16. Wahlperiode

Drucksache **16/1679**

HESSISCHER LANDTAG

11. 12. 2003

Stellungnahme der Landesregierung

betreffend den Einunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Drucksache 15/4790

Eingegangen am 11. Dezember 2003 · Ausgegeben am 15. Januar 2004

Druck: Druckerei Chmielorz GmbH · Ostring 13 · 65205 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Stellungnahme zu:

1.	Vorwort	5
	"Kernpunkte des 31. Tätigkeitsberichts"	5
2.	Terrorismusbekämpfung	5
3.	Querschnittsthemen	5
3.1	Videoüberwachung	5
3.1.1	Gemeinsame Verfahren	6
3.1.2	Neue Anlagen in Kommunen	6
3.1.3	Videoüberwachung in Verkehrsmitteln	6
3.1.4	Videoüberwachung der Sicherheitszone einer Justizvollzugsanstalt	6
3.2	Auftragsdatenverarbeitung im Raumordnungsverfahren – Ausbau des Rhein-Main-Flughafens	7
3.3	Datenverarbeitung im Zusammenhang mit der Verleihung von Auszeichnungen und Ehrungen	7
3.4	Verweigerung der Auskunft über eigene Dateien	7
3.4.1	Justizvollzug	7
3.4.2	Strafverfolgung	8
3.4.3	Ausländer	8
3.4.4	Verfassungsschutz	8
3.4.5	Polizei	8
3.4.5.1	Unfallaufnahme	8
3.4.5.2	Noch ein Haftbefehl	8
3.4.6	Finanzämter	9
3.5	Elektronisches Fahrgeldmanagement	9
4.	Europa – Schengener Durchführungsübereinkommen	9
4.1	Gemeinsame Geschäftsstelle	9
4.2	Erneuerung des Schengener Informationssystems	9
5.	Justiz	11
5.1	Rahmenbedingungen für den IT-Einsatz in der Justiz	11
5.2	Unzulässige Auskunftsersuchen an Pflichtverteidiger nach Steuerdaten	11
6.	Polizei- und Strafverfolgungsbehörden – "Vorbeugende" Fahndung nach einem Zechpreller	11
7.	Ordnungswidrigkeiten	11
8.	Verfassungsschutz	12
8.1	Neues Verfassungsschutzgesetz	12
8.2	Keine Abhörbefugnisse gegenüber Journalisten und anderen besonders geschützten Personengruppen	12
8.3	Personenbezogene Daten in Sachakten des Verfassungsschutzes	14
8.4	Informationsbesuch beim Landesamt für Verfassungsschutz	15
9.	Ausländerrecht	15
9.1	Prüfung des Einbürgerungsverfahrens	15

9.2	Datenübermittlung aus dem Erziehungsregister	17
10.	Finanzwesen	17
10.1.1	Zugriff auf Firmen-EDV	17
10.1.2	Umsatzsteuer-Nachschau	17
10.1.3	Steuernummern auf Rechnungen	18
10.1.4	Freistellungsbescheinigungen im Internet	18
10.1.5	Kontenevidenz	18
10.1.6	Steuerdatenabrufverordnung	18
10.1.7	Finanzrechtsprechung und Kontrollmitteilungen	18
10.2	Steuernummern von Unternehmen – ein ungeschütztes Datum?	19
10.2.1	Steuernummern auf der Rechnung	19
10.2.2	Steuerabzug bei Bauleistungen	19
10.3	Keine zusätzlichen Kontrollmitteilungen zur geplanten Abgeltungssteuer	20
11.	Recht der Presse, Medien- und Teledienste	20
11.1.	Datenschutzvorschriften für die hessische Presse	20
11.1.1	Auffangregelung	21
11.1.2	Redaktionsinterner Datenschutzbeauftragter	21
11.1.3	Zusätzliche Privilegierung	21
11.2	Novelliertes Datenschutzrecht für Tele- und Mediendienste	22
12.	Entwicklungen und Empfehlungen im Bereich der Technik	22
12.1	Mobile Computing	22
12.1.1	Überblick über die Technologien	22
12.2	Einsatz von Windows 2000 und Active Directory	22
12.3	Software-Sicherheitslücken	23
12.4	Sichere Internetanbindung über eine Terminalserverlösung (Graphical Firewall – GFW)	23
12.5	Prüfung von Softwareprodukten, die mit Dateiservern eingesetzt werden	24
13.	Kommunen	24
13.1	Briefwahlunterlagen per E-Mail beantragen	24
13.2	Unzulässige Datenübermittlung durch ein städtisches Frauenbüro	25
13.3	Erfassung von Auskunftssperren im Einwohnermelderegister	25
14.	Hochschulen	25
14.1	Evalutation der Lehre an hessischen Hochschulen	25
15.	Schulverwaltung und Schulen	26
16.	Archivwesen	26
17.	Gesundheitswesen	27
18.	Sozialwesen	27
18.1	"Offensiv-Gesetz"	27
18.2	Dienstaufsicht und Sozialdatenschutz	27
18.3	Auskunftsansprüche im Kinder- und Jugendhilferecht	27
18.4	Datenschutz im Adoptionsvermittlungsverfahren	27

19.	Personalwesen	28
19.1	Weitergabe dienstlicher Unterlagen bei der Anrufung des Hessischen Datenschutzbeauftragten durch einen Personalrat	28
19.2	Übertragung der Zuständigkeiten für Untersuchungen zur Dienstfähigkeit von Beamtinnen und Beamten in der hessischen Landesverwaltung auf die Versorgungsämter	28
20.	Verkehrswesen	29
21.	Vermessungswesen	29
22.	Kammern	29
23.	Bilanz	29
23.1	Einsatz des so genannten IMSI-Catchers durch Strafverfolgungsbehörden und Polizei (30. Tätigkeitsbericht, Nr. 13.2)	29
23.2	Neue Informationssysteme für die Polizei (30. Tätigkeitsbericht, Nr. 8.1)	29
23.3	Projekt "Elektronische Fußfessel" (28. Tätigkeitsbericht, Nr. 6; 29. Tätigkeitsbericht, Nr. 20.2)	30
23.4	Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen (30. Tätigkeitsbericht, Nr. 8.4)	30
23.5	Modellprojekt Mammographie-Screening (30. Tätigkeitsbericht, Ziff 11.1)	31
23.6	Datenschutz in der Abgabenordnung (30. Tätigkeitsbericht, Nr. 10.2 und 27.7)	31
23.7	Zusammenarbeit bei der Produktion von Fernsehsendungen – Reality TV (30. Tätigkeitsbericht, Nr. 8.2)	31

Zu 1. Vorwort

Die Landesregierung nimmt die Feststellung des Hessischen Datenschutzbeauftragten, dass im Berichtsjahr willentliche Verstöße gegen die datenschutzrechtlichen Vorschriften in größerem Umfang nicht aufgetreten sind, diese vielmehr überwiegend auf unbedachtem Fehlverhalten beruhten, mit Befriedigung zur Kenntnis. Die Landesregierung missbilligt jedes auf einen willentlichen Verstoß gegen datenschutzrechtliche Vorschriften zielende Verhalten und geht davon aus, dass alle in Behörden und Einrichtungen des Landes tätigen Beschäftigten ihre Aufgaben in diesem Bewusstsein wahrnehmen.

Zu "Kernpunkte des 31. Tätigkeitsberichts"

Die Ziffern in diesem Abschnitt des Tätigkeitsberichts fassen im Wesentlichen den jeweiligen Inhalt der nachfolgenden Abschnitte zusammen, ohne darüber hinaus neue Aspekte anzusprechen. Eine gesonderte Stellungnahme dazu erübrigt sich daher.

Zu 2. Terrorismusbekämpfung

Die aufgrund der Anschläge vom 11. September 2001 eingeleitete "Rasterfahndung" ist inzwischen abgeschlossen.

Entgegen der Ansicht des Hessischen Datenschutzbeauftragten, die von den Datenschutzbeauftragten der anderen Bundesländer nicht aufgegriffen wurde, sieht die Landesregierung in der Anordnung keinen Verwaltungsakt gegenüber dem Betroffenen, dessen Daten herausgegeben werden sollen. Nach § 35 Verwaltungsverfahrensgesetz setzt ein Verwaltungsakt eine hoheitliche Regelung mit Außenwirkung voraus, woran es im vorliegenden Fall in Bezug auf die betroffenen Personen fehlt.

Die Landesregierung ist der Auffassung, dass der neu gefasste § 26 HSOG eine gut handhabbare Regelung der "Rasterfahndung" enthält und dass das Hessische Landeskriminalamt (HLKA) von dieser Bestimmung in zutreffender Weise Gebrauch gemacht hat. Sie hat keinen Zweifel daran, dass die Maßnahme geeignet ist, so genannte "Schläfer" aufzuspüren. Dabei ist zu berücksichtigen, dass die "Rasterfahndung" nur einen Zwischenschritt auf dem Weg zur Klärung der Gefährdungslage darstellt. Personen, die als "Trefferfälle" erscheinen, werden anschließend einzeln durch die örtlichen Staatsschutzdienststellen anhand von weiteren Kriterien überprüft, die sich für einen automatisierten Abgleich nicht eignen. Erst nach dieser arbeitsaufwändigen Überprüfung kann eine Aussage dazu getroffen werden, ob es in Hessen überhaupt "Schläfer" gibt. Sollte es sich erweisen, dass das entgegen den Befürchtungen nicht der Fall ist, würde dieses erfreuliche Ergebnis die Eignung der "Rasterfahndung" keineswegs in Frage stellen. Die Eignung von Gefahrerforschungseingriffen hängt naturgemäß nicht davon ab, ob die Gefahr tatsächlich besteht. Aus diesem Grunde ist es unerheblich, ob die "Rasterfahndung" in anderen Bundesländern Ergebnisse zeitigt oder, wie der Hessische Datenschutzbeauftragte meint, tatsächlich "ohne vorzeigbare Erkenntnisse geblieben" ist.

Zu 3. Querschnittsthemen

Zu 3.1 Videoüberwachung

Der Hessische Datenschutzbeauftragte führt aus, die Zahl der Videoüberwachungsanlagen habe auch im Berichtsjahr weiter zugenommen bzw. es sei zu einer stetigen Ausweitung der Videoüberwachung in den Städten gekommen (siehe auch "Kernpunkte des 31. Tätigkeitsberichts" Nr. 5). Dadurch könnte ein falscher Eindruck über den tatsächlichen Umfang der Videoüberwachung entstehen. In Hessen werden zurzeit (Stand Oktober 2003) insgesamt nur acht Videoüberwachungsanlagen von den Polizeibehörden in Kooperation mit den Kommunen an einzelnen Kriminalitätsbrennpunkten auf öffentlichen Straßen und Plätzen genutzt. Es handelt sich um Anlagen in Darmstadt (Kleinschmidtsteg), Frankfurt (Konstablerwache), Fulda (Bahnhofsvorplatz), Gießen (Marktplatz), Hofheim (Busbahnhof), Kassel (Straßenzug Untere Königstraße/Landgraf-Philipp-Platz), Limburg (Bahnhofsvorplatz einschl. Unterführung) und Wiesbaden (Platz der deutschen Einheit). Dabei wird die Anlage in Hofheim ausschließlich von der Kommune genutzt, die lediglich im Bedarfsfall die Aufzeichnungen der Polizei zur Verfügung stellt.

Darüber hinaus äußert der Hessische Datenschutzbeauftragte die Auffassung, dass Videoüberwachung dort erfolgreich sei, wo ihr Ziel auf eine Verlagerung von Kriminalitätsschwerpunkten ausgerichtet ist. Ziel der Videoüberwachung ist jedoch nicht die Verlagerung sondern vielmehr die Reduzierung von Kriminalitätsbrennpunkten und die Verbesserung des Sicherheitsgefühls. Die Erfahrungen zeigen, dass in allen videoüberwachten Bereichen die registrierten Fallzahlen im Vergleich zum Zeitraum vor der Einführung der Videoüberwachungsanlagen gesunken sind. Die Videoüberwachung erfährt eine hohe Akzeptanz in der Bevölkerung.

Zu 3.1.1 Gemeinsame Verfahren

Die Schilderung des Hessischen Datenschutzbeauftragten trifft im Wesentlichen zu. Allerdings hat das Landespolizeipräsidium aufgrund der Unzulässigkeit gemeinsamer Verfahren nach § 15 HDSG im Anwendungsbereich des HSOG stets darauf geachtet, dass der Einsatz der Videoüberwachungsanlagen in einer Weise geregelt wurde, dass eine gleichzeitige Nutzung durch Polizei und Gefahrenabwehrbehörde ausgeschlossen ist. Nach einem Hinweis des Hessischen Datenschutzbeauftragten, dass auch die gemeinsame Nutzung einer Aufzeichnungseinheit zu einem gemeinsamen Verfahren führe, wurden die Unterlagen erneut geprüft. Dabei konnte festgestellt werden, dass dieses Kriterium einzig auf die Anlage in Fulda zutrifft. Das Polizeipräsidium Osthessen wurde gebeten, nach Lösungsmöglichkeiten zu suchen. Ein Bericht steht noch aus.

Im Zuge des anstehenden HSOG-Änderungsgesetzes ist vorgesehen, die Zusammenarbeit zwischen Polizeibehörden und Gefahrenabwehrbehörden rechtlich zu vereinfachen und das Problem einer gesetzlichen Klärung zuzuführen.

Zu 3.1.2 Neue Anlagen in Kommunen

Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend.

Die Videoanlage am Gießener Marktplatz wird nach wie vor allein von dem zuständigen Polizeipräsidium Mittelhessen betrieben. Die Stadt Gießen hat keinen Zugriff auf die Daten der Videoüberwachungsanlage. Vor einer Realisierung, deren Zeitpunkt derzeit nicht absehbar ist, wird die Rechtslage hinsichtlich der Zulässigkeit eines gemeinsamen Verfahrens der Datenverarbeitung sowie der Voraussetzungen des § 14 Abs. 4 HSOG geprüft werden. Zudem wird das Polizeipräsidium Mittelhessen die in Bearbeitung befindliche Dienstanweisung im Sinne der Anregung des Hessischen Datenschutzbeauftragten deutlicher formulieren.

Die vom Hessischen Datenschutzbeauftragten geforderte technische Ausgestaltung der Videoüberwachungsanlage im Hinblick auf die so genannte "Privatzonenschaltung" war bereits bei Installation der Anlage vorgesehen. Wegen einer technischen Störung konnte sie allerdings erst Ende Mai aktiviert werden.

Zu 3.1.3 Videoüberwachung in Verkehrsmitteln

Die Entscheidung über den Einbau von Videoüberwachungseinrichtungen in Bussen und Bahnen des öffentlichen Nahverkehrs obliegt den jeweiligen Betreibern der Verkehrslinie. Die Landesregierung ist daran nicht beteiligt.

Zu 3.1.4 Videoüberwachung der Sicherheitszone einer Justizvollzugsanstalt

Der Vorgang wurde ohne Beteiligung des Fachressorts zwischen dem Hessischen Datenschutzbeauftragten und der Justizvollzugsanstalt behandelt. Die Vorschläge des Hessischen Datenschutzbeauftragten wurden aufgegriffen und durch Abklebungen erreicht, dass ein über den Sicherheitsbereich hinausgehendes Betrachten mittels der Kamera nicht mehr möglich ist. Der Beschwerde der Anwohner wurde einvernehmlich abgeholfen.

Zu 3.2 Auftragsdatenverarbeitung im Raumordnungsverfahren – Ausbau des Rhein-Main-Flughafens

Die Landesregierung hat dem Bericht des Hessischen Datenschutzbeauftragten nichts hinzuzufügen.

Zu 3.3 Datenverarbeitung im Zusammenhang mit der Verleihung von Auszeichnungen und Ehrungen

Nach eingehender Prüfung hat sich die Landesregierung entschieden, von einer Initiative für ein Gesetz über den Datenschutz bei öffentlichen Auszeichnungen und Ehrungen Abstand zu nehmen.

Öffentliche Auszeichnungen und Ehrungen sind staatliche Gunsterweise, die auf der Grundlage von Vergabekriterien und -verfahren verliehen werden, die allein der jeweilige Stifter bestimmt. Im Bund erfolgt dies auf der Grundlage von Stiftungserlassen des Bundespräsidenten, auf Landesebene in der Regel auf der Grundlage von Erlassen des Ministerpräsidenten und in den Kommunen auf der Grundlage eigenständiger kommunaler Regelungen.

Die überwiegende Zahl der Bundesländer und der Bund verfügen über diese Bestimmungen hinaus nicht über eine besondere gesetzliche Vorschrift zur Datenverarbeitung in diesem Bereich und sehen insoweit auch keinen aktuellen Handlungsbedarf. Dort hält man ein solches Gesetz offenbar nicht für erforderlich. Der Bundesbeauftragte für den Datenschutz hat diese Frage bereits früher geprüft und in seinem im Jahr 2001 vorgelegten 18. Tätigkeitsbericht mitgeteilt, im Hinblick auf die Deregulierungsbestrebungen der Bundesregierung habe er dem Bundesinnenministerium sein Verständnis signalisiert, "in dieser Frage auf eine normative Regelung zu verzichten".

Selbst diejenigen Länder, die über eine besondere Bestimmung zur Datenverarbeitung bei der Vergabe öffentlicher Auszeichnungen in ihren Landesdatenschutzgesetzen verfügen, beurteilen den notwendigen Umfang einer Regelung anders als der Hessische Datenschutzbeauftragte. Eine nähere Prüfung zeigte, dass keine dieser Regelungen alle Anforderungen des Hessischen Datenschutzbeauftragten, wie er sie im Tätigkeitsbericht stellt, erfüllt. Die Frage, ob ein Gesetz über die Datenverarbeitung bei der Verleihung von öffentlichen Auszeichnungen und Ehrungen erforderlich ist und welche Regelungen es treffen muss, wird also zurzeit in Bund und Ländern sehr unterschiedlich beantwortet.

Die Landesregierung geht davon aus, dass nicht nur die Landesbehörden sondern auch die eigenverantwortlich handelnden kommunalen Stellen, die mit der Vergabe von Auszeichnungen und Ehrungen befasst sind, beim Umgang mit personenbezogenen Daten den Vorschriften des Hessischen Datenschutzgesetzes entsprechend verfahren. Damit dürfte dem Schutz des informationellen Selbstbestimmungsrechts der Betroffenen bereits ausreichend Rechnung getragen werden. Eine besondere gesetzliche Regelung zum Schutz personenbezogener Daten bei der Verleihung von Auszeichnungen und Ehrungen ist nicht erforderlich und stünde dem von der Landesregierung verfolgten Ziel der Deregulierung daher völlig entgegen.

Zu 3.4 Verweigerung der Auskunft über eigene Daten

Die Landesregierung teilt die Auffassung des Hessischen Datenschutzbeauftragten zur Bedeutung des Auskunftsrechts. Die Feststellung des Hessischen Datenschutzbeauftragten, es komme "recht häufig" vor, dass Betroffenen die Auskunft über die zur eigenen Person gespeicherten Daten verweigert werde, ist für die Landesregierung angesichts fehlender statistischen Erhebungen zu dieser Frage nicht nachvollziehbar.

Zu 3.4.1 Justizvollzug

Der Vorgang wurde nur zwischen der Justizvollzugsanstalt und dem Hessischen Datenschutzbeauftragten behandelt. Nach entsprechender Intervention stellte die Justizvollzugsanstalt sicher, dass dem Gefangenen die vom Gesetz vorgesehenen Auskünfte in ausreichendem Umfang gegeben wurden. Da aus anderen Justizvollzugsanstalten keine diesbezüglichen Beschwerden bekannt

wurden, geht die Landesregierung davon aus, dass es sich um einen Einzelfall handelte, der auf der Nachlässigkeit eines Bediensteten beruhte.

Zu 3.4.2 Strafverfolgung

Es sind zwei Vorgänge angesprochen, in denen der Hessische Datenschutzbeauftragte gegenüber der Amtsanwaltschaft in Frankfurt am Main sowie einer nicht näher benannten Staatsanwaltschaft die den jeweils Betroffenen erteilte Auskunft, über die in der zentralen Namenskartei zu ihrer Person gespeicherten Daten, moniert hat. Rechtsgrundlage für die Auskunftserteilung ist insoweit § 491 StPO. Es ist bekannt, dass es hinsichtlich der Frage der so genannten Negativauskunft immer wieder zu Auffassungsunterschieden kommt, da die Staatsanwaltschaften bei laufenden Verfahren zurecht bemüht sind, nicht den Untersuchungserfolg durch die Auskunftserteilung zu gefährden (§ 491 Abs. 2 StPO).
In den im Tätigkeitsbericht angesprochenen Fällen konnte jeweils eine Lösung erzielt werden. Zu einer Beteiligung des Ministeriums der Justiz kam es dabei nicht.

Zu 3.4.3 Ausländer

Die Anmerkung des Hessischen Datenschutzbeauftragten bezieht sich auf die Anwendung des § 34 Abs. 3 Ausländerzentralregistergesetz durch das Bundesverwaltungsamt. Da es sich dabei um eine Bundesbehörde handelt, fehlt es der Landesregierung an der Grundlage für eine Beurteilung. Das Verhalten hessischer Stellen wird vom Hessischen Datenschutzbeauftragten nicht beanstandet.

Zu 3.4.4 Verfassungsschutz

Der Hessische Datenschutzbeauftragte stellt fest, dass das Landesamt für Verfassungsschutz die gesetzlichen Regelungen in allen an ihn herangetragenen Fällen korrekt angewendet hat. Eine Stellungnahme der Landesregierung ist nicht erforderlich.

Zu 3.4.5 Polizei

Zu 3.4.5.1 Unfallaufnahme

Die Verweigerung der Auskunft durch die Polizeidienststelle stand nicht im Einklang mit der angeführten Verwaltungsvorschrift. Die Intervention des Hessischen Datenschutzbeauftragten erfolgte zu Recht.

Zu 3.4.5.2 Noch ein Haftbefehl

In dem geschilderten Fall musste das HLKA davon ausgehen, dass es sich um einen Ausforschungsversuch handelt. Aus der Anfrage des Bevollmächtigten des Antragstellers war nämlich nicht erkennbar, dass dieser Kenntnis von der bestehenden Fahndung hatte. Die Anfrage war vielmehr allgemein gehalten. Sie bezog sich sowohl auf die ausschreibende Behörde als auch auf das Aktenzeichen.

Im Falle einer aktuellen Fahndung liegen grundsätzlich die Voraussetzungen einer Auskunftsverweigerung nach § 29 Abs. 3 HSOG vor. Danach besteht der Auskunftsanspruch nicht, soweit eine Abwägung ergibt, dass die dort gewährten Rechte der betroffenen Person hinter dem öffentlichen Interesse an der Geheimhaltung zurücktreten müssen.

Um Ausforschungen zu vermeiden, wird im HLKA folgende Verfahrensweise praktiziert:

Sämtlichen Antragstellern, die sich nur pauschal über die zu Ihrer Person gespeicherten Daten erkundigen, wird im Auskunftsbescheid mitgeteilt, dass sich die Auskunft nicht auf aktuelle Fahndungen erstreckt. Sofern eine diesbezügliche Auskunft gewünscht wird, ist dies ausdrücklich zu beantragen. Wird ein entsprechender Antrag gestellt, was in der Praxis äußerst selten geschieht, verfährt das HLKA nach § 29 Abs. 3 HSOG. Die Abwägung hängt von den Umständen ab, die die betroffene Person zur Begründung ihres Antrages vorträgt oder die sonst aus den polizeilichen Unterlagen erkennbar sind. So kann ausnahmsweise eine Auskunft erteilt werden, wenn

der Betroffene mit der Fahndung rechnet, z.B. weil er unter der Auflage, innerhalb einer bestimmten Frist nicht wieder nach Deutschland einzureisen, von der Strafvollstreckung verschont und ins Ausland abgeschoben worden ist. Sind derartige besondere Umstände nicht ersichtlich und trägt auch der Antragsteller keine Gründe vor, die ein schützenswertes besonderes Interesse an der Auskunft erkennen lassen, wird diese unter Beachtung der Formalien des § 29 Abs. 5 HSOG abgelehnt.

Zum Zeitpunkt der Bekanntgabe des Haftbefehls ist im Übrigen anzumerken, dass der Haftbefehl dem Beschuldigten gemäß § 114a StPO "bei der Verhaftung" bekannt zu geben ist und nicht, wie der Hessische Datenschutzbeauftragte meint, "spätestens mit der Verhaftung". Die Vorschrift, die § 35 StPO ergänzt, bildet eine Ausnahme von dem Grundsatz, dass gerichtliche Entscheidungen dem Betroffenen vor ihrer Vollstreckung bekannt gegeben werden.

Zu 3.4.6 Finanzämter

Konkrete Angaben über den Sachverhalt können nicht gemacht werden, da der Hessische Datenschutzbeauftragte der Bitte der Verwaltung nicht nachkam, das betroffene Finanzamt zu benennen. Die Akteneinsicht durch Mitarbeiter des Hessischen Datenschutzbeauftragten erfolgte "vollständig und reibungslos". Im Ergebnis wurde festgestellt, dass die Akte vollständig und korrekt vorlag; einer besonderen Überprüfung bedurfte es daher nicht.

Die Abgabenordnung scheint als datenschutzrechtliche Grundlage ausreichend, um bereichsspezifische Datenschutzbelange der Finanzverwaltung zu regeln. Zwar besteht eine Auskunftspflicht nicht, doch sind Auskünfte auch nicht ausgeschlossen. Ein Auskunftsrecht bedürfte auch einer besonders umfangreichen Pflege der Akten und wäre damit sehr personalintensiv.

Zu 3.5 Elektronisches Fahrgeldmanagement

Der Landesregierung fehlt die Grundlage für eine Stellungnahme, da sie sich im Rahmen ihrer Aufgaben noch nicht mit diesem Thema zu befassen hatte.

Zu 4. Europa - Schengener Durchführungsübereinkommen

Zu 4.1 Gemeinsame Geschäftsstelle

Über die Tätigkeit der Gemeinsamen Kontrollinstanz liegen der Landesregierung keine Informationen vor, noch gehört es zu ihren Aufgaben, deren Tätigkeit zu bewerten. Eine Stellungnahme zur Arbeit der Gemeinsamen Kontrollinstanz ist daher nicht möglich.

Zu 4.2 Erneuerung des Schengener Informationssystems

Soweit der Bericht die Stellungnahme der Gemeinsamen Kontrollinstanz zur anstehenden Erneuerung des Schengener Informationssystems (SIS) referiert, ist aus Sicht der Landesregierung dazu Folgendes anzumerken:

"Zugriff der nationalen staatlichen Kraftfahrzeugregisterstellen auf bestimmte SIS-Daten"

Die Landesregierung stimmt den von der Gemeinsamen Kontrollinstanz getroffenen Feststellungen zu.

"Zugriff von EUROJUST auf das SIS"

In seinem Bericht für das Jahr 2002 führt EUROJUST aus, dass für die Arbeit von EUROJUST ein Zugang zum SIS unbedingt erforderlich sei. Es hätten bereits einige nationale Mitglieder von EUROJUST Vorbereitungen unternommen, um einen direkten bzw. indirekten Zugang zu Informationen nach Art. 95 und 98 des Schengener Übereinkommens zu erhalten. Nach derzeitigem Informationsstand besteht noch kein Zugriffsrecht für EUROJUST auf das SIS. Es ist jedoch zu erwarten, dass angesichts der Förderung von EUROJUST durch die Staaten der Europäischen Union ein Zugriffsrecht eingeräumt werden wird.

"Hinzufügung bestimmter Einzelangaben einer gesuchten Person oder Sache"

Die Gemeinsame Kontrollinstanz hat sich gegen die Verarbeitung "subjektiver" Angaben (z.B. "Art der Straftat", "flüchtige Person") im SIS ausgesprochen, da sich dieses durch die Aufnahme weiterer Angaben von einem "Treffer/kein Treffer"-System zu einem System mit neuer Funktion (Textdatei) entwickeln würde.

Unter griechischer Ratspräsidentschaft wurde am 25. April 2003 seitens des Rats festgestellt, dass das SIS ein "Treffer/kein Treffer"-System bleiben solle. Dennoch wurde in den diesbezüglichen Schlussfolgerungen des Rats festgelegt, das SIS zumindest in technischer Hinsicht so zu entwickeln, dass z.B. eine Aufnahme neuer Kategorien von Ausschreibungen sowohl zu Personen als auch zu Sachen oder eine Aufnahme neuer Felder in den Ausschreibungen möglich ist. Innerhalb der Delegationen der Mitgliedstaaten wurde bezüglich der konkreten Inhalte bislang noch kein Konsens erzielt. Inwieweit eine Verarbeitung weiterer Angaben zu im SIS ausgeschriebenen Personen zukünftig ggf. realisiert werden wird, ist deshalb bislang nicht abzusehen.

"Konventionelle Unterlagen in den SIRENE-Büros"

Der Gemeinsamen Kontrollinstanz ist darin zuzustimmen, dass eine Regelung für den Umgang mit den konventionellen Unterlagen der SIRENE nach Löschung des SIS-Datensatzes erforderlich ist.
Wie im Einzelnen zu verfahren ist, bedarf aus Sicht der Landesregierung noch einer eingehenden Prüfung.

"Aufnahme von Lichtbildern und Fingerabdrücken"

In den bereits angesprochenen Schlussfolgerungen unter griechischer Ratspräsidentschaft hat der Rat am 25. April 2003 festgelegt, dass das SIS zumindest technisch die Speicherung, Übertragung und den eventuellen Abruf biometrischer Daten, insbesondere von Lichtbildern und Fingerabdrücken ermöglichen muss. Es ist nach Auffassung des Rates technisch nicht besonders problematisch, in das System, welches bereits Fingerabdrücke umfasst, auch andere biometrische Daten einzubeziehen.

Die Landesregierung hält die Einbeziehung anderer biometrischer Daten für notwendig. Dazu bedarf es einer umfassenden Debatte und einer gründlichen Untersuchung. Insoweit entspricht die Aussage im Tätigkeitsbericht, dass es nur noch um die Einstellung von Lichtbildern und Fingerabdrücken gehe, nicht dem aktuellen Diskussionsstand auf EU-Ebene.

Die Einschätzung des Rats entspricht dem Ziel einer grenzübergreifenden wirkungsvollen Strafverfolgung bei der auf wirksame Methoden zur Personenidentifizierung und Täterermittlung auch innerhalb des SIS nicht verzichtet werden kann.

"Vollprotokollierung aller Abrufe aus dem SIS"

Die vorgesehene Erweiterung der Vollprotokollierung wird aufgrund positiver Erfahrungen im Bereich der hessischen Polizei begrüßt.

"Verlängerung der Speicherfristen für die Ausschreibungen im SIS"

Die Frage der Ersetzung von Höchstfristen durch Prüffristen kann nur im Zusammenhang mit einem die Einzelheiten festlegenden Regelwerk geprüft werden. Daher ist gegenwärtig keine Stellungnahme möglich. Es wird jedoch darauf hingewiesen, dass die hessische Polizei mit Prüffristen und Aussonderungsprüffristen arbeitet, ohne dass dies zu grundsätzlichen Beanstandungen des Hessischen Datenschutzbeauftragten geführt hätte.

Die Aussagen nach dem letzten Spiegelstrich bezüglich der Vorschläge der spanischen Ratspräsidentschaft geben nicht den Stand der gegenwärtigen Schlussfolgerungen des Rates zum Schengener Informationssystem wieder. Derzeit wird versucht zu klären, welche Behörden einen (erweiterten) Zugriff auf das SIS erhalten sollten und zu welchem Zweck sie diesen Zugriff nutzen dürften. Außerdem soll geprüft werden, welche

neuen Kategorien von Personen (z.B. gewalttätige Randalierer) in das SIS aufgenommen bzw. welche neuen Kategorien von Sachen im SIS ausgeschrieben werden sollten (z.B. Kunstwerke, Luxusgüter). Weitere Prüfungen, die nach dem Willen des Rates vorgenommen werden sollen, betreffen die Auswahl und Speicherung biometrischer Daten im SIS sowie die Änderung von Speicherungsfristen.

Zu 5. Justiz

Zu 5.1 Rahmenbedingungen für den IT-Einsatz in der Justiz

Die ausführliche Darstellung des "Ringens" um ein für die Justiz und deren besonderen Anforderungen unter dem Gesichtspunkt des Datenschutzes und der Datensicherheit einsetzbares Konzept spiegelt die Diskussion mit dem Hessischen Datenschutzbeauftragten zutreffend wider.

Entscheidend im Hinblick auf das gezogene Fazit ist, dass mit dem Netzkonzept eine alle Interessen berücksichtigende, tragfähige Lösung gefunden wurde, die der Verwirklichung des Projektes nicht entgegen steht. Hinsichtlich der Diskussion um die Einbindung der Hessischen Zentrale für Datenverarbeitung (HZD) als Administrationseinheit und der Notwendigkeit der weit gehenden Aufsicht durch das Ministerium der Justiz ist der Hinweis auf den nunmehr abgeschlossenen Fernwartungsvertrag (vgl. Nr. 5.1.2.3 am Ende) wichtig.

Die Erfahrungen des letzten Jahres zeigen, dass dieses Konzept praktikabel ist und - insbesondere von der Richterschaft - angenommen wird.

Der Hessische Datenschutzbeauftragte hebt wiederum seine Auffassung zu einer möglichen Kollision mit der richterlichen Unabhängigkeit und dem Grundsatz der Gewaltenteilung hervor. Leider begründet er sie auch hier (vgl. Nr. 5.1.2.3) nicht.

Zu 5.2 Unzulässige Auskunftsersuchen an Pflichtverteidiger nach Steuerdaten

Der Erlass des Ministeriums der Finanzen vom 18. Februar 1981 ist Anfang 1992 außer Kraft getreten. Die Prüfung der Aufrechnungslage vor Auszahlung ist nicht mehr vorgesehen. Das Sollkonzept, das für die nach § 71a Landeshaushaltsordnung kaufmännisch buchenden Verwaltungseinheiten (Buchungskreise) und das Hessische Competence Center (HCC) verbindlich ist, sieht bewusst keine Prüfung vor, ob der Kreditor Steuerschuldner ist.

Der Hessische Datenschutzbeauftragte führt zutreffend aus, dass von Seiten des Ministeriums der Justiz alle hessischen Gerichte mit Schreiben vom 19. September 2002 (5650 - I/7 - 252/02) auf die bestehende Rechtslage hingewiesen wurden.

Bis zum heutigen Tag ist kein weiterer Fall bekannt geworden, bei dem ein Gericht, Richter oder Rechtspfleger von einem Pflichtverteidiger vor Anweisung seiner Gebühren die Angabe von Steuerdaten (Steuernummer) verlangt hätte.

Zu 6. Polizei- und Strafverfolgungsbehörden
"Vorbeugende" Fahndung nach einem Zechpreller

Der vom Hessischen Datenschutzbeauftragten geschilderte Fall macht deutlich, dass eine Sichtweise, bei der das Interesse des Bürgers, von staatlichen Datenverarbeitungseingriffen verschont zu bleiben, einem staatlichen Gefahrenabwehrinteresse gegenübergestellt wird, häufig den vielfältigen Facetten der Lebenswirklichkeit nicht gerecht wird. Die Bewertung des Hessischen Datenschutzbeauftragten wird geteilt.

Zu 7. Ordnungswidrigkeiten

Der Hessische Datenschutzbeauftragte bemängelt auf Grund mehrere Eingaben von Zeugen, dass Behörden bei der Verfolgung und Ahndung von Ordnungswidrigkeiten dem Datenschutzinteresse des Zeugen nicht die erforderliche Beachtung schenkten.

Diese Kritik basiert auf zurückliegenden, zwischenzeitlich bereinigten Auffassungsunterschieden zwischen dem Hessischen Datenschutzbeauftragten und der Landesregierung (vgl. 28. Tätigkeitsbericht - Nr. 21). Die Auffassung der Landesregierung, dass erst im Bußgeldbescheid sowohl Name als auch Wohnort des Zeugen anzugeben sind, im Rahmen der Anhörung dies jedoch nicht erforderlich ist, hat sich im Ergebnis durchgesetzt.
Gegenwärtig bestehen keine inhaltlichen Auffassungsunterschiede mehr.

Sowohl bei der automatisierten Vorgangsbearbeitung mit dem System HESOWI, als auch bei Verwendung der landeseinheitlichen Vordrucke wird die Zeugenangabe im Anhörungsbogen unterdrückt.

Da der Hessische Datenschutzbeauftragte keine konkreten Behörden anführt, sondern abstrakt davon spricht, dass die Verfolgungsbehörden (richtigerweise Ahndungsbehörden) den Ermessensspielraum fehlerhaft ausübten, hat das Ministerium des Innern und für Sport die Ressorts sowie den nachgeordneten Bereich des Ministeriums mit Schreiben vom 30. Juli 2003 lediglich allgemein auf das gerügte Umsetzungsdefizit bzw. die angemessene Verfahrensweise hinweisen können.

Im Übrigen ist die Darstellung des Hessischen Datenschutzbeauftragten teilweise fachlich unzutreffend.

Wird dem Betroffenen ein Verwarnungsgeldangebot nach § 56 OWiG unterbreitet, kann dies nur angenommen oder abgelehnt werden. Eine Akteneinsicht nach § 49 Abs. 1 OWiG erfolgt nicht (5. Absatz). Beantragt der Betroffene nach Erhalt des Verwarnungsgeldangebotes Akteneinsicht, wird damit konkludent das Verwarnungsgeldangebot abgelehnt und eine gründliche Sachverhaltsprüfung gewünscht. In der Praxis wird die Gelegenheit zur Anhörung mit dem Verwarnungsgeldangebot in einem Schreiben verbunden, um Kosten zu sparen.

Auch in diesem Stadium ist nach Auffassung der Landesregierung die genaue Zeugenangabe noch nicht erforderlich. Erst im Bußgeldbescheid selbst sind die Beweismittel nach § 66 Abs. 1 Nr. 4, § 46 Abs. 1 OWiG i.V.m. § 222 Abs. 1 StPO genau zu bezeichnen, das heißt, Name und Wohnort anzugeben. Dieser Auffassung hat sich zwischenzeitlich auch der Hessische Datenschutzbeauftragte angeschlossen.

Zu 8. Verfassungsschutz

Zu 8.1 Neues Verfassungsschutzgesetz

In dem Bericht wird zutreffend dargestellt, welche Positionen der Hessische Datenschutzbeauftragte zu der Änderung des Gesetzes über das Landesamt für Verfassungsschutz (LfVG) durch das Gesetz vom 30. April 2002 (GVBl. I S. 82) im Gesetzgebungsverfahren vertreten und inwieweit der Gesetzgeber diese berücksichtigt hat.

Zu 8.2 und Nr. 3 der "Kernpunkte des 31. Tätigkeitsberichts" - Keine Abhörbefugnisse gegenüber Journalisten und anderen besonders geschützten Berufsgruppen

Zu der vom Hessischen Datenschutzbeauftragten aufgeworfenen Frage der Abhörbefugnis des Landesamts für Verfassungsschutz (LfV) gegenüber Journalisten und anderen Berufsgruppen ist zunächst darauf hinzuweisen, dass es sich - jedenfalls bisher - um eine mehr akademische Frage als um eine Frage mit praktischer Relevanz handelt. Die Landesregierung schließt sich zu dieser Frage dem Bericht des Rechtsausschusses des Bundestages zum Entwurf eines Gesetzes zur Änderung des Grundgesetzes (Artikel 13 GG) an (BT-Drucks. 13/9660, S. 4). In dem Bericht ist zu diesen Fragen folgendes ausgeführt:

> "Die elektronische Wohnungsüberwachung stellt eine erhebliche Grundrechtseinschränkung dar, die nur unter sehr engen Voraussetzungen zulässig ist. Unterfällt ein Sachverhalt nach den vom Bundesverfassungsgericht entwickelten Maßstäben dem durch Artikel 1 und Artikel 19 Abs. 2 GG geschützten unantastbaren Kernbereich privater Lebensgestaltung (BVerfGE 80, 367, 373 ff.), scheidet eine Überwachung von vornherein

aus. In diesem Bereich können selbst schwerwiegende Interessen der Allgemeinheit Eingriffe nicht rechtfertigen, eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes findet nicht statt (BVerfG a. a. O., S. 374 f.). Unterfällt ein Sachverhalt diesem absolut geschützten Kernbereich nicht, bleibt der Grundsatz der Verhältnismäßigkeit stets zu beachten, demzufolge die Zulässigkeitsvoraussetzungen um so strenger zu handhaben sind, je intensiver sich die Maßnahme im Einzelfall auswirken würde. Vor allem soweit neben dem Schutzgut der Wohnung andere grundrechtlich gewährleistete Rechtsgüter besonders intensiv betroffen sind, wird deshalb die Zulässigkeit einer elektronischen Wohnraumüberwachung nicht selten überhaupt zu verneinen sein. Insbesondere unterliegen Gespräche zwischen Beschuldigten und zur Verweigerung des Zeugnisses berechtigten Personen verfassungsrechtlichem Schutz: So bleiben das Beichtgeheimnis und die Vertraulichkeit seelsorgerlicher Gespräche mit Beichtcharakter unberührt. Die Beichte gehört zum verfassungsrechtlichen Kernbereich der Religionsausübung im Sinne des Artikels 4 Abs. 1 und 2 GG. Dies gilt ebenso für seelsorgerliche Gespräche, soweit ihnen Beichtcharakter zukommt. Die durch Artikel 4 GG geschützten Beichtgespräche und seelsorgerlichen Gespräche mit Beichtcharakter dürfen von Verfassung wegen nicht abgehört werden. Auch für vertrauliche Gespräche mit Angehörigen verschiedener Berufsgruppen ergibt sich -- aus unterschiedlichen Bestimmungen -- verfassungsrechtlicher Schutz: So setzt etwa bei Gesprächen mit Pressevertretern die in Artikel 5 Abs. 1 Satz 2 GG gewährleistete Pressefreiheit, bei Gesprächen zwischen Anwalt und Mandant das aus Artikel 20 Abs. 3 GG folgende Rechtsstaatsprinzip (namentlich bei Verteidigergesprächen die Gewährleistungen im Hinblick auf ein faires Verfahren) und bei Gesprächen zwischen Arzt und Patient dessen allgemeines Persönlichkeitsrecht (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG) der elektronischen Wohnraumüberwachung enge Grenzen. Entsprechendes ergibt sich für vertrauliche Gespräche mit Abgeordneten aus deren verfassungsrechtlichem Status (Artikel 38 Abs. 1 Satz 2, vgl. Artikel 47 GG). Schließlich haben höchstpersönliche Gespräche mit engsten Familienangehörigen am Schutz der durch Artikel 2 Abs. 1 GG i. V. m. Artikel 1 Abs. 1 GG garantierten Intimsphäre teil. Zwar ist die Grenze des absolut geschützten Bereichs privater Lebensführung nicht abstrakt bestimmbar, weil insbesondere die Schutzwürdigkeit von Räumlichkeiten von ihrer konkreten Nutzung bestimmt wird. Doch dürfen Abhörmaßnahmen um so weniger erfolgen, je größer die Wahrscheinlichkeit ist, dass mit ihnen zutiefst private und deshalb absolut geschützte Gespräche erfasst würden (die zudem gerade wegen ihres rein privaten Inhalts für die Strafverfolgungsbehörden uninteressant wären). Sind solche Maßnahmen -- irrtümlich -- doch einmal getroffen worden, so müssen die dabei gefertigten Aufzeichnungen unverzüglich gelöscht werden."

Ob darüber hinaus für den Bereich des Verfassungsschutzes eine Regelung in Anlehnung an § 103 d StPO sinnvoll sein kann, wird von der Landesregierung geprüft. Nach gegenwärtiger Einschätzung spricht vieles dafür, dass die vor einer Abhörmaßnahme gezogenen engen materiellen Grenzen des Verfassungsschutzgesetzes (§ 5 Abs. 2 LfVG) und der Verfassung (s.o.), die in jedem Einzelfall geprüft werden müssen, keiner entsprechenden Ergänzung bedürfen.

Der Hessische Datenschutzbeauftragte empfiehlt dem Gesetzgeber in Nr. 3 der "Kernpunkte des 31. Tätigkeitsberichts", auch ins HSOG Ausnahmeregelungen aufzunehmen, die die Kommunikation von Journalisten für redaktionelle Zwecke entsprechend der Neuregelung des Zeugnisverweigerungsrechts in der Strafprozessordnung von Überwachungsmaßnahmen freistellt.

Die Datenerhebung aus dem durch Art. 13 GG geschützten Bereich ist nach § 15 Abs. 4 HSOG nur möglich, wenn es zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. Bei einer solchen Gefahrenlage hat die Polizei den mit den notwendigen Maßnahmen zum Schutz von bedeutenden, höchstpersönlichen Rechtsgütern verbundenen Eingriff gegen das Interesse eines Journalisten an freier Berichterstattung abzuwägen.

In diesem Zusammenhang ist eine Entscheidung des Bundesverfassungsgerichts (BVerfG) vom 12. März 2003 - 1BvR 330/96 u. 1 BVR 348/99 - von besonderem Interesse. Darin hat sich das Bundesverfassungsgericht mit der

Gewichtung der Medienfreiheit im Verhältnis zum staatlichen Interesse an der Strafverfolgung auseinander und ausgeführt (a.a.O., Absatz Nr. 112 ff.):

> "aa) Presse- und Rundfunkfreiheit sind nicht unbegrenzt gewährleistet. Nach Art. 5 Abs. 2 GG finden sie ihre Schranken in den Vorschriften der allgemeinen Gesetze, zu denen auch die Strafprozessordnung und die sie ergänzenden Vorschriften mit ihrer prinzipiellen Verpflichtung für jeden Staatsbürger zählen, zur Wahrheitsermittlung im Strafverfahren beizutragen und die im Gesetz vorgesehenen Ermittlungsmaßnahmen zu dulden. Die in den allgemeinen Gesetzen bestimmten Schranken der Presse- und der Rundfunkfreiheit müssen allerdings ihrerseits im Lichte dieser Grundrechtsverbürgungen gesehen werden. Im Rahmen der gebotenen Abwägung ist das Gewicht des Rechtsguts zu berücksichtigen, dessen Schutz das einschränkende Gesetz dient (vgl. BVerfGE 77, 65 <75>).
>
> bb) Bei der Gewichtung der Medienfreiheit im Verhältnis zu dem staatlichen Interesse an der Strafverfolgung ist zu berücksichtigen, dass die betroffenen Handlungen auf beiden Seiten auf die Erlangung von Informationen zielen, ohne dass einem der dabei verfolgten Interessen abstrakt ein eindeutiger Vorrang gebührt. Der Gesetzgeber ist weder gehalten noch steht es ihm frei, der Presse- und Rundfunkfreiheit absoluten Vorrang vor anderen wichtigen Gemeinschaftsgütern einzuräumen. Er hat insbesondere auch den Erfordernissen der Rechtspflege Rechnung zu tragen (vgl. BVerfGE 77, 65 <75 f.>).
>
> …
>
> Auch die Tätigkeit der Strafverfolgungsbehörden liegt im öffentlichen Interesse und hat in einem Rechtsstaat hohe Bedeutung (siehe oben II 3 b aa). Die durch Strafverfolgungsmaßnahmen mögliche Aufklärung von Straftaten und ihr Beitrag zur Sicherung der Befolgung der Strafgesetze können durch Zeugnisverweigerungsrechte oder ähnliche verfahrensrechtliche Beschränkungen der Strafverfolgung empfindlich berührt werden (vgl. BVerfGE 77, 65 <76>).
>
> Dass das Strafverfolgungsinteresse grundsätzlich hinter dem Rechercheinteresse der Medien zurückzutreten hat, lässt sich verfassungsrechtlich nicht begründen. Darauf aber liefe ein allgemein und umfassend verankerter Schutz von Journalisten hinaus, von Maßnahmen der Erhebung von Informationen über den Telekommunikationsverkehr bei der Aufklärung von Straftaten verschont zu bleiben. Umgekehrt lässt sich auch nicht in abstrakter Weise feststellen, dass das Strafverfolgungsinteresse generell dem Interesse der Medien vorgeht."

Die Ausführungen des Bundesverfassungsgerichts zum Strafverfolgungsinteresse gelten in besonderem Maße auch für Maßnahmen des Staates zur Gefahrenabwehr. Primäres Ziel staatlichen Handelns muss es sein, die gefährdeten Rechtsgüter zu schützen und eine Verletzung der Rechtsordnung zu verhindern. Die vom Bundesverfassungsgericht geforderte Abwägung der grundrechtlich geschützten Interessen findet dabei in jedem Einzelfall in der zu erlassenden Anordnung statt (vgl. § 4 HSOG und den Bericht des Rechtsausschusses des Bundestages zur Änderung des Grundgesetzes (BT-Drucks. 13/9660) zitiert bei Nr. 8.2).

Nach gegenwärtiger Einschätzung bedürfen die für eine Abhörmaßnahme gezogenen engen materiellen Grenzen des § 15 Abs. 4 HSOG und der Verfassung, die ohnehin in jedem Einzelfall geprüft werden müssen, deshalb keiner Ergänzung im HSOG.

Zu 8.3 Personenbezogene Daten in Sachakten des Verfassungsschutzes

Die Landesregierung teilt die Ansicht des Hessischen Datenschutzbeauftragten, dass personenbezogene Daten, die nach § 6 Abs. 5 LfVG in der neuen Fassung nicht mehr nur zu sperren sondern zu löschen sind, grundsätzlich nicht mehr verwertet werden dürfen, wenn diese Daten in Sachakten nicht gelöscht wurden. Der entsprechende Formulierungsvorschlag des Hessischen Datenschutzbeauftragten zur letzten Änderung des Gesetzes über das Lan-

desamt für Verfassungsschutz Hessen, der erst in einem sehr späten Stadium jenes Gesetzgebungsverfahrens gemacht wurde, wird von der Landesregierung im Rahmen einer anstehenden Änderung verschiedener Sicherheitsgesetze (Hessisches Ausführungsgesetz zum G 10-Gesetz, Gesetz über das Landesamt für Verfassungsschutz Hessen) erneut geprüft.

Zu 8.4 Informationsbesuch beim Landesamt für Verfassungsschutz

Der Hessische Datenschutzbeauftragte berichtet zutreffend über seine Erkenntnisse beim Landesamt für Verfassungsschutz.

Zu 9. Ausländerrecht

Zu 9.1 Prüfung des Einbürgerungsverfahrens

Soweit die Datenschutzprