausches von Informationen für Strafverfolgungszwecke, wobei deutlich mehr personenbezogene Daten zwischen den Mitgliedstaaten ausgetauscht werden. Auch wenn der Datenaustausch an sich für die Bekämpfung von Kriminalität und Terrorismus notwendig sein mag, ist die Liste der von dem Beschluss erfassten Straftaten groß und geht weit über den relativ engen Katalog von Straftaten hinaus, wie sie in anderen EU-Instrumenten erfasst werden, wie z. B. in der Europol-Konvention. Auch die Kategorie von Personen, über die Daten ausgetauscht werden können, ist weit gefasst; insbesondere Artikel 6 Buchstabe c ist unklar und könnte zu einem weitgehenden Datenaustausch von Personen führen, die überhaupt nicht verdächtigt werden, Straftaten begangen zu haben. Es sollte klare Kriterien für die Festlegung geben, wann personenbezogene Daten ausgetauscht werden können.

Der Entwurf des Rahmenbeschlusses führt eine Verpflichtung zum Austausch von Informationen ein, wenn diese verfügbar sind. Angesichts der potentiell weit reichenden Auswirkungen dieser Entwicklung möchten wir hervorheben, wie wichtig eine Prüfung der Verhältnis-

mäßigkeit dieses Vorschlags ist. Die Bekämpfung des Terrorismus wird immer mehr als Begründung für neue Initiativen in diesem Bereich herangezogen, viele davon gehen aber weit über diesen Zweck hinaus. Es ist daher wichtig zu erkennen, dass eine Einschränkung von Grundrechten, die für die Bekämpfung des Terrorismus gerechtfertigt sein kann, nicht notwendigerweise gerechtfertigt ist, wenn es um andere kriminelle Aktivitäten geht.

Durch die Einführung des Grundsatzes, dass Daten bei Verfügbarkeit ausgetauscht werden müssen, wird eine Verbindung zum Haager Programm hergestellt, in dem das Verfügbarkeitsprinzip eingeführt wird. Das Haager Programm legt strikte Bedingungen fest, die einzuhalten sind, wenn das Verfügbarkeitsprinzip angewendet werden soll, wie z. B. das Erfordernis, die Informationsquellen und die Vertraulichkeit der Daten zu schützen, das Erfordernis, die Integrität der auszutauschenden Daten zu gewährleisten, die Aufsicht darüber, dass der Datenschutz beachtet wird, sowie geeignete Kontrollen vor und nach dem Austausch der Daten. Der Rahmenbeschlussentwurf entspricht jedoch nicht diesen strikten Bedingungen, sodass es daher notwendig ist, diese Bedingungen im Beschluss zu entwickeln.

Nach dem Beschlussentwurf sollen bestehende Kommunikationskanäle für den Datenaustausch genutzt werden, und es sollen bestehende Datenschutzregelungen Anwendung finden. So einfach ist dies aber nicht. Es gibt Unterschiede zwischen Datenschutzregelungen, die gemäß Schengen Anwendung finden, und jenen, die z. B. für EUROPOL gelten. Darüber hinaus wurden die Regelungen europaweit noch nicht harmonisiert. Die Regelungen, die für das SIRENE-Büro gelten, sind in den einzelstaatlichen Rechtsvorschriften jedes Mitgliedstaates enthalten; sie sind nicht harmonisiert worden. Dies kann zu Diskrepanzen führen, und es kann durchaus eine Situation entstehen, in der Daten in einem empfangenden Mitgliedstaat längere Zeit aufbewahrt werden, als sie in dem die Daten bereitstellenden Mitgliedstaat aufbewahrt worden wären. Um diese Komplikationen zu vermeiden und im Interesse der Klarheit sollten die Datenschutzregelungen, die für den Datenschutz gemäß diesem Beschluss gelten, im Text des Beschlusses selbst auch enthalten sein. So wie diese Regelungen Fragen der Aufbewahrung, der Datenqualität, Sicherheit und Kontrolle behandeln sollten, sollten diese auch deutlich machen, wer für die weitere Verarbeitung der gemäß diesem Beschluss ausgetauschten Daten verantwortlich ist. Ein besonderes Paket von Datenschutzregeln ist in der Stellungnahme zur Strafverfolgung und zum Informationsaustausch in der EU enthalten, der von der Konferenz in Krakau verabschiedet wurde.

Schlussfolgerung

Um alle erforderlichen Sicherheitsvorkehrungen zu bieten, die für ein angemessenes Niveau im Datenschutz in Einklang mit dem bestehenden rechtlichen Rahmen sorgen, empfiehlt die Konferenz, dass der Rahmenbeschluss unter Berücksichtigung der in dieser Stellungnahme enthaltenen Bemerkungen geändert werden sollte.

Anlage 29

Europäische Konferenz der Datenschutzbeauftragten vom 25. - 26. April 2005
in Krakau (Polen)

Erklärung von Krakau

Verschiedene Initiativen auf EU-Ebene sind darauf gerichtet, den von der Europäischen Union angestrebten Raum der Freiheit, der Sicherheit und des Rechts zur verwirklichen. In ihrem neuen mehrjährigen Programm – dem Haager Programm – wiederholt die Union die Notwendigkeit, das organisierte grenzüberschreitende Verbrechen zu bekämpfen und der terroristischen Bedrohung Einhalt zu gebieten.
Die Frühjahrskonferenz 2005 der Europäischen Datenschutzbehörden ist sich der Notwendigkeit einer engeren Zusammenarbeit zwischen Strafverfolgungsbehörden sowohl innerhalb der EU als auch mit Drittstaaten sehr wohl bewusst. Gleichzeitig ist es offensichtlich, dass die Datenschutzkonvention des Europarats von 1981 (Konvention 108), anwendbar in der Union und in den Mitliedsaaten, zu allgemein gehalten ist, um den Datenschutz im Bereich der Strafverfolgung wirksam zu schützen. Ausgehend von der Verpflichtung der Union zur Achtung der Menschenrechte und Grundfreiheiten, sollten daher Initiativen zur Verbesserung der Strafverfolgung in der EU, wie zum Beispiel das Verfügbarkeitsprinzip, nur auf der Grundlage von Datenschutzregelungen eingeführt werden, die einen hohen und gleichwertigen Datenschutzstandard gewährleisten.
Die Konferenz stellte mit Befriedigung fest, dass das Haager Programm das Verfügbarkeitsprinzip strengen Bedingungen hinsichtlich der Achtung der Grundsätze des Datenschutzes unterstellt.
Die Konferenz begrüßt ebenfalls den Ansatz der Kommission, sich für einen Kernbestand von Leitprinzipien beim Umgang mit personenbezogenen Daten im Bereich der Dritten Säule einzusetzen, der in enger Zusammenarbeit mit den Datenschutzbehörden entwickelt werden soll. Außerdem ist die Konferenz durch Schritte ermutigt worden, welche die Kommission zur Entwicklung eines neuen rechtlichen Rahmen zum Datenschutz in der Dritten Säule unternommen hat, der hoffentlich zu einem angemessenen Bestand von Regelungen für Strafverfolgungen in Übereinstimmung mit dem gegenwärtigen Datenschutzniveau in der Ersten Säule führen wird. Bei der Entwicklung dieser detaillierten Datenschutzregelungen soll der Datenschutzstandard der Richtlinie 95/46/EG als Grundlage dienen.
Angesichts der Notwendigkeit einen harmonisierten Datenschutzansatz in der Union zu entwickeln, liegt es nahe, dass, sobald der Europäische Verfassungsvertrag in Kraft tritt, ein umfassendes Europäisches Datenschutzgesetz gelten sollte, das sämtliche Bereiche der Verarbeitung personenbezogener Daten abdeckt.
Das neue Rechtsinstrument würde die wichtigste Fortentwicklung des Datenschutzrechts seit der Annahme der Datenschutzrichtlinie 95/46/EG sein und große Auswirkungen auf die zukünftige Architektur des Datenschutzes in Europa haben. Um Unterschiede zwischen der Ersten und der Dritten Säule zu vermeiden, was einen negativen Einfluss auf Durchsetzung und Transparenz hätte, und im Hinblick auf die Grundrechtscharta und die kommende Europäische Verfassung, welche die Säulen abschaffen wird, ruft die Konferenz zur Wahrung – und, wo nötig, zur Wiederherstellung des Zusammenhangs, der Konsistenz und der Einheit des Datenschutzes auf. Die Grundsätze der Richtlinie 95/46 sollten den gemeinsamen Kernbereich eines umfassenden europäischen Datenschutzgesetzes bilden. Die darin enthaltenen Vorschriften über die Grundsätze der Zulässigkeit, die Rechte der Betroffenen und

die Regeln der Durchsetzung sind hier besonders zu nennen. In Bezug auf ihre institutionellen Vorschriften ist die Notwendigkeit einer EU-Arbeitsgruppe hervorzuheben, die sich aus Vertretern der nationalen und der EU-Datenschutzaufsichtsbehörden zusammensetzt, die unabhängig arbeiten und die mit Aufgaben der Zusammenarbeit, der Kontrolle sowie mit Beratungsaufgaben zu betrauen sind.
Die Konferenz hat das beigefügte Positionspapier zur Strafverfolgung und zum Informationsaustausch in der EU angenommen. Dieses Papier richtet sich als konstruktiver Beitrag zu aktuellen Initiativen und insbesondere im Hinblick auf die Arbeit der Kommission an einem Datenschutzinstrument für die Dritte Säule vor allem an die EU-Institutionen. Selbstverständlich ist die Konferenz der EU-Datenschutzbehörden weiterhin gerne bereit, an der Schaffung eines praktikablen Rahmens mitzuwirken, der auch die Grundrechte achtet.

Anlage 30

27th International Conference of Data Protection and Privacy Commissioners

Erklärung von Montreux

„Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt“

Die Beauftragten für Datenschutz und den Schutz der Privatsphäre sind auf ihrer 27. Internationalen Konferenz in Montreux (14. bis 16. September 2005) übereingekommen, die Anerkennung des universellen Charakters der Datenschutzgrundsätze zu fördern, und haben folgende Schlusserklärung angenommen:

Die Datenschutzbeauftragten

1. Entsprechen der bei der 22. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Venedig verabschiedeten Erklärung,

2. Erinnern an die auf der 25. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Sydney angenommene Entschließung über den Datenschutz und die internationalen Organisationen,

3. Stellen fest, dass die Entwicklung der Informationsgesellschaft durch die Globalisierung des Informationsaustausches, den Einsatz zunehmend invasiver Datenverarbeitungstechnologien und verstärkte Sicherheitsmassnahmen beherrscht wird,

4. Sind besorgt angesichts der wachsenden Risiken einer allgegenwärtigen Personenüberwachung auf der ganzen Welt,

5. Verweisen auf die Vorteile und potentiellen Risiken der neuen Informationstechnologien,

6. Sind besorgt über die weiterhin bestehenden Abweichungen zwischen den Rechtssystemen in verschiedenen Teilen der Welt und insbesondere über den mancherorts herrschenden Mangel an Datenschutzgarantien, der einen effektiven und globalen Datenschutz untergräbt,

7. Sind sich bewusst, dass aufgrund des rasch wachsenden Kenntnisstandes im Bereich der Genetik Daten über die menschliche DNA zu den sensibelsten überhaupt werden können, und dass die Gewährleistung eines angemessenen rechtlichen Schutzes dieser Daten angesichts der beschleunigten Wissensentwicklung wachsende Bedeutung erlangt,

8. Erinnern daran, dass die Erhebung personenbezogener Daten und ihre spätere Verarbeitung im Einklang mit den Erfordernissen des Datenschutzes und des Schutzes der Privatsphäre erfolgen müssen,

9. Anerkennen die in einer demokratischen Gesellschaft bestehende Notwendigkeit einer wirksamen Bekämpfung des Terrorismus und des organisierten Verbrechens, wobei jedoch daran zu erinnern ist, dass dieses Ziel unter Achtung der Menschenrechte und insbesondere der menschlichen Würde besser erreicht werden kann,

10. Sind der Überzeugung, dass das Recht auf Datenschutz und den Schutz der Privatsphäre in einer demokratischen Gesellschaft unabdingbare Voraussetzung für die Gewährleistung der Rechte der Personen, des freien Informationsverkehrs und einer offenen Marktwirtschaft ist,

11. Sind überzeugt, dass das Recht auf Datenschutz und den Schutz der Privatsphäre ein grundlegendes Menschenrecht ist,

12. Sind überzeugt, dass die universelle Geltung dieses Rechts verstärkt werden muss, um eine weltweite Anerkennung der Grundsatzregeln für die Verarbeitung personenbezogener Daten unter gleichzeitiger Beachtung der rechtlichen, politischen, wirtschaftlichen und kulturellen Vielfalt durchzusetzen,

13. Sind überzeugt, dass allen Bürgern und Bürgerinnen der Welt bei der Verarbeitung sie betreffender personenbezogener Daten ohne jegliche Diskriminierung individuelle Rechte zugesichert werden müssen,

14. Erinnern daran, dass der Weltgipfel zur Informationsgesellschaft (Genf 2003) in seiner Grundsatzerklärung und seinem Aktionsplan die Bedeutung des Datenschutzes und des Schutzes der Privatsphäre für die Entwicklung der Informationsgesellschaft hervorgehoben hat,

15. Erinnern daran, dass die internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation empfiehlt, im Rahmen multilateraler Abkommen den von ihr im Jahre 2000 erarbeiteten Zehn Geboten zum Schutz der Privatheit Rechnung zu tragen[1],

16. Anerkennen, dass die Datenschutzprinzipien auf verbindlichen und nicht verbindlichen internationalen Rechtsurkunden beruhen, namentlich den Leitlinien der OECD für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten, dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, den Richtlinien der Vereinten Nationen betreffend personenbezogene Daten in automatisierten Dateien, der europäischen Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und den Datenschutz-Leitsätzen der Asian Pacific Economic Cooperation (APEC),

17. Erinnern daran, dass es sich dabei insbesondere um folgende Prinzipien handelt:
    - Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten,
    - Prinzip der Richtigkeit,
    - Prinzip der Zweckgebundenheit,
    - Prinzip der Verhältnismäßigkeit,
    - Prinzip der Transparenz,

- Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen,
- Prinzip der Nicht-Diskriminierung,
- Prinzip der Sicherheit,
- Prinzip der Haftung,
- Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen,
- Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr.

In Anbetracht dieser Erwägungen

bekunden die Datenschutzbeauftragten ihren Willen, den universellen Charakter dieser Grundsätze zu stärken. Sie vereinbaren eine Zusammenarbeit insbesondere mit den Regierungen und den internationalen und supranationalen Organisationen bei der Ausarbeitung eines universellen Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten.

Zu diesem Zweck ersuchen die Datenschutzbeauftragen

a. die Organisation der Vereinten Nationen um Vorbereitung einer verbindlichen Rechtsurkunde, in der das Recht auf Datenschutz und Schutz der Privatsphäre als vollstreckbare Menschenrechte im Einzelnen aufgeführt werden;
b. sämtliche Regierungen der Welt, sich für die Annahme von Rechtsurkunden zum Datenschutz und zur Wahrung der Privatsphäre gemäss den Grundprinzipien des Datenschutzes einzusetzen, auch in ihren gegenseitigen Beziehungen;
c. den Europarat, gemäss Artikel 23 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten die Nichtmitgliedstaaten des Europarates, die über eine Datenschutzgesetzgebung verfügen, zum Beitritt zu dem Übereinkommen und seinem Zusatzprotokoll aufzufordern;

Zudem ermutigen die Datenschutzbeauftragten

die Staats- und Regierungschefs, die sich im Rahmen des Weltgipfels zur Informationsgesellschaft in Tunis (16.-18. November 2005) versammeln, in ihre Schlusserklärung die Verpflichtung aufzunehmen, einen Rechtsrahmen zu entwickeln oder zu verstärken, der das Recht auf Privatsphäre und den Schutz der Personendaten aller Bürgerinnen und Bürger der Informationsgesellschaft gewährleistet, im Einklang mit der Verpflichtung, die die iberoamerikanischen Staats- und Regierungschefs im November 2003 in Santa Cruz (Bolivien) sowie die Staats- und Regierungschefs der frankophonen Länder am Gipfel in Ouagadougou (November 2004) eingegangen sind.

Die Datenschutzbeauftragten richten im Weiteren eine Aufforderung an

a. die internationalen und supranationalen Organisationen, damit diese sich verpflichten, mit den wichtigsten internationalen Urkunden betreffend den Datenschutz und den Schutz der Privatsphäre vereinbare Grundsätze einzuhalten und insbesondere unabhängige und mit Kontrollbefugnissen ausgestattete Aufsichtsbehörden einzurichten;

b. die internationalen nichtstaatlichen Organisationen wie Wirtschafts- und Handelsverbände oder Verbraucherorganisationen zur Ausarbeitung von Normen, die auf den Grundprinzipien des Datenschutzes beruhen oder mit diesen Prinzipien im Einklang sind;
c. die Hersteller von Informatikmaterial und Software zur Entwicklung von Produkten und Systemen, deren integrierte Technologien den Schutz der Privatsphäre gewährleisten.

Die Datenschutzbeauftragten kommen außerdem überein

a. namentlich den Informationsaustausch, die Koordinierung ihrer Überwachungstätigkeiten, die Entwicklung gemeinsamer Standards, die Förderung der Information über die Aktivitäten und die Entschließungen der Konferenz zu verstärken;
b. die Zusammenarbeit mit den Staaten zu fördern, die noch nicht über unabhängige Datenschutz-Aufsichtsbehörden verfügen;
c. den Informationsaustausch mit den im Bereich des Datenschutzes und des Schutzes der Privatsphäre tätigen nichtstaatlichen internationalen Organisationen zu fördern;
d. mit den Datenschutzberatern von Organisationen zusammenzuarbeiten;
e. eine ständige Website einzurichten, die insbesondere als gemeinsame Informations- und Ressourcenverwaltungsdatenbank dienen soll.

Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre vereinbaren, die Zielvorgaben der vorliegenden Erklärung regelmäßig auf ihre Verwirklichung zu überprüfen. Eine erste Beurteilung wird anlässlich der 28. Internationalen Konferenz im Jahre 2006 erfolgen.

---

[1] http://www.datenschutz-berlin.de/doc/int/iwgdpt/tc_en.htm

Anlage 31

27. Internationale Konferenz der Datenschutzbeauftragten
Montreux, 16. September 2005

Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten

Die 27. Internationale Konferenz der Datenschutzbeauftragten beschließt:

In Anbetracht der Tatsache, dass Regierungen und internationale Organisationen, namentlich die Internationale Zivilluftfahrtorganisation (ICAO), sich zur Zeit anschicken, Vorschriften und technische Normen zur Integration biometrischer Daten (Fingerabdrücke, Gesichtserkennung) in Pässe und Reisedokumente zu beschließen, um zum einen den Terrorismus bekämpfen und zum andern Grenzkontrollen und Check-in-Verfahren beschleunigen zu können;

Wissend, dass auch im Privatsektor zunehmend biometrische Daten verarbeitet werden, meistens auf freiwilliger Basis;

Unter Berücksichtigung des Umstandes, dass biometrische Daten gesammelt werden können, ohne dass die betroffene Person Kenntnis davon erhält, da sie biometrische Spuren unbewusst hinterlassen kann;

Im Hinblick darauf, dass die Biometrie den menschlichen Körper „maschinenlesbar“ machen wird und dass biometrische Daten als weltweit einheitlicher Identifikator benutzt werden könnten;

Unter Hinweis darauf, dass die verbreitete Verwendung der Biometrie weitreichende Folgen für die Weltgesellschaft haben wird und deshalb Gegenstand einer offen geführten weltweiten Diskussion bilden sollte;

fordert die Konferenz

1. wirksame Schutzmassnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, damit die der Biometrie inhärenten Risiken vermindert werden können,

2. die strikte Trennung zwischen biometrischen Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z. B. Grenzkontrollen) gesammelt und gespeichert werden, und solchen, die mit Einwilligung zu Vertragszwecken gesammelt und gespeichert werden,

3. die technische Beschränkungen der Verwendung biometrischer Daten in Pässen und Identitätskarten auf den Zweck der Identifizierung durch Vergleich der Daten des Dokuments mit Daten des Dokumentinhabers im Moment der Dokumentvorlage.

Anlage 32

Europäische Datenschutzkonferenz
Budapest 24. - 25. April 2006

Erklärung von Budapest

Die Ausweitung des grenzüberschreitenden Informationsaustausches und die - dem Prinzip der Verfügbarkeit unterliegende - gemeinsame Nutzung von in nationalen Dateien gespeicherten Daten als Teil der Zusammenarbeit von Polizei- und Justizbehörden auf der Ebene der Europäischen Union bilden mittlerweile den Brennpunkt der Diskussionen in Europa.
In diesem Zusammenhang erinnert die Konferenz der Europäischen Datenschutzbeauftragten die Mitgliedstaaten daran, dass die gemeinsame Nutzung personenbezogener Informationen durch ihre Strafverfolgungsbehörden nur auf der Grundlage von datenschutzrechtlichen Vorschriften zulässig ist, die ein hohes und harmonisiertes Datenschutzniveau auf europäischer Ebene und in allen Teilnehmerstaaten gewährleisten. Ansonsten könnten Situationen entstehen, in denen aufgrund der unterschiedlichen Schutzstandards und des Mangels an gemeinsamen Vorschriften für Zugangsbeschränkungen die Mindeststandards für den Datenschutz nicht eingehalten werden. In ihrer Erklärung von Krakau hatte die Konferenz betont, dass die bestehenden, in der EU angewandten Rechtsinstrumente des Datenschutzes zu allgemein gehalten sind, um einen wirksamen Datenschutz im Bereich der Strafverfolgung zu gewährleisten. Daher begrüßt die Konferenz den Vorschlag der Europäischen Kommission, den Datenschutz bei Polizei- und Justizbehörden durch die Schaffung von datenschutzrechtlichen Sicherungen in der Dritten Säule zu harmonisieren und zu stärken, die beim Informationsaustausch unter dem Prinzip der Verfügbarkeit angewandt werden müssen.
Es gibt keine Alternative zur Schaffung eines hohen und harmonisierten Datenschutzstandards in der Dritten Säule der EU. Dies ist eine logische Konsequenz des Haager Programms, dem zufolge die Wahrung der Freiheit, der Sicherheit und des Rechts unteilbare Bestandteile der Aufgabe der EU als Ganzes sind, ebenso wie die kürzlich auf EU-Ebene unternommenen Schritte auf Gebieten wie etwa des VISA Informationssystems (VIS), des Schengener Informationssystems II (SIS II), oder der Interoperabilität zwischen europäischen Datenbanken im Bereich der justiziellen und inneren Angelegenheiten. Allein mittels eines derartigen Standards wird es möglich sein, den rechten Ausgleich zwischen den bestehenden und künftigen Formen des Informationsaustausches zwischen den europäischen Strafverfolgungsbehörden zu finden und den Grundsatz der Verhältnismäßigkeit zu beachten, in dem auf der einen Seite die Sicherheit der EU-Bürgerinnen und Bürger geschützt wird und auf der anderen Seite ihre Freiheitsrechte in einem Raum der Freiheit, der Sicherheit und des Rechts gewährleistet werden. Die Konferenz ruft die Parlamente - sowohl das Europäische Parlament als auch die nationalen Vertretungsorgane - dazu auf, ihren Einfluss auf die Regierungen der EU-Mitgliedstaaten geltend zu machen, um dieses Ziel zu erreichen. Die Konferenz appelliert an die Regierungen der Mitgliedstaaten, beim Ausbau der Möglichkeiten des Informationsaustauschs zwischen den Strafverfolgungsbehörden der Mitgliedstaaten die Freiheitsrechte der in der EU lebenden Bürgerinnen und Bürger zu berücksichtigen und zu stärken.
Die Konferenz erachtet es als dringend notwendig, dass entsprechende datenschutzrechtliche Regelungen auf diesem Gebiet so schnell wie möglich verabschiedet und angewandt

werden. Infolge dessen empfiehlt sie bei der Verabschiedung des Vorschlags der Europäischen Kommission für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, die Berücksichtigung der Inhalte der Stellungnahme, die am 24. Januar 2006 von der Konferenz der Europäischen Datenschutzbeauftragten verabschiedet wurde.

Budapest, den 25. April 2006

Anlage 33

Erklärung verabschiedet von den Europäischen Datenschutzbehörden in London am 2. November 2006

Der Ausbau des grenzüberschreitenden Informationsaustausches und die vorbehaltlich des Grundsatzes der Verfügbarkeit erfolgende Weitergabe von in nationalen Dateien gespeicherten Daten im Rahmen der Zusammenarbeit zwischen den Polizei- und Justizbehörden auf EU-Ebene stehen im Mittelpunkt der Diskussionen in Europa. In diesem Zusammenhang haben die Europäischen Datenschutzbehörden bereits wiederholt hervorgehoben, dass angesichts der Tatsache, dass die Union verpflichtet ist, die Menschenrechte und Grundfreiheiten zu achten, Initiativen zur Verbesserung der Kriminalitätsbekämpfung in der EU, wie z.B. der Grundsatz der Verfügbarkeit, nur auf der Grundlage eines angemessenen Systems von Datenschutzmaßnahmen eingeführt werden sollten, die ein hohes und vergleichbares Datenschutzniveau gewährleisten, das den Standards der Ersten Säule entspricht.

Die Europäischen Datenschutzbehörden fordern die Mitgliedstaaten auf, die bürgerlichen Freiheiten der in der EU lebenden Bürger zu respektieren und zu stärken und ein angemessenes System von Datenschutzmaßnahmen aufzubauen, das ein hohes und vergleichbares Datenschutzniveau für die gesamte Datenverarbeitung im Bereich der Kriminalitätsbekämpfung gewährleistet.

Es gibt keine Alternative zum Aufbau eines hohen und harmonisierten Datenschutzstandards im Rahmen der Dritten Säule der EU. Dies ist eine logische Konsequenz aus dem Haager Programm, dem zu folge die Wahrung der Freiheit, der Sicherheit und des Rechts unteilbarer Bestandteil der Aufgabe der EU insgesamt ist. Einschlägige Datenschutzbestimmungen im Bereich der Kriminalitätsbekämpfung sollten so bald als möglich verabschiedet und umgesetzt werden, so dass ein angemessenes und harmonisiertes System von Datenschutzmaßnahmen geschaffen wird, die sich nicht nur auf den Datenaustausch zwischen den Mitgliedstaaten, sondern auf die gesamte Verarbeitung personenbezogener Daten im Rahmen der Kriminalitätsbekämpfung beziehen. Ein hohes Schutzniveau sollte auch für die Weitergabe von Daten an Drittstaaten und internationale Stellen gelten, die vorbehaltlich der auf der Grundlage gemeinsamer Europäischer Standards zu treffenden Feststellung eines angemessenen Datenschutzniveaus erfolgt.

Jeder andere, weniger umfassende Ansatz wäre nicht praktikabel und ungeeignet, das für eine wirksame Kooperation im Bereich der Kriminalitätsbekämpfung erforderliche Vertrauen zu schaffen.

Anlage 34

28. Internationale Konferenz der Datenschutzbeauftragten
London, Vereinigtes Königreich
2. und 3. November 2006

Entschließung zum Datenschutz bei Suchmaschinen[1]

- Übersetzung aus dem Englischen -

Vorgeschlagen von: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland

Unterstützer: Deutschland (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), Irland (Datenschutzbeauftragter), Neuseeland (Datenschutzbeauftragter), Norwegen (Datatilsynet), Polen (Generalinspektor für den Schutz personenbezogener Daten)

Entschließung[2]

Heutzutage sind Suchmaschinen der Schlüssel zum „cyberspace“ geworden, um in der Lage zu sein, Informationen im Internet aufzufinden, und damit ein unverzichtbares Werkzeug.

Die steigende Bedeutung von Suchmaschinen für das Auffinden von Informationen im Internet führt zunehmend zu erheblichen Gefährdungen der Privatsphäre der Nutzer solcher Suchmaschinen.

Anbieter von Suchmaschinen haben die Möglichkeit, detaillierte Interessenprofile ihrer Nutzer aufzuzeichnen. Viele IP-Protokolldaten, besonders wenn sie mit den entsprechenden Daten kombiniert werden, die bei Zugangsdiensteanbietern gespeichert sind, erlauben die Identifikation von Nutzern. Da die Nutzung von Suchmaschinen heute unter den Internet-Nutzern eine gängige Praxis ist, erlauben die bei den Anbietern populärer Suchmaschinen gespeicherten Verkehrsdaten, ein detailliertes Profil von Interessen, Ansichten und Aktivitäten über verschiedene Sektoren hinweg zu erstellen
(z. B. Berufsleben, Freizeit, aber auch über besonders sensitive Daten, z. B. politische Ansichten, religiöse Bekenntnisse, oder sogar sexuelle Präferenzen).

Die Datenschutzbeauftragten sind bereits in der Vergangenheit hinsichtlich der Möglichkeit zur Erstellung von Profilen über Bürger besorgt gewesen[3]. Die im Internet verfügbare Technologie macht diese Praxis jetzt in einem gewissen Umfang auf globaler Ebene technisch möglich.

Es ist offensichtlich, dass diese Informationen unter Umständen auf einzelne Personen zurückgeführt werden können. Deswegen sind sie nicht nur für die Betreiber von Suchmaschinen selbst von Nutzen, sondern auch für Dritte. So hat zum Beispiel vor kurzem ein Ereignis

das Interesse unterstrichen, dass Strafverfolgungsbehörden an diesen Daten haben: Im Frühjahr 2006 forderte das Justizministerium der Vereinigten Staaten von Amerika von Google, Inc. die Herausgabe von Millionen von Suchanfragen für ein Gerichtsverfahren, das unter anderem den Schutz vor der Verbreitung von kinderpornographischen Inhalten im Internet zum Gegenstand hatte. Google weigerte sich, dieser Aufforderung nachzukommen und gewann letztendlich das Verfahren. Im weiteren Verlauf desselben Jahres publizierte AOL eine Liste von beinahe 20 Millionen scheinbar anonymisierten Suchanfragen, die ungefähr 650.000 AOL-Nutzer über einen Zeitraum von drei Monaten in die AOL-Suchmaschine eingegeben hatten. Laut Presseberichten konnten daraus einzelne Nutzer auf der Basis des Inhalts ihrer kombinierten Suchanfragen identifiziert werden. Diese Liste war – obwohl sie von AOL umgehend zurückgezogen wurde, als der Fehler dort erkannt worden war – zum Zeitpunkt des Zurückziehens Berichten zufolge bereits vielfach heruntergeladen und neu publiziert, und in durchsuchbarer Form auf einer Anzahl von Websites verfügbar gemacht worden.

Es muss darauf hingewiesen werden, dass nicht nur die Verkehrsdaten, sondern auch der Inhalt von Suchanfragen personenbezogene Informationen darstellen können.

Diese Entwicklung unterstreicht, dass Daten über zurückliegende Suchvorgänge, die von Anbietern von Suchmaschinen gespeichert werden, bereits jetzt in vielen Fällen personenbezogene Daten darstellen können. Insbesondere in Fällen, in denen Anbieter von Suchmaschinen gleichzeitig auch andere Dienste anbieten, die zur einer Identifikation des Einzelnen führen (z. B. E-Mail), können Verkehrs- und Inhaltsdaten über Suchanfragen mit anderen personenbezogenen Informationen kombiniert werden, gewonnen aus diesen anderen Diensten innerhalb derselben Sitzung (z. B. auf der Basis des Vergleichs von IP-Adressen). Der Prozentsatz von Daten über Suchanfragen, die auf Einzelpersonen zurückgeführt werden können, wird vermutlich in der Zukunft weiter ansteigen wegen der Zunahme der Nutzung fester IP-Nummern in Hochgeschwindigkeits-DSL oder anderen Breitbandverbindungen, bei denen die Computer der Nutzer ständig mit dem Netz verbunden sind. Er wird noch weiter ansteigen, sobald die Einführung von Ipv6 abgeschlossen ist.

Empfehlungen

Die Internationale Konferenz fordert die Anbieter von Suchmaschinen auf, die grundlegenden Regeln des Datenschutzes zu respektieren, wie sie in der nationalen Gesetzgebung vieler Länder sowie auch in internationalen Richtlinien und Verträgen (z. B. den Richtlinien der Vereinten Nationen und der OECD zum Datenschutz, der Konvention 108 des Europarates, dem APEC Regelungsrahmen zum Datenschutz, und den Datenschutzrichtlinien der Europäischen Union) niedergelegt sind, und gegebenenfalls ihre Praktiken entsprechend zu ändern:

1. Unter anderem sollten Anbieter von Suchmaschinen ihre Nutzer im Vorhinein in transparenter Weise über die Verarbeitung von Daten bei der Nutzung der jeweiligen Dienste informieren.
2. Im Hinblick auf die Sensitivität der Spuren, die Nutzer bei der Nutzung von Suchmaschinen hinterlassen, sollten Anbieter von Suchmaschinen ihre Dienste in einer datenschutzfreundlichen Art und weise anbieten. Insbesondere sollten sie keine Informationen über eine Suche, die Nutzern von Suchmaschinen zugeordnet werden können, oder über die Nutzer von Suchmaschinen selbst aufzeichnen. Nach dem Ende eines Suchvorgangs

sollten keine Daten, die auf einen einzelnen Nutzer zurückgeführt werden können, gespeichert bleiben, außer der Nutzer hat seine ausdrückliche, informierte Einwilligung dazu gegeben, Daten, für die Erbringung eines Dienstes die notwendig sind, speichern zu lassen (z. B. zur Nutzung für spätere Suchvorgänge).

3. In jedem Fall kommt der Datenminimierung eine zentrale Bedeutung zu. Eine solche Praxis würde sich auch zugunsten der Anbieter von Suchmaschinen auswirken, indem die zu treffenden Vorkehrungen bei Forderungen nach der Herausgabe nutzerspezifischer Informationen durch Dritte vereinfacht würden.

Für den Zweck dieser Erklärung bedeutet „Dritter“ jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle außer der betroffenen Person, dem für die Verarbeitung Verantwortliche, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsdatenverarbeiters befugt sind, die Daten zu verarbeiten.

_____

Fußnoten:

[1] Diese Entschließung bezieht sich nicht auf Suchfunktionen, die von Inhalteanbietern für ihre eigenen Angebote angeboten werden. Für den Zweck dieser Entschließung wird „Suchmaschine“ definiert als ein Service zum Auffinden von Ressourcen im Internet über verschiedene Websites hinweg und basierend auf nutzerdefinierten Suchbegriffen.

[2] Diese Entschließung betrifft nicht Probleme, die durch die Praxis vieler Betreiber von Suchmaschinen aufgeworfen werden, Kopien des Inhalts von Internetseiten einschließlich darauf enthaltener personenbezogener Daten, die dort legal oder illegal veröffentlicht werden, zu speichern und zu veröffentlichen („caching“).

[3] Vgl. z. B. den gemeinsamen Standpunkt zu Datenschutz und Suchmaschinen (zuerst verabschiedet auf der 23. Sitzung in Hongkong SAR, China ,15. April 1998, überarbeitet und aktualisiert bei der 39. Sitzung, 6. – 7. April 2006, Washington D. C.) der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation;

http://www.datenschutzberlin.de/doc/int/iwgdpt/search_engines_de.pdf. Vgl. ebenfalls Kapitel 5: „Surfen und Suchen“ des Arbeitsdokuments der Artikel-29-Gruppe „Privatsphäre im Internet“ – ein integrierter EU-Ansatz zum Online-Datenschutz“;
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpddocs/2000/wp37de.pdf.

Anlage 35

Organisationsplan

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Herr Dr. von Bose

Referat 1	Referat 2	Referat 3
Geschäftsstellenleitung, Landtag, Justizverwaltung, Justizvollzug, Staatsanwaltschaft, Allgemeines Ordnungswidrig-keitenrecht	Grundsatzfragen des Datenschutzes, Öffentlicher Dienst, Rundfunk- und Presserecht, Hochschulen, Kammern	Grundsatzfragen der Technik und Organisation des Datenschutzes und der Informationstechnik, eGovernment, Wirtschaft, Verkehr,
Polizei, Gefahrenabwehrrecht, Verfassungsschutz und Nachrichtendienste	Sozialwesen, Personenstandswesen, Verwaltungsverfahrensrecht	Vermessungswesen und Geoinformation, Statistik, Handwerk und Gewerbe, IT der Geschäftsstelle
Kommunalrecht, Finanzen, Ausländer und Staatsangehörigkeit, Pass- und Ausweiswesen, Europäischer und Internationaler Datenschutz, Landwirtschaft und Umwelt	Gesundheitswesen, Kinder- und Jugendhilfe, Kultur, Wissenschaft und Forschung, Schulen, Archivwesen	Betriebssysteme, Datenbanksysteme, Telekommunikation, Netze, Neue Medien, IT der Geschäftsstelle
Verwaltungsangelegenheiten der Geschäftsstelle	Meldewesen, Personalaktenrecht, Personalvertretung, Wahlen	
Registratur und Schreibdienst		
Vorzimmer, Bücherei und Schreibdienst		

Dienstgebäude: Berliner Chaussee 9
39114 Magdeburg

Postanschrift: Postfach 19 47
39009 Magdeburg

Telefon: (0391) 8 18 03 - 0
Telefax: (0391) 8 18 03 - 33

E-Mail: poststelle@lfd.lsa-net.de

Internet: http://www.datenschutz.sachsen-anhalt.de

Stand: 23.02.2007

Abkürzungsverzeichnis

A

AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
ARGE	Arbeitsgemeinschaft

B

BA	Bundesagentur für Arbeit
bcc	blind carbon copy
BDSG	Bundesdatenschutzgesetz
BG LSA	Beamtengesetz Sachsen-Anhalt
BGBl. I	Bundesgesetzblatt, Teil I
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMWA	Bundesministerium für Wirtschaft und Arbeit
BNDG	Gesetz über den Bundesnachrichtendienst
BR-Drs.	Bundesratsdrucksacke
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT-Drs.	Bundestagsdrucksache
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts

C

cc	carbon copy
CC	Common Criteria
CERT	Computer Emercency Response Team

D

DMS	Dokumentenmanagementsystem
DNA	Deoxyribonucleic acid (Desoxyribonukleinsäure)
DNS	Desoxyribonucleinsäure
DoS	Denial of Service
DSG-LSA	Gesetz zum Schutz personenbezogener Daten der Bürger
DVBl.	Deutsches Verwaltungsblatt
DVB-T	Digital Video Broadcasting-Terrestrial

E

EG	Europäische Gemeinschaften

EHUG	Gesetz über elektronische Handelsregister und Genossenschafts-register sowie das Unternehmensregister
ELENA	Elektronischer Einkommensnachweis
ePA	elektronischer Personalausweis
EU	Europäische Union

F

FRV	Fahrzeugregisterverordnung
FRZ	Finanzrechenzentrum
FZV	Fahrzeug-Zulassungsverordnung

G

GBO	Grundbuchordnung
GBV	Verordnung zur Durchführung der Grundbuchordnung
GDG LSA	Gesundheitsdienstgesetz des Landes Sachsen-Anhalt
GewO	Gewerbeordnung
GG	Grundgesetz
GIAZ	Gemeinsames Informations- und Auswertungszentrum islamistischer Terrorismus
GmbH	Gesellschaft mit beschränkter Haftung
GO LSA	Gemeindeordnung für das Land Sachsen-Anhalt
GPS	Global Positioning System
GVBl. LSA	Gesetz- und Verordnungsblatt des Landes Sachsen-Anhalt

H

HandwO	Handwerksordnung
HBCI	Home Banking Computer Interface
HeimG	Heimgesetz
HMG-LSA	Hochschulmedizingesetz des Landes Sachsen-Anhalt

I

IA	Integrationsamt
IFD	Integrationsfachdienst
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen
IGLU	Internationale Grundschul-Lese-Untersuchung
IKT	Informations- und Kommunikationstechnologien
IMA-Org	Interministerieller Arbeitskreis „Organisation“
IMSI	International Mobile Subscriber Identity (Internationale eindeutige Teilnehmerkennung)
IT	Informationstechnik
IT-KA	Koordinierungsausschuss Informationstechnik
ITN-LSA	Informationstechnisches Netz Sachsen-Anhalt
IP-Adresse	Internet Protokoll-Adresse (Internet Protocol Address)

J

JVA	Justizvollzugsanstalt

K

KDS	Kerndatensatz
KHG LSA	Krankenhausgesetz Sachsen-Anhalt
KiFöG	Kinderförderungsgesetz des Landes Sachsen-Anhalt
KLIFD	Klientenverwaltungssystem für Integrationsfachdienste
KMK	Kultusministerkonferenz

L

LIS	Landesleitstelle für IT-Strategie
LIZ	Landesinformationszentrum
LPSA	Landesportal Sachsen-Anhalt
LT-Drs.	Landtagsdrucksache
LuftSiG	Luftsicherheitsgesetz
LVwA	Landesverwaltungsamt

M

MADG	Gesetz über den Militärischen Abschirmdienst
MBl. LSA	Ministerialblatt des Landes Sachsen-Anhalt
MDK	Medizinischer Dienst der Krankenversicherung
MDR	Mitteldeutscher Rundfunk
MDStV	Mediendienste-Staatsvertrag

N

NASA	National Aeronautices and Space Administration
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht

O

OSCI	Online Services Computer Interface

P

Pay-TV	Bezahlfernsehen
PIN	Personal Identification Number/Persönliche Identifikationsnummer
PISA	Programme for International Student Assessment
PKI LSA	Public Key Infrastruktur Land Sachsen-Anhalt
PP	Protection Profile (Schutzprofil)
PPP	public-private-partnership-Projekt

Q

R

RdErl.	Runderlass
RettDG LSA	Rettungsdienstgesetz Sachsen-Anhalt
RFID	Radio Frequency Identification (Funkfrequenzkennzeichnung)
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren

S

Schüler-ID	Schüleridentifikationsnummer
SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
SchwarzArbG	Gesetz zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung
SGB	Sozialgesetzbuch
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SSL	Secure Socket Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Stasiunterlagengesetz
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
SÜG-LSA	Sicherheitsüberprüfungs- und Geheimschutzgesetz
SWIFT	Society for Worldwide Interbank Financial Telecommunication

T

TAN	Transaktionsnummer
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TIMSS	Trends in International Mathematics and Science Study
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMF	Telematikplattform
TMG	Telemediengesetz
TPA	Technisches Polizeiamt

U

USB	Universal Seriel Bus

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
VPS	Virtuelle Poststelle

VS	Verschlusssache
VSA	Verschlusssachenanweisung für das Land Sachsen-Anhalt
VV-DSG-LSA	Verwaltungsvorschriften zum Gesetz zum Schutz personenbezogener Daten der Bürger
VwRehaG	Verwaltungsrechtliches Rehabilitierungsgesetz
VwVfG LSA	Verwaltungsverfahrensgesetz des Landes Sachsen-Anhalt
VwVG LSA	Verwaltungsvollstreckungsgesetz des Landes Sachsen-Anhalt

W

www	World Wide Web

Stichwortverzeichnis

(Fundstelle zitiert nach Tätigkeitsbericht und Seite, ab VI. Tätigkeitsbericht nach Tätigkeitsbericht und Ziffer)

A

B

C

D

E

F

G

H

J

K

L

M

N

O

P

S

T

U

V

W

X

Z