Landtag von Sachsen-Anhalt **Drucksache 5/1097**
Fünfte Wahlperiode **23.01.2008**

Unterrichtung

Chef der Staatskanzlei Magdeburg, 16. Januar 2008

Stellungnahme der Landesregierung zum VIII. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2005 bis 31. März 2007

Sehr geehrter Herr Präsident,

als Anlage übersende ich gemäß § 22 Abs. 4a Satz 2 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) die

> Stellungnahme der Landesregierung zum VIII. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 2005 bis 31. März 2007 (Drs. 5/715 vom 15. Juni 2007)

mit der Bitte um Kenntnisnahme.

Zu TOP 20 Punkt 5 des Berichtes weise ich auf die Entscheidungen des Bundesverfassungsgerichts vom 20. Dezember 2007 (2 BvR 2433/04 und 2 BvR 2434/04) hin, wonach Arbeitsgemeinschaften gemäß § 44b SGB II dem Grundsatz eigenverantwortlicher Aufgabenwahrnehmung widersprechen und danach unzulässig sind.

Mit freundlichen Grüßen

Rainer Robra

Verfügung des Präsidenten des Landtages von Sachsen-Anhalt:

Die Unterrichtung des Landtages erfolgt gemäß § 54 Abs. 1 Satz 1 der Geschäftsordnung des Landtages (GO.LT).

Gemäß § 40 Abs. 1 GO.LT überweise ich die Unterrichtung an die Ausschüsse für Inneres (federführend) sowie für Recht und Verfassung.

Hinweis: *Die Drucksache steht vollständig digital im Internet/Intranet zur Verfügung. Die Anlage 1 ist in Word als Objekt beigefügt und öffnet durch Doppelklick den Acrobat Reader.*
Die Anlage wird aufgrund des Umfangs zur Einsichtnahme in der Bibliothek des Landtages von Sachsen-Anhalt bereitgestellt und kann in gedruckter Form abgefordert werden.

(Ausgegeben am 23.01.2008)

Stellungnahme der Landesregierung zum VIII. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz des Landes Sachsen-Anhalt (Drs. 5/715 vom 15. Juni 2007)

Vorbemerkung

Der Landesbeauftragte für den Datenschutz (LfD) hat sich für die Vorlage des VIII. Tätigkeitsberichts mehr Zeit genommen als für frühere Berichte. Dafür ist der Bericht aber auch – hierauf hat der LfD in den Medien hingewiesen - der bislang umfangreichste. Dies ist der genauen Schilderung von Verhandlungsabläufen, der jeweils gesonderten Darstellung von Defiziten hinsichtlich seiner rechtzeitigen Unterrichtung oder Wiederholungen (vgl. z. B. Nr. 19.4.2/20.21) geschuldet. Eine einfache und kurze Darstellung befördert mitunter das Verständnis für komplizierte Sachverhalte – auch in der Öffentlichkeit. Dazu gehört, bei der Abhandlung von Themen die Ergebnisse und verbliebenen Vorbehalte konkret darzustellen (anders z. B. Nr. 6.4, 10.8, 19.3, 19.4, 20.17).

Die Landesregierung sieht sich auch diesmal in der Pflicht, den Bericht durch ihre Stellungnahme für jedermann zu erschließen, auch durch die Abhandlung zusammenhängender Themen an einer Stelle. Die Landesregierung verzichtet – wie in der Vergangenheit – schon aus Achtung der Parlamente darauf, auf kritische Äußerungen des LfD zu im Berichtszeitraum verabschiedeten Bundes- oder Landesgesetzen einzugehen. Grundsätzlich wird auch keine Stellungnahme zu Themen abgegeben, die außerhalb des Aufgabenbereichs des LfD liegen. Überdies erübrigt sich eine Stellungnahme zu Punkten, die nach den Ausführungen des LfD einer datenschutzgerechten Lösung zugeführt worden sind.

Zu 1.1 Freiheit und Sicherheit

Der LfD ist der Ansicht, dass sich der Staat - um den Bedrohungen durch den internationalen Terrorismus wirksam zu begegnen – zunehmend in Richtung Präventionsstaat entwickele. Im Interesse der Gefahrenvorsorge, der Gefahrenabwehr und der Strafverfolgung würden über jeden Bürger unterschiedslos immer mehr Daten über sein Kommunikationsverhalten und sein Auftreten in der Öffentlichkeit gespeichert und auf längere Zeit zum Zwecke späterer Auswertung vorgehalten. Der LfD befürchtet Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung des Bürgers, die mit der ständigen Rechtsprechung des Bundesverfassungsgerichts zu diesem Thema (u. a. BVerfGE 65, 1, 44 und BVerfGE 115, 166, 188) nicht vereinbar seien. Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. „Ein von der Grundrechtsausübung abschreckender Effekt fremden Geheimwissens muss nicht nur im Interesse der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl würde hierdurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist“.

Die Landesregierung steht in der Pflicht, den auch durch Artikel 6 der Landesverfassung (VerfLSA) garantierten Rechten der Bürger auf Schutz ihrer personenbezogenen Daten und auf informationelle Selbstbestimmung so weit wie möglich Wirkung zu verschaffen. Diese Rechte bestehen nicht schrankenlos. Eingriffe in das Recht auf

informationelle Selbstbestimmung sind auf das erforderliche Minimum zu beschränken. An dieser Maxime ist das Vorgehen der Landesregierung generell ausgerichtet. Dies gilt insbesondere bei der Landesgesetzgebung sowie bei der Mitwirkung an Bundesgesetzen und an Rechtvorschriften auf europäischer Ebene. Die Einflussmöglichkeiten der Landesregierung sind allerdings – z. B. bei bundesgesetzlichen Regelungen - beschränkt, wenn zwingende Vorgaben des Europarechts umzusetzen sind.

Die Landesregierung muss regelmäßig verschiedene Rechtsgüter (z. B. Schutz vor Gefahren, Gewährleistung einer effektiven Strafverfolgung und Schutz des Rechts auf informationelle Selbstbestimmung) zu einem gerechten Ausgleich bringen. Hieran wird sie durch die Landesverfassung zusätzlich erinnert, weil Eingriffe in das Recht auf informationelle Selbstbestimmung dem Zitiergebot unterliegen. Die Landesregierung vertraut bei der vorzunehmenden Güterabwägung auf die sachverständige Unterstützung durch den LfD. Seine Vorstellungen zur Bundesgesetzgebung kann der LfD vor allem über den Bundesbeauftragten für den Datenschutz einbringen.

Prof. Dr. Dr. Di Fabio, Richter am Bundesverfassungsgericht, hat am 6. November 2007 in einem Vortrag an der Bundesakademie für Sicherheitspolitik zum Spannungsfeld „Freiheit und Sicherheit“ u. a. ausgeführt, dass

- angesichts der neuen tückischen Bedrohungen durch den internationalen Terrorismus das Ergreifen aller notwendigen Maßnahmen zum Kampf gegen diese Gefahren eine Selbstverständlichkeit sei,
- effektive Polizeiarbeit nicht per se eine Bedrohung für die Freiheit der Bürger, sondern schlichte Notwendigkeit einer freiheitlichen Gesellschaft sei, in der die Menschen grundsätzlich furchtlos leben können müssten,
- die deutsche und europäische Innenpolitik viele erregende Diskussionen (biometrische Merkmale, Rasterfahndung, Online-Durchsuchung, Terrorlisten) kenne, die nicht alle über längere Zeit ihre vordergründige Bedeutung behaupteten,
- eine pure Selbstverständlichkeit sei, dass alle Ebenen der europäischen Politik , vor allem aber die Staaten als letztverantwortliche Garanten von Freiheit und Sicherheit, bei neuen massiven Bedrohungen alle Maßnahmen ergriffen, sofern sie damit nicht den Kerngehalt der Freiheitsrechte beschädigten und die Maßnahmen auch tatsächlich geeignet seien und nicht außer Verhältnis zum angestrebten Sicherheitsgewinn stünden,
- vielen Menschen bei einer Bedrohung Sicherheit wichtiger als Freiheit erscheine; Freiheit und Sicherheit seien aber keine unversöhnlichen Widersprüche, sondern stünden in einem Komplementärverhältnis,
- derjenige, der Sicherheit in Freiheit wolle, den Pragmatismus mehr lieben solle als das intellektuelle Spiel mit dem Grenzfall. Auch das Recht der inneren und äußeren Sicherheit sei nicht sakrosant für sachliche Anpassungen und die Klarstellung der Kompetenzen. Wer jede Sicherheitsmaßnahme als Weg in den Überwachungstotalitarismus brandmarke, überziehe und verliere Glaubwürdigkeit. Wer aber die vielleicht schwindende Alltagsvernunft durch den harten Lehrmeister des gesetzlosen Ausnahmezustandes zu ersetzen gedenke, setze das zivilisatorische Niveau des Westens auf Spiel.

Die Landesregierung ist um den pragmatischen Ausgleich bei der Gewährleistung von Freiheit und Sicherheit bemüht und vertraut – wie bereits ausgeführt - in diesem Bestreben auf die Unterstützung durch den LfD.

Zu 1.3 eGovernment und Technik

Nach Auffassung des LfD hat es in der Vergangenheit Defizite hinsichtlich seiner rechtzeitigen Unterrichtung nach § 14 Abs. 1 Satz 2 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten gegeben, vgl. auch die Ausführungen unter Nr. 4.1, 4.2, 12.1, 18.11... des Tätigkeitsberichts.

Die Pflicht zur rechtzeitigen Unterrichtung des LfD ist Ende 2005 durch eine Änderung des DSG-LSA stärker in das Blickfeld der hierfür verantwortlichen Stellen, insbesondere der obersten Landesbehörden, gerückt worden. Nachdem bereits in der Stellungnahme der Landesregierung zum VII. Tätigkeitsbericht des LfD (vgl. LT-Drs. 4/2524, zu Nr. 2.2) konkretisierende – mit allen Ministerien abgestimmte - Ausführungen zum Gegenstand und zum Zeitpunkt der Unterrichtung gemacht wurden und inzwischen auch die Verwaltungsvorschriften zum DSG-LSA in diesem Punkt aktualisiert wurden, dürften in Zukunft Defizite bei der Unterrichtung vermieden werden.

Auch außerhalb des Anwendungsfalls des § 14 Abs. 1 S. 2 DSG-LSA misst die Landesregierung der beratenden Tätigkeit des LfD erhebliche Bedeutung bei. Sie hat deshalb in § 40 Satz 2 der Gemeinsamen Geschäftsordnung der Ministerien – Allgemeiner Teil – (GGO LSA I) ausdrücklich festgelegt, dass der LfD zu beteiligen ist, soweit die Verarbeitung personenbezogener Daten geregelt werden soll. Ergänzend wird auf die Ausführungen zu Nr. 25.1 verwiesen.

Der LfD hat auch seine Einbindung in bundesweit geplante Anwendungen angesprochen, z. B. das Registerportal der Länder (Nr. 4.2) oder die „Koordinierte neue Softwareentwicklung der Steuerverwaltung – KONSENS“ (Nr. 8.5). Selbst wenn im Einzelfall Besonderheiten länderspezifischer Organisation und marginale Unterschiede im (Datenschutz-)Recht der beteiligten Länder bestehen, überwiegen die Gemeinsamkeiten. Würde jedes Land isoliert seinen LfD in die Planungen einbinden, könnten hierdurch Verzögerungen in der Projektrealisierung eintreten. Die Landesregierung begrüßt daher die organisatorischen Maßnahmen aller LfD, wie sie unter Nr. 8.5 dargestellt sind. Sie bittet den LfD, für alle länderübergreifenden Verfahren auf eine entsprechende generelle Absprache hinzuwirken. Dies würde bei allen Beteiligten den Verwaltungsaufwand erheblich verringern.

Unabhängig von Kritik im Einzelfall gab es in der Vergangenheit einen fachlichen Austausch zu den aufgeführten Vorhaben bzw. Maßnahmen mit dem LfD auf Arbeitsebene. Dies gilt insbesondere für das Ministerium des Innern (MI), dem für eGovernment-Maßnahmen und den IT-Koordinierungsausschusses (ITN-LSA) zuständigen Ministerium, und für seinen nachgeordneten Bereich, das Landesinformationszentrum (LIZ). Der LfD ist zu allen Sitzungen des IT-KA eingeladen. In diesem Gremium stellen die Staatskanzlei und Ressorts die Konzepte und Arbeitsfortschritte für verschiedene eGovernmentmaßnahmen (Aktionspläne, Leitprojekte/Basiskomponenten sowie Ergebnisse von Bund-Länder-Gremien usw.) vor. Die Protokolle und die vorbereitenden Papiere dieser Sitzungen werden auch dem LfD zugeleitet. Er

nimmt darüber hinaus an allen Sitzungen der interministeriellen Redakteure des Landesportals in der Staatskanzlei teil und ist somit über sämtliche öffentlichkeitsrelevanten eGovernment-Prozesse, die über diese IT-Plattform (Basiskomponente Dienstleistungsportal) koordiniert werden, informiert.

Das ITN-LSA ist technische Plattform und Schnittstelle sowohl für die Kommunikation innerhalb der Landesverwaltung als auch für die Kommunikation mit den Bürgerinnen und Bürgern sowie der Wirtschaft und anderen Stellen. Zur datenschutzgerechten Nutzung ist es erforderlich, dass nicht nur das Netz selbst den technisch-organisatorischen Vorgaben des § 6 DSG-LSA entspricht und sichere Übergänge in andere Netze gewährleistet, sondern darüber hinaus ein einheitliches Identifizierungs- und Zugangsmanagement zulässt. Gefährdungen, die bisher durch unterschiedliche Zugangsmechanismen, Passworte, Kennungen usw. gegeben sind, sollen künftig u. a. durch die Verwendung zertifikatsgestützter Signaturkarten ausgeräumt werden. In diese Projekte ist der LfD eingebunden.

Hinsichtlich des IT-Infrastrukturdienste-Konzepts für das ITN-LSA oder der Einführung von „Voice over IP“ in der Landesverwaltung wird dem LfD eine rechtzeitige Beteiligung zugesichert. Beide Projekte befinden sich in der Vorplanung.

Zu 1.4 Zusammenfassung und Ausblick

Die Landesregierung beobachtet wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam. Sie ist sich bewusst, dass der Landesgesetzgeber notfalls durch ergänzende Rechtssetzung korrigierend eingreifen muss (BVerfGE 112, 304). Einbußen an grundrechtlich geschützter Freiheit dürfen nicht in unangemessenem Verhältnis zu den Zwecken stehen, denen die Grundrechtsbeschränkung dient (BVerfGE 113, 348, 382).

Datenschutz ist angesichts der zunehmenden Globalisierung von Datenverarbeitungsprozessen und der Europäisierung des Rechts längst nicht mehr alleinige Angelegenheit der Staaten. Schon die letzte umfassende Novellierung des DSG-LSA im Jahr 2001 stand unter dem Vorzeichen der Umsetzung von europäischem Recht, nämlich der EG-Datenschutzrichtlinie. Den Risiken, denen das Persönlichkeitsrecht heute durch die moderne Informationstechnik – etwa durch das Internet oder die Verwendung von RFID-Technik - ausgesetzt ist, kann vielfach nur durch Anerkennung weltweit akzeptierter Mindeststandards begegnet werden. Auf europäischer Ebene steht insbesondere die weitere Vereinheitlichung des Rechts auch der Mitgliedsstaaten im Bereich der „Dritten Säule“ an, also auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit.

In Deutschland wird vor allem das allgemeine Datenschutzrecht - stärker als bisher – einerseits technikneutrale und andererseits technikabhängige Vorgaben und Verfahrensregelungen zum datenschutzgerechten Umgang mit personenbezogenen Daten treffen müssen. Der Landesregierung sieht – auch im Interesse der Rechtseinheitlichkeit und Anwenderfreundlichkeit des Rechts – insoweit nur einen engen Spielraum für landesspezifische Regelungen. Vor diesem Hintergrund ist die Aussage zu einer umfassenden weiteren Novellierung des DSG-LSA nicht vor einer Änderung des Bundesdatenschutzgesetzes zu sehen.

Zu 2.2 Schwerpunkte – Empfehlungen an Landtag und Landesregierung

Zu den vom LfD angeführten Schwerpunkten seiner Tätigkeit im Berichtszeitraum wird auf die nachfolgende Stellungnahme im Einzelnen verwiesen. Gleiches gilt für die dort ausgesprochenen Empfehlungen.

Soweit der LfD vorschlägt, Gesetze, die in das Recht auf informationelle Selbstbestimmung eingreifen, zu befristen und zu evaluieren, geht die Landesregierung davon aus, dass er entsprechende Empfehlungen jeweils im Einzelfall im Rahmen seiner Beteiligung an Gesetzgebungsverfahren gibt. Die generelle Befristung von Gesetzen kommt entsprechend dem Beschluss der Landesregierung über die Grundsätze der Rechtsförmlichkeit nicht in Betracht. Sie mag allenfalls gerechtfertigt sein, wenn ausnahmsweise nicht absehbar ist, ob die ergriffene Maßnahme angemessen und tauglich ist, also bei so genannten Erprobungsgesetzen.

Zu 2.3 Zusammenarbeit mit anderen Institutionen

Der vom LfD bemängelte Runderlass des MI zum Datenschutz bei den Polizeibehörden und -einrichtungen vom 9. September 2002 ist am 25. November 2002 im Ministerialblatt des Landes Sachsen-Anhalt veröffentlicht worden. Gemäß seiner Nr. III ist der Runderlass mit Ablauf des 26. November 2007 außer Kraft getreten. Es ist beabsichtigt, eine neue Erlassregelung zum Datenschutz bei der Polizei mit dem LfD abzustimmen.

Zu 3.1 Fortentwicklung des Datenschutzrechts und
Zu 3.2 Änderungen im Datenschutzgesetz Sachsen-Anhalt

Auf die Ausführungen zu Nr. 1.4 wird verwiesen.

Zu 3.3 Unabhängigkeit der Datenschutzaufsicht

Dieses Thema ist, obwohl es nicht zu seinem Aufgabenbereich gehört, ein Steckenpferd des LfD. Es veranlasst die Landesregierung – abweichend von der Vorbemerkung – zu den nachfolgenden Anmerkungen.

Die Ausführungen des LfD lassen erkennen, dass er – trotz bekannter verfassungsrechtlicher Hindernisse - eine Verlagerung der Zuständigkeit für die Kontrolle des Datenschutzes im nicht-öffentlichen Bereich vom Landesverwaltungsamt zu seiner Behörde anstrebt. Die Landesregierung hat Verständnis dafür, dass der LfD die Bedeutung seines Amtes durch Anreicherung mit weiteren Aufgaben zu mehren sucht. Sie ist hierfür - soweit es sich mit seiner unabhängigen Stellung als Kontroll- und Beratungsinstitution vereinbaren lässt - offen. Beweis hierfür ist, dass der LfD nach dem Entwurf der Landesregierung für ein Informationszugangsgesetz Sachsen-Anhalt (LT-Drs. 5/748) auch die Aufgaben eines Landesbeauftragten für die Informationsfreiheit wahrnehmen soll. Die Zuständigkeit für den nicht-öffentlichen Datenschutz ist aber gerade kein geeignetes Objekt für derartige Überlegungen.

Schon die Sachverhaltsdarstellung des LfD muss in zwei Punkten korrigiert werden:

- Die Europäische Kommission hält das deutsche System der Kontrolle des Datenschutzes im nicht-öffentlichen Bereich nicht nur in einzelnen, sondern in allen Ländern für nicht vereinbar mit der EG-Datenschutzrichtlinie. Auch in den Län-

dern, die diese Aufgabe dem jeweiligen LfD übertragen haben, sei „völlige Unabhängigkeit“ bei der Erfüllung der Aufgabe wegen des Bestehens von (mindestens) Dienstaufsicht nicht gegeben.

- Das Zusatzprotokoll zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr ist in der Bundesrepublik Deutschland nach Maßgabe folgender Erklärung (Bekanntmachung vom 8. Juni 2004 – BGBl. II S. 1093) in Kraft getreten:
  „Die Bundesrepublik Deutschland erinnert an ihre bereits in der Sitzung des Beratenden Ausschusses nach Artikel 18 der Datenschutzkonvention vom 6. bis 8. Juni 2000 abgegebene Erklärung, dass die bestehende Praxis der Datenschutzkontrolle in Deutschland die Anforderungen von Artikel 1 Abs. 3 des Zusatzprotokolls erfüllt, weil die Datenschutz-Kontrollstellen – auch wenn sie in einen hierarchischen Verwaltungsaufbau eingebunden sind – ihre Aufgaben in völliger Unabhängigkeit wahrnehmen.“

Die Datenschutzbeauftragten des Bundes und der Länder meinen, sie könnten entsprechend den Vorstellungen der Kommission eine einheitliche Datenschutzkontrolle des öffentlichen und nicht-öffentlichen Bereichs in völliger Unabhängigkeit sicherstellen. Dazu müssten sie nur als eigenständige oberste Behörden, die keinerlei Weisungen unterliegen, eingerichtet werden. Sie verkennen dabei, dass es bei klassischer Eingriffsverwaltung - hierzu gehört die Kontrolle des Datenschutzes im nicht-öffentlichen Bereich - keine ministerialfreien Räume geben kann.

In einer – von der Landesregierung mitgetragenen - Mitteilung der Regierung der Bundesrepublik Deutschland vom 13. Februar 2007 ist der Kommission der Europäischen Gemeinschaften dargelegt worden, dass das deutsche Kontrollsystem richtlinienkonform ist. Den wesentlichen Inhalt der Stellungnahme (Anlage 1) hat der LfD im Tätigkeitsbericht dargestellt. Die Kommission hat am 22. November 2007 Klage gegen die Bundesrepublik Deutschland beim Gerichtshof der Europäischen Gemeinschaften (EuGH) erhoben. Die Klageschrift wurde am 29. November 2007 zugestellt. Die Bundesrepublik Deutschland geht davon aus, dass die Klage der Kommission keinen Erfolg haben wird.

Gegen eine Aufgabenverlagerung zum LfD sprechen gewichtige Gründe, die bereits in der Sitzung des Ausschusses für Recht und Verfassung am 11. Januar 2006 angeführt worden sind.

Der LfD ist eine parlamentsnahe Institution. Seine Dienststelle ist beim Präsidenten des Landtages eingerichtet. Ihm obliegt – ohne Zuweisung von Eingriffsbefugnissen – die Kontrolle der Einhaltung des Datenschutzes im öffentlichen Bereich. Würde dem LfD die Kontrolle des Datenschutzes auch im nicht-öffentlichen Bereich übertragen, bekäme er gegenüber nicht-öffentlichen Stellen Eingriffsbefugnisse. Er müsste Ordnungswidrigkeiten verfolgen und ahnden. Solche Aufgaben des Verwaltungsvollzugs passen unter dem Gesichtspunkt der Gewaltenteilung nicht zu einer parlamentsnahen Institution.

Wollte man dem LfD die Aufgabe der Datenschutzkontrolle im nicht-öffentlichen Bereich übertragen, bedürfte es nach Art. 63 Abs. 1 Satz 2 VerfLSA eines formellen Gesetzes, das mit Verfassungsänderungen einhergehen müsste. So könnte die bis-

herige Zuordnung des LfD zum Landtag wohl nur bei einer Änderung des Art. 86 Abs. 1 VerfLSA bestehen bleiben, wonach die öffentliche Verwaltung durch die Landesregierung, die ihr nachgeordneten Behörden und durch die Träger der Selbstverwaltung ausgeübt wird. Auch bei einer Änderung der Anbindung wären weitere Gesetzes- bzw. Verfassungsänderungen erforderlich. So dürfte Art. 49 Abs. 4 VerfLSA, der die Ernennung und Entlassung des LfD durch den Präsidenten des Landtages regelt, zu ändern sein. Klargestellt werden müsste, dass der LfD als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich keine Unabhängigkeit im Sinne des Art. 63 Abs. 1 Satz 2 VerfLSA genießen kann. Er müsste insoweit der Aufsicht des zuständigen Ressortministers oder zumindest der Landesregierung unterstellt werden. Eine Entlassung aus dieser Verantwortung wäre nur bei einer – insoweit als verfassungswidrig einzustufenden - Änderung des Art. 68 Abs. 2 VerfLSA möglich. Auch dürfte - als letztes Aufsichtsmittel - in Art. 63 Abs. 1 VerfLSA die Möglichkeit der Abwahl des LfD in Erwägung zu ziehen sein. Die verfassungsrechtlichen Vorbehalte können auch nicht durch den Hinweis entkräftet werden, dass in einzelnen Ländern LfD trotz ihrer Zuordnung zum Parlament zu Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich bestimmt worden sind. Denn die Landesregierung kann nur die Verfassungslage in Sachsen-Anhalt beurteilen.

Die Landesregierung beabsichtigt gegenwärtig nicht, die Zuständigkeit für die Kontrolle des Datenschutzes im nicht-öffentlichen Bereich zu ändern. Der Ausgang des Vertragsverletzungsverfahrens soll abgewartet werden. Mit dieser Begründung ist im Jahr 2007 im Saarland und in Brandenburg abgelehnt worden, die dortigen LfD zu Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich zu bestimmen, (vgl. Protokoll über die 37. Sitzung des Landtages des Saarlandes am 25. April 2007, S. 2188 ff, sowie die Beratung zum Entwurf eines Dritten Gesetzes zur Änderung des Brandenburgischen Datenschutzgesetzes und weiterer Gesetze (LT-Drs. 4/5330)).

Sollte der EuGH in Deutschland die Organisation der Datenschutzkontrolle im nicht-öffentlichen Bereich tatsächlich als nicht richtlinienkonform ansehen, wird er zugleich ein mit den Grundzügen des EG-Vertrages und den allgemeinen Verfassungsgrundsätzen vereinbares Regelungsmodell aufzeigen müssen. Dieses könnte – würde man sich heute zu einer Aufgabenzuweisung an den LfD entschließen – eine erneute Gesetzes- bzw. Verfassungsänderung erfordern. Eine Regelung „ins Blaue“ entspricht nicht den Vorstellungen der Landesregierung von Gesetzgebungsökonomie.

Zu 4.1 IT-Konzept der Landesverwaltung Sachsen-Anhalt

Wie vom LfD dargestellt, ist die IT-Organisation in Sachsen-Anhalt seit Ende 2006 grundlegend geändert worden. Für grundsätzliche, nicht ausschließlich ressortspezifische Angelegenheiten sind innerhalb der Landesregierung nunmehr die Staatskanzlei (StK), das Ministerium der Finanzen (MF) und das MI zuständig.

Bei der StK wurde die Landesleitstelle IT-Strategie (LIS) eingerichtet. Zu ihren vordringlichsten Aufgaben gehört, eine ressortübergreifende IT-Strategie für das Land Sachsen-Anhalt zu entwerfen. Das entsprechende Thesenpapier wird unter Beteiligung des IT-KA erarbeitet. Eine Beteiligung des LfD erfolgt im Rahmen des IT-KA. Unabhängig davon wurde dem LfD mit Schreiben der StK vom 21. Dezember 2006 eine frühzeitige Unterrichtung bei der Erstellung strategischer Grundlagenpapiere zugesichert.

Beim MF wurde der Aufbaustab zur Konsolidierung des IT-Betriebes in der Landesverwaltung als Stabsstelle gebildet. Er soll die fachlichen und organisatorischen Maßnahmen der IT-Neuorganisation umsetzen. Sein Auftrag ist die Bildung des IT-Betriebsstättenverbundes und als dessen Bestandteil die Errichtung eines Landesrechenzentrums (LRZ). Dort sollen die IT-Aufgaben wahrgenommen werden, die zentral erledigt werden können. Der IT-Betriebsstättenverbund soll die Rechenzentren im Land organisatorisch zusammenfassen.

Der Aufbaustab achtet auf die Einbindung des LfD bereits in der Planungsphase. Der LfD ist als Projektbeirat regelmäßig vor Beschlussfassung über alle avisierten Schritte informiert. Er hat aktive Gestaltungs- und Mitwirkungsrechte. Dementsprechend erhielt der LfD bereits vor Abschluss der Mitzeichnungsrunde diesbezügliche Kabinettsvorlagen zur Kenntnis.

MI obliegt die Koordinierung der eGovernment-Projekte der gesamten Landesverwaltung, insbesondere auch hinsichtlich der Auswirkungen auf den kommunalen Bereich. Im eGovernment-Maßnahmenplan sind alle Vorhaben detailliert beschrieben.

Zu 4.2 eGovernment-Maßnahmenplan 2007

MI wird den LfD vor künftigen Beschlussfassungen des Kabinetts über eGovernment-Maßnahmen unterrichten.

Dem LfD ist beizupflichten, dass sich eGovernment immer mehr von reinen Informationsangeboten hin zu interaktiver Verwaltung entwickelt. Entsprechende Angebote nimmt der Bürger aber nur an, wenn er darauf vertrauen kann, dass das Internetportal des Landes und die dort verfügbaren Online-Dienstleitungsangebote der Verwaltung datenschutzgerecht gestaltet sind, also insbesondere den Anforderungen der Datensicherheit genügen. Schon deshalb ist die Einbindung des LfD in diese Projekte erforderlich.

Zu 8.3 Elektronische Signatur in der Finanzverwaltung

Seit dem 1. Januar 2006 ist das ELSTER-Online-Verfahren am Netz, um Steuerpflichtigen die Möglichkeit zu geben, ihre Steuererklärung in elektronischer Form beim Finanzamt einzureichen. Sofern von dieser Möglichkeit Gebrauch gemacht wird, dient die elektronische Signatur (vgl. § 87a Abs. 3 Satz 2 AO) als Ersatz für die eigenhändige Unterschrift. § 87a Abs. 6 AO sieht vor, dass das Bundesministerium der Finanzen (BMF) mit Zustimmung des Bundesrates durch Rechtsverordnung *neben der qualifizierten elektronischen Signatur* bis zum 31.12.2011 auch ein *anderes sicheres Verfahren* zulassen kann, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt.

Von dieser Möglichkeit ist durch § 6 Abs. 1 i. V. m. § 1 Abs. 3 Satz 1 der Steuerdaten-Übermittlungsverordnung (StDÜV) Gebrauch gemacht worden. Danach ist bei der elektronischen Übermittlung keine qualifizierte elektronische Signatur erforderlich, wenn ein dem jeweiligen Stand der Technik entsprechendes Verfahren eingesetzt wird, welches einerseits den Datenübermittler authentifiziert und andererseits die Anforderungen an die Authentizität, Vertraulichkeit und Integrität der Daten erfüllt. Im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden. Damit ist klargestellt, dass nur sichere Verfahren zugelassen werden können. Die Beschreibung dieser Verfahren ist nicht Gegenstand der Verordnung.

Zu 8.5 KONSENS

Voraussetzung für einen effizienten und effektiven Steuervollzug ist die Anwendung einer bundeseinheitlichen Software für die Steuerbehörden der Länder. Aus diesem Grund haben die Finanzministerinnen und Finanzminister des Bundes und der Länder das Verwaltungsabkommen für das Vorhaben „Koordinierte neue Softwareentwicklung der Steuerverwaltung“ - KONSENS - abgeschlossen, das zum 1. Januar 2007 in Kraft getreten ist.

Gegenstand des Abkommens ist die Beschaffung, die arbeitsteilige Entwicklung, die Finanzierung, die Pflege und der Einsatz einheitlicher Software für das Besteuerungsverfahren sowie das Steuerstraf- und Bußgeldverfahren. Die Festlegung und Steuerung der Strategie und Architektur obliegt auf der Grundlage eines von den Ländern genehmigten Vorhabensplans der Steuerungsgruppe IT, in welcher der Bund und die Länder Baden-Württemberg, Bayern, Hessen, Niedersachsen und Nordrhein-Westfalen vertreten sind.

Der Arbeitskreis Steuerverwaltung der Datenschutzbeauftragten des Bundes und der Länder hat im Rahmen einer Tagung im April 2006 auf Anregung des Hessischen Ministeriums der Finanzen einen Vorschlag für die datenschutzrechtliche Begleitung bundeseinheitlicher IT-Verfahren in der Steuerverwaltung unterbreitet. Die empfohlene Vorgehensweise für ein koordiniertes Vorgehen wird von den am Vorhaben KONSENS beteiligten Gremien begrüßt. Die Steuerungsgruppe IT sieht darin eine praktikable Möglichkeit für das auftragnehmende Land, bei der Entwicklung der einheitlichen Software eine möglichst einheitliche Vorgabe für die zu berücksichtigenden datenschutzrechtlichen Aspekte zu erhalten.

Datenschutzrechtliche Fragen werden durch das auftragnehmende Land mit dem jeweiligen LfD geklärt. Dieser ist für die Zeit der Verfahrensentwicklung Ansprechpartner für datenschutzrechtliche Fragen und übernimmt eine Mittlerfunktion gegenüber den LfD der übrigen Länder. Diese Verfahrensweise sichert die rechtzeitige Abstimmung in Grundsatzfragen. Unabhängig davon wird vor dem Einsatz eines Verfahrens in jedem Bundesland eine Abstimmung mit dem LfD vorgenommen. Diese Vorgehensweise hat sich bereits bei der Abstimmung des Nutzungskonzeptes zum bundesweiten Einsatz des Verfahrens LUNA 2.0 (Länderumfassende Namensabfrage) durch das auftragnehmende Land Hessen bewährt. Die hierbei gewonnenen Erfahrungen werden für die weitere Zusammenarbeit berücksichtigt.

Zu 10.2 Elektronischer Heilberufsausweis

Um Missbrauch im Umgang mit der elektronischen Gesundheitskarte auszuschließen, soll der Zugriff auf die hierauf gespeicherten Daten nur Personen ermöglicht werden, die im Besitz eines Heilberufsausweises bzw. eines besonderen Berufsausweises sind.

Ohne den elektronischen Heilberufsausweis können die Funktionen und die medizinischen Daten der elektronischen Gesundheitskarte nicht genutzt werden. Der elektronische Heilberufsausweis soll eine eindeutige Identifikation des Heilberuflers, sein Photo sowie die Gültigkeitsdauer enthalten. Er ist wie die elektronische Gesundheitskarte mit einem Mikroprozessor ausgerüstet, der die Dienste Authentifizierung, Verschlüsselung und elektronische Signatur ermöglicht.

Gem. § 291a Abs. 5a SGB V bestimmen die Länder die Stellen, die für die Ausgabe der elektronischen Heilberufsausweise zuständig sind. Für die verkammerten Berufe, wie z. B. die Ärzte oder Apotheker, wird die Ausgabe von den Kammern der jeweiligen Heilberufe übernommen.

Im Tätigkeitsbericht ist auch die Frage aufgeworfen worden, welche Stellen den elektronischen Heilberufsausweis für Angehörige der so genannten nicht verkammerten Berufe ausstellen sollen. Die Gesundheitsministerkonferenz vom 4./5. Juli 2007 hat sich mehrheitlich dafür entschieden, ein nationales Berufsregister einzurichten, das für die Ausgabe der elektronischen Berufsausweise an diese Berufsgruppe zuständig sein soll. Sachsen-Anhalt hat dem zugestimmt.

Zu der grundsätzlichen Frage, ob eine Datensammlung als nationales Berufsregister überhaupt erforderlich ist oder die Aufgaben auch dezentral von den bisher zuständigen Behörden wahrgenommen werden könnten, ist Folgendes anzumerken:

Die Schwierigkeit, Angelegenheiten des elektronischen Heilberufsausweises dezentral wahrzunehmen, gäbe es bei den Gesundheitsfachberufen (z. B. Physiotherapeuten, Orthopädiehandwerkern, Hebammen). Hier bestünde das Problem, dass eine Vielzahl von Stellen, die in Deutschland für die Ausgabe elektronischer Berufsausweise für den jeweiligen Beruf zuständig wären, untereinander kommunizieren müssten, um abzusichern, dass bei entzogener Berechtigung zur Berufsausübung auch der elektronische Ausweis eingezogen wird. Grund dafür ist, dass die Behörde, die den elektronischen Ausweis ausgeben wird, nicht immer mit der Behörde identisch sein muss, die die Berufsberechtigung zu entziehen hat. Die Behörde, die den elektronischen Ausweis ausstellt, wird diejenige sein, in deren Bezirk die Berufsangehörigen ihren Beruf ausüben oder ihren gewöhnlichen Aufenthalt haben (dem § 3 Abs. 1 Nrn. 2 und 3 Buchst. a VwVfG entsprechende landesgesetzliche Regelungen). Demgegenüber ist die Behörde, die die Berufsberechtigung entzieht, diejenige, in deren Bezirk der Anlass für die Aufhebung der Berechtigung entstanden ist (dem § 3 Abs. 1 Nr. 4 VwVfG entsprechende landesgesetzliche Regelungen). Infolge eines Wechsels des Ortes, des gewöhnlichen Aufenthalts oder der Ausübung des Berufs können hier unterschiedliche örtliche Zuständigkeiten von Behörden gegeben sein.

Im Regelfall wird eine Behörde, die die Berufsberechtigung entzogen hat, nicht wissen, welche Behörde den elektronischen Berufsausweis ausgestellt hat. Sie müsste sich an sämtliche in Deutschland in Frage kommenden zuständigen Stellen wenden, um zu erreichen, dass auch der elektronische Berufsausweis entzogen bzw. für ungültig erklärt wird. Dies können im Bereich der Gesundheitsfachberufe, bei denen es z. B. in Nordrhein-Westfalen eine Zuständigkeit von Kommunen gibt, im Einzelfall etwa 100 Behörden in Deutschland sein. Eine Einbindung all dieser Behörden wäre mit überflüssigem Verwaltungsaufwand verbunden und zudem nicht datenschutzgerecht. Nur die Behörde, die im Einzelfall für den Entzug des elektronischen Berufsausweises zuständig ist, muss diese Information erhalten.
Um eine Übermittlung personenbezogener Daten an eine Vielzahl - für den Einzelfall nicht zuständige - Stellen zu verhindern, ist ein nationales Berufsregister als zentrale Stelle für die Ausgabe der elektronischen Berufesausweise und die Entgegennahme von Mitteilungen über die Entziehung von Berufsberechtigungen eine sinnvolle und datenschutzgerechte Lösung.

Zu 12.1 Auftragsdatenverarbeitung – mit bekannten Problemen

Die Hinweise zur Auftragsdatenverarbeitung werden beachtet. Vertiefte Ausführungen zu diesem Thema finden sich in den vom MI in Abstimmung mit dem LfD verfassten Hinweisen auf der Internetseite des LfD unter http://www.sachsen-anhalt.de/LPSA/index.php?id=20554. Es wird davon ausgegangen, dass die verantwortlichen Stellen ihre Beauftragten für den Datenschutz nach § 14a Abs. 4 DSG-LSA in die Auftragsvergabe einbinden, damit diese bei der Vertragsgestaltung darauf hinwirken können, dass den materiellrechtlichen und formellen Anforderungen Rechnung getragen wird. Unabhängig davon können die Beauftragten für den Datenschutz auch bestehende Verträge auf die Vereinbarkeit mit datenschutzrechtlichen Vorschriften prüfen (vgl. § 14a Abs. 4 S. 2 Nr. 1 DSG-LSA).

Es trifft zu, dass bei der Einbeziehung Dritter in die Entsorgung von Personalcomputern und der Vernichtung von Festplatten Auftragsverarbeitung vorliegt, sofern personenbezogene Daten wiederherstellbar gespeichert sind. Dieses Problem stellt sich nicht, wenn - wie z. B. im Organisationsbereich des Ministeriums für Wirtschaft und Arbeit - personenbezogene Daten nur auf zentralen Servern, nicht aber in Personalcomputern gespeichert sind.

12.5 E-Mail-Verteiler

Der Hinweis auf die BCC-Funktion ist nützlich. Er zeigt dem Anwender auf, wie er in einem Arbeitsgang gleiche Texte an mehrere Personen versenden kann, ohne dass für den jeweiligen Empfänger die anderen Adressaten sichtbar werden.

Zu 13.1 Hochschulmedizingesetz

Die im Bericht beschriebenen Aktivitäten zur Änderung des Hochschulmedizingesetzes (HMG LSA) werden aus der Mitte des Parlaments betrieben. Es ist kein vom Kultusministerium (MK) betreutes Verfahren. Soweit hier bekannt, haben die Abgeordneten von sich aus Gespräche mit dem LfD zu diesem Thema geführt.

Gemäß § 27 Abs. 3 HMG LSA hat die Landesregierung allerdings bis zum Ende des Jahres 2008 durch eine Überprüfung in geeigneter Form festzustellen, ob die Zielvorgaben des HMG LSA erreicht werden können. Hierüber ist dem Landtag zu berichten. Für die Überprüfung wurde der Wissenschaftsrat gewonnen.

Es ist nicht auszuschließen, dass die hier im Bericht des LfD angesprochene mögliche Problemlage auch in diesem Zusammenhang eine Rolle spielen wird. Das MK wird dann ggf. den Bericht des Wissenschaftsrats auswerten, die Anregungen des LfD aufnehmen und u. U. einen Gesetzentwurf vorlegen.

Zu 15.2 Anschluss der Mitglieder des Landtages und der Fraktionen an das Intranet der Landesverwaltung

Der Anschluss der Mitglieder des Landtages an das Intranet ist seit dem 1. April 2007 realisiert. Die Unterrichtung des LfD über die Durchführung der Vorabkontrolle obliegt den Ressorts in eigener Verantwortung.

Zu 16.3 Erfolglose Bewerbungen in Personalunterlagen

Der Auffassung des LfD, dass Unterlagen über erfolglose Bewerbungen aus datenschutzrechtlichen Gründen nicht in die Personalakte des Betroffenen aufzunehmen sind, wird zugestimmt. Gemäß § 90 Abs. 1 Satz 2 BG LSA gehören nur Unterlagen zur Personalakte, soweit sie mit dem Dienstverhältnis eines Beamten in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Dies ist bei Unterlagen über erfolglose Bewerbungen, deren Zweck sich mit Abschluss des Bewerbungsvorganges erledigt hat, nicht der Fall. Bei Tarifbeschäftigten ist entsprechend zu verfahren.

Zu 17.1 SOG LSA – Kernbereichsschutz
Zu 17.2 Rasterfahndung

Der LfD regt an, die Regelungen des § 17 Abs. 4 bis 6 des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) zur akustischen oder optischen Wohnraumüberwachung unter Berücksichtigung neuerer Rechtsprechung zum unantastbaren Kernbereich privater Lebensgestaltung (BVerfGE 113, 348; VGH Rheinland-Pfalz vom 29. Januar 2007 – DVBl. S. 569) einzuschränken. Des Weiteren schlägt er unter Hinweis auf die Entscheidung BVerfGE 115, 320 vor, Rasterfahndungen in § 31 SOG LSA nur bei Vorliegen konkreter Gefahren zuzulassen.

Nach Abschluss der Polizeistrukturreform ist vorgesehen, im Jahr 2009 einen Entwurf zur Änderung des SOG LSA vorzulegen. Dabei wird auch entschieden, inwieweit den Anregungen des LfD gefolgt werden kann. Eine besondere Dringlichkeit besteht nicht. Das SOG LSA enthält keine Regelung zur präventiven Überwachung der Telekommunikation. Die akustische oder optische Wohnraumüberwachung kann in der Praxis so gestaltet werden, dass keine Eingriffe in den unantastbaren Kernbereich privater Lebensführung erfolgen. Rasterfahndung ist die absolute Ausnahme; sie lässt sich auch ohne ausdrückliche Festlegung im Gesetzestext auf das Vorliegen konkreter Gefahren beschränken.

Zu 17.3 Gesprächsaufzeichnungen bei der Polizei

Im Oktober 2007 wurde dem LfD ein überarbeiteter Erlassentwurf mit Regelungen zur Aufzeichnung von Anrufen über Notrufeinrichtungen, sonstigen Anrufen und des Sprechfunkverkehrs bei der Polizei zugeleitet. Am 19. November 2007 teilte der LfD mit, dass gegen den Erlassentwurf keine datenschutzrechtlichen Bedenken bestehen.

Zu 18.1 Gerichtsvollzieher und Medien

Hinsichtlich des konkreten Sachverhalts und vergleichbarer Fallgestaltungen ist die Landesregierung übereinstimmend mit dem LfD der Auffassung, dass bezüglich der möglichen Dokumentation von hoheitlichen Maßnahmen zunächst das Einverständnis der betroffenen Bürgerinnen und Bürger einzuholen ist, bevor eventuell danach personenbezogene Daten übermittelt werden dürfen, wie etwa die Information, dass – wie vorliegend – eine bestimmte Vollstreckungshandlung vorgesehen sei.

Anders dürfte der Fall liegen, wenn die Presse aufgrund eigener Recherchen Kenntnis von bevorstehenden Maßnahmen der Gerichte und Strafverfolgungsbehörden erlangt hat und dies etwa durch vor Ort gewonnenes Bildmaterial dokumentiert.

Unter Berücksichtigung der erfolgten Auswertung des Vorfalls geht die Landesregierung davon aus, dass es sich vorliegend um einen sich nicht wiederholenden Einzelfall handeln dürfte.

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

Die Frage, in welchem Umfang die Benachrichtigung der Beteiligten der überwachten Telekommunikation gemäß 101 StPO zu erfolgen hat, ist mit dem vom Bundestag am 9. November 2007 beschlossenen „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ in einer Weise neu geregelt worden, die der bisherigen Praxis weitgehend entspricht und die schutzwürdigen Belange des Beschuldigten und der Betroffenen beachtet.
§ 101 Abs. 4 Satz 4 StPO bestimmt, dass u. a. in den Fällen der Telekommunikationsüberwachung die Benachrichtigung unterbleiben kann, wenn eine der Personen, gegen die sich die Maßnahme nicht gerichtet hat, von der Maßnahme in nur unerheblicher Weise betroffen wurde und anzunehmen ist, dass kein Interesse an einer Benachrichtigung besteht. Diese Regelung trägt dem Umstand Rechnung, dass von den in Bezug genommenen Maßnahmen zwar regelmäßig viele Personen in ihrem Grundrecht aus Artikel 10 GG betroffen werden, dies aber im Einzelfall in einer vergleichsweise so geringfügigen Weise, dass ein Interesse an einer Benachrichtigung oftmals nicht anzunehmen ist.

Bei Telekommunikationsüberwachungsmaßnahmen wird dies beispielsweise dann der Fall sein, wenn für die Strafverfolgung irrelevante Gespräche zur Besorgung von Alltagsgeschäften mit erfasst wurden (z. B. Terminvereinbarungen mit Handwerkern; telefonische Bestellungen etwa bei Bringdiensten; Reklamationen, die über so genannte Callcenter bearbeitet werden). Die Regelung in Satz 4 ist nicht als zwingende Regelung, sondern als Ermessensvorschrift ausgestaltet. Dies trägt zwei Aspekten Rechnung: Zum einen ist kein Grund gegeben, die Benachrichtigung gesetzlich zu verbieten, wenn eine Person in nur unerheblicher Weise von der Maßnahme betroffen wurde und anzunehmen ist, dass kein Interesse an der Benachrichtigung besteht. Zum anderen kann es in Einzelfällen für die Strafverfolgungsbehörden effizienter sein, eine Benachrichtigung durchzuführen, als eingehende Überlegungen dazu anzustellen, ob das Maß der Betroffenheit bereits die Unerheblichkeitsschwelle überschritten hat bzw. welche Punkte für oder gegen ein Interesse an der Benachrichtigung sprechen.

Die Neuregelung entspricht weitgehend der bisherigen Praxis und der Auslegung in der verfassungsgerichtlichen Rechtsprechung und strafrechtlichen Kommentarliteratur. Danach sind in jedem Fall der Beschuldigte und der Anschlussinhaber zu informieren. Gleiches gilt für die bekannten Nutzer eines privaten Telefonanschlusses, also für die im Haushalt lebenden Familienangehörigen oder Bewohner einer Wohnungsgemeinschaft, falls dieser Personenkreis den Anschluss auch tatsächlich während der Überwachung benutzt hat. Auch die sich zufällig in der Wohnung aufhaltenden Personen, die das überwachte Telefon benutzt haben, sind zu benachrichtigen,

falls deren Identität und Privatanschrift bekannt sind. Damit ist dem gesetzlichen Gebot der Benachrichtigung und den schutzwürdigen Belangen des Beschuldigten hinreichend Genüge getan (vgl. Löwe-Rosenberg, StPO, 5. Aufl., § 101 Rn. 4). Würde man darüber hinaus jeden Beteiligten benachrichtigen, mit dem der Beschuldigte lediglich telefonisch beispielsweise einen Termin vereinbart hätte, so würden diese von der Überwachung dieses Gesprächs und damit zwangsläufig auch von dem gegen den Beschuldigten vorhanden gewesenen Verdacht unterrichtet werden müssen. Derartiges würde jedoch die schutzwürdigen Belange des Beschuldigten tangieren. Dieser dürfte kein Interesse daran haben, dass mehr Personen als nötig Kenntnis von der Tatsache erhalten, dass sein Telefonanschluss überwacht wird.

Die Landesregierung geht davon aus, dass die Neuregelung in § 101 Abs. 4 StPO zu größerer Rechtssicherheit und -klarheit führen wird.

Zu 18.4 Auskunft aus den Dateien der Staatsanwaltschaft

Die Landesregierung vermag eine widersprüchliche Beantwortung zu der Frage der Praxis der Auskunftserteilung aus staatsanwaltlichen Informationssystemen nicht zu erkennen. Sie teilt die Auffassung des LfD, wonach Betroffene grundsätzlich einen Anspruch auf Auskunftserteilung haben und die Berechtigung des Auskunftsanspruches entsprechend den gesetzlichen Regelungen aufgrund einer Einzelfallentscheidung zu beurteilen ist.

Einen anderen Fall betrifft die vom LfD im zweiten Teil von Nr. 18.4 angesprochene Problematik der Beauskunftungspraxis bei verdeckten Ermittlungen, speziell beim Einsatz verdeckter Ermittler. Dieser ist von den allgemeinen Auskunftserteilungsgrundsätzen zu unterscheiden. Die Auskunft auf die Anfrage einer dritten Person, ob verdeckte Ermittlungen gegen sie geführt werden oder geführt worden sind, richtet sich in erster Linie nach § 110d StPO. Nach Absatz 1 dieser Vorschrift beschränkt sich die Benachrichtigungspflicht allerdings lediglich auf den Wohnungsinhaber, deren Wohnung der verdeckte Ermittler betreten hat (§ 110b Abs. 2 Nr. 2 StPO), während allein der Einsatz des verdeckten Ermittlers gegen einen bestimmten Beschuldigten (§ 110b Abs. 2 Nr. 1 StPO) diesem ebenso wenig mitzuteilen ist wie Dritten, die vom Einsatz eines verdeckten Ermittlers betroffen sein könnten (Lutz Meyer-Goßner, StPO, 50. Aufl., § 110d Rn. 1).

Zu 18.5 Handakten der Staatsanwaltschaft ... wie auch anderer Dienststellen

Die Landesregierung teilt nicht die Auffassung des LfD, dass § 15 DSG-LSA einen Anspruch Betroffener auf Einsicht in oder Auskunft aus staatsanwaltschaftlichen Handakten, insbesondere von Personen, die nicht Beschuldigte in einem Verfahren sind, begründet.

Die Auffassung des LfD dürfte auf die Ausführungen in der Bundestagsdrucksache 14/2595 zum Strafverfahrensänderungsgesetz 1999 zurückgehen. Dort heißt es auf S. 29: „Da die bereichsspezifischen Regelungen der StPO nicht abschließend sind und im Übrigen das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze zur Anwendung kommen sollen, …“. Hieraus zieht er den Schluss, dass Einsichts- bzw. Auskunftsrechte in bzw. aus staatsanwaltschaftlichen Handakten spezialgesetzlich nicht in der StPO geregelt sind und sich deshalb nach dem allgemeinen Daten-

schutzrecht richten und der Gesetzgeber ersichtlich nicht davon ausging, dass die in der Strafprozessordnung getroffenen Regelungen nicht für sämtliche personenbezogene Daten enthaltene Unterlagen im strafprozessualen Verfahren abschließend sein sollen. Nach Ansicht der Landesregierung ist der Hinweis auf die BT-Drs. 14/2595 zum Strafverfahrensänderungsgesetz 1999 nicht geeignet, ein Einsichtsrecht in staatsanwaltschaftliche Handakten zu begründen.

Die dort zitierten Ausführungen des 6. Ausschusses des Deutschen Bundestages zu dem Gesetzesentwurf beziehen sich auf die Bestimmungen des § 487 StPO des Entwurfs mit dem Inhalt: „Werden personenbezogene Daten in Dateien gespeichert, hat die speichernde Stelle die nach den Datenschutzgesetzen vorgeschriebenen technischen und organisatorischen Maßnahmen zu treffen."

Diese Bestimmung hielt der Ausschuss für überflüssig mit der Begründung: „Einer bereichsspezifischen Regelung, dass die speichernde Stelle die erforderlichen technischen und organisatorischen Maßnahmen zu treffen hat, bedarf es nicht; sie ergibt sich für die speichernden Stellen des Bundes und der Länder bereits aus dem BDSG bzw. den Landesdatenschutzgesetzen. Da die bereichsspezifischen Regelungen der StPO nicht abschließend sind und im Übrigen das BDSG und die Landesdatenschutzgesetze zur Anwendung kommen sollen, ist die Vorschrift entbehrlich."

Damit wird nach Ansicht der Landesregierung nur zum Ausdruck gebracht, dass es damals in der Strafprozessordnung Bereiche gab, die datenschutzrechtlich nicht abschließend geregelt waren, wie beispielsweise der Umgang mit Dateien.
Keineswegs ist damit gesagt, dass die Strafprozessordnung überhaupt keine abschließenden bereichsspezifischen Regelungen kennt. Das Gegenteil ist gerade für die Einsicht in Ermittlungs- und Strafakten der Fall. Hierzu enthalten die Vorschriften der §§ 474 ff. StPO, zu denen noch der § 147 StPO hinzutritt, ersichtlich abschließende Regelungen.

Die Handakten der Staatsanwaltschaft zählen nun allerdings nicht zu den dort genannten Akten (Lüdersen, LR, 25. Aufl., § 147 Rn. 31 und Hillger, LR, § 474 Rn. 5 m. w. N.). Für jene wurden gerade keine besonderen Regelungen geschaffen, weil hierzu keine Notwendigkeit bestand. Sie waren schon immer unzweifelhaft jedem Zugriff Dritter entzogen. Die Handakten, die nach der Aktenordnung (§ 49) „stets in den Händen der Staatsanwaltschaft" bleiben müssen, enthalten nämlich „nur die den inneren Dienst betreffenden Schriftstücke, namentlich den Schriftwechsel über die Sachbehandlung mit vorgesetzten Behörden und Behörden anderer Verwaltungen".

Soweit dort überhaupt personenbezogene Daten aufgenommen sind, handelt es sich um Teile der den Beschuldigten ohnehin in der StPO geregelten Umfang zugänglichen Ermittlungsakten wie z. B. Entwürfe zu Anklageschriften. Hätte der Gesetzgeber Anlass zur Akteneinsicht in die Handakten gesehen, wäre dies in den §§ 474 ff. StPO (die ja ausschließlich dem Datenschutz im Strafverfahren dienen) auch ausdrücklich geregelt und nicht den allgemeinen Datenschutzgesetzen überlassen. Sonst hätte der Gesetzgeber nämlich in Kauf genommen, dass auf die (für Außenstehende bislang unzugänglichen) Handakten eher zugegriffen werden könnte als auf die Hauptakten selbst, deren Einsichtnahme in der StPO gesetzlich beschränkt ist.

18.6 Aktenaufbewahrungsgesetz

Obwohl die Datenschutzbeauftragten des Bundes und der Länder schon viel früher eine gesetzliche Regelung zur Aufbewahrung von Akten und Dateien im weitesten Sinne forderten, kam die Diskussion über die Notwendigkeit derartiger Vorschriften in der Justiz selbst erst im Jahre 2000 in Bewegung. Bis dahin waren die Landesjustizverwaltungen mehrheitlich der Auffassung, dass es besonderer gesetzlicher Aufbewahrungsbestimmungen nicht bedürfe. Nach und nach wurde jedoch ein Regelungsbedarf für die Phase zwischen Verfahrensbeendigung und Aktenübergabe an die Landesarchive gesehen. Hier sind weder die speziellen Verfahrens- noch die Archivgesetze anwendbar.

Die 71. Konferenz der Justizministerinnen und Justizminister vom 24./25. Mai 2000 setzte durch Beschluss zum TOP I.1. eine länderoffene Arbeitsgruppe unter Federführung Nordrhein-Westfalens ein, die geeignete Vorschläge unterbreiten sollte. Bereits zur 72. Konferenz der Justizministerinnen und Justizminister vom 11. bis 13. Juni 2001 lag der Abschlussbericht der Arbeitsgruppe vor. Dieser bildete die Grundlage für die Entscheidung der Justizministerinnen und Justizminister, eine Arbeitsgruppe ins Leben zu rufen, deren Aufgabe es war, den Entwurf für ein Aufbewahrungsgesetz zu erarbeiten. Das Gesetz sollte die grundsätzlichen Voraussetzungen für die Aufbewahrung von Schriftgut der Justiz beinhalten. Darüber hinaus sollte eine Ermächtigung die Länder in die Lage versetzen, die konkreten Aufbewahrungsfristen in abgestimmten Rechtsverordnungen oder Verwaltungsvorschriften zu regeln. Die Federführung wurde auf die Herbstkonferenz am 22. November 2001 vertagt. Dort blieb ein dahingehender Beschluss allerdings aus.

Am 1. April 2005 trat das Gesetz zur Aufbewahrung von Schriftgut der Gerichte des Bundes und des Generalbundesanwalts nach Beendigung des Verfahrens (Schriftgutaufbewahrungsgesetz – SchrAG) vom 22. März 2005 (BGBl. I S. 837, 852) in Kraft. Der Bund hat damit ausschließlich für seine Gerichte und den Generalbundesanwalt geltende Aufbewahrungsvorschriften geschaffen, da er sich für den Bereich der Länder nicht rechtsetzungsbefugt sah. Die 76. Justizministerkonferenz vom 29./30. Juni 2005 forcierte nun die Schaffung von Aufbewahrungsgesetzen der Länder, wozu Nordrhein-Westfalen die Federführung der bereits eingesetzten Arbeitsgruppe übertragen wurde.

Die Arbeitsgruppe legte im Sommer des vergangenen Jahres einen ersten Gesetzentwurf zur Aufbewahrung von Schriftgut in der Justiz vor, der sich inhaltlich am Schriftgutaufgewahrungsgesetz des Bundes orientierte. Die anschließende Diskussion ergab vereinzelten Änderungsbedarf, woraufhin am 4. April 2007 ein überarbeiteter Entwurf übersandt wurde. Diesen haben die Justizministerinnen und Justizminister auf ihrer 78. Konferenz am 28. Juni 2007 durch Beschluss zur Kenntnis genommen. Das MJ hat auf dieser Grundlage einen Gesetzentwurf für das Land Sachsen-Anhalt erarbeitet, der von der Landesregierung im Dezember 2007 zur Anhörung freigegeben worden ist. Die Länder arbeiten bereits an einer einheitlichen Ausführungsverordnung.

18.7 Schülergerichte

Der LfD setzt sich kritisch mit dem Pilotprojekt Schülergerichte auseinander.

Die Tätigkeit der in Sachsen-Anhalt zum Zwecke der deutlichen Abgrenzung von der ordentlichen Gerichtsbarkeit als Schülergremien bezeichneten kriminalpädagogischen Einrichtung ist im staatsanwaltschaftlichen Ermittlungsverfahren angesiedelt. Darin ist in bestimmten Fällen von Jugendkriminalität eine Verfahrensbeendigung ohne Anklageerhebung bzw. Urteil möglich (sog. Diversionsverfahren). Hier sind die Schülergremien aufgefordert, mit Jugendlichen im Alter von 14 bis 17 Jahren Gespräche zu führen, die einer Straftat aus dem Bereich der leichteren Jugendkriminalität beschuldigt werden. Die Mitglieder der Schülergremien stammen aus unterschiedlichen Schulformen. Dabei wird das Modellprojekt mit Schülern eines Gymnasiums und einer Sekundarschule in Halberstadt gestartet. Die Ausbildung der Schüler, die den Gremien angehören werden, wird zum Teil im Rahmen einer Art schulischen Arbeitsgemeinschaft stattfinden.

Die eigentlichen Gremiensitzungen gemeinsam mit den jugendlichen Beschuldigten werden jedoch nicht als schulische Veranstaltung durchgeführt werden, sondern in Zusammenarbeit mit der zuständigen Staatsanwaltschaft Magdeburg – Zweigstelle Halberstadt - und dem zum „Träger und Projektmittler“ ausgewählten Anti-Gewalt-Zentrum Harz e. V. (AGZ e. V.), bei dem es sich um einen gemeinnützigen Verein und anerkannten Träger der Jugendhilfe handelt.

Sofern der jeweilige Beschuldigte mit dem Verfahren vor dem Schülergremium einverstanden ist, unterbreiten die Gremienmitglieder auf der Grundlage eines erzieherischen Gesprächs mit dem Beschuldigten eine Maßnahme, die der Beschuldigte erfüllen soll. Deren Erfüllung wird der Staatsanwaltschaft mitgeteilt, wonach sie in aller Regel das Verfahren außergerichtlich einstellt.

Nach der ersten Konzeption sollte der Projektträger diese Unterrichtung unter Rücksendung der (ihm alleine gemäß § 155b StPO zugeleiteten) Ermittlungsakten vornehmen. Wie noch darzustellen sein wird, plant das MJ eine Verfahrensweise, die den berechtigten Interessen der Verfahrensbeteiligten in datenschutzrechtlicher Hinsicht noch stärker Rechnung tragen wird. Eine Nutzung der Akten durch die Schülergremien selbst ist entgegen der Annahme des LfD in jedem Falle damit nicht verbunden.

Die Landesregierung teilt die Bedenken des LfD gegen die Verhältnismäßigkeit des Verfahrens vor dem Schülergremium nicht.

Handlungsgrundlage für die Tätigkeit der Schülergremien ist nicht lediglich das Einverständnis des Beschuldigten mit der Durchführung des Verfahrens. Vielmehr eröffnet § 45 Abs. 2 des Jugendgerichtsgesetzes der Staatsanwaltschaft als Herrin des strafrechtlichen Ermittlungsverfahrens die Möglichkeit, von der Verfolgung der Tat abzusehen, wenn eine erzieherische Maßnahme bereits durchgeführt oder eingeleitet ist und eine richterliche Beteiligung nicht für erforderlich gehalten wird. Bei den Schülergremien handelt es sich um eine solche erzieherische Maßnahme, die über den bereits erwähnten Trägerverein vermittelt wird. Das Verfahren vor dem Schülergremium stellt sich dabei als ein zusätzliches Angebot an den Beschuldigten im Rahmen der Diversion dar, welches in jedem Fall auf Freiwilligkeit beruht. Die Umstände, warum sich ein Beschuldigter nicht auf ein Verfahren vor dem Schülergremium einlässt, sind denkbar vielfältig, so dass aus der Ablehnung keine Rückschlüsse gezogen werden können, mithin Nachteile hieraus nicht entstehen werden. Die an-

derweitige Erledigung des Ermittlungsverfahrens nach den bisherigen Möglichkeiten der Diversion bleibt unberührt.

Die Beschuldigten werden in einem auf ihren Verständnishorizont zugeschnittenen Merkblatt über das Pilotprojekt aufgeklärt. Zugleich wird ihr schriftliches Einverständnis und jenes der gesetzlichen Vertreter eingeholt, ohne dessen Vorliegen ein Verfahren vor dem Schülergremium nicht stattfindet. Bei dem Projekt wird Wert darauf gelegt, dass alle Verfahrensbeteiligten den Beschuldigten in verständlicher Weise klarmachen, dass ihr Mitwirken freiwillig ist und eine eventuelle Weigerung sanktionslos bleiben wird. Die jugendlichen Mitglieder des Gremiums („Schülerrichter“) erhalten keine Akteneinsicht. Diese wird allenfalls dem Projektleiter des AGZ e. V. gewährt, der die Gremienmitglieder über die dem Beschuldigten zur Last gelegte Tat informiert. Es ist jedoch auch insoweit vorgesehen, dass die Staatsanwaltschaft in der Regel dem Projektleiter lediglich einen Kurzbericht übersendet. Darüber hinaus ist beabsichtigt, die Gremienmitglieder nach dem Verpflichtungsgesetz zu verpflichten. Dies wird in Bayern und Nordrhein-Westfalen, die bereits seit mehreren Jahren die Institution der dort z. T. als „Schülergerichte“ bezeichneten Gremien haben, ebenso gehandhabt. In gleicher Weise verfährt Sachsen, wo im letzten Jahr mit einem entsprechenden Projekt begonnen wurde. In Hamburg findet keine förmliche Verpflichtung der Gremienmitglieder statt.

Das MJ hat mit Schreiben vom 4. April 2007 und vom 15. Mai 2007 dem LfD geantwortet. Darin wurde er auch gebeten, über etwaige Ergänzungs- oder Änderungswünsche zu den mitüberreichten Formularentwürfen zu unterrichten. Die im Schreiben vom 15. Mai 2007 enthaltene ausführliche Stellungnahme hat im Bericht des LfD noch keine Berücksichtigung gefunden. Nachdem dem LfD besagtes Schreiben vorgelegen hatte, hat dieser mit Schreiben vom 20. August 2007 um Übersendung eines weiteren, die Verpflichtungserklärungen erfassenden Formularentwurfs und um einen aktuellen Sachstandsbericht gebeten. Abermalige Kritik im Sinne des Tätigkeitsberichts ist nicht erfolgt.

Zu 19.1 Umstellung der Schulstatistik auf Individualdaten mit bundeseinheitlichem Kerndatensatz

Die Umstellung der Schulstatistik auf Individualdaten mit bundeseinheitlichem Kerndatensatz geht auf einen Beschluss der Kultusministerkonferenz (KMK) aus dem Jahr 2000 zurück. Inhalt und Umfang des Kerndatensatzes wurden durch die KMK festgelegt.

Das Statistische Landesamt führt statistische Erhebungen von Daten im Schulbereich auf der Grundlage des Schulgesetzes des Landes Sachsen-Anhalt durch. Die statistische Aufbereitung erfolgt im abgeschotteten Bereich des Statistischen Landesamtes. Die erhobenen Einzeldaten unterliegen der statistischen Geheimhaltung. Dies trifft auch für die statistische Aufbereitung von Individualdaten in anderen Bildungsstatistiken (Studenten- und Prüfungsstatistik, Personalstatistik an den Hochschulen und Statistik der Berufsbildenden Schulen) zu.

Um Schülerinnen und Schüler während ihrer gesamten Schulzeit begleiten zu können und bei Bedarf die Möglichkeit zu schaffen, Informationen länderübergreifend auszutauschen, sollen alle Schülerinnen und Schüler bundesweit eine Identifizierungsnummer (Schüler-ID) erhalten. Aus statistischer Sicht ist eine Schüler-ID nicht

zwingend erforderlich. Für die statistische Aufbereitung und Plausibilisierung der zu erhebenden Daten aus dem Kerndatensatz ist eine beliebige Kennzeichnung des Datensatzes ausreichend.

Bisher lehnt Sachsen-Anhalt einen nationalen Kerndatensatz grundsätzlich ab. Sollte diese Position aufgegeben werden – auch mit Blick auf Rechtsentwicklungen in anderen Ländern – würden in Sachsen-Anhalt einer Entscheidung über die Einführung des Kerndatensatzes umfassende Prüfungen unter Einbindung des LfD vorausgehen.

Zu 20.5 Zuständigkeit der ARGEn nach dem SGB II

Im Zuge der Kreisgebietsreform ist den Landkreisen mit Blick auf § 44b SGB II mitgeteilt worden, dass je Landkreis nur eine Arbeitsgemeinschaft (ARGE) mit der Arbeitsverwaltung gebildet wird. Die Landkreise sind daher gebeten worden, mehrere Arbeitsgemeinschaften innerhalb eines neuen Landkreises in eine ARGE zu überführen. Die hierzu erforderlichen Vereinbarungen sollten mit den beteiligten Agenturen für Arbeit bereits vorbereitet werden; eine abschließende Entscheidung ist jedoch dem neu gebildeten Landkreis überlassen worden.

Insofern ist die Aussage im Tätigkeitsbericht grundsätzlich richtig, wonach „Veränderungen wohl erst Anfang 2008 zu erwarten seien, wenn die ARGEn innerhalb eines Landkreises fusionieren“. Es ist allerdings zu betonen, dass dies so beabsichtigt war, um dem jeweils neuen Landkreis die Entscheidung – auch über das „Wie“ der Fusion – überlassen zu können.

Zur Zuständigkeit ist festzustellen, dass es nicht in der allgemeinen Verfügungsmacht des Landes oder seiner Kommunen steht, wie die Aufgaben beim Vollzug des SGB II gestaltet werden, denn die Aufgaben sind zwischen dem Bund und den Kommunen geteilt.

Das Land hat die Regionaldirektion der Bundesagentur für Arbeit gebeten, bei der Zusammenlegung der Arbeitsgemeinschaften des SGB II in den neuen Landkreisen behilflich zu sein. Dabei wird auch versucht, die Zuständigkeit für die Arbeitssuchenden des SGB III neuen Agenturen für Arbeit zuzuordnen. Es war und bleibt der ausdrückliche Wunsch des Landes, dass die fünf Zulassungen kommunaler Träger für Anhalt-Zerbst, Bernburg, Merseburg-Querfurt, Schönebeck und Wernigerode erhalten bleiben. Werden diese früheren Landkreise mit "ARGE"-Landkreisen zusammengelegt oder auf solche aufgeteilt, können Arbeitgemeinschaften bestehen bleiben, wenn diese nicht zusammengelegt werden können. Dabei ist bis längstens 31. Dezember 2010 in Kauf zu nehmen, dass früher selbständige Gebietseinheiten von unterschiedlichen Agenturen für Arbeit betreut werden.

Zu 20.14 Fehlbelegungsprüfungen durch den MDK in Krankenhäusern

Die Krankenkassen sind verpflichtet, bei der Erbringung von Leistungen – insbesondere zur Prüfung von Voraussetzungen, Art und Umfang der Leistung – und bei Auffälligkeiten zur Prüfung der ordnungsgemäßen Anrechnung eine gutachtliche Stellungnahme des Medizinischen Dienstes der Krankenkassen (MDK) einzuholen (§ 275 Abs. 1 Nr. 1 SGB V). Dies gilt in den gesetzlich bestimmten Fällen oder wenn es nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krank-

heitsverlauf erforderlich ist. Der MDK darf Sozialdaten erheben und speichern, soweit dies für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen notwendig ist. Haben die Krankenkassen eine gutachtliche Stellungnahme oder Prüfung durch den MDK veranlasst, sind die Leistungserbringer verpflichtet, hierfür erforderliche Sozialdaten auf Anforderung des MDK unmittelbar an diesen zu übermitteln (§ 276 Abs. 2 SGB V). Die MDK-Ärzte sind im Einzelfall und im Rahmen des Erforderlichen zu einer gutachtlichen Stellungnahme über die Notwendigkeit und Dauer der stationären Behandlung des Versicherten befugt, die Räume der Krankenhäuser zu betreten, um dort die Krankenunterlagen einzusehen und den Versicherten untersuchen zu können (§ 276 Abs. 4 SGB V).

Auch Krankenhausbehandlungen sind wie dargelegt vom MDK überprüfbar. Einerseits ist der MDK zur Erhebung und Speicherung von Sozialdaten berechtigt, andererseits sind die Leistungserbringer – also (auch) die Krankenhäuser – verpflichtet, diese Daten dem MDK bereitzustellen. Diese Verpflichtung umfasst insbesondere auch die Bereitstellung von Krankenunterlagen in Kopie. Das Betreten der Krankenhausräume durch den MDK zur Prüfung vor Ort ist lediglich im Einzelfall vorgesehen.

Insoweit werden die Ausführungen des LfD – die Prüfung der Unterlagen habe grundsätzlich im Krankenhaus stattzufinden und die Mitnahme von Kopien sei auf das Unverzichtbare zu reduzieren – nicht geteilt. Im Übrigen hat sich die Anforderung kompletter Unterlagen (in Kopie) zur Prüfung beim MDK im Einzelfall nach dem Erforderlichkeitsgrundsatz auszurichten. Die vom LfD genannten Rechtsgrundlagen finden sich nicht im Krankenhausgesetz des Landes Sachsen-Anhalt. Vielmehr wird inhaltlich auf das Verfahren nach § 17c des Krankenhausfinanzierungsgesetzes über die Prüfung der Abrechnung von Pflegesätzen durch MDK-Stichproben Bezug genommen. Laut der Krankenhausgesellschaft Sachsen-Anhalt sind bisher keine Stichprobenprüfungen auf Grundlage dieses Bundesgesetzes bei den sachsen-anhaltischen Krankenhäusern durch den MDK durchgeführt worden.

Zu 20.19 Schutzauftrag bei Kindeswohlgefährdung – Einführung

Nachdem die Bundesregierung sich ablehnend gegenüber einer bundesgesetzlichen Regelung zur verbindlichen Teilnahme an Kinderuntersuchungen (diese werden im Bericht des LfD als Früherkennungsuntersuchungen bezeichnet) geäußert hat, hat die Landesregierung beschlossen, ein eigenes Gesetz zum Kinderschutz vorzulegen. Dieses Gesetz soll – unter Berücksichtigung von Erfahrungen in anderen Ländern - ein Einladungssystem zu Kinderuntersuchungen vorsehen, wenn Kinder nicht an bestimmten ärztlichen Untersuchungen teilgenommen haben. Kommen die Erziehungsberechtigten den Einladungen nicht nach, soll eine Meldung an das örtliche Jugendamt erfolgen. Das Jugendamt kann dann weitere Schritte unternehmen.

Der LfD wurde sehr früh in die Planungen für das Gesetz einbezogen. Im Laufe des Jahres 2007 fanden mehrere Gespräche zwischen dem Ministerium für Gesundheit und Soziales (MS) und dem LfD statt. Der LfD wird weiterhin informiert.

Zu 20.20 Fragebogen für künftige Pflegeeltern

Der unter Mithilfe der Jugendämter entwickelte Muster-Fragebogen enthält die wichtigsten Fragen, die zukünftigen Pflegeltern gestellt werden. Eine Pflicht der Jugendämter, diesen Fragebogen zu benutzen, besteht nicht, da es sich bei den Hilfen zur

Erziehung nach §§ 27, 33 SGB VIII (Pflegekinderwesen) um eine Aufgabe der Kommunen im eigenen Wirkungskreis handelt. Der Fragebogen soll lediglich eine Arbeitserleichterung für die zuständigen Mitarbeiter der Jugendämter darstellen - er kann den Bedürfnissen des Einzelfalles entsprechend abgeändert werden.

Der Muster-Fragebogen für zukünftige Pflegeeltern befindet sich in einer ständigen qualitativen Weiterentwicklung, wobei die Hinweise des LfD insbesondere unter dem Aspekt der effizienten und sparsamen Datennutzung und berücksichtigt werden.

Zu 20.21 Prüfung von Kindertagesstätten

Hinsichtlich der Zusammenarbeit zwischen Kindertagesstätten und Grundschulen (vgl. Nr.19.4.2) prüft das MS derzeit, wie Eltern in die Erhebung und Nutzung der Daten zur Bildungs- und Entwicklungsbiographie ihrer Kinder einbezogen werden sollen. Es ist zu klären, welche Daten zur Bildungs- und Entwicklungsbiographie von der Grundschule benötigt werden und welche die Kindertageseinrichtungen liefern können.

Da die Einwilligung der Eltern in die Weitergabe dieser Daten an Grundschulen einzuholen ist, empfiehlt es sich hierfür, dass das MS und das MK gemeinsam ein Merkblatt für Eltern erarbeiten, welches über das Bildungsprogramm informiert und für die Datenerhebung und Nutzung „wirbt“. Eltern müssen die Möglichkeit der Kenntnisnahme erhalten, welche Daten ihrer Kinder übermittelt werden sollen. Zur Umsetzung dieses Anliegens wurde eine Arbeitsgruppe aus MS und MK gebildet, die sich mit Fragen zum Übergang zwischen Kindergarten und Schule beschäftigt. Weiterhin ist ein Merkblatt für die Träger von Kindertageseinrichtungen zu entwickeln, welches als Anhang ein Muster einer Einverständniserklärung der Eltern enthalten soll. Beide Merkblätter sollten den Kindertageseinrichtungen zur Verfügung gestellt werden, damit diese den Eltern – ggf. im Rahmen des Abschlusses des Betreuungsvertrages – ausgehändigt werden können.

Der LfD wird rechtzeitig einbezogen.

Zu 22.1 Datenschutz und ein großes Investitionsprojekt: PPP-Burg

Die Landesregierung ist mit dem LfD der Auffassung, dass auch dann, wenn das Land zur Erfüllung seiner Aufgaben im Strafvollzug die Hilfe Privater in Anspruch nimmt, weiterhin öffentlich-rechtliche Grundsätze und damit grundsätzlich die Kontrollzuständigkeit des LfD besteht. Deshalb handelt es sich bei der späten Übermittlung des Datenschutzkonzepts der künftigen JVA Burg auch nicht um den Versuch, den LfD in der Unabhängigkeit seiner Amtsführung zu beeinträchtigen. Vielmehr war der Zeitpunkt der Übermittlung den einschlägigen vergaberechtlichen Vorschriften geschuldet, die anderenfalls ein Verfahren zur Unterzeichnung einer „Vertraulichkeitsvereinbarung“ nach § 16 der Verordnung über die Vergabe öffentlicher Aufträge notwendig gemacht hätten.

Zu 22.2 Kontrollen in Justizvollzugsanstalten

Die Ausführungen des LfD zur grundsätzlichen Unzulässigkeit der Vernichtung von Justizvollzugsakten im Wege der Auftragsdatenverarbeitung sind in zweifacher Hinsicht bemerkenswert.

Erstens zeigen sie die Probleme von Vollregelungen zum Datenschutz in Fachgesetzen auf. Solche Gesetze kommen – das Beispiel der §§ 67 ff SGB X mag dies verdeutlichen – nicht ohne Verweisungen auf einzelne Regelungen des allgemeinen Datenschutzrechts aus. Einfacher, normensparsamer und die Rechtsanwendung erleichternd ist es, fachgesetzlich nur die Abweichungen vom allgemeinen Datenschutzrecht zu regeln. Im vorliegenden Fall kann man sich durchaus fragen, ob der Ausschluss der Auftragsdatenverarbeitung im Bereich des Strafvollzugsrechts vom Gesetzgeber gewollt oder unabsichtlich normiert wurde.

Zweitens hätte der LfD aufzeigen können, wie sich Strafvollzugsbehörden bei der Vernichtung von Strafvollzugsakten der technischen Möglichkeiten von renommierten Unternehmen der Datenträgervernichtung hätten bedienen können, ohne dass Auftragsdatenverarbeitung im Sinne des Datenschutzrechts vorgelegen hätte. Dies ist der Fall, wenn durch technische und organisatorische Vorgaben sichergestellt wird (z. B. durch Aufbewahrung des zu vernichtenden Schriftguts in geschlossenen Behältnissen, die nur durch Justizbedienstete geöffnet werden können, und durch Vernichtung der Unterlagen im Beisein eines Justizbediensteten), dass zu keiner Zeit Mitarbeiter des Aktenentsorgungsunternehmens Kenntnis vom Inhalt der zu vernichtenden Unterlagen erlangen können. In diesem Fall liegt keine Auftragsdatenverarbeitung vor. Das Unternehmen leistet dann nur technische Hilfe, weil es Technik zur Verfügung stellt, über die die Verwaltung nicht verfügt.
Mit dem am 16. November 2007 vom Landtag verabschiedeten Gesetz über den Vollzug der Jugendstrafe in Sachsen-Anhalt (JStVollzG LSA) wird dem Anliegen des LfD Rechnung getragen, klare Rechtsgrundlagen für eine Datenverarbeitung im Auftrag zu schaffen (§ 106 JStVollzG LSA i. V. m. § 8 DSG LSA).

Zu 22.3 Neuregelung für den Jugendstrafvollzug

Die Landesregierung begrüßt das Angebot des LfD, alle damit zusammenhängenden Vorhaben beratend zu begleiten. Dementsprechend wurde der LfD an der Erarbeitung des Entwurfs eines Jugendstrafvollzugsgesetzes Sachsen-Anhalt beteiligt. Auch hatte er Gelegenheit, im Rahmen der Anhörung durch den Ausschuss für Recht und Verfassung am 12. September 2007 seine Position darzustellen. Zudem ist der LfD in die Erarbeitung der Verwaltungsvorschriften zu diesem Gesetz eingebunden worden. Die Landesregierung geht davon aus, dass sie der LfD auch bei künftigen Gesetzen zum Strafvollzug beraten wird.

Zu 23.2 Speicherung von IP-Adressen

Es wurde eine einvernehmliche Lösung erarbeitet. Eine Speicherung von IP-Adressen ist für statistische Auswertungen nicht nötig und auch organisatorisch durch den Dienstleister, das Landesinformationszentrum (LIZ), nicht realisierbar. IP-Adressen werden jedoch mit Zustimmung des LfD zur Missbrauchsbekämpfung und für technische Schutzmaßnahmen fünf Tage gesichert, bevor sie überschrieben werden. Die rechtliche Grundlage für dieses Vorgehen sind §§ 100, 109 des Telekommunikationsgesetz (TKG).

Zu 23.5 E-Mail und Internet am Arbeitsplatz – Spamfilterung bei privater E-Mail-Nutzung

Der LfD hat die Änderung der Musterdienstanweisung über die Bereitstellung und Nutzung von Internetzugängen angemahnt. Diese Änderung sollte eigentlich kurz nach Veröffentlichung seines aktuellen Tätigkeitsberichts durch einen Beschluss der Staatssekretärskonferenz herbeigeführt werden. Die Beschlussfassung musste aber zurückgestellt werden, da der LfD gegen den Entwurf einer Vorlage für die Staatssekretärskonferenz mit Schreiben vom 5. September 2007 erneut Vorbehalte anbrachte. Dies überraschte insoweit, als alle Formulierungsvorschläge des LfD berücksichtigt worden waren, die dieser mit Schreiben vom 27. März 2006 für den Fall vorgelegt hatte, dass weiterhin die ausnahmsweise private Nutzung des Internets einschließlich der Verwendung der dienstlichen E-Mail-Adresse durch Mitarbeiter geduldet werden sollte. Der LfD fordert in seinem Schreiben vom 5. September 2007, die private Nutzung des dienstlichen E-Mail-Dienstes zu untersagen und die Mitarbeiter auf die Inanspruchnahme anderer Web-Mail-Server zu verweisen.

Der LfD hat am 5. September 2007 auch darauf hingewiesen, dass der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die bestehende Orientierungshilfe zur Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz überarbeitet. Diese Orientierungshilfe hat der LfD dem MI mit Schreiben vom 13. November 2007 zugeleitet. Unter Berücksichtigung der angeführten Schreiben und neuerer Gutachten wird in Kürze die Musterdienstanweisung nochmals überarbeitet. Sie dürfte – unter Einbindung des LfD – Anfang 2008 vorliegen.

Zu 24.2 GIAZ

Das Gemeinsame Informations- und Analysezentrum islamistischer Terrorismus (GIAZ) ist im Landeskriminalamt Sachsen-Anhalt angesiedelt und mit Angehörigen des LKA und der Verfassungsschutzbehörde besetzt. Durch das GIAZ sind insbesondere folgende Aufgaben wahrzunehmen:

1. Zusammenführung von Informationen/Erkenntnissen insbesondere von Polizei und Verfassungsschutz,

2. gemeinsame Auswertung und Analyse dieser Erkenntnisse mit dem Ziel,

   - aktuelle Gefährdungslagebeurteilungen zu erstellen,

   - Ermittlungsansätze (präventiv und repressiv) zu gewinnen,

   - Maßnahmen abzustimmen und zu koordinieren sowie

   - bestehende Informationssysteme effizienter zu nutzen.

3. Verbindungsstelle zu den Informations- und Analysestellen des Bundes und anderer Länder.

Der LfD führt zutreffend aus, dass die Zusammenarbeit von Polizei und Verfassungsschutz durch das Trennungsgebot begrenzt wird.

Der LfD bemängelt, dass ihm bis zum 31. März 2007 - also bis zum Ende des Berichtszeitraumes - keine Darstellung über eine seinen Vorstellungen entsprechende

Evaluierung geliefert wurde. Diese Aussage ist irreführend, denn kurz darauf - mit Schreiben vom 4. Mai 2007 - wurde dem LfD insbesondere mitgeteilt, dass eine Evaluierung stattgefunden habe mit dem Ergebnis, dass die Weiterführung des GIAZ erforderlich sei. Dem LfD wurde zwecks weitergehender Erörterung und Auswertung der Evaluierungsergebnisse sowohl ein Besuch im GIAZ als auch persönliche Gespräche angeboten. Eine Reaktion des LfD hierauf erfolgte bisher nicht.

Mit dem GIAZ ist in Sachsen-Anhalt eine zentrale Stelle geschaffen worden, die maßgeblich dazu beitragen soll, den islamistischen Extremismus und Terrorismus ganzheitlich zu bekämpfen. Im GIAZ werden auf der Grundlage bestehender gesetzlicher Regelungen unter anderem Informationsbeziehungen geknüpft und der Informationsaustausch deutlich beschleunigt. Außerdem haben die beteiligten Stellen zulässigerweise Erkenntnisse unterschiedlicher Art und Qualität gewonnen, die sie ohne GIAZ so nicht erlangt hätten.

Die Sicherheitsbehörden haben durch GIAZ einen deutlich besseren Überblick auch über in Sachsen-Anhalt bestehende islamistische Strukturen, Kontakte und Beziehungen. Hierin liegt der Mehrwert für die Stellen, die unmittelbar (Polizei, Verfassungsschutz) und mittelbar (z. B. Ausländerbehörden, Staatsanwaltschaften, Justizvollzugsanstalten) beteiligt sind.

Zu 24.4 Änderung des Verfassungsschutzgesetzes

Das Gesetz zur Änderung verfassungsschutzrechtlicher Vorschriften und zur Stärkung des Verfassungsschutzes ist am 2. Februar 2006 in Kraft getreten. Zu kritischen Anmerkungen des LfD wird nicht Stellung genommen (vgl. auch Vorbemerkung S. 1 Abs. 2).

Zu 24.5 Beobachtung von Demonstranten

Das Instrument der Videoaufzeichnung wird von der Verfassungsschutzbehörde bei Demonstrationen zurückhaltend und ausschließlich zur Informationsgewinnung eingesetzt. Dies geschieht im Rahmen der Aufgabenerfüllung nach § 4 des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt (VerfSchG-LSA) mit den nach § 7 VerfSchG-LSA zur Verfügung stehenden Befugnissen. Danach dürfen gem. § 7 Abs. 3 VerfSchG-LSA u. a. Informationen mit Hilfe von Bild- und Tonaufzeichnungen verdeckt erhoben werden. Die Durchführung einer solchen Maßnahme stellt zwar einen Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 6 VerfLSA, nicht aber eine Einschränkung des Grundrechts der Versammlungsfreiheit aus Art. 8 GG dar.

Die Verfassungsschutzbehörde beobachtet im Rahmen ihrer Aufgaben Bestrebungen gegen die freiheitliche demokratische Grundordnung. Das ist ausdrücklich in § 4 VerfSchG-LSA geregelt. Sie darf dabei gem. § 7 Abs. 3 VerfSchG-LSA nachrichtendienstliche Mittel – auch Bild- und Tonaufzeichnungen – einsetzen. Dies ist im VerfSchG-LSA für jedermann nachlesbar. Wer also an Versammlungen teilnimmt, bei denen extremistische Inhalte transportiert werden, muss ohnehin davon ausgehen, dass eine solche Veranstaltung beobachtet wird. Die Umstände, die zu einer möglichen Beobachtung führen, sind für den Grundrechtsträger damit nachvollziehbar.

Der Verzicht auf die Teilnahme an einer Versammlung durch Einflussnahme des Staates erscheint im Falle des § 20 des Versammlungsgesetzes (VersG) viel wahrscheinlicher. Zwar wird hier auf die Einschränkung des Grundrechts aus Art. 8 GG hingewiesen, jedoch ist die Befugnis der Polizei, Bild- und Tonaufzeichnungen zu fertigen, nach § 12a VersG an das Vorliegen bestimmter Voraussetzungen gebunden. Ob diese Voraussetzungen im Rahmen einer Veranstaltung gegeben sind und in der Folge tatsächlich Aufzeichnungen erfolgen, erschließt sich dem Grundrechtsträger nicht. Entsprechend ist der Unsicherheitsfaktor für ihn hier erheblich größer als im Falle des § 7 Abs. 3 VerfSchG-LSA.

Zu 25.1 Kfz-Zulassungsvoraussetzungsgesetz

Zutreffend stellt der LfD dar, dass der Ursprungsentwurf des Kfz-Zulassungsvoraussetzungsgesetzes, zu dem er eine zustimmende Stellungnahme abgegeben hatte, kurz vor der abschließenden Kabinettsbefassung geändert und so dem Landtag im Oktober 2006 zur Beschlussfassung zugeleitet wurde.

Sofern der LfD nach § 40 GGO LSA I Gelegenheit hatte, zu einem Gesetzentwurf Stellung zu nehmen, löst eine spätere Änderung des Gesetzentwurfs in datenschutzrelevanten Punkten keine erneute Pflicht zur Beteiligung des LfD aus. Seine Stellungnahme dient der Beratung der Landesregierung, entfaltet aber keine Bindungswirkung. Der LfD kann im weiteren Gesetzgebungsverfahren, insbesondere während der Beratung durch die Ausschüsse des Landtages, seine Vorstellungen einbringen. Hat zu einem Gesetzentwurf eine Anhörung stattgefunden, wird regelmäßig deren Ergebnis im Vorblatt oder in der Begründung zum Gesetzentwurf dargestellt; dies gilt auch hinsichtlich der Anhörung des LfD.

Die Feststellung des LfD, dass eine Reaktion des MLV auf eine kritische Wertung vom November 2006 ausgeblieben sei, trifft nicht zu. Vielmehr fanden mehrere Gespräche mit dem LfD statt. Der Pflicht zur Beteiligung des LfD nach der GGO LSA I wurde somit Genüge getan.

Zu der weitergehenden Anregung des LfD, durch eine Änderung des Straßenverkehrsgesetzes und der seit 1. März 2007 geltenden Fahrzeug-Zulassungsverordnung (FZV) eine klare Verknüpfung des Zulassungsrechts mit dem Gebührenrecht zu schaffen, wird auf Folgendes hingewiesen:

Mit der FZV ist das Prinzip der Standortzulassung der Fahrzeuge aufgegeben worden. Nunmehr ist das Fahrzeug am Wohnort des Halters zuzulassen. Wollte man, um der Gebührenerhebung zu entgehen, sein Fahrzeug bei einer anderen Zulassungsbehörde zulassen, müsste gleichzeitig der Wohnsitz (Hauptwohnung) verlegt werden. Da die hiermit verbundenen Kosten die Gebührenrückstände im Einzelfall bei weitem übersteigen dürften, wird dieser Fall nur selten vorkommen. Andererseits wäre die tagesaktuelle landes- bzw. bundesweite Rückstandsmeldung durch die Zulassungsbehörde mit einem erheblichen Verwaltungsaufwand verbunden. Zudem sind die Mittel und Möglichkeiten des Verwaltungsvollstreckungsrechts weiterhin gegeben und können in den wenigen Fällen eines Wohnsitzwechsels angewendet werden. Daher wird zunächst eine entsprechende Gesetzesänderung nicht als notwendig erachtet. Sollten die Erfahrungen in der Praxis diese Annahme nicht bestätigen, wird in der Zukunft erneut über eine dementsprechende Bundesratsinitiative des Landes Sachsen-Anhalt zu entscheiden sein.

Mitteilung
der Regierung der Bundesrepublik Deutschland
an die Kommission der Europäischen Gemeinschaften
vom 13. Februar 2007

Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland gemäß Artikel 226 EG-Vertrag
hier: Umsetzung der Richtlinie 95/46/EG in innerstaatliches Recht

- Verfahren Nr. 2003 / 4820 -

Bezug: - Aufforderungsschreiben der EG-Kommission vom 05.07.2005
- Mitteilung der Bundesregierung vom 12.09.2005
- Mit Gründen versehene Stellungnahme der EG-Kommission vom 12.12.2006

Anlagen: - 2 -

Die Bundesregierung beehrt sich, der Kommission der Europäischen Gemeinschaften folgendes mitzuteilen:

A. ZUSAMMENFASSUNG

I.

Die Europäische Kommission legt in ihrer begründeten Stellungnahme vom 12. Dezember 2006 ihre Rechtsauffassung dar, dass die Bundesrepublik Deutschland gegen ihre Verpflichtung aus Art. 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG (im Folgenden: Richtlinie) verstoßen habe, indem sie die für die Überwachung der Datenverarbeitung im nicht-öffentlichen Bereich zuständigen Kontrollstellen in den 16 deutschen Ländern einer staatlichen Aufsicht unterwerfe und damit die Vorgabe einer „völligen Unabhängigkeit" der Datenschutz-Aufsichtsbehörden fehlerhaft umsetze. Die Mitgliedstaaten seien verpflichtet, Regelungen zu treffen, die eine institutionelle, funktionelle und materielle Unabhängigkeit der Aufsichtsbehörden gewährleisten. Danach dürften diese keiner anderen Staatsgewalt untergeordnet sein (institutionelle Unabhängigkeit), in Bezug auf den Inhalt und Umfang ihrer Tätigkeit keinerlei Weisungen unterliegen (funktionelle Unabhängigkeit), und müssten selbständig über einen eigenen Haushalt verfügen können (materielle Unabhängigkeit).

Hiermit unvereinbar sei es, die Wahrnehmung der Datenschutzaufsicht für den nicht-öffentlichen Bereich Behörden der allgemeinen Verwaltung zu übertragen. Auch die Übertragung der Aufgabe auf die Landesdatenschutzbeauftragten sei mit Art. 28 Abs. 1 Satz 2 der Richtlinie unvereinbar, soweit die Landesdatenschutzbeauftragten einer inhaltlichen und/oder organisatorischen staatlichen Aufsicht unterworfen seien.

II.

Die Bundesrepublik Deutschland hält demgegenüber an ihrer zuletzt mit Schreiben vom 12. September 2005 an die Kommission übermittelten Auffassung fest, dass die Organisation der Datenschutzkontrolle in Deutschland der Richtlinie entspricht. Die Aufsichtsbehörden nehmen ihre Aufgaben in der von Art. 28 Abs. 1 Satz 2 der Richtlinie geforderten völligen Unabhängigkeit wahr. Mit "Unabhängigkeit" meint die Richtlinie eine funktionelle Unabhängigkeit in dem Sinne, dass die Aufsichtsbehörden bei der Wahrnehmung ihrer Aufgaben unabhängig von den Stellen sein müssen, die ihrer Datenschutzkontrolle unterliegen. Eine darüber hinaus gehende Unabhängigkeit insbesondere in organisatorischer Hinsicht verlangt die Richtlinie nicht und wäre auch nicht durch die Kompetenz der Gemeinschaft gem. Art. 95 EG zum Erlass der Richtlinie gedeckt.

B. SACHVERHALT

I.

Das Datenschutzrecht in Deutschland unterscheidet bereits im Ansatz zwischen Datenschutz im öffentlichen sowie im nicht-öffentlichen Bereich und trifft insoweit jeweils besondere Regelungen. Für die Datenverarbeitung der öffentlichen Stellen des Bundes, d. h. für Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes gelten insbesondere die §§ 12 bis 21 Bundesdatenschutzgesetz (BDSG). Für die Datenverarbeitung der öffentlichen Stellen der Länder und Kommunen treffen die Landesdatenschutzgesetze die einschlägigen Regelungen. Die Datenverarbeitung nicht-öffentlicher Stellen ist insbesondere durch §§ 27 bis 35 BDSG geregelt.

Diese Regelungstechnik, die in der Richtlinie 95/46/EG nicht angelegt, aber unstreitig mit ihr vereinbar ist, spiegelt sich in der Organisation der Datenschutzaufsicht in Deutschland wider: Die Datenschutzkontrolle bei den öffentlichen Stellen des Bundes obliegt gem. § 24 Abs. 1 BDSG dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Für die Datenschutzkontrolle bei den öffentlichen Stellen der Länder und Kommunen sind die jeweiligen Landesdatenschutzbeauftragten zuständig. Die Datenschutzkontrolle bei nicht-öffentlichen Stellen ist nach § 38 Abs. 1 Satz 1 BDSG Aufgabe der Datenschutz-Aufsichtsbehörden. Diese werden nach § 38 Abs. 6 BDSG durch die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmt und unterliegen, abhängig von den im Einzelnen unterschiedlichen Regelungen in den Ländern, teils einer Fach- und teils einer bloßen Rechtsaufsicht eines Landesministeriums oder der Landesregierung. In den Ländern Baden-Württemberg, Brandenburg, Niedersachsen und Saarland wird die Datenschutzaufsicht über den nicht-öffentlichen Bereich durch das Innenministerium selbst geführt.

Der Datenschutzkontrolle über den öffentlichen und über den nicht-öffentlichen Bereich ist gemeinsam, dass die jeweilige Kontrollstelle stets völlig unabhängig von denjenigen Stellen ist, die von ihr kontrolliert werden: Die Beauftragten für den Datenschutz des Bundes und der Länder sind von den jeweiligen Parlamenten (Bundestag und Landesparlamente) gewählte Beauftragte, die nur diesen rechenschaftspflichtig sind. Sie unterliegen keinerlei Aufsicht, Weisungen oder sonstigem Einfluss durch die öffentlichen Stellen, die von ihnen kontrolliert werden. Der im Einzelnen unterschiedlichen Organisation der Datenschutz-Aufsichtsbehörden für den nicht-öffentlichen Bereich ist gemeinsam, dass diese keinerlei Aufsicht, Weisungen oder sonstigem Einfluss durch die nicht-öffentlichen Stellen unterliegen, die von ihnen kontrolliert werden.

II.

Der Sachverhalt, von dem die begründete Stellungnahme ausgeht, bedarf im Übrigen der Aktualisierung.

Die Kommission nimmt an, dass im Land Sachsen die Datenschutzaufsicht im nicht-öffentlichen Bereich durch eine Behörde der Mittelinstanz in der allgemeinen Landesverwaltung wahrgenommen wird (I. 4.). Durch Gesetz vom 14. Dezember 2006 zur Neufassung des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz, Sächsisches Gesetz- und Verordnungsblatt 2006, Seite 530, Anlage 1) ist die Aufsicht über den nicht-öffentlichen Bereich indes dem Sächsischen Datenschutzbeauftragten übertragen worden, § 30a Satz 1 Sächsisches Datenschutzgesetz.

Im Land Niedersachsen wird die Datenschutzaufsicht über den nicht-öffentlichen Bereich seit dem 1. Februar 2007 wieder durch den Landesbeauftragten für den Datenschutz geführt. Dies hat die Landesregierung Niedersachsen am 19. Dezember 2006 beschlossen (Niedersächsisches Ministerialblatt Nr. 6/2007, S. 108, Anlage 2). Die begründete Stellungnahme geht noch davon aus, dass das Niedersächsische Ministerium für Inneres und Sport Aufsichtsbehörde ist.

C. Rechtliche Würdigung der begründeten Stellungnahme vom 12. Dezember 2006

I.

Art. 28 Abs. 1 Satz 2 der Richtlinie verlangt keine institutionelle Unabhängigkeit der Datenschutz-Aufsichtsbehörden in dem Sinne, dass diese keiner anderen Staatsgewalt untergeordnet sein dürfen. Bereits aus dem Wortlaut der Vorschrift ergibt sich, dass das Erfordernis der Unabhängigkeit nicht für die institutionelle Stellung, sondern für die Art und Weise der Aufgabenwahrnehmung der Aufsichtsbehörden gilt. Die Kommission gesteht unter Punkt II.15. (3. Absatz) der begründeten Stellungnahme vom 12. Dezember 2006 selbst zu, dass der Wortlaut der Richtlinie einer Auslegung entgegensteht, die eine unabhängige organisatorische Stellung der Aufsichtsbehörde verlangt. Für die Behauptung der Kommission, dass Art. 28 Abs. 1 Satz 2 der Richtlinie nur ein weiteres Erfordernis neben einer ohnehin gebotenen organisatorisch-institutionellen Unabhängigkeit der Aufsichtsbehörden schaffe, ist jedoch keine Begründung erkennbar – gerade auch unter dem Blickwinkel der praktischen Wirksamkeit des Gemeinschaftsrechts (*effet utile*). Denn der *effet utile*-Grundsatz verlangt eine Auslegung, die dem Gemeinschaftsrecht zur vollen Entfaltung verhilft, nicht aber eine Interpretation, die die Richtlinie über den Wortlaut hinaus ausdehnt.

Der Hinweis der Kommission auf Art. 286 EG geht fehl. Art. 286 Abs. 1 EG verpflichtet die Organe und Einrichtungen der Gemeinschaft zur Einhaltung von Rechtsakten der Gemeinschaft zum Datenschutz. Absatz 2 der Norm befasst sich mit der Einrichtung einer unabhängigen Kontrollinstanz, der nur die Datenschutzkontrolle bei Organen und Einrichtungen der Gemeinschaft obliegt. Der Europäische Datenschutzbeauftragte ist insoweit mit der Stellung der Datenschutzbeauftragten in Bund und Ländern vergleichbar, die bei der Kontrolle des Datenschutzes im öffentlichen Bereich in gleicher Weise unabhängig sind. Für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ergibt sich dies beispielsweise aus § 22 Abs. 4 Satz 2 BDSG. Diese Beauftragten sind indes Einrichtungen zur Verwaltungskontrolle ohne eigene Durchsetzungsbefugnisse. Im Gegensatz dazu haben die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, deren Stellung Gegenstand des Vertragsverletzungsverfahrens ist, Eingriffsbefugnisse gegenüber außenstehenden Dritten, die insbe-

sondere Grundrechtsträger sind und daher auch und gerade nach Gemeinschaftsrecht besonderen rechtlichen Schutz genießen (vgl. EuGH, Urteil v. 21. September 1989, verb. Rs. 46/87 und 227/88, *Hoechst/Kommission*, Slg. 1989, 2859, Rn. 19).

Auch der Verweis auf Art. 8 der Charta der Grundrechte der Europäischen Union vermag ein Erfordernis für eine institutionelle Unabhängigkeit der Datenschutzaufsichtsbehörden für den nichtöffentlichen Bereich nicht zu begründen. Zwar sieht Art. 8 Abs. 3 der Charta vor, dass die Einhaltung der Vorschriften zum Datenschutz von einer unabhängigen Stelle überwacht wird. Dies ist in Deutschland jedoch gerade der Fall. Art. 8 Abs. 3 der Charta – die bisher übrigens lediglich indikative Wirkung hat und noch nicht verbindliches Recht darstellt (vgl. EuGH, Urteil vom 27. Juni 2006, Rs. C-540/03, *EP/Rat*, Slg. 2006, I-5769, Rn. 38) – geht schon vom Wortlaut nicht über die Regelung in Art. 28 Abs. 1 der Richtlinie hinaus und kann daher keine erweiternde Auslegung rechtfertigen.

II.

Mit "Unabhängigkeit" meint Art. 28 Abs. 1 Satz 2 der Richtlinie eine funktionelle Unabhängigkeit in dem Sinne, dass die Aufsichtsbehörden bei der Wahrnehmung ihrer Aufgaben unabhängig von den Stellen sein müssen, die ihrer Datenschutzkontrolle unterliegen. Sie dürfen darüber hinaus keinen sachfremden Einflüssen ausgesetzt sein. Eine noch weiter gehende Unabhängigkeit verlangt die Richtlinie nicht. Insbesondere verbietet sie es nicht, die Datenschutzaufsichtsbehörden für den nichtöffentlichen Bereich rechtmäßigen Weisungen anderer staatlicher Stellen zu unterwerfen. Dabei haben sich diese Weisungen im Rahmen dessen zu halten, was insbesondere die Bindung der Verwaltung an Gesetz und Recht, der Gleichbehandlungsgrundsatz und die Kontrolle der Verwaltung durch Parlament und Gerichte ge-statten.

1.

Dem stehen weder Art. 1 Nr. 3 des Zusatzprotokolls zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr noch Ziffer 17 des erläuternden Berichts entgegen.
Ob das bisher erst von 12 EU-Mitgliedstaaten ratifizierte Zusatzprotokoll zur Auslegung von Gemeinschaftsrecht herangezogen werden kann, mag dahinstehen. Es verlangt jedenfalls keine erweiternde Auslegung der Richtlinie, da es den gleichen Wortlaut hat. Zudem ist dieses Zusatzprotokoll in der Bundesrepublik Deutschland nur nach Maßgabe folgender Erklärung in Kraft getreten (Bekanntmachung vom 8. Juni 2004 - BGBl. II, S. 1093):

> „Artikel 1 Abs. 3 des Zusatzprotokolls sieht (ebenso wie Absatz 2 der Präambel) vor, dass die Kontrollstellen ihre Aufgaben in völliger Unabhängigkeit wahrnehmen.
>
> Die Bundesrepublik Deutschland erinnert an ihre bereits in der Sitzung des Beratenden Ausschusses nach Artikel 18 der Datenschutzkonvention vom 6. bis 8. Juni 2000 abgegebene Erklärung, dass die bestehende Praxis der Datenschutzkontrolle in Deutschland die Anforderungen von Artikel 1 Abs. 3 des Zusatzprotokolls erfüllt, weil die Datenschutz-Kontrollstellen – auch soweit sie in einen hierarchischen Verwaltungsaufbau eingebunden sind – ihre Aufgaben in völliger Unabhängigkeit wahrnehmen."

Diese Erklärung wurde auch deshalb abgegeben, weil die Europäische Kommission teilweise von der bei der Verabschiedung der EG-Datenschutzrichtlinie erzielten Verständigung über das Wesen unabhängiger Aufgabenwahrnehmung abzurücken begann.

Der erläuternde Bericht zum Zusatzprotokoll hingegen hat keinerlei Rechtswirkungen. Im Vorspruch zum erläuternden Bericht (vor Ziff. 1, erhältlich unter: <http://conventions.coe.int/Treaty/en/Reports/Html/181.htm>) wird dies vom Europarat eindeutig klargestellt:

> „The text of this explanatory report does not constitute an instrument providing an authoritative interpretation of the Protocol, although it might be of such a nature as to facilitate the application of the provisions contained therein."

Auch der Hinweis der Kommission auf das Urteil des Europäischen Gerichtshofs „Österreichischer Rundfunk u. a." (EuGH, Verbundene Rechtssachen C-465/00, C-138/01 und C-139/00, Urteil vom 20. Mai 2003) geht fehl, nach dem einzelstaatliche Regelungen, die unvereinbar mit Artikel 8 der Europäischen Menschenrechtskonvention sind, auch nicht den Anforderungen der Datenschutzrichtlinie 95/46/EG genügen können. Eine Verletzung von Art. 8 der Europäischen Menschenrechtskonvention ist nicht ersichtlich – auch mit Blick auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte.

2.
Die von der Bundesrepublik Deutschland vertretene Position zur Auslegung von Art. 28 Abs. 1 Satz 2 der Richtlinie wird durch die Entstehungsgeschichte der Vorschrift gestützt. Deutschland hat sich seit den ersten Beratungen zur EG-Datenschutzrichtlinie dafür eingesetzt, dass die hier bestehende Organisation der Datenschutzaufsicht beibehalten werden kann (vgl. Beschluss des Bundesrates vom 14.12.1990, BR-Drs. 690/90, Nr. 7). Daher hat sich Deutschland in den Beratungen auch gegen den von der Kommission zunächst vorgelegten Entwurf der Vorschrift ausgesprochen, der noch eine organisatorische Unabhängigkeit der Datenschutzaufsichtsbehörden vorsah. Dieser lautete:

„Jeder Mitgliedstaat benennt eine unabhängige staatliche Behörde, die für die Gewährleistung des Datenschutzes zuständig ist."

Nur mit der hier vertretenen Auslegung hat die deutsche Delegation der Kompromissformulierung der Kommission für den schließlich beschlossenen Art. 28 Abs. 1 Satz 2 der Richtlinie zugestimmt. Der Vorsitzende der Ratsarbeitsgruppe im 2. Halbjahr 1994, der Bundesbeauftragte für den Datenschutz Dr. Joachim Jacob, hat in der entscheidenden Sitzung im September 1994 das deutsche System der Datenschutzaufsicht erläutert und erklärt, dass das deutsche Kontrollsystem mit der Forderung nach funktionaler Unabhängigkeit i. S. v. Art. 28 Abs. 1 Satz 2 der Richtlinie vereinbar sei. Hiergegen wurde in der Ratsarbeitsgruppe kein Widerspruch erhoben.

Vielmehr hat der Vertreter der Kommission zur Frage der Unabhängigkeit der Kontrollbehörden für den nichtöffentlichen Bereich in der Vorbesprechung zur Sitzung der Gruppe „Wirtschaftsfragen (Datenschutz)" am 12./13./14. September 1994 ausgeführt, die Formulierung ziele auf Unabhängigkeit von der zu kontrollierenden Stelle sowie auf die Vermeidung rechtswidriger Einflüsse auf die Aufsichtstätigkeit ab. Die Möglichkeit eines als oberste Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich zuständigen Ressortministers, innerhalb seines Verantwortungsbereichs Weisungen zu erteilen, sowie dessen Verantwortlichkeit gegenüber dem Parlament würden nicht angetastet. Das deutsche Kontrollsystem entspreche den Vorstellungen der Richtlinie. Da von diesen Maßstäben auch die anderen Mitgliedstaaten - wie selbstverständlich – ausgingen, sei eine weitere Präzisierung des Textes nicht erforderlich.

Dagegen vertritt die Kommission in der begründeten Stellungnahme vom 12. Dezember 2006 die Auffassung, die schließlich beschlossene Fassung der Richtlinie schmälere nicht die im ursprünglichen Entwurf vorgesehene Unabhängigkeit der Aufsichtsbehörden, sondern stärke sie (Punkt II.15), indem sie nicht (nur) eine unabhängige organisatorische Stellung, sondern auch unabhängiges Handeln der Aufsichtsbehörden gebiete. Wie dargelegt, ist dies mit der Entstehungsgeschichte der Vorschrift unvereinbar.

3.

Ob bei einer solchen Auslegung die gemäß Art. 95 i.V.m. 251 EG-Vertrag erforderliche qualifizierte Mehrheit im Rat für die Richtlinie zustande gekommen wäre, ist zu bezweifeln. Die Bundesrepublik Deutschland hätte der Richtlinie 95/46/EG jedenfalls nicht zustimmen können, wenn sie neben der funktionalen Unabhängigkeit von den zu kontrollierenden Stellen auch eine organisatorische Unabhängigkeit der Kontrollstellen verlangen würde. Denn die Übertragung der Aufgabe der Datenschutzaufsicht über die Privatwirtschaft auf eine von der Exekutive völlig unabhängige Institution wäre mit deutschem Verfassungsrecht – und wohl auch mit europäischen Verfassungsprinzipien – nicht vereinbar. Das in Art. 6 Abs. 1 EU-Vertrag und Art. 20 Abs. 2, Art. 28 Abs. 1 GG verankerte Demokratieprinzip und der Grundsatz der parlamentarischen Verantwortung der Regierung verlangen grundsätzlich die Abhängigkeit aller Amtswalter von Weisungen des zuständigen Ressortministers, der einer kontinuierlichen Kontrolle durch das Parlament unterliegt. Aus dem Demokratieprinzip folgt eine grundsätzliche Weisungsgebundenheit der Verwaltung gegenüber der Regierung (vgl. zum deutschen Verfassungsrecht: BVerfGE 93, 37 ff., 66 ff.). Nach deutschem Verfassungsverständnis dürfen insbesondere Eingriffe in die Rechte der Bürger und Unternehmen, wie sie die Datenschutz-Aufsichtsbehörden in Ausübung ihrer Anordnungen, Betretungs- und Einsichtsbefugnisse vornehmen (Art. 28 Abs. 3 Richtlinie 95/46/EG), nur durch Hoheitsträger erfolgen, bei denen zumindest die Rechtsaufsicht des zuständigen Ressortministers gewährleistet ist. Diese Grundsätze sind – über Art. 6 EU-Vertrag – auch der europäischen Rechtsordnung inhärent.

Daher geht auch der Hinweis der Kommission auf S. 12 der begründeten Stellungnahme fehl (Punkt II.22). Die dort angeführten Stellen greifen entweder nicht unmittelbar in die Rechte Einzelner ein oder unterstehen gerade doch einer – zumindest mittelbaren – Aufsicht (vgl. § 52 Gesetz gegen Wettbewerbsbeschränkungen).

Dem kann die Kommission nicht mit Hinweis auf die parlamentarische Verantwortung der Datenschutzbeauftragten des Bundes und der Länder entgegnen. Denn bei den Datenschutzbeauftragten handelt es sich um Einrichtungen der Verwaltungskontrolle, bei denen sich die Frage der Grundrechtsbeeinträchtigung nicht stellt. Im Gegensatz dazu verfügen die Datenschutz-Aufsichtsbehörden für den nicht-öffentlichen Bereich über Eingriffsbefugnisse gegenüber Grundrechtsträgern.

III.

Bei der Auslegung von Artikel 28 Abs. 1 Satz 2 der Richtlinie sind zudem die gemeinschaftsrechtlichen Kompetenz- und Kompetenzausübungsregeln zu beachten.

1.

Die Gemeinschaft darf gemäß dem in Art. 5 Abs. 1 EG statuierten Prinzip der begrenzten Einzelermächtigung und der Subsidiarität nur innerhalb der Grenzen der ihr in diesem Vertrag zugewiesenen Befugnisse und gesetzten Ziele tätig werden. Die Europäische Gemeinschaft hätte dagegen keine Kompetenz, gestützt auf die sog. Binnenmarktklausel des Art. 95 EG eine Regelung zu erlassen, nach der zwingend eine organisatorische Unabhängigkeit der Datenschutzaufsicht erforderlich ist. Dies zeigt gerade auch die von der Kommission herangezogene Rechtsprechung des EuGH (Punkt II.24 der begründeten Stellungnahme). Denn eine organisatorische Regelung des Verwaltungsaufbaus für Aufsichtsbehörden dient nicht den Zwecken des Binnenmarktes. Die von der Kommission ebenfalls ins Feld geführte Charta der Grundrechte kann keinesfalls eine Kompetenz der EG begründen. Dies ergibt sich zunächst schon aus der Rechtsnatur der Charta, aber vor allem aus ihrem Wortlaut: Art. 51 Abs. 2 der Charta stellt klar, dass sie weder neue Aufgaben noch neue Zuständigkeiten begründet.

2.

Jedenfalls müsste sich eine Regelung, die dazu zwingen würde, die Organisation der Datenschutzaufsicht in Widerspruch zum bestehenden Verwaltungsaufbau in den Mitgliedstaaten zu regeln, an dem in Art. 5 Abs. 3 EG statuierten Verhältnismäßigkeitsprinzip messen lassen. Nach Art. 5 Abs. 3 EG dürfen Maßnahmen der Gemeinschaft nicht über das für die Erreichung des Ziels dieses Vertrages erforderliche Maß hinausgehen. So ist anerkannt, dass die grundsätzliche Entscheidung über die Zuständigkeit und die Einrichtung von Behörden den Mitgliedstaaten verbleibt, wenn es sich wie hier um den mitgliedstaatlichen Vollzug von Gemeinschaftsrecht handelt. Dem entspricht auch das Protokoll über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit (unter Nr. 7): „Unter Einhaltung der gemeinschaftsrechtlichen Rechtsvorschriften sollten bewährte nationale Regelungen sowie Struktur und Funktionsweise der Rechtssysteme der Mitgliedstaaten geachtet werden."

3.

Im Übrigen besteht nach Art. 10 EG der allgemeine Grundsatz der loyalen Zusammenarbeit zwischen den Mitgliedstaaten und den Gemeinschaftsorganen. Nach diesem Grundsatz sind nicht nur die Mitgliedstaaten verpflichtet, alle geeigneten Maßnahmen zu ergreifen, um die Geltung und die Wirksamkeit des Gemeinschaftsrechts zu gewährleisten. Vielmehr erlegt er auch den Gemeinschaftsorganen entsprechende Pflichten zur loyalen Zusammenarbeit mit den Mitgliedstaaten auf. Daraus folgt, dass die Organe der Gemeinschaft bei der Ausübung ihrer Kompetenzen die Wirkungen auf behördliche Zuständigkeiten innerhalb der Mitgliedstaaten zu beachten haben.

4.

Vor diesem Hintergrund ist Art. 28 Abs. 1 Satz 2 der Richtlinie so zu verstehen, dass er keine organisatorische Unabhängigkeit der Datenschutz-Aufsichtsbehörden verlangt. Vielmehr kann er nur verlangen, dass die Datenverarbeitung öffentlicher Stellen durch eine unabhängige Stelle kontrolliert wird, die ihrerseits von anderen öffentlichen Stellen unabhängig sein muss. Denn bei der Datenschutzaufsicht für den öffentlichen Bereich ist zur Gewährleistung einer unabhängigen Aufgabenwahrnehmung in der Tat die Unabhängigkeit der Kontrollstellen von der Exekutive erforderlich (und in Deutschland auch entsprechend umgesetzt), da hier gerade die Einrichtungen der Exekutive die zu überprüfenden Stellen sind. Bei der Aufsicht über den nicht-öffentlichen Bereich kommt es demgegenüber auf die Unabhängigkeit von den zu kontrollierenden Stellen der Privatwirtschaft an. Dass eine nicht der Aufsicht durch die Ressortminister unterliegende Stelle eher vor einer sachfremden Einflussnahme durch Wirtschaftsunternehmen gefeit wäre, ist jedoch weder beleg- noch nachvollziehbar.

Auch die begründete Stellungnahme legt nicht dar, warum eine unterschiedliche Form der Unabhängigkeit der Datenschutzkontrollstellen für den öffentlichen Bereich einerseits und für den nicht-öffentlichen Bereich andererseits nicht zugelassen sein soll. Um den Erfordernissen des Art. 5 EG zu genügen, müsste die Kommission dabei aufzeigen, dass bei der Datenschutzkontrolle des öffentlichen Bereichs einerseits und des nicht-öffentlichen Bereichs andererseits die Unabhängigkeit der Datenschutzkontrollstellen von anderen staatlichen Stellen jeweils im gleichen Umfang erforderlich ist. Dass dies nicht gelingen kann, ergibt sich aus dem Vorstehenden.

IV.

Schließlich ist an dem Hinweis festzuhalten, dass die Richtlinie in Art. 26 Abs. 3 UAbs. 2 selbst eine Einflussmöglichkeit auf die Datenschutz-Aufsichtsbehörden für den nicht-öffentlichen Bereich vorsieht: Die Kommission ist nach dieser Vorschrift berechtigt, im Verfahren nach Art. 31 Abs. 2 Maßnahmen gegen eine erteilte Genehmigung zum Datenexport in einen Drittstaat zu erlassen. Zu diesen Maßnahmen gehört insbesondere die Untersagung des genehmigten Datentransfers. Gemäß Art. 26 Abs. 3 UAbs. 3 müssen die Aufsichtsbehörden in diesem Fall gegen einen zuvor möglicherweise von ihnen selbst genehmigten Datentransfer vorgehen.

In der begründeten Stellungnahme weist die Kommission darauf hin, dass dieses Verfahren eine einheitliche Genehmigungspraxis für Datenübermittlungen in Drittstaaten gewährleisten solle. Die Unabhängigkeit der Datenschutz-Aufsichtsbehörden sei dadurch nicht in Frage gestellt.

Dies zeigt jedoch, dass die grundsätzliche Auffassung der Kommission nicht haltbar ist, nach der Datenschutz-Aufsichtsbehörden in Bezug auf den Inhalt und Umfang ihrer Tätigkeit keinerlei Weisung (Punkt II.10) oder sonstigen rechtlichen Möglichkeiten, auf ihre Entscheidungen Einfluss zu nehmen (Punkt II.25), unterliegen dürfen.

D. Schlussfolgerungen und Ergebnis

Die Organisation der Datenschutzaufsicht in Deutschland für den nicht-öffentlichen Bereich wird den so auszulegenden Anforderungen von Art. 28 Abs. 1 Satz 2 der Richtlinie gerecht. Sie wird zunächst dadurch gewährleistet, dass § 38 Abs. 1 Satz 2 BDSG eine funktionale Abgrenzung der Aufsichtsbehörde bewirkt. § 38 Abs. 1 Satz 2 BDSG legt fest, dass die bei der Kontrolltätigkeit gewonnenen Erkenntnisse ausschließlich für Zwecke der Aufsicht verwendet werden dürfen. Damit ist die Aufsichtsbehörde funktional abgegrenzt und unabhängig von den Informationsinteressen der übrigen Verwaltung, ganz gleich, wo sie institutionell angesiedelt ist.

Die Datenschutz-Aufsichtsbehörden in Deutschland entscheiden unabhängig von sachfremden Einflüssen, insbesondere unabhängig von den zu überprüfenden Stellen. Dies gilt unabhängig davon, ob diese Aufgaben durch Datenschutzbeauftragte, nachgeordnete Behörden der Ministerialverwaltung oder ein Ministerium selbst wahrgenommen werden. Zu überprüfende Unternehmen haben keinerlei Einfluss auf die Entscheidung der Kontrollbehörden. Auch gibt es keine personellen Verflechtungen. Dies wird dadurch gestützt, dass die Kontrollstellen überwiegend mit auf Lebenszeit beschäftigtem Personal ausgestattet sind.

Zusammengefasst nehmen die Datenschutz-Kontrollstellen in der Bundesrepublik Deutschland - auch soweit sie in einem hierarchischen Verwaltungsaufbau eingebunden sind - ihre Aufgaben mit der von der Richtlinie 95/46/EG geforderten völligen Unabhängigkeit wahr.

Ein Vertragsverstoß liegt daher nicht vor. Demgemäß bittet die Bundesregierung um Einstellung des Verfahrens.