15. Wahlperiode

Drucksache **15/4658**

HESSISCHER LANDTAG

26. 11. 2002

Stellungnahme der Landesregierung

betreffend den Dreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Drucksache 15/3705

Eingegangen am 26. November 2002 · Ausgegeben am 17. Dezember 2002

Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Vorbemerkung

Das Recht auf informationelle Selbstbestimmung bleibt auch zukünftig gemeinsames Anliegen von Landesregierung und Datenschutzbeauftragtem. Die Landesregierung misst der Beachtung dieses Rechts der Bürgerinnen und Bürger einen hohen Stellenwert bei. Sie dankt dem Datenschutzbeauftragten für seine - auch aus ihrer Sicht zutreffende - Bewertung, die gemeinsamen Gespräche seien stets sachorientiert gewesen.

Die Stellungnahme der Landesregierung zum Tätigkeitsbericht des Datenschutzbeauftragten hat in diesem Jahr einen deutlich größeren Umfang als in den vergangenen Jahren. Nachdem der 29. Tätigkeitsbericht des Datenschutzbeauftragten und die Stellungnahme der Landesregierung zu diesem Bericht dem Landtag vorlagen, stellte die Fraktion BÜNDNIS 90/DIE GRÜNEN den Dringlichen Antrag (Drs. 15/3584):

"Der Landtag wolle beschließen:
Der Landtag fordert die Landesregierung auf, zukünftig substanziiert auf die Tätigkeitsberichte des Datenschutzbeauftragten einzugehen und detailliert zu jedem Punkt Stellung zu beziehen.

Der Landtag fordert die Landesregierung auf, auch positive Übereinstimmungen mit den einzelnen Bemerkungen des Datenschutzbeauftragten zu dokumentieren und dies in ihre Stellungnahme aufzunehmen."

Die Fraktionen erörterten den Antrag eingehend im Innenausschuss. Der Innenausschuss fasste darauf hin folgenden Beschluss (Drs. 15/3609):

"Der Innenausschuss empfiehlt dem Plenum, den ersten Satz des Dringlichen Antrags abzulehnen und den zweiten anzunehmen."

Der Landtag nahm in seiner 99. Sitzung am 28. Februar 2002 die Beschlussempfehlung des Innenausschusses zu dem Dringlichen Antrag an.

Die Landesregierung hat während der Beratung des Dringlichen Antrags auf die Probleme hingewiesen, die Folge einer Verpflichtung wären, zu jedem Punkt des Tätigkeitsberichts Stellung nehmen zu müssen. Diese Probleme resultieren aus den grundsätzlich verschiedenen Aufgabenstellungen, die der Datenschutzbeauftragte und die Landesregierung jeweils zu erfüllen haben. Der Datenschutzbeauftragte hat u.a. den gesetzlichen Auftrag, die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise Daten verarbeitender Stellen zu beobachten (§ 24 Abs. 2 HDSG) und Verbesserungen des Datenschutzes anzuregen (§ 30 Abs. 1 HDSG), wobei es ihm möglich ist, sein Augenmerk nach eigenem Ermessen auf bestimmte Vorgänge zu konzentrieren. Demgegenüber hat die Landesregierung bestehende Gesetze zu vollziehen oder bei der Gesetzgebung in Bund und Land mitzuwirken. In diesem Rahmen vollzieht sich die Meinungsbildung der Landesregierung. Es gibt deshalb Themen, die der Datenschutzbeauftragte in seinem Tätigkeitsbericht - im Einklang mit seinen Aufgaben - anspricht oder referiert, mit denen sich die Landesregierung im Rahmen ihrer Aufgaben jedoch bislang nicht befassen musste. Das gilt in Bezug auf den 30. Tätigkeitsbericht z.B. für das im Vorwort erwähnte "Transparenzgesetz" im Gesundheitswesen, für die unter Nr. 27 wiedergegebenen rechtspolitischen Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder oder die unter Nr. 28 zusammengestellten Materialien zum Datenschutz. Für solche Themen, mit denen sie im Rahmen der Aufgabenerfüllung nicht befasst war, fehlt der Landesregierung die Grundlage, eine Stellungnahme abzugeben.

Es würde die Arbeit der Landesregierung nachhaltig beeinträchtigen, wenn sie gezwungen wäre, sich aus Anlass des Tätigkeitsberichts erklären zu müssen, obwohl dies im Rahmen ihrer gewöhnlichen Aufgabenerfüllung nicht erforderlich oder sogar untunlich wäre. Die vorliegende Stellungnahme spart daher solche Teile des Tätigkeitsberichts aus, für die ihr die Beurteilungsgrundlagen fehlen. Vorbehaltlich dieser Einschränkung ist die Landesregierung selbstverständlich bemüht, zu allen im Tätigkeitsbericht angesprochenen Punkten Stellung zu nehmen.

Zu 1. Vorwort

Die Diskussion um die Zulässigkeit der praktizierten Rasterfahndung ist durch das OLG Frankfurt am Main (Beschluss vom 21. Februar 2002) für Hessen verbindlich entschieden worden, auch wenn die Entscheidung von denen der Obergerichte anderer Bundesländer abweicht. Die Fraktionen der CDU und der FDP haben einen Gesetzentwurf zur Schaffung einer neuen Regelung in den Landtag eingebracht (Drs. 15/3755).

Widersprochen werden muss der Behauptung des Hessischen Datenschutzbeauftragten, das Innenministerium habe die Meinung vertreten, der Gesamtbestand der Daten müsse bis zum Schluss des Abgleichs zusammengehalten werden. Es habe sich deswegen einer Löschung der Datensätze derjenigen betroffenen Personen widersetzt, die im Zuge des Rasterabgleichs ausgeschieden sind. Eine solche Meinungsverschiedenheit hat es nicht gegeben. Vielmehr wurden die Grunddatensätze (Daten der Einwohnermeldeämter, der Universitäten und Hochschulen sowie des Ausländerzentralregisters) am 18. und 19. Februar 2002 gelöscht, nachdem der Rasterlauf am 30. Januar 2002 durchgeführt und die Prüffälle am 4. Februar 2002 in die für die weitere Verarbeitung vorgesehene CRIME-Datenbank überspielt worden waren. Die Löschung geschah mithin unabhängig von dem Beschluss des OLG Frankfurt am Main vom 21. Februar 2002, durch den die "Rasterfahndung" in Hessen gestoppt worden ist.

Die vom Datenschutzbeauftragten in seinem Tätigkeitsbericht aufgezählten zahlreichen Einzelvorschläge zur Umsetzung des Grundrechtes auf informationelle Selbstbestimmung in der Abgabenordnung wurden dem Bundesministerium der Finanzen mit der Bitte um Erörterung auf der nächsten Sitzung der Arbeitsgruppe "Datenschutz in der Abgabenordnung" bzw. der Koordinierungsrunde vorgelegt.

Nach Mitteilung des Bundesministeriums der Finanzen ist das Thema "Änderungsbedarf der AO aus Sicht der Datenschutzbeauftragten des Bundes und der Länder" zur Erörterung in der geplanten Sitzung der zwischen den obersten Finanzbehörden der Länder und Vertretern der Datenschutzbeauftragten des Bundes und der Länder beschlossenen Koordinierungsgruppe unter Leitung des Bundesministeriums der Finanzen vorgesehen. Als Grundlage für diese Besprechung sollen abgestimmte Vorschläge der Datenschutzbeauftragten des Bundes und der Länder dienen, die nach Angaben des zuständigen Vertreters des Bundesbeauftragten für den Datenschutz demnächst übersandt werden. Es ist davon auszugehen, dass die Vorschläge des Hessischen Datenschutzbeauftragten insoweit einfließen.

Die Auffassung des Datenschutzbeauftragten, die Europäische Datenschutzrichtlinie mache es erforderlich, die Aufsichtsbehörden für den nicht öffentlichen Bereich aus den Regierungspräsidien herauszulösen, war bereits mehrfach Gegenstand der Stellungnahme der Landesregierung. Die Landesregierung hält diese Auffassung nach wie vor nicht für überzeugend; zur Vermeidung von Wiederholungen wird auf die Ausführungen in den Stellungnahmen zum 26. Tätigkeitsbericht (Drs. 14/4167, S. 3) und zum 28. Tätigkeitsbericht (Drs. 15/1538, S. 2) verwiesen.

Auch das vom Datenschutzbeauftragten zitierte Schreiben der EU-Kommission an den Berliner Datenschutzbeauftragten verhilft in der Frage, was unter "Unabhängigkeit" im Sinn der Datenschutzrichtlinie zu verstehen ist, nicht zu neuen Erkenntnissen. Die Kommission nennt darin nämlich lediglich allgemein einige "Elemente, die diese Unabhängigkeit ausmachen können" und der gegenwärtig in Hessen bestehenden Zuständigkeitsregelung nicht widersprechen. Im Übrigen äußert sich die Kommission nicht über konkret bestehende Zuständigkeiten, sondern verweist darauf, dass diese Frage von der Kommission noch "im Rahmen der Überprüfung der deutschen Datenschutzgesetze untersucht und beurteilt" werde.

Zu dem erwähnten Wiesbadener Forum Datenschutz ist zu bemerken, dass die Landesregierung den Entwurf eines Gesetzes zur Änderung des Hessischen Pressegesetzes vorbereitet, mit dem die datenschutzrechtlichen Vorgaben des § 41 Bundesdatenschutzgesetz in das Landesrecht umgesetzt werden sollen. Der Gesetzentwurf befindet sich zur Zeit (bei Redaktionsschluss dieser Stellungnahme Ende Juli) in der Anhörung.

Ausführungen zu weiteren vom Datenschutzbeauftragten im Vorwort angesprochenen Punkten sind im Zusammenhang mit der Abhandlung des jeweiligen Themas zu finden.

Zu 2. Terrorismusbekämpfung
Biometrische Merkmale in Pässen und Personalausweisen

Das zweite Terrorismusbekämpfungsgesetz regelt bezüglich der Aufnahme biometrischer Merkmale in Ausweispapieren keine Einzelheiten. Die Kritik des Hessischen Datenschutzbeauftragten greift gerade solche Einzelheiten auf, über die erst in einem weiteren Gesetzgebungsverfahren auf Bundesebene zu entscheiden sein wird.

Die Bundesregierung hat in ihrer Antwort auf die Kleine Anfrage der Abgeordneten Ulla Jelpke und der Fraktion der PDS (BT-Drs. 14/8720) dazu unter anderem Folgendes ausgeführt (vgl. BT-Drs. 14/8839):

"Die Einführung weiterer biometrischer Merkmale in Pässen und Personalausweisen dient der Verbesserung der Identifizierung von Personen, die sich mit Reisedokumenten ausweisen. Der Missbrauchsgefahr von Reisedokumenten durch Terroristen wird damit entgegengewirkt. Die Bedrohung der Sicherheit durch den internationalen Terrorismus ist kein zeitlich begrenztes Phänomen.

Nach Artikel 7 und 8 des Terrorismusbekämpfungsgesetzes ist für die Aufnahme weiterer biometrischer Merkmale (neben Lichtbild und Unterschrift) in Pässen und Personalausweisen ein Bundesgesetz erforderlich. Ein Gesetzentwurf kann erst nach Abschluss aller erforderlichen Vorarbeiten vorgelegt werden. Der Zeitpunkt hierfür steht gegenwärtig noch nicht fest, da zahlreiche wissenschaftlich-technische Fragen in Bezug auf die Anwendung biometrischer Verfahren zu klären sind.

Die Bundesregierung beabsichtigt, in den ausländerrechtlichen Dokumenten, wie in § 39 Abs. 1 Ausländergesetz vorgesehen, Angaben über die Größe der Person und die Farbe der Augen sowie ein Lichtbild und die Unterschrift der Person des Inhabers aufzunehmen. Im Hinblick auf die verschlüsselte Speicherung biometrischer Daten ist auch die weitere Entwicklung auf europäischer Ebene von Bedeutung.

Unter Berücksichtigung des gegenwärtigen Forschungs- und Entwicklungsstandes zu biometrischen Merkmalen und Verfahren beabsichtigt die Bundesregierung zunächst eine Prüfung der bestehenden Technologien. Vom Ausgang dieser Prüfung werden die weiteren Entscheidungen der Bundesregierung zur Einführung der geeigneten biometrischen Verfahren abhängen, wozu auch die Frage gehört, welches technische Verfahren für die Speicherung biometrischer Daten benutzt wird.

Die im Bundesministerium des Innern eingerichtete Projektgruppe Biometrie hat unter anderem den Auftrag, eine Bestandsaufnahme verfügbarer biometrischer Systeme und Verfahren vorzunehmen und diese im Hinblick auf ihre Tauglichkeit für mögliche Anwendungsfelder zu bewerten. Zu den Erkenntnisquellen werden dabei auch technische Studien und der länderübergreifende Vergleich gehören."

Die Zweckbindung der im Pass- und Personalausweisgesetz enthaltenen verschlüsselten Merkmale und Angaben ergibt sich aus den durch das Terrorismusbekämpfungsgesetz eingeführten § 16 Abs. 6 des Passgesetzes und § 3 Abs. 5 Satz 4 und 5 des Personalausweisgesetzes. Danach dürfen die verschlüsselten Merkmale und Angaben nur zur Überprüfung der Echtheit der Dokumente und zur Identitätsprüfung ausgelesen und verwendet werden. Auf Verlangen hat die Passbehörde bzw. die Personalausweisbehörde dem Pass- bzw. Ausweisinhaber Auskunft über den Inhalt der verschlüsselten Merkmale und Angaben zu erteilen. Eine bundesweite Datei wird nicht eingerichtet.

Hessen hat dem Terrorismusbekämpfungsgesetz zugestimmt.
Die Landesregierung hält die Aufnahme biometrischer Merkmale in Pässen und Personalausweisen für unbedingt erforderlich.

Zu 3. Novelle des Bundesdatenschutzgesetzes

Die vom Hessischen Datenschutzbeauftragten erwähnte Prüfung der EG-Kommission, ob die EG-Datenschutzrichtlinie korrekt in nationales Recht umgesetzt wurde, ist ein Standardverfahren, das stets nach Ablauf der Umsetzungsfrist für eine EG-Richtlinie durchgeführt wird. Ein Prüfungsergebnis liegt noch nicht vor. Das gilt auch hinsichtlich der damit in Zusammenhang stehenden Frage nach der organisatorischen Stellung der Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich. Die Landesregierung sieht - ebenso wie die Bundesregierung - in der derzeitigen Organisation des Datenschutzes im privaten Bereich keinen Verstoß gegen die EG-Richtlinie.

Zu 4. Elektronische Signatur und Verwaltungsverfahrensänderungsgesetz

Der Referentenentwurf für das Verwaltungsverfahrensänderungsgesetz wurde von den Verwaltungsverfahrensrechtsreferenten des Bundes und der Länder als Mustergesetzentwurf erarbeitet. Er hat in dem Entwurf eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften der Bundesregierung Eingang gefunden. Mit dem Gesetzentwurf wird das gesamte Verwaltungsverfahrensrecht des Bundes an die Entwicklungen des modernen Rechtsverkehrs angepasst. Bürger und Verwaltung sollen grundsätzlich in allen Fachgebieten und jeder Verfahrensart elektronische Kommunikationsformen gleichberechtigt neben der Schriftform und der mündlichen Form rechtswirksam verwenden können. Die Verwaltungsverfahrensgesetze des Bundes (Verwaltungsverfahrensgesetz, Sozialgesetzbuch X, Abgabenordnung) und die Fachgesetze werden deshalb für die Möglichkeit der rechtsverbindlichen elektronischen Kommunikation auf der Basis qualifizierter elektronischer Signaturen geöffnet.

Im Interesse der Einheitlichkeit der Verwaltungsverfahrensgesetze in Bund und Ländern beabsichtigen die Länder, die Änderungen des Verwaltungsverfahrensgesetzes des Bundes in ihre Verwaltungsverfahrensgesetze aufzunehmen. Aus diesem Grunde fanden auch in Hessen eine Ressortbeteiligung und eine Beteiligung des Hessischen Datenschutzbeauftragten an den Erörterungen des Mustergesetzentwurfs statt. Die vom Hessischen Datenschutzbeauftragten vorgetragenen Anregungen und Bedenken wurden dem Bundesministerium des Innern und den Verfahrensbeteiligten aus den anderen Ländern zur Kenntnis gebracht. Sie fanden weitgehend in dem Mustergesetzentwurf bzw. im Bundesratsverfahren zum Dritten Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften Berücksichtigung, wie beispielsweise die Regelung über die Zustellungsfiktion, die Einwilligung des Empfängers elektronischer Dokumente und die Beglaubigung beim "Medienbruch". Nicht aufgenommen wurde das vom Hessischen Datenschutzbeauftragten geforderte Verschlüsselungsgebot, weil sich dieses bereits aus dem Geheimhaltungsgebot des § 31 VwVfG ergibt.

Zu 5. Videoüberwachung
Zu 5.1 Videoüberwachung auf Grundlage des § 14 Abs. 3 und 4 HSOG

Der Darstellung des Hessischen Datenschutzbeauftragten, der Einsatz von Videoüberwachungsanlagen werde zum Teil sehr extensiv genutzt, muss entschieden widersprochen werden. Nach Auffassung der Landesregierung werden Videoüberwachungsanlagen auf Grundlage des § 14 Abs. 3 und 4 HSOG vielmehr - in Abstimmung mit dem Datenschutzbeauftragten - sehr maßvoll eingesetzt.
Im Übrigen ist zu den Ausführungen des Datenschutzbeauftragten Folgendes anzumerken:

Der Begriff "Videoschutzanlage" stellt keineswegs eine "Verharmlosung" der Überwachungseinrichtung dar, sondern umschreibt zutreffend den mit ihr angestrebten Zweck. Sie dient dem Schutz der Örtlichkeit und der Bevölkerung vor Straftaten und nicht der Ausforschung von Menschen und ihrem Verhalten.

Zu der Überwachungsanlage am Bahnhofsvorplatz in Limburg an der Lahn (Tz. 5.1.1) empfiehlt der Hessische Datenschutzbeauftragte, für die weitere Zukunft an den Einsatz von Kamerasystemen zu denken, die die Gesichter durch Raster unkenntlich machen. Die Entschlüsselung der aufgezeichneten

Klardaten solle besonders dazu berufenen Bediensteten der Gefahrenabwehr- und Strafverfolgungsbehörden vorbehalten bleiben.

Bei Videoüberwachungsanlagen kann jedoch eine Rasterung nicht in Betracht gezogen werden, weil diese mit der präventiven Zielsetzung der Einrichtung unvereinbar wäre. Für die Bewertung einer Situation als gefahrenträchtig kann es nämlich gerade auf die Beobachtung des Gesichts und der Mimik der erfassten Person ankommen (z.B. suchendes Umschauen nach Opfern, Mittätern oder für den Täter mit Risiken behafteten Umständen, Verständigung mit Mittätern durch Mimik oder Zurufen). Nur durch die vollständige Aufnahme der betreffenden Personen lassen sich Gefahrenlagen angemessen beurteilen. Im Übrigen wird auf die Ausführungen zu Tz. 26.3 verwiesen.

Zu 5.2 Der Videoeinsatz zur Gefahrenabwehr hält auch bei den Hochschulen Einzug

Die Universität Frankfurt überwacht besonders gefährdete Bereiche der Hochschule mit Hilfe von Videoanlagen, um die Sachbeschädigung und den Diebstahl von besonders wertvollen Sachgütern zu verhindern. Geeignete andere Mittel zur Verhinderung solcher Straftaten stehen nicht zur Verfügung. Die Modalitäten sind nach der neuen Rechtsvorschrift des § 14 Abs. 4 HSOG mit dem Datenschutzbeauftragten vorher abgeklärt worden. Bei einer Begehung war festgestellt worden, dass ein entsprechender Hinweis auf die laufende Videoüberwachung noch fehlt. Dies wurde unverzüglich nachgeholt, sodass entsprechende Informationen jetzt an den überwachten Türen angebracht sind.

Zu 6. Internet
Zu 6.1 Internettestwahl in Marburg

Die Ausführungen des Datenschutzbeauftragten sind zutreffend. Allerdings ist auf Folgendes aufmerksam zu machen:

Zu 6.1.1 Ausgestaltung der Testwahl

Der Datenschutzbeauftragte führt aus, dass eine Referenz zwischen laufender Nummer und den verschlüsselten Stimmdaten erforderlich sei, da es bis 18:00 Uhr am Wahltage noch möglich sein müsse, Stimmen für ungültig zu erklären und nicht zu zählen. Das Wahlamt teile nach Schließung der Wahllokale dem Wahlvorstand mit, welche der Stimmzettel ungültig seien; diese Stimmzettel würden dann vor Beginn der Stimmauszählung aussortiert.

Da die Internet-Testwahl entsprechend den gesetzlichen Vorgaben für die Briefwahl durchgeführt werden sollte, ist dies ungenau formuliert. Wird ein Wahlberechtigter, der bereits einen Wahlschein erhalten hat, im Wählerverzeichnis gestrichen, ist der erteilte Wahlschein für ungültig zu erklären, §§ 18 Abs. 7 Satz 1, 60 der Kommunalwahlordnung (KWO). Wahlbriefe, denen kein gültiger Wahlschein beiliegt, werden nach §§ 21a Abs. 1 Nr. 2 2. Alt., 41 Satz 1 des Hessischen Kommunalwahlgesetzes (KWG) zurückgewiesen; die Stimmen werden nicht als ungültig gezählt, sondern sie gelten als nicht abgegeben (§§ 21 Abs. 2, 41 Satz 1 KWG).

Entsprechend wird dem Wahlvorstand vom Wahlamt auch nicht mitgeteilt, welche Stimmen für ungültig erklärt worden sind, sondern es wird ihm nur ein Verzeichnis der für ungültig erklärten Wahlscheine oder die Mitteilung übergeben, dass keine Wahlscheine für ungültig erklärt worden sind, §§ 52 Abs. 2 Satz 2, 60 KWO.

Zu 6.1.2 Probleme, die vor einer Echtwahl gelöst werden müssen

Der Datenschutzbeauftragte sieht es als eine notwendige Voraussetzung für einen Einsatz der Internet-Technologie bei Wahlen an, dass die Server in gesicherten Räumen untergebracht werden müssen, zu denen nur Wahlhelfer Zutritt haben.

Der Begriff des "Wahlhelfers" sollte im Hinblick auf den Zugriff auf die Server nicht verwendet werden. Unter dem gesetzlich nicht definierten Begriff des "Wahlhelfers" können neben den gesetzlich vorgesehenen Wahlorganen auch so genannte Hilfskräfte (vgl. § 4 Abs. 10 KWO) verstanden werden. Es ist unter

Berücksichtigung der erheblichen Bedeutung der tatsächlichen Zugriffsmöglichkeit auf die Server ausgeschlossen, dass dafür Hilfskräfte eingesetzt werden. Da ein entsprechendes Wahlorgan für diese Aufgabe derzeit nicht existiert, besteht für den Einsatz der Internet-Technologie bei Wahlen derzeit noch eine Regelungslücke.

Zu 6.2 Anonymität bzw. das Recht auf informationelle Selbstbestimmung im Internet

Die durch den Datenschutzbeauftragten dargestellten Möglichkeiten zur anonymen Nutzung des Internets sind aus technischer Sicht zutreffend.

Zu 6.3 Dienstliche und private Nutzung von E-Mail und www

Der Datenschutzbeauftragte weist auf die entstehenden datenschutzrechtlichen Probleme bei dienstlicher und privater Nutzung der Internetdienste E-Mail und www hin. Diese Problematik wurde bereits im Rahmen einer Ressortbesprechung unter Einbeziehung des Datenschutzbeauftragten diskutiert. Ziel ist die Schaffung einer "Richtlinie zur Behandlung elektronischer Post", die als Rahmenregelung für alle Dienststellen des Landes verbindlich eingeführt werden soll. In der Besprechung wurde die Einschätzung des Datenschutzbeauftragten weitgehend geteilt. Die Diskussion ist aber noch nicht abgeschlossen. Die geforderte Einrichtung von gesonderten Postfächern für Funktionsträger (z.B. Personalrat, Suchtbeauftragte), die in den Dienststellen eine besondere Vertrauensstellung genießen, wird als unproblematisch erachtet.
Die Verabschiedung der Richtlinie ist noch für dieses Jahr vorgesehen.

Zu 7. Justiz
Zu 7.1 Insolvenzveröffentlichungen im Internet

Die Verordnung, auf die sich die Ausführungen des Datenschutzbeauftragten beziehen, ist von der Bundesministerin der Justiz inzwischen erlassen worden und in Kraft getreten (Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet vom 12. Februar 2002, BGBl. I. S. 677). Der Forderung des Datenschutzbeauftragten, die Zulassung von öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet mit den notwendigen datenschutzrechtlichen Rahmenregelungen zu verbinden, kann grundsätzlich zugestimmt werden. Die Bundesministerin der Justiz hat dazu bereits in der Begründung des Verordnungsentwurfs ausgeführt:

"Allerdings sind mit der gesteigerten Publizität des neuen Informations- und Kommunikationssystems auch Gefahren für die Schuldner verbunden. Deshalb muss gewährleistet sein, dass die in das Internet eingestellten Daten auch tatsächlich von den Gerichten stammen, den Lauf des Verfahrens getreu abbilden und möglichst nicht von Internetnutzern elektronisch kopiert werden können. Die Landesjustizverwaltungen haben dies durch geeignete Vorkehrungen sicherzustellen."

Die erforderlichen Vorkehrungen zum Datenschutz spielten deshalb im Rechtssetzungsverfahren, insbesondere auch in den Ausschüssen des Bundesrates, eine wichtige Rolle. Die Verordnung sieht nunmehr vor:

- Es muss sichergestellt sein, dass die Daten bei der elektronischen Übermittlung von dem Insolvenzgericht oder dem Insolvenzverwalter an die für die Veröffentlichung zuständige Stelle elektronisch signiert werden (§ 2 Abs. 1 S. 1 Nr. 1 der Verordnung).
- Nach dem Stand der Technik ist dafür Sorge zu tragen, dass die genannten Daten durch Dritte elektronisch nicht kopiert werden können (§ 2 Abs. 1 S. 3 der Verordnung).
- Die im Internet erfolgte Veröffentlichung von Daten aus einem Insolvenzverfahren einschließlich des Eröffungsverfahrens wird spätestens einen Monat nach der Aufhebung oder Rechtskraft der Einstellung des Insolvenzverfahrens gelöscht (§ 3 Abs. 1 S. 1 der Verordnung).

Damit ist in der nunmehr in Kraft getretenen Verordnung den Vorschlägen des Datenschutzbeauftragten weitestgehend Rechnung getragen.

Zu 7.2 Der Einsatz von EUREKA in der Verwaltungsgerichtsbarkeit

Das Verfahren EUREKA-Fach ist in der hessischen Verwaltungsgerichtsbarkeit flächendeckend zur Zufriedenheit der Anwender im Einsatz. Es handelt sich um ein erprobtes Verfahren, das mittlerweile in vielen Bundesländern in unterschiedlichen Fachgerichtsbarkeiten eingesetzt wird. Das Verfahren wird unter Steuerung eines Lenkungskreises, in dem alle beteiligten Länder vertreten sind, gepflegt und weiterentwickelt.

Bemerkungsfelder

Es wird näher festgelegt werden, welche Art von Zusatzinformationen in den uneingeschränkt recherchierbaren Bemerkungsfeldern abgelegt werden dürfen. Dies stellt insofern kein Problem dar, da EUREKA-Fach ein zusätzliches Feld für persönliche Bemerkungen zur Verfügung stellt, das nur von dem einzelnen Nutzer einsehbar ist.

Adressdatei

Die beanstandete Möglichkeit des Nutzers, bei der Suche nach bestimmten Personen die gesamt Adressliste einzusehen, ist nur durch eine die Arbeit mit EUREKA-Fach deutlich erschwerende Beschränkung der Einsicht in die Namens- und Adresstabelle möglich. Mit den Folgen und den notwendigen programmtechnischen Änderungen wird sich der Lenkungskreis auseinander zu setzen haben. Dies wird von Hessen dort eingebracht werden.

Aufbewahrung der Dokumente in der Textverarbeitung

Die Aufbewahrung von Texten in der Textverarbeitung ist nicht durch EUREKA-Fach, sondern durch den Einsatz zusätzlicher Archivierungs- bzw. Lösch-Tools zu lösen. Hierzu wird ebenfalls eine gemeinsame Vorgehensweise in dem Lenkungskreis abgestimmt werden.

Zugriffsmöglichkeiten auf die Anwendung

Mit der Anwendung EUREKA-Fach lassen sich umfassende und hinreichende Zugriffsbegrenzungen einstellen. Die Beanstandung der unzureichenden Abbildung dieser Zugriffsbegrenzungen auf den NT-Dateibaum ist durch die geplante Umstellung des Datenbanksystems auf Oracle zu beheben. Entsprechende Arbeiten sind angelaufen.

Löschprogramm

Das Problem einer fehlenden Routine zur automatisierten Löschung bzw. Reduzierung der unter EUREKA-Fach aufgenommenen Daten ist dem Lenkungskreis bewusst und es wurde bereits ein Auftrag zur Erstellung eines Programms zur Datenarchivierung und Datenlöschung erteilt.

Zu 7.3 Das elektronische Grundbuch

Das vom Datenschutzbeauftragten beschriebene elektronische Grundbuch-System "SOLUM-Star V 2.12." wurde zwischenzeitlich weiter verbessert und ist nunmehr in der Version V 2.14 K1 im Einsatz.

Der unter datenschutzrechtlichen Gesichtspunkten bisher beanstandungsfreie Einsatz des elektronischen Grundbuches bei mittlerweile 13 hessischen Amtsgerichten sowie die gleichzeitige Nutzung durch mehr als 200 externe User bestätigen die Sicherheit dieses breit angelegten Justizverfahrens.
Die nunmehr fast 10 Millionen eingescannten Grundbuchseiten sind sicher im zentralen Rechenzentrum der HZD in Hünfeld gespeichert. Die Justizmitarbeiter haben über das verschlüsselte Landesnetz HCN 2000 Zugriff darauf.

Digitale Signatur

Das bislang in Solum-Star genutzte technische Verfahren zur Erzeugung und Verwaltung digitaler Signaturen ist noch vor In-Kraft-Treten des Signatur-Gesetzes und der SignaturVO konzipiert worden und stellte sich zum Zeitpunkt der Realisierung (1995/96) als ausgesprochen fortschrittlich und vorausschauend dar. Da digitale Signaturen im bestehenden Solum-Star-Verfahren nur für Grundbucheintragungen - also ausschließlich behördenintern - genutzt werden, genügt die derzeitige, noch nicht vollständig signatur-

gesetzkonforme Konzeption auch nach Auffassung des Datenschutzbeauftragten den Anforderungen ohne Einschränkung.

Im Rahmen der umfassenden Neukonzeption des Elektronischen Grundbuchs, mit der die Arbeitsgruppe "Redesign" des Entwicklerverbundes Solum-Star betraut worden ist und die nach derzeitigem Erkenntnisstand auch die Möglichkeit elektronischer Antragstellung durch Notare umfassen soll, wird die Verfahrensintegration signaturgesetzkonformer digitaler Signaturen realisiert werden. Eine Verifikationsfunktion für Teilnehmer am automatisierten Abrufverfahren wird ebenso wie die Speicherung geheimer Signaturschlüsseln auf Chipkarten Gegenstand der Prüfungen sein.

Langzeitarchivierung

Auch die Langzeitarchivierung elektronischer Grundbücher in einem geeigneten, auf Dauer lesbaren Datenformat und auf geeigneten Speichermedien wird Gegenstand der Prüfung im Rahmen des Redesigns sein.

Terminalserver-Verfahren

Mit Recht hebt der Datenschutzbeauftragte u.a. die hochwertig verschlüsselte Datenübermittlung und die geringere benötigte Übertragungsleistung als wesentliche Vorteile der Terminalserver-Technik hervor.

Den Bedenken des Datenschutzbeauftragten, dass bei Nutzung des Terminalserver-Verfahrens ein an ein anderes Gericht versetzter Grundbuchamtsmitarbeiter mit seiner "alten" Kennung weiterhin auf die Daten seines früheren Gerichts zugreifen könnte, wird organisatorisch dadurch Rechnung getragen, dass Anwenderkennungen bei Ausscheiden eines Mitarbeiters generell umgehend gelöscht und identische Kennungen niemals erneut vergeben werden. Eine "Weiternutzung" ist dadurch ausgeschlossen.

Im Übrigen unterliegt auch das Terminalserver-Verfahren ständiger Fortentwicklung und Verbesserung. Die von der HZD entwickelte technische Lösung ist inzwischen von der Herstellerfirma von Solum-Star geprüft und bestätigt worden. Es steht nunmehr auch anderen Bundesländern offiziell zur Nutzung zur Verfügung. Die Fortentwicklung - auch unter datenschutzrechtlichen Gesichtspunkten - wird damit nun auch durch den Entwicklerverbund Solum-Star mitgetragen.

Zu 7.4 Datenübermittlung an gefährdete Personen

Die Einschätzung des Datenschutzbeauftragten wird geteilt.

Zu 7.5 Zweckwidrige Verwendung von Daten im Strafvollzug

Die Beanstandung des Datenschutzbeauftragten ist gerechtfertigt.

Der Übersendung des Protokolls mit Daten des betreffenden Gefangenen ging voraus, dass das Landgericht Gießen in einer Entscheidung bezüglich eines Mitgefangenen dessen im Rahmen der Vollzugsplankonferenz erstelltes Behandlungsprotokoll erbeten hatte. Da dieses nicht auffindbar war, wurde eine Unterlage angefordert, aus der erkennbar war, welchen Inhalts ein solches Behandlungsprotokoll sein könnte. Ohne zu bedenken, dass dieses übersandte Protokoll im Wege des rechtlichen Gehörs auch außenstehenden Dritten zugänglich werden würde, wurde das Behandlungsprotokoll eines anderen Gefangenen, zufällig das des betroffenen Gefangenen, genommen und nach Schwärzung des Namens übersandt.

Im Nachhinein ist den Mitarbeitern bewusst, dass sich auch nach Schwärzung des Namens für Mitgefangene aus der JVA Butzbach aus den sonstigen Angaben im Protokoll auf die Person des Gefangenen schließen lässt.

Die Bediensteten der JVA Butzbach wurden durch den Behördenleiter entsprechend belehrt, sodass Wiederholungen für die Zukunft ausgeschlossen sein dürften.

Zu 7.6 Datenübermittlungen im Zusammenhang mit Geldüberweisungen

Die Beanstandung des Datenschutzbeauftragten ist gerechtfertigt.

Nach Auskunft des Leiters der JVA Butzbach ist die Anfang des Jahres 2001 erneut auf den Überweisungsträgern eines Gefangenen angebrachte Absenderangabe "Justizvollzugsanstalt Butzbach" darauf zurückzuführen, dass der Leiter der Zahlstelle seit Dezember 2000 krankheitsbedingt ausgefallen war und in der Sachbearbeitung zu gleicher Zeit ein Mitarbeiterwechsel stattfand. Dem neuen Mitarbeiter waren die vorhergehenden Beanstandungen nicht bekannt, sodass es erneut zu diesem datenschutzrechtlichen Verstoß kam.

Durch Verfügung des Leiters der Justizvollzugsanstalt Butzbach an alle in der Zahlstelle eingesetzten Bediensteten dürfte nunmehr sichergestellt sein, dass ähnliche Verstöße nicht mehr vorkommen werden.

Zu beiden Vorfällen sind keine weiteren einschlägigen Verstöße gegen den Datenschutz bekannt geworden, sodass davon auszugehen ist, dass die getroffenen Maßnahmen die gewünschte Wirkung erzielt haben.

Zu 8. Polizei- und Strafverfolgungsbehörden

Zu 8.1 Neue Informationssysteme für die Hessische Polizei - Das Verfahren POLAS

POLAS

Die Entwicklung zu dem neuen polizeilichen Informationssystem POLAS wird zutreffend wiedergegeben. Bei dieser Entwicklung war der Hessische Datenschutzbeauftragte im Rahmen der vertrauensvollen Zusammenarbeit eingebunden. Auch im weiteren Verlauf des Projektes wurde und wird seine Beratung in Anspruch genommen.

Die Entscheidung für die Einführung des Systems POLAS in Kooperation mit Hamburg war Ende des Jahres 2000 notwendig geworden, da das damalige polizeiliche Informationssystem HEPOLIS, 1975 eingeführt, zwischenzeitlich aufgrund systemtechnischer Bedingungen nicht mehr in der Lage war, mit dem für 2001 geplanten Verbund-System INPOL-neu zu kommunizieren. Hinsichtlich des fachlichen Leistungsumfangs von POLAS wurden die Funktionalitäten von HEPOLIS übernommen und die dort vorhandenen Daten in das neue System migriert (ca. 11 Mio. Datensätze in den Bereichen Fall, Personen- und Sachfahndung). Am 14. Juli 2001 wurde HEPOLIS abgeschaltet und POLAS in Betrieb gesetzt. Seit diesem Zeitpunkt können alle Polizeibeamtinnen und -beamten auf das System POLAS zugreifen.

IT-Sicherheitskonzept

Zum Ende des vergangenen Jahres wurde dem Landespolizeipräsidium ein IT-Sicherheitskonzept für die hessische Polizei vorgelegt, das in Zusammenarbeit mit dem PTLV von einem externen Berater erarbeitet worden war. Der Hessische Datenschutzbeauftragte hat dieses Papier zur Kenntnis erhalten. Derzeit befindet sich das IT-Sicherheitskonzept in einer Konkretisierungs- und Umsetzungsphase. Hierzu sind erste organisatorische Maßnahmen ergriffen worden, darunter die Bennennung eines IT-Sicherheitsbeauftragten für die hessische Polizei im PTLV.

ComVor

Unmittelbar nach der Einführung von POLAS in Hessen wurde Ende 2001 das Projekt ComVor aufgesetzt, das die bereits in Hamburg in Betrieb befindliche Vorgangsbearbeitung ComVor nach entsprechender Anpassung auf das Flächenland Hessen bis zum September 2003 flächendeckend einführen soll.

INPOL-neu

Das Projekt INPOL-neu befindet sich derzeit in einer Redesign-Phase, die das bereits entwickelte Kernsystem um ein POLAS-basiertes operatives Front-End ergänzt.

Nach ausführlichen Erörterungen in den zuständigen Gremien zum Jahresende 2001 und im Januar 2002 hat die Ständige Konferenz der Innenminister und -senatoren der Länder mit Umlaufbeschluss vom 30. Januar 2002 der

neuen strategischen Ausrichtung und damit verbundenen neuen Planung für INPOL-neu zugestimmt.

Die Kernaussagen lauten dabei:

- Trennung in operative und dispositive Datenbanken, jeweils optimiert nach Einsatzzweck Abfrage bzw. kriminalistische Recherche.
- Entwicklungsgrundlage für das zentrale operative System, das die Anwenderbedürfnisse für die meisten Abfragenden in den Ländern abdeckt, ist POLAS-Hessen.
- Beschränkung zunächst auf Funktionsumfang INPOL-aktuell, ggf. ergänzt um weitere Falldaten. Ansonsten wird das derzeitige INPOL-aktuell zunächst auf eine neue technische, modernere Plattform gestellt.
- Den Ländern wird durch das BKA ein INPOL-Land-System (entspricht von der Zielsetzung dem bisherigen AGIL) zur Verfügung gestellt werden, das bis März 2003 in einer ersten Version (entspricht im Wesentlichen dem Funktionsumfang von POLAS-Hessen) in den Ländern eingeführt werden wird und damit im Jahr 2003 die Abschaltung von INPOL-aktuell ermöglicht. Hierzu wurde ein Teilprojekt INPOL-Land unter der Gesamtverantwortung des BKA aufgesetzt. Die Kooperation Hamburg/Hessen wird hier intensiv mitarbeiten und unterstützen. Die Leitung hat der bisherige Projektleiter POLAS aus Hamburg. Die Kooperation Hamburg/Hessen wird INPOL-Land jeweils testen und sukzessive in den jeweiligen Entwicklungsstufen im Vorfeld in produktiven Betrieb nehmen.
- Derzeit wollen alle Länder bis auf Rheinland Pfalz INPOL-Land einführen. Rheinland-Pfalz beabsichtigt, sein INPOL-Landessystem selbst neu zu entwickeln.
- Ablösung ZEVIS (Zentrales Verkehrsinformationssystem bei Kraftfahrtbundesamt) zum 30. Juni 2002.

Nach derzeitiger Planung wird durch das BKA keine Auftragsdatenverarbeitung mehr angeboten, die Länder müssen jeweils eine eigene Landesdatenhaltung vorsehen.

Zu 8.2 Zusammenarbeit bei der Produktion von Fernsehsendungen - Reality-TV

Der Datenschutzbeauftragte bestätigt die vom Ministerium des Innern und für Sport getroffene Maßnahme als sachgerecht.

Zu 8.3 Der Hausmeister der Universität als Ermittler der Polizei

Die Darstellung des Sachverhalts und des rechtlichen Dissenses, der keine Datenschutzfrage betrifft, ist zutreffend.

Zu 8.4 Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen

Aufbewahrung von erkennungsdienstlichen Unterlagen

Der Datenschutzbeauftragte kritisiert, dass nach den KPS-Richtlinien erkennungsdienstliche Unterlagen ebenso lange aufzubewahren sind wie die Kriminalakten, obwohl an ihre Speicherung, die das Fortbestehen einer Negativprognose erfordert, nach Änderung des § 20 Abs. 4 HSOG schärfere Anforderungen gestellt würden, als an die Aufbewahrung der übrigen Unterlagen.

Richtig ist, dass § 20 Abs. 4 HSOG durch Gesetz vom 3. November 1998 (GVBl. I S. 399) neu gefasst worden ist, wobei das Erfordernis der Negativprognose entfallen ist. Im Hinblick auf Aufnahme und Aufbewahrung von ed-Unterlagen hat sich dadurch jedoch nichts geändert. Die bei Bejahung einer Negativprognose angefertigten Unterlagen werden als Bestandteil des jeweiligen Falles zur Kriminalakte genommen. Ihre weitere Aufbewahrung richtet sich nach den entsprechend anzuwendenden Vorschriften der Prüffristenverordnung (Hess. VGH, NVwZ-RR 1994, 655). Das gilt auch für die Regelung des § 5 Abs. 1 PrüffristVO, wonach sich die Aussonderungsprüf-

frist durch neue Fälle weiter hinausschiebt. Es versteht sich im Übrigen von selbst, dass ein neu hinzugekommener Fall die früher gestellte Negativprognose nur bestätigen und nicht infrage stellen kann. Ob der neue Fall bei isolierter Betrachtung eine Negativprognose gerechtfertigt hätte, ist schon nach altem Recht unerheblich gewesen, weil die Negativprognose im Lichte aller Erkenntnisse über die betroffene Person erstellt werden muss.

Übermittlung von Informationen aus Kriminalakten

Den Vorschlag des Datenschutzbeauftragten, wonach bei der Übermittlung von Daten aus Ermittlungsverfahren immer zusätzlich mitzuteilen ist, wie das Verfahren ausgegangen ist bzw. dass der Verfahrensausgang unbekannt ist, hat das LKA in den überarbeiteten Entwurf der neuen KPS-Richtlinien aufgenommen. Nach den Ausführungen des Datenschutzbeauftragten kam es gerade in diesem Punkt immer wieder zu Rügen Betroffener und datenschutzrechtlichen Beanstandungen. Seitens des LKA war die Aufnahme einer diesbezüglichen Regelung zunächst abgelehnt worden, da dort bisher keine direkten Beschwerden von Betroffenen oder Beanstandungen durch den Datenschutzbeauftragten bekannt waren. Auch wurde die Richtlinie vom LKA nicht so ausgelegt, dass bei unbekanntem Aktenzeichen oder Verfahrensausgang ein entsprechender Hinweis zu unterbleiben hat.

Auswertung der Verfahrensausgangsmitteilung der Staatsanwaltschaft

Die KPS-Richtlinien sehen in Nr. 17.3.1.1 vor, dass der Vorgang bei Einstellungen nach § 170 Abs. 2 StPO wegen Beweismangels in der Kriminalakte verbleibt. Diese Regelung, die der Gesetzgeber durch eine Klarstellung des § 20 Abs. 4 HSOG mit Gesetz vom 3. November 1998 ausdrücklich bestätigt hat, setzt voraus, dass der Tatverdacht fortbesteht, die Beweislage für eine Anklageerhebung im Hinblick auf eine mögliche Verurteilung jedoch nicht ausgereicht hat. Da in den genannten Fällen mithin ein "Anfangsverdacht" durch zureichende tatsächliche Anhaltspunkte (vgl. § 152 Abs. 2 StPO) belegt ist, spricht nichts gegen die Beibehaltung der Regelung in den KPS-Richtlinien. Dies schließt die vom Datenschutzbeauftragten bezeichneten Fälle aus, in denen lediglich eine reine Vermutung oder Beschuldigung vorliegt.

Zu 8.5 Datenübermittlung aus dem Zentralen Verkehrsinformationssystem (ZEVIS) beim Kraftfahrbundesamt

Die Landesregierung stimmt der rechtlichen Beurteilung des Hessischen Datenschutzbeauftragten zu.

Zu 9. Verfassungsschutz
Zu 9.1 Änderung des Verfassungsschutzgesetzes

Das Gesetz über das Landesamt für Verfassungsschutz wurde inzwischen durch das Gesetz zur Änderung des Gesetzes über das Landesamt für Verfassungsschutz vom 30. April 2002 (GVBl. I S. 82) geändert. Im Rahmen dieser Gesetzesänderung wurden auch bereits die Änderungen des Bundesverfassungsschutzgesetzes durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) berücksichtigt. Die Stellungnahme des Datenschutzbeauftragten bezieht sich zum Teil auf den von der Landesregierung eingebrachten Änderungsentwurf, zum Teil auf Vorschläge, die der Ursprungsfassung des Referentenentwurfs des Terrorismusbekämpfungsgesetzes entnommen waren. Bei den Beratungen über den Gesetzentwurf waren jedoch bereits die - zum Teil nicht unerheblich abweichenden - Fassungen der Vorschriften des Terrorismusbekämpfungsgesetzes bekannt, die im Bund Gesetz geworden sind. Erst diese letzteren Formulierungen wurden Grundlage des Hessischen Änderungsgesetzes.

Zu 9.1.1 Einbeziehung der organisierten Kriminalität in den Aufgabenbereich des Verfassungsschutzes

Nach der inzwischen beschlossenen Gesetzesänderung dient das Landesamt für Verfassungsschutz auch dem Schutz vor organisierter Kriminalität und beobachtet zur Erfüllung dieser Aufgabe Bestrebungen und Tätigkeiten der organisierten Kriminalität im Geltungsbereich des Grundgesetzes (§ 2 Abs. 1 Satz 2, Abs. 2 Satz 1 Nr. 5 LfVG).

Schon im Rahmen der bisherigen Zuständigkeiten des Landesamts für Verfassungsschutz hat dieses auch bei der Verhütung oder Verfolgung von Straftaten mitgewirkt (vgl. § 10 LfVG für Staatsschutzdelikte, § 11 Abs. 1 Nr. 2 und 3 LfVG für die Katalogstraftaten des § 110 a StPO und Straftaten im Rahmen der organisierten Kriminalität). Diese Art der Zusammenarbeit des Verfassungsschutzes mit Polizei- und Ordnungsbehörden sowie Staatsanwaltschaften ist deshalb nichts grundsätzlich Neues. Dies gilt auch für das Problem der Verwendung von Informationen des Verfassungsschutzes in Gerichtsverfahren.

Auch im Bereich der Beobachtung von Bestrebungen und Tätigkeiten der organisierten Kriminalität gilt das Trennungsgebot weiterhin uneingeschränkt. Das von den drei alliierten Militärgouverneuren im so genannten Polizeibrief vom 14. April 1949 ausgesprochene Trennungsgebot besagt, dass Nachrichtendienste keine polizeilichen Befugnisse haben sollen ("shall have no police authority"). Dies ist in § 1 Abs. 1 Satz 2 LfVG umgesetzt, da das LfV danach mit Polizeidienststellen organisatorisch nicht verbunden werden darf, und in § 3 Abs. 5 LfVG enthalten, da dem LfV polizeiliche Befugnisse oder Weisungsbefugnisse nicht zustehen und das LfV Polizeibehörden auch im Wege der Amtshilfe nicht um Maßnahmen ersuchen darf, zu denen es selbst nicht befugt ist. Der Gesetzgeber hat die genannten Vorschriften mit dem Änderungsgesetz nicht geändert, weshalb sie für alle Aufgaben des LfV gelten. Der Hinweis auf die Gestapo ist im Zusammenhang mit der Übertragung der Aufgabe zur Vorfeldbeobachtung der organisierten Kriminalität deplatziert.

Entgegen der Auffassung des Datenschutzbeauftragten gibt es sehr wohl Fälle, in denen der Verfassungsschutz tätig werden kann, die Polizei aber (noch) nicht. Einfachstes Beispiel hierfür sind Erkenntnisse, die von ausländischen Diensten ausschließlich dem Landesamt für Verfassungsschutz mitgeteilt werden, nicht aber der Polizei. Solche Erkenntnisse konnten bislang nicht verwertet werden. Das Informationsverhalten ausländischer Dienste lässt sich auch durch Novellierung des HSOG nicht steuern.

Zu 9.1.2 Erweiterung der Befugnisse zum Abhören und Anfertigen von Bildaufnahmen in Wohnungen

Die in Ausschöpfung der Vorgaben des durch das Gesetz zur Änderung des Grundgesetzes vom 26. März 1998 (BGBl. I S. 610) geänderten Art. 13 GG geschaffenen neuen Regelungen über den verdeckten Einsatz besonderer technischer Mittel zur Informationsgewinnung sind auch weiterhin restriktiv. Sie setzen zum einen tatsächliche Anhaltspunkte für den Verdacht der Planung oder Begehung von Straftaten von erheblicher Bedeutung voraus (§ 5 Abs. 2 Nr. 1-3 LfVG). Zum Anderen entsprechen sie den restriktiven Regelungen des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298), geändert durch Gesetz vom 9. Januar 2002 (BGBl. I S. 391), mit der durch Art. 13 GG gebotenen Abweichung, dass für die Anordnung dieser Maßnahmen der Beschluss eines Richters erforderlich ist. Außerdem wurde durch das Änderungsgesetz die zulässige Frist für die Dauer einer solchen Anordnung auf längstens vier Wochen begrenzt. Durch diese - im Vergleich zum Recht des Bundes und anderer Länder kürzere - Befristung wird dem Grundrecht des Art. 13 GG in besonderer Weise Rechnung getragen.

Die Ansicht des Datenschutzbeauftragten, dass die Voraussetzungen für eine Gefahr im Verzug schwer zu begründen sein dürften, da der zuständige Richter des Amtsgerichts Wiesbaden jederzeit erreicht werden könne, mag zutreffen. Dies spricht jedoch nicht gegen die gesetzliche Regelung für diesen - wenn auch vielleicht seltenen - Ausnahmefall, sondern begründet lediglich, warum von dieser Notkompetenz kaum Gebrauch gemacht werden kann. Im Übrigen sieht das Gesetz für diese Fälle vor, dass eine richterliche Entscheidung unverzüglich, d.h. ohne schuldhaftes Zögern, nachzuholen ist.

Die vom Datenschutzbeauftragten für notwendig gehaltenen Regelungen über die Zweckbindung der so erhobenen Daten findet sich in § 5 Abs. 5 LfVG.

Zu 9.1.3 Auskunftspflichten gegenüber dem Landesamt für Verfassungsschutz

Im beschlossenen Änderungsgesetz sind Auskunftspflichten in enger Anlehnung an die Formulierungen im Bundesverfassungsschutzgesetz geregelt worden, die der Datenschutzbeauftragte als datenschutzrechtlich besser und rechtsstaatlicher beurteilt. Die Kritik des Datenschutzbeauftragten richtet sich jedoch nicht gegen den damals noch nicht vorliegenden hessischen Gesetzentwurf, sondern gegen Vorüberlegungen, die den damaligen Stand des entsprechenden Entwurfs aus Bundesebene widerspiegelten.

Weitergehend als der Bund sieht das hessische Gesetz auch Auskunftspflichten im Bereich der traditionellen Aufgaben des Verfassungsschutzes vor. Diese sind auch erforderlich, wenn z.B. das Verbot eines rechtsextremistischen oder eines islamistischen Vereins bevorsteht. Im Vorfeld eines solchen Verbots müssen z.B. Kontonummern und ihre Zuordnung zu dem betreffenden Verein festgestellt werden, damit dann mit diesen Angaben beim zuständigen Verwaltungsgericht eine Beschlagnahme des Kontos nach dem Vereinsrecht beantragt werden kann. Für die Feststellung der Zuordnung eines örtlichen Vereins zu einem Dachverein können dabei auch regelmäßige Kontobewegungen zwischen diesen Vereinen von Belang sein, wenn die Zuordnung nicht auf andere Weise feststeht.

Im Übrigen haben die Forderungen des Datenschutzbeauftragten in den detaillierten Regelungen des § 4 Abs. 7-12 LfVG ihren Niederschlag gefunden; sie entsprechen den auch im Bereich des Bundes geltenden Regelungen.

Zu 9.1.4 Herabsetzung des speicherungsrelevanten Alters von Jugendlichen

Das Alter wurde nicht - wie vom Datenschutzbeauftragten kritisiert - von 16 auf 12 Jahre, sondern auf 14 Jahre herabgesetzt. Dies entspricht der Regelung, die in einer Reihe von Ländern z.T. schon seit vielen Jahren gilt (z.B. Bayern, Berlin, Bremen, Hamburg, Rheinland-Pfalz).

Zu 9.1.5 Verlängerung der Lösch- und Prüffristen

Hier entspricht die Änderung des Landesrechts dem Bundesrecht.

Zu 9.2 Prüfung von Akten des Landesamts für Verfassungsschutz

Die Landesregierung begrüßt ausdrücklich die kontinuierliche Prüfung von Akten des Landesamts für Verfassungsschutz durch den Datenschutzbeauftragten und auch die Mitteilung der Prüfungsergebnisse im öffentlichen Tätigkeitsbericht, wenn dabei berechtigten Belangen des Geheimschutzes hinreichend Rechnung getragen wird. Dies ist im vorliegenden Bericht der Fall.

Zu 9.2.1 Kontrolle der Sicherheitsüberprüfungsakten

Die Ansicht des Datenschutzbeauftragten, für Sicherheitsüberprüfungen gäbe es in Hessen keine gesetzliche Grundlage, kann die Landesregierung, wie schon in früheren entsprechenden Stellungnahmen, so nicht teilen. Nach § 3 Abs. 3 LfVG setzt eine Sicherheitsüberprüfung zumindest die Kenntnis der betroffenen Person von der Einleitung der Überprüfung oder deren Zustimmung voraus. Auch weitere Personen dürfen nur mit ihrer Zustimmung in die Überprüfung einbezogen werden (§ 3 Abs. 3 LfVG). Außerdem ist die Mitwirkung des Landesamts für Verfassungsschutz bei der Sicherheitsüberprüfung gesetzlich geregelt (§ 2 Abs. 5 und 6, § 4 Abs. 2 und 5 LfVG).

Darüber hinaus wird in Anbetracht der Entwicklung in anderen Ländern und beim Bund geprüft, auch in Hessen den Entwurf eines Sicherheitsüberprüfungsgesetzes vorzulegen. Dies wird jedoch in dieser Legislaturperiode nicht mehr möglich sein.

Auf den Hinweis des Datenschutzbeauftragten, in der Sicherheitserklärung würden auch dann Angaben zu Referenz- und Auskunftspersonen erfragt, wenn diese gar nicht benötigt werden, wurde der Vordruck um den Zusatz "Nur auszufüllen bei einer Sicherheitsüberprüfung des Geheimhaltungsgrads Streng Geheim oder besonderer Anforderung des Geheimschutzbeauftragten" ergänzt.

Zu 9.2.2 Prüfung der Einsichtnahme des Landesamtes für Verfassungsschutz in Register und Akten öffentlicher Stellen sowie die darüber anzufertigenden Nachweise

Das berechtigte Monitum des Datenschutzbeauftragten hat dazu geführt, dass seit September 2001 beim Landesamt für Verfassungsschutz ein einheitliches Formular über den Nachweis entsprechender Einsichtnahmen verwendet wird, aus dem insbesondere das Aktenzeichen und der Zweck der Register- oder Akteneinsicht zu entnehmen ist.

Zu 10. Finanzwesen

Zu 10.1 Die Allgemeine Nachschau in der Abgabenordnung

Die angesprochene Umsatzsteuer-Nachschau wurde aus rechtssystematischen Gründen nicht in die Abgabenordnung, sondern in das Umsatzsteuergesetz (§ 27b) übernommen. Mit der Regelung wird der Finanzverwaltung die Möglichkeit eingeräumt, zu branchenüblichen Geschäfts- bzw. Arbeitszeiten die Geschäftsräume von Unternehmen unangekündigt in Augenschein zu nehmen. Auf diese Weise kann sich die Finanzverwaltung zeitnah einen objektiven, nicht geschönten Eindruck von den tatsächlichen betrieblichen Verhältnissen eines Unternehmers verschaffen. Eine vorherige Anmeldung eröffnet dagegen die Möglichkeit, einen ordnungsgemäßen Geschäftsbetrieb vorzutäuschen, sodass eine effektive Kontrolle erheblich erschwert wird.
Die Regelung wurde durch das Steuerverkürzungsbekämpfungsgesetz eingeführt und muss deshalb immer unter dem damit verfolgten Aspekt gesehen werden, den Umsatzsteuerbetrug - insbesondere in Form der so genannten Karussellgeschäfte - zu bekämpfen. Der steuerehrliche Unternehmer soll und wird von der Maßnahme verschont werden, da eine Konzentration auf die Problembereiche und die sich in diesem Umfeld bewegenden Unternehmer erfolgen wird. Dieser gesetzgeberischen Intention wird der Verwaltungsvollzug - schon allein aufgrund der vorgegebenen personellen Ressourcen - Rechnung tragen, sodass von der erweiterten Nachschaumöglichkeit nur mit Augenmaß und in begründeten Verdachtsfällen Gebrauch gemacht werden wird. Die zwischenzeitlich ergangenen Verwaltungsanweisungen zur Durchführung einer Umsatzsteuer-Nachschau tragen diesen Vorgaben Rechnung.
Die in den Bemerkungen des Datenschutzbeauftragten geäußerten Bedenken gegen die Umsatzsteuer-Nachschau werden deshalb nicht geteilt. Insbesondere ist darauf hinzuweisen, dass von der neuen Nachprüfungsmöglichkeit nicht - wie in den Bemerkungen wiederholt zum Ausdruck gebracht wird - willkürlich "ohne Anlass" bzw. "ohne vorausgehendes Fehlverhalten" Gebrauch gemacht wird. Vielmehr soll das neue Instrumentarium entsprechend dem Gesetzeszweck nur in begründeten Verdachtsfällen zum Einsatz gelangen, sodass steuerehrliche Unternehmer nichts zu befürchten haben werden.

Zu 10.2 Abgabenordnung und Datenschutz - ein altes Thema neu belebt

Den Ausführungen des Datenschutzbeauftragten, seitens der Finanzverwaltung bestünde ein "fast grenzenloser Ermittlungswunsch", kann nicht gefolgt werden. Die durchgeführte Datenerhebung ist vielmehr notwendiger Ausfluss aus dem gesetzlichen Auftrag, die Steuern gleichmäßig und vollständig festzusetzen und zu erheben (§ 85 AO).
Vor dem Hintergrund zahlreicher Beanstandungen des Verhaltens der Steuerverwaltungen der Länder durch Datenschutzbeauftragte der Länder, zunehmend aber auch von Beanstandungen des Bundesbeauftragten für den Datenschutz im Bereich der Verwaltung des steuerlichen Kindergeldes, wurde durch die Arbeitsgruppe "Datenschutz in der Abgabenordnung" im Oktober 2001 angeregt, zur besseren Abklärung der jeweiligen tatsächlichen und rechtlichen Fragen, zur Problembündelung, aber auch zur Klimapflege eine Koordinierungsrunde mit Vertretern der Datenschutzbeauftragten und Vertretern der obersten Finanzbehörden der Länder unter Leitung des BMF einzurichten, die sich mit grundsätzlichen Fragen, die Anlass von Einzelbeanstandungen im Bereich des Verfahrensrechts sind, befassen und Lösungsempfehlungen für die jeweiligen Gremien erarbeiten könnte. Der Vorschlag wurde in der Sitzung der Vertreter der obersten Finanzbehörden des Bundes und der Länder über Fragen der Abgabenordnung im Dezember einstimmig begrüßt und mittlerweile auch seitens der Datenschutzbeauftragten angenommen, sodass auf eine erfolgreiche Fortführung der vom Datenschutzbeauftragten aufgezeigten Gespräche zu hoffen ist.

Erfreulich ist die Beurteilung des Datenschutzbeauftragten, nach der im Rahmen der Automation die datenschutzrechtlichen Anforderungen an die Datensicherheit in Hessen beachtet werden.

Zu 10.3 Steuerliche Ermittlungen: Auskunftsersuchen, Rasterfahndung oder Zeugenbefragung ohne Grenzen?

Es ist zutreffend, dass das Finanzamt Wetzlar im Rahmen von präventiven steuerlichen Überprüfungen in seinem Zuständigkeitsbereich eine Vielzahl von Firmen aus dem Bauhaupt- und Baunebengewerbe nach §§ 85, 88, 90, 92, 93, 97 und 208 Abs. 1 Satz 1 Nr. 3 AO um steuerliche Auskunft gebeten hat. Gesetzliche Aufgabe der Steuerfahndung ist u.a. die Aufdeckung und Ermittlung unbekannter Steuerfälle. In diesem Aufgabenbereich ist das Stellen eines Sammelauskunftsersuchens eine zulässige Ermittlungsmaßnahme. Das Auskunftsersuchen beruht auf einer Ermessenentscheidung des Finanzamts Wetzlar, die im Rahmen von umfangreichen Vorfeldermittlungen getroffen wurde. Die Finanzverwaltung hat die Rechtmäßigkeit der steuerlichen Auskunftsersuchen des Finanzamts Wetzlar vom 27. Oktober 2000 eingehend geprüft. Die Prüfung hat ergeben, dass die Ermittlungsmaßnahmen des Finanzamts Wetzlar rechtmäßig sind. Das Ergebnis der Überprüfung und die hierfür maßgebenden Gründe wurden dem Datenschutzbeauftragten mit Schreiben des Ministeriums der Finanzen vom 25. Oktober 2001 - S 0320 A - 3 - II A 11 bereits mitgeteilt.

Zu 11. Gesundheit

Die Aussagen und Bewertungen des Datenschutzbeauftragten bedürfen keiner Ergänzung und treffen zu.

Zu 12. Statistik

Die Landesregierung hat das Zensusvorbereitungsgesetz im Gesetzgebungsverfahren unterstützt. Sie setzt sich nachhaltig für das zutreffend beschriebene Verfahren aus den genannten Gründen ein. Als ein weiteres Argument für den zu prüfenden Registerabgleich könnten Kosteneinsparungen aufgeführt werden. Ein Registerabgleich könnte nach dem derzeitigen Erkenntnisstand Kosteneinsparungen in beträchtlicher, aber noch nicht endgültig bezifferbarer Höhe erbringen.

Zu 13. Telekommunikation
Zu 13.1 Telekommunikations-Überwachungsverordnung

Die neue Telekommunikations-Überwachungsverordnung ist am 29. Januar 2002 in Kraft getreten. Die Neuregelung ist im Grundsatz zu begrüßen, da dadurch endlich die noch auf dem alten Fernmelderecht beruhende Fernmeldeverkehrsüberwachungsverordnung (FÜV) abgelöst worden ist. Inhaltlich stellt die Verordnung einen Kompromiss dar zwischen den öffentlichen Belangen und den Belangen der Wirtschaft, der die Polizeibehörden nur beschränkt zufrieden stellt. Dem Datenschutzbeauftragten ist darin beizupflichten, dass es erforderlich gewesen wäre, die Nutzung der IMEI-Gerätenummer ausdrücklich in der Verordnung zu regeln.

Zu 13.2 Einsatz des so genannten IMSI-Catchers durch Strafverfolgungsbehörden und Polizei
Zu 13.2.1 Einsatz zu repressiven Zwecken

Auch die Landesregierung erachtet es als wünschenswert, dass der Einsatz des so genannten "IMSI-Catchers" für Zwecke des Strafverfahrens auf eine präzise Rechtsgrundlage gestellt wird. Es handelt sich dabei um ein sinnvolles und angesichts der im mobilen Fernsprechverkehr eröffneten Möglichkeiten - etwa des Kartentausches - unerlässliches Ermittlungsinstrument. So hat sich auch die 72. Konferenz der Justizministerinnen und -minister vom 11. bis 13. Juni 2001 in Trier im Sinne eines diesbezüglich klarstellenden gesetzgeberischen Handlungsbedarfs ausgesprochen. Die Landesregierung hat daher den Gesetzesantrag der Freistaaten Bayern und Thüringen zu dem Entwurf eines Gesetzes zur Verbesserung des strafrechtlichen Instrumentariums für die Bekämpfung des Terrorismus und der Organisierten Kriminalität (BR-Drs. 1014/01) sowie die Initiative des Landes Niedersachsen zu dem Entwurf eines Gesetzes zur Verbesserung der Ermittlungsmaßnahmen wegen

des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Sanktionen (BR-Drs. 275/02), die entsprechende Ergänzungen der Strafprozessordnung vorsehen, unterstützt. Ein klarstellender Regelungsbedarf ergab sich auch daraus, dass mit dem Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 9. Januar 2002 (BGBl. I S. 361) in § 9 Abs. 4 des Bundesverfassungsschutzgesetzes für die Dienste eine ausdrückliche, spezialgesetzliche Regelung des Einsatzes des IMSI-Catchers zu den dortigen Zwecken geschaffen worden ist.

Allerdings sieht auch die Bundesregierung grundsätzlich den Einsatz des IMSI-Catchers GA 090 im strafprozessualen Bereich bereits durch die Vorschriften in den §§ 100a ff., 161 StPO als gedeckt an - so die Antwort der Bundesregierung vom 10. September 2001 auf eine Kleine Anfrage der Abgeordneten Dr. Edzard Schmidt-Jortzig, Jörg van Essen, Rainer Funke, Dr. Wolfgang Gerhardt und der Fraktion der FDP (BT-Drs. 14/6885).

Mit dem vom Bundestag am 17. Mai 2002 verabschiedeten und im Bundesrat am 21. Juni 2002 abschließend beratenen Gesetz zur Änderung der Strafprozessordnung (BR-Drs. 452/02) wurde in § 100i StPO eine gesetzliche Regelung zum Einsatz des IMSI-Catchers aufgenommen, sodass die Diskussion um die Zulässigkeit dieser Ermittlungsmaßnahme ihren Abschluss gefunden haben dürfte.

Zu 13.2.2 Einsatz zu präventiven Zwecken

Im präventivpolizeilichen Bereich besteht Einigkeit mit dem Datenschutzbeauftragten darüber, dass § 15 Abs. 1 Nr. 2 HSOG den Einsatz des IMSI-Catchers umfasst. Ob und ggf. mit welchem Inhalt die vom Datenschutzbeauftragten geforderte spezielle Regelung notwendig ist, wird nach Abschluss der einschlägigen bundesrechtlichen Rechtsänderungen zu prüfen sein.

Zu 14. Entwicklung im Bereich der Technik
Zu 14.1 Sicherheit von Anmeldeprozeduren an IT-Systemen und
Zu 14.2 Sicherheit von Windows NT Passwörtern

Die unter den Nr. 14.1 und 14.2 dargestellten technischen Möglichkeiten zur Anmeldung an IT-Systeme können aus fachlicher Sicht bestätigt werden. Zur Problematik der Passworte (Nr. 14.1.1) ist zu ergänzen, dass die mit dem Datenschutzbeauftragten abgestimmte, vom Landesautomationsausschuss verabschiedete Sicherheitsrichtlinie zu dem Verzeichnisdienst "Active Directory" die Sicherheit durch entsprechende Regelungen erhöht.
Die Nutzung von Chipkarten wird zur Zeit im Rahmen der Thematik "elektronische Signatur" im Zusammenhang mit Identifikation und Authentisierung diskutiert. Neben den technischen sind hier insbesondere organisatorische Probleme (Aufbau einer Ausgabestelle, "Trustcenter" u.Ä.) zu bewältigen.
Der Einsatz biometrischer Systeme ist bisher nicht vorgesehen.

Zu 14.3 Mitschneiden von Tastatureingaben

Die dargestellten Möglichkeiten sind aus der entsprechenden Literatur bekannt. Ein legaler oder illegaler Einsatz des Bauteils hat in der hessischen Landesverwaltung, soweit bekannt, noch nicht stattgefunden.

Zu 14.4 Personal Firewalls

Der Einsatz von "Personal Firewalls" ist - wie vom Datenschutzbeauftragten beschrieben - technisch möglich. Dieser Einsatz setzt jedoch erhebliche Kenntnisse im Bereich der Informationstechnik und der IT-Organisation voraus und verlangt vom Anwender einen nicht unerheblichen Zeitaufwand im Betrieb (ständige technische und organisatorische Updates). Daher wird der Einsatz von "Personal Firewalls" nur für am Internet befindliche "stand alone" PC empfohlen.

Der beste Firewall-Schutz wird durch den Anschluss an das Landesdatennetz (HCN 2000) mit einer durch die HZD professionell betriebenen "Firewall" erreicht. Diese Firewall ist stets auf dem neuesten Stand der technischen Möglichkeiten und wird ständigen Prüfungen unterzogen.

Zu 14.5 Ergebnisse von Prüfungen der Datensicherheit mithilfe eines Portscanners

Die vom Datenschutzbeauftragten angeführte Prüfung der Datensicherheit mithilfe eines Portscanners wurde in Zusammenarbeit mit der HZD durchgeführt. Dabei ist festzuhalten, dass der Portscanner innerhalb des Sicherheitsbereiches eingesetzt wurde. Ein Szenario, das davon ausging, dass ein "Intruder" uneingeschränkten Zugang zum TCP/IP-basierten Netz der Hessischen Landesverwaltung hat.

Die festgestellten besonders schwerwiegenden Schwachstellen wurden soweit möglich sofort, in den meisten Fällen innerhalb einer kurzen Frist abgestellt. Die zur mittleren und leichten Kategorie zählenden Schwachstellen wurden, soweit es sich um organisatorische und infrastrukturelle Probleme handelte, kurzfristig abgestellt. Soweit die Probleme systembedingt waren, wurde entschieden, im Bereich Microsoft auf das nächste "Service Pack" und bei den UNIX-Derivaten auf das nächste "Release" zu warten, in denen die aufgetretenen systemtechnischen Probleme durch die Hersteller abgearbeitet wurden.

Der Verbesserung der Sicherheit des gesamten Netzwerkes wird ein ständiges Augenmerk zuteil. Die HZD hat sich aufgrund der Aktion des Datenschutzbeauftragten ein "Intrusion Detection System", das auch einen Portscanner beinhaltet, beschafft und setzt das System regelmäßig zur Überprüfung und Überwachung des gesamten Netzwerkes ein.

Zu 14.6 Überprüfung einer übersandten Festplatte

Die vom Datenschutzbeauftragten dargestellte Sicherheitslücke bei der Folgenutzung von PC-Systemen (Speichereinheiten, Festplatten) hat zu einer Überprüfung der praktischen Handhabung geführt.

Es müssen Verfahren gefunden werden, die sicherstellen, dass alle Vorgängerdaten so verändert werden, dass sie nicht mehr rekonstruiert werden können. Bei vielen Hochschulen wird bereits jedes PC-System, das in einem anderen Arbeitsbereich eingesetzt werden soll, überprüft und die Festplatte mit einem speziellen Programm mit Nullen und Einsen überspielt und anschließend neu formatiert. Durch dieses Verfahren ist es technisch nahezu unmöglich, auf diesen Datenspeichern die vorher gesicherten Daten zu rekonstruieren. Ein solches Verfahren ist vor allem in den Arbeitsbereichen leicht zu verwirklichen, in denen die PC-Systeme zentral verwaltet und beschafft werden. Dies gilt vor allem für die Hochschulverwaltungen. Im Wissenschaftsbereich erfolgt meist eine dezentrale Administration der PC-Systeme. Die Hochschulen beabsichtigen daher, die Bemerkungen im Tätigkeitsbericht des Datenschutzbeauftragten zum Anlass zu nehmen, den Wissenschaftsbereich auf den sachgerechten Umgang mit Altsystemen und die Löschung von personenbezogenen Daten auf Datenträgern, insbesondere den Festplatten, hinzuweisen.

Zu 15. Soziales
Zu 15.1 Akteneinsichtsrecht und Auskunftsanspruch

Die Landesregierung teilt die rechtliche Einschätzung des Datenschutzbeauftragten.

Zu 15.2 Planung im Sozialleistungsbereich

Die Landesregierung teilt die Auffassung des Datenschutzbeauftragten. Bei der beabsichtigten Befragung der Sozialhilfeempfänger in der Stadt Frankfurt durch ein Privatunternehmen, u.a. über die Qualität der Arbeit des Sozialamtes, handelt es sich nicht um eine Auftragsdatenverarbeitung im Sinne § 80 SGB X, sondern, wie im Tätigkeitsbericht richtig dargestellt, um einen Fall des § 75 SGB X, welcher die Übermittlung von Sozialdaten u.a. für Vorhaben der Planungen im Sozialleistungsbereich regelt. Die Voraussetzungen für eine Erhebung nach § 75 SGB X sind wesentlich enger geknüpft (zumutbare Einwilligung der Betroffenen) als nach § 80 SGB X. Ein Antrag der Stadt Frankfurt am Main auf Genehmigung der Übermittlung von Sozialdaten für die Forschung und Planung nach § 75 SGB X liegt dem Sozialministerium bisher nicht vor (bei Redaktionsschluss dieser Stellungnahme Ende Juli).

Zu 15.3 Bekanntgabe von Heimbeiratsmitgliedern

Die Landesregierung teilt die rechtliche Einschätzung des Datenschutzbeauftragten. Allerdings dürfte die vorgeschlagene "Konsulatslösung" nicht praktikabel sein, denn die Heimaufsichtsbehörden sind nicht die Poststelle von Interessenverbänden. Praxisnäher wäre es, Interessenverbände unmittelbar an die Heimträger oder die Heimleitung zu verweisen, die Informationsmaterialien an den Heimbeirat weiterleiten können.

Zu 15.4 Sozialdatenschutz bei der Adoptionsvermittlung

Der Datenschutzbeauftragte geht im Rahmen seines Berichts nur auf die datenschutzrechtlichen Vorschriften des SGB I und X ein, die bei der Adoptionsvermittlung von Bedeutung sein können. Darüber hinaus sind bei der Adoptionsvermittlung aber die nachfolgenden spezialgesetzlichen Bestimmungen zu beachten:

- § 1758 BGB regelt ein so genanntes Offenbarungs- und Ausforschungsverbot.
- § 9b Abs. 2 Adoptionsvermittlungsgesetz enthält eine Regelung über die Akteneinsicht bei Vermittlungsakten. Die Vorschrift wurde im Rahmen des Gesetzes zur Neuregelung von Rechtsfragen auf dem Gebiet der internationalen Adoption und zur Weiterentwicklung des Adoptionsvermittlungsrechts vom 5. November 2001 (BGBl. S. 2950) in das Adoptionsvermittlungsgesetz eingefügt.

Zu 15.5 Rechtswidrige Übermittlung von Sozialdaten durch das Sozialamt der Kreisstadt Groß-Gerau an die Führerscheinstelle

Der geschilderte Sachverhalt ist der Landesregierung nicht bekannt, die Rechtsauffassung des Datenschutzbeauftragten wird geteilt. Aufgrund des Hinweises des Datenschutzbeauftragten ist davon auszugehen, dass künftig die Einhaltung der Datenschutzvorschriften durch die genannte Behörde sichergestellt ist.

Zu 15.6 Datenerhebung der Landesversicherungsanstalt Hessen

Die Darlegungen geben die korrekte Verfahrensweise der Datenerhebung bei der LVA Hessen zutreffend wieder. So dürfen Informationen über den Gesundheitszustand der Behinderten nur mit dessen Einwilligung erhoben werden.

Zu 15.7 Verfahren der Unfallkasse Hessen zur Beauftragung eines medizinischen Gutachters

Die Landesregierung teilt die Ansicht des Datenschutzbeauftragten, wonach die Träger der gesetzlichen Unfallversicherung die Betroffenen vor der Erteilung eines Gutachterauftrags auf ihr Widerspruchsrecht hinweisen und sie über den Zweck des Gutachtens informieren müssen.

Zu 16. Kammern

Die datenschutzrechtliche Beurteilung des Datenschutzbeauftragten hinsichtlich der von einigen hessischen Industrie- und Handelskammern geplanten Neuorganisation der Stammdatenerhebung und -verwaltung ihrer Mitgliedsbetriebe wird von der Landesregierung geteilt. Den Ausführungen ist aus rechtsaufsichtlicher Sicht nichts hinzuzufügen.

Zu 17. Ausländerrecht

Die vom Datenschutzbeauftragten bei der Ausländerbehörde des Landrats des Landkreises Offenbach beanstandeten 52 Ausschreibungsfälle wurden - wie zugesagt - korrigiert. Der Gesamtbestand der SIS-Ausschreibungen ist überprüft worden.

Die Mitarbeiterinnen und Mitarbeiter der Ausländerbehörde des Landrats des Landkreises Offenbach und des Oberbürgermeisters der Stadt Offenbach wurden erneut auf die strikte Einhaltung der Ausschreibungskriterien und den sorgfältigen Umgang mit personenbezogenen Daten hingewiesen.

Zu 18. Kommunen

Laut Bericht des Datenschutzbeauftragten hat die Gemeinde den Fehler behoben und die Homepage umgestaltet. Es besteht kein weiterer Handlungsbedarf.

Zu 19. Personalwesen
Zu 19.1 Evaluation der Lehre

Entsprechend der erprobt guten Zusammenarbeit der Hochschulen mit dem Datenschutzbeauftragten wird auch die datenschutzrechtliche Absicherung des § 3 Abs. 8 Satz 2 des Hessischen Hochschulgesetzes geschehen.

Die erforderlichen Satzungen werden derzeit noch in den Hochschulen diskutiert. Die vom Datenschutzbeauftragten in seinem Tätigkeitsbericht gemachten Ausführungen und ein von ihm erarbeitetes Grundsatzpapier vom 26. Juni 2001 stellen dabei eine wichtige Unterstützung dar. Im Übrigen wurde auch dieses Thema bereits mehrfach bei den Tagungen der Behördlichen Datenschutzbeauftragten der Hochschulen (vgl. zu 23.) behandelt.

Bei den zum Finanzressort gehörenden Schulen ist sichergestellt, dass personenbezogene Evaluierungsergebnisse nur im Einklang mit den datenschutzrechtlichen Bestimmungen verwendet werden.

Zu 19.2 Personaldatenverarbeitung in der Hessischen Versorgungsverwaltung

Die Übernahme eines lauffähigen modernen IT-Verfahrens aus Schleswig-Holstein war für die Verwaltung und die betroffenen Bürgerinnen und Bürger in jedem Fall ein Gewinn, da einerseits spätestens auf die zum 1. Januar 2002 anstehende Euro-Einführung zu reagieren war und andererseits der flächendeckende Verfahrenseinsatz bereits heute intern zu einer spürbaren Effektivitätssteigerung und damit zu kürzeren Bearbeitungszeiten im Sinne der Bürgerinnen und Bürger führt.

Im Zuge der Verfahrensübernahme wurde leider das Problem der Bearbeitung der Schwerbehindertenverfahren der eigenen Beschäftigten der hessischen Versorgungsverwaltung nicht ausreichend bedacht. Die in Schleswig-Holstein anderen organisatorischen Rahmenbedingungen und unterschiedlichen Datenschlüssel führten dazu, dass die im Verfahren vorhandenen Sicherungsmerkmale nicht automatisch gegriffen haben. Die Aussagefähigkeit dieser für kurze Zeit lesbaren Informationen muss jedoch an den aus dem alten hessischen Verfahren übernommenen Daten gemessen werden. Hier wurden die bundesweiten statistischen Behinderungsschlüssel genutzt, die das Krankheitsbild nur sehr pauschal formulierten und wenig geeignet waren, Rückschlüsse auf die tatsächlich vorliegenden Krankheiten zu geben. Bezeichnungen wie "Herz- und Kreislauferkrankungen mit einem weiteren inneren Leiden" oder "Verlust oder Teilverlust einer oberen Gliedmaße" mögen dies verdeutlichen. Erst mit dem neuen Verfahren werden konkrete, sich an den Krankheiten orientierende Behinderungsschlüssel, wie z.B. speziell für die Alzheimer Erkrankung, verwendet. Diese Schlüssel, gepaart mit weiteren Detailinformationen, erlauben erst eine Auskunfts- und Bearbeitungstätigkeit auch ohne Hinzuziehen der Akte. Diese Anpassung führt aktuell zu erheblichen und sehr aufwendigen Nacherfassungsarbeiten am übernommenen Datenbestand.

Anwender des Verfahrens sind insgesamt ca. 200 Beschäftigte in den Schwerbehindertenabschnitten der hessischen Versorgungsverwaltung. Zum Zeitpunkt der Beanstandung am 19. November 2001 stand jedoch dieses neue Verfahren den Dienststellen Darmstadt, Fulda und Bensheim noch überhaupt nicht zur Verfügung. Vorauszuschicken ist ferner, dass alle Mitarbeiterinnen und Mitarbeiter der Versorgungsverwaltung einer strengen Verschwiegenheitspflicht unterliegen. Bei mehr als 800.000 aktuellen Schwerbehindertenfällen hessenweit stellen die Bearbeitungsfälle der Mitarbeiterinnen und Mitarbeiter der Versorgungsverwaltung nur einen verschwindend geringen Anteil dar. Wenn weiter berücksichtigt wird, dass jeder Mitarbeiter pro Jahr ca. 800 Fälle zu bearbeiten hat, der freie Zugang zu den beanstandeten "Mitarbeiterfällen" nur für einen kurzen Zeitraum bestand und diese Daten nur dann verfügbar waren, wenn ausdrücklich nach ihnen recherchiert

wird deutlich, dass die potenzielle Gefährdung, so ärgerlich der Vorgang insgesamt auch ist, überschaubar war.

Mit der Verfahrensumstellung am 19. November 2001 und der zusätzlichen Bereitstellung des Merkmals "Mitarbeiter" ist der Zugriff auf die Daten von Beschäftigten der hessischen Versorgungsverwaltung durch die normalen Schwerbehindertensachbearbeiterinnen bzw. -sachbearbeiter ausgeschlossen. Über dieses Merkmal und die Amtskennung pro Bearbeitungsfall ist die direkte Zuordnung nur zu der/dem speziell beauftragten Sachbearbeiterin/ Sachbearbeiter gegeben.

Den Vorgaben des § 35 Abs. 1 Satz 3 SGB I folgend bzw. im Vorgriff darauf besteht seit Einführung des Verwaltungsverfahrens "Schwerbehindertenrecht" in Hessen die Weisung, dass die Bearbeitung von "Beschäftigtenfällen" in jeweils einem anderen Amt abzuwickeln ist. So werden z.B. die Fälle des Amtes Wiesbaden in Darmstadt bearbeitet. Die Bearbeitung erfolgt außerhalb der Personalsachbearbeitung von speziell beauftragten Mitarbeitern aus dem Fachbereich "Schwerbehindertenrecht". Nicht zuletzt deshalb ist eine Kollision mit der zuvor skizzierten Vorschrift ausgeschlossen, da die berechtigten Personen per dienstlicher Stellung grundsätzlich keinen Einfluss auf Personalentscheidungen haben.

Dem vom Datenschutzbeauftragten aus der zuvor genannten Regelung abgeleiteten Vorschlag für eine allgemeine Neuordnung der Zuständigkeitsregelung kann hingegen nicht gefolgt werden. Sie würde die Organisationsfähigkeit und angestrebte Neuausrichtung der Versorgungsverwaltung hin zu einem Mehr an Dienstleistung gegenüber dem Bürger nachteilig berühren. Die angedachte Zuordnung auch der allgemeinen Bearbeitungsfälle (z.B. nach Buchstaben sortiert) gegenüber festen Bearbeitern würde dazu führen, dass z.B. die Einrichtung zentraler Auskunfts- und Anlaufstellen in Form von Bürgerbüros praktisch unmöglich würde. Gerade solche Stellen und auch eine reibungslose Vertretung bei einer ausgesprochen niedrigen Personalausstattung sind ein wesentliches Element der anstehenden Verwaltungsmodernisierung.

Der Zugriff auf den hessenweiten Datenbestand orientiert sich grundsätzlich an den vorgegebenen Zuständigkeiten der Ämter. Dabei greifen die Sachbearbeiterinnen und Sachbearbeiter auf den Datenbestand in ihrem Amt zu. Dort liegen alle Fälle vom zentralen Datenbestand per Amtskennung selektiert vor. Die automatisierte Replikation zum zentralen Datenbestand erfolgt einmal pro Tag. Der zentrale Datenbestand ist nötig, um anhand eindeutiger Identifizierungen Doppelfeststellungen in Hessen zu vermeiden. Dieser Abgleich geschieht lediglich über Personendaten (Name, Vorname, Geburtsdatum, Anschrift). Die Falldaten über Krankheiten bzw. Feststellungen werden auf dieser Ebene nicht angezeigt.

Die abschließende Feststellung des Datenschutzbeauftragten kann nicht nachvollzogen werden. Zum einen wurde ohne jeden Zeitverzug eine akzeptable Lösung im Sinne der schwerbehinderten Beschäftigten "quasi über Nacht" realisiert, dem Vertreter des Datenschutzbeauftragten am 19. November 2001 präsentiert und von diesem so auch akzeptiert. Zu dem Problem insgesamt wurde mit Schreiben vom 13. Februar 2002 gegenüber dem Datenschutzbeauftragten ausführlich Stellung genommen. Eine Reaktion oder ergänzende Anforderungen vonseiten des Datenschutzbeauftragten liegen nicht vor. Offen ist lediglich noch die Vorlage der angekündigten Verfahrensdokumentation des Softwareherstellers. Diese wurde durch das Sozialministerium zugunsten notwendiger hessenspezifischer Softwareanpassungen in der Prioritätensetzung zunächst zeitlich zurückgestellt; sie wird nachgereicht.

Zu 20. Europa

Zu 20.1 Einrichtung einer gemeinsamen Geschäftsstelle für Schengen und Europol

Die Ausführungen des Datenschutzbeauftragten sind zutreffend.

Zu 20.2 Erneuerung des Schengener Informationssystems

Die Ausführungen sind im Wesentlichen zutreffend. Hinsichtlich der im 3. Spiegelstrich aufgezählten Stellen, die Zugang zum SIS erhalten sollen, ist

allerdings eine Klarstellung erforderlich. Eine Online-Anbindung der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) steht nicht zur Diskussion. Es ging bisher nur um einen indirekten Zugang zu nicht personenbezogenen Daten über gesuchte Dokumente. Eine Nutzung durch Rechtsanwälte und Notare ist ausweislich der Protokolle der Ratsarbeitsgruppe "SIS" bislang jedenfalls nicht explizit erörtert worden.

Zu 20.3 Geltendmachung des Auskunftsrechts

Die Landesregierung sieht sich durch den Bericht des Datenschutzbeauftragten in ihrer Auffassung bestätigt, dass sich die Akzeptanz des Datenschutzes in Deutschland - gerade bei Behörden und auch im Vergleich zu anderen Staaten in der EU - auf einem sehr hohen Niveau befindet.

Zu 20.4 Kontrolle des zentralen Teils des Schengener Informationssystems (CSIS)

Die Landesregierung sieht dem Bericht über das Ergebnis der Kontrolle des CSIS mit Interesse entgegen.

Zu 21. Archive

Um den Anliegen der Gedenkstätten, Archive, Museen und Forschungsstellen im Ausland zu entsprechen, ist das Hessische Archivgesetz novelliert worden. Die in Abstimmung mit dem Datenschutzbeauftragten formulierte und in seinem Bericht vorgestellte Regelung des § 17a ist inzwischen in Kraft getreten (vgl. GVBl. I 2002, S. 34).

Zu 22. Bibliotheken

Die dargestellten Mängel, die bei einer exemplarischen Prüfung der Stadt- und Universitätsbibliothek Frankfurt festgestellt wurden, sind zwischenzeitlich bereinigt worden. Eine Vereinbarung über die Zusammenarbeit auf dem Gebiet der Bibliotheksdatenverarbeitung (PICA) zwischen der Johann-Wolfgang-Goethe-Universität und der Stadt Frankfurt wurde am 11./12. Januar 2002 geschlossen. Der Datenschutzbeauftragte wurde über den Vertragsabschluss bereits informiert.

Die übrigen Hochschulen haben die Bemerkungen zum praktizierten Verfahren im Bibliotheksbereich zum Anlass genommen, die jeweils vor Ort geltende Praxis zu überprüfen und sind dabei, diese ggf. an die rechtlichen Erfordernisse anzupassen.

Zu 23. Hochschulen

Seit Jahren findet ein enger, vertrauensvoller Informations- und Erfahrungsaustausch zwischen den Behördlichen Beauftragten für den Datenschutz der Hochschulen des Landes Hessen statt. An diesen regelmäßigen Tagungen nehmen auch Vertreter des Datenschutzbeauftragten teil. Diese Art der Abstimmungen und Beratungen, bereits im Vorfeld von möglichen Problemen sowie Schwierigkeiten bei der Umsetzung der Datenschutzgesetzgebung, hat sich bewährt. Vor allem nützt die frühzeitige Einbeziehung des Datenschutzbeauftragten der konkreten Umsetzung der Datenschutzregelungen. Die Informationswege werden vereinfacht und beschleunigt. Aus diesem Grund soll diese gemeinsame Abstimmungsrunde auch beibehalten werden, da sie eine wichtige Unterstützung der täglichen Arbeit bei Fragen zum Datenschutz in den Behörden darstellt. Gleichzeitig wird eine hohe Transparenz bereits im Vorfeld von Entscheidungen über Datenschutzregelungen geschaffen, damit rechtzeitig über allgemein verträgliche Konzepte entschieden werden kann. Damit bedarf es in aller Regel nicht mehr nachträglicher Korrekturen.

Der Datenschutzbeauftragte wird somit in einem sehr frühen Planungsstadium beteiligt und sein Sachverstand kann in aller Regel bereits vor der verwaltungstechnischen Umsetzung berücksichtigt werden.

Die Einführung neuer Verwaltungsverfahren, z.B. die Chipkarte als ein wichtiger Bestandteil für eine Vereinfachung von Verwaltungsprozessen, dürfte eines dieser sehr positiven Beispiele sein, bei denen trotz unterschiedlicher gedanklicher Ansätze bei einzelnen Hochschulen eine datenschutz-

rechtlich unbedenkliche Lösung gemeinsam mit dem Datenschutzbeauftragten gefunden wurde.

Zu 24. Rundfunk

Der Datenschutzbeauftragte hat das Problem an die Staatskanzlei herangetragen und angeregt, bei der nächsten Änderung des Rundfunkgebührenstaatsvertrags (RfGebStV) die Regelung des § 4 Abs. 5 Satz 1 dahin zu modifizieren, dass Rundfunkteilnehmer zur Auskunft nur verpflichtet sind, wenn sich an ihrem Teilnehmerverhältnis seit der Anmeldung eines Rundfunkempfangsgeräts etwas verändert hat.

Die Staatskanzlei hat das Anliegen auf Fachebene im Kreise der Rundfunkreferenten der Länder zur Diskussion gestellt. Das Ergebnisprotokoll der Rundfunkreferentensitzung vom 18./19. November 2001 weist hierzu folgendes aus:

"Das Anliegen wurde erörtert. Es wurde darauf hingewiesen, dass im Rahmen der großen Lösung zur Novellierung des Rundfunkgebührenrechts sogar ein erweiterter Datenabgleich für die Anstalten geprüft werden muss. Angesichts dieser Sachlage sind die Anregungen des Hessischen Datenschutzbeauftragten in dieser Diskussion zu bewerten."

Die in dem Protokoll erwähnten Überlegungen zur Neustrukturierung der Rundfunkgebühr zielen darauf, die Rundfunkgebühr im privaten Bereich künftig haushaltsbezogen zu erheben. Es soll eine widerlegliche Vermutung im Rundfunkgebührenstaatsvertrag verankert werden, dass in einem privaten Haushalt üblicherweise Rundfunkempfangsgeräte (Hörfunk- und Fernsehen) bereitgehalten werden. Im Rahmen der staatsvertraglichen Umsetzung der geplanten Neustrukturierung der Rundfunkgebühr wird auch der Rundfunkgebührenstaatsvertrag - und damit auch § 4 Abs. 5 - zu modifizieren sein. Die politischen und fachlichen Beratungen hierzu sind allerdings noch nicht abgeschlossen. Die Staatskanzlei hat den Datenschutzbeauftragten hierüber mit Schreiben vom 22. Dezember 2001 informiert.

Das Problem wird in der Praxis - bezogen auf den Hessischen Rundfunk - dadurch entschärft, dass der Hessische Rundfunk Anschriften von Rundfunkteilnehmern, sofern dies gewünscht wird, aus dem so genannten Mailing-Verfahren herausnimmt. Zudem hat der Intendant des Hessischen Rundfunks zugesagt, gegenüber der GEZ auf eine moderate Gestaltung des betreffenden Mailing-Formulars zu dringen.

Die rechtliche Auslegung des § 4 Abs. 5 Satz 1 RfGebStV, wie sie der Datenschutzbeauftragte seiner Beanstandung zugrunde legt, ist nicht unbestritten. Nach Sinn und Zweck des § 4 Abs. 5 Satz 1 RfGebStV und mit Blick auf das Ziel, die Rundfunkgebühren-Belastung der Bürger in Grenzen zu halten, lässt sich sehr wohl die Auffassung vertreten, die Vorschrift rechtfertige auch die in längeren Zeitintervallen wiederholte Nachfrage, ob ein Teilnehmer, der in der Vergangenheit z.B. nur ein Hörfunkgerät angemeldet hatte, nunmehr auch ein Fernsehgerät nutzt. Die Frage, ob das Auskunftsersuchen positiv oder als Negativ-Attest ausgestaltet ist, erscheint in diesem Zusammenhang von nachrangiger Bedeutung. Angesichts der bevorstehenden Änderung des Rundfunkgebührenstaatsvertrags kann die Entscheidung über die "richtige" Auslegung des § 4 Abs. 5 aber letztlich dahin stehen. Dem Datenschutzbeauftragten ist jedenfalls darin recht zu geben, dass die Rundfunkanstalten gehalten sind, ihr Auskunftsrecht nach § 4 Abs. 5 RfGebStV "bürgerschonend" wahrzunehmen. Der Hessische Rundfunk hat hierzu - wie oben erwähnt - bereits entsprechende Erklärungen abgegeben.

Zu 25. Wahlrecht

Die unter dieser Ziffer angesprochenen Gesetzesänderungen sind durch das Gesetz zur Änderung des Landtags- und des Kommunalwahlgesetzes vom 6. Februar 2002 (GVBl. I S. 22) mittlerweile in Kraft getreten.

Soweit vom Datenschutzbeauftragten zu der Regelung des § 17 Abs. 5 des Landtagswahlgesetzes bzw. § 6 Abs. 5 KWG angemerkt wurde, dass es datenschutzrechtlich wünschenswert wäre, die von der Übermittlung betroffenen Personen vor der Herausgabe der Daten über die beabsichtigte Übermittlung zu informieren, wird an der ebenfalls in dieser Ziffer wiedergegebenen Stellungnahme festgehalten. Die vorgenannten Vorschriften stellen für die Gemeindebehörden bzw. Gemeindevorstände keine eigenständige Ermächti-

gungsgrundlage zur Datenerhebung bei Landtags- bzw. Kommunalwahlen dar, sondern erlauben nur einen Zugriff auf die für Bundestagswahlen nach § 9 Abs. 5 BWG erhobenen Daten. Da das Bundeswahlrecht in die ausschließliche Gesetzgebungskompetenz des Bundes fällt (Art. 38 Abs. 3, 70 Abs. 1 GG), kann auch nur der Bund eine Regelung über die vom Datenschutzbeauftragten gewünschte Information der Betroffenen schaffen.

Zu 26. Bilanz

Zu 26.1 Prüfung von Statistikstellen (27. Tätigkeitsbericht, Ziff. 19; 28. Tätigkeitsbericht, Ziff. 19)

Die Landesregierung nimmt mit Befriedigung zur Kenntnis, dass in allen geprüften Kommunen eine dem Datenschutz genügende Lösung realisiert werden konnte.

Zu 26.2 Gesetzesinitiative für ein Informationszugangsgesetz (29. Tätigkeitsbericht, Ziff. 3)

Nachdem der Gesetzentwurf von den Fraktionen der CDU und der FDP abgelehnt wurde, erübrigt sich eine Stellungnahme der Landesregierung hierzu.

Zu 26.3 Verkehrsüberwachung durch Videoaufzeichnung (29. Tätigkeitsbericht, Ziff. 4.2)

Die Firma ZN Vision Technologies AG hat ein Verfahren entwickelt, das Gesichter auf einer Videoaufnahme erst nach einer zielgerichteten Entschlüsselung erkennbar macht. Das Verfahren befindet sich derzeit allerdings noch in einem Laborstadium. Die ursprünglich noch für Mai dieses Jahres vorgesehene Vorführung des Verfahrens in der Hessischen Polizeischule musste kurzfristig abgesagt werden. Zu dieser Präsentation wurde bzw. wird auch der Datenschutzbeauftragte eingeladen werden.

Über die Kosten des Verfahrens kann eine Aussage erst nach Eintritt der Produktionsreife getroffen werden. In diesem Zusammenhang ist darauf hinzuweisen, dass die um die Verschlüsselungstechnik erweiterten Videogeräte erst nach erneuter Prüfung und Zulassung durch die Physikalisch-Technische Bundesanstalt (PTB) eingesetzt werden dürften.

Zu 26.4 Späte aber richtige Einsicht (29. Tätigkeitsbericht, Ziff. 6.1.1)

Die Darlegungen des Datenschutzbeauftragten geben die Stellungnahme der Landesregierung zum 29. Tätigkeitsbericht im Ergebnis zutreffend wieder.

Zu 26.5 Das Finanzamt im Firmennetz (29. Tätigkeitsbericht, Ziff. 8.2)

Wie im Tätigkeitsbericht dargestellt, wurden die Forderungen des Datenschutzbeauftragten auf Eingrenzung des Datenzugriffsrechts nach § 147 Abs. 6 AO durch die im BMF-Schreiben vom 16. Juli 2001 (BStBl I, 415) dargestellten Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen weitgehend berücksichtigt. Eine Regelung über eine besondere Protokollierungspflicht bezüglich der Zugriffe ist nicht erforderlich.
Die hessischen Finanzämter wurden inzwischen darauf hingewiesen, dass durch den Datenzugriff der sachliche Umfang der Betriebsprüfung nicht erweitert werde. Sie wurden angewiesen, aus diesem Grund einen systematischen und routinemäßigen Abgleich der Daten verschiedener Steuerpflichtiger zu unterlassen (OFD-Rdvfg. vom 22. April 2002 - S 1500 A - 4 - St III 20, Betriebsprüfungskartei der OFD Frankfurt am Main, § 8 BpO, Karte 1). Somit wurde auch dieser Forderung des Datenschutzbeauftragten entsprochen.

Zu 26.6 Medizinische Forschungsnetze

Bei dem Kompetenznetz Parkinson e.V. handelt es sich offenbar um ein universitätsgebundenes Forschungsnetzwerk. Das Projekt war im Sozialministerium bisher nicht bekannt.

Wiesbaden, 25. November 2002

Der Hessische Ministerpräsident
Koch

Der Hessische Minister des Innern
und für Sport
Bouffier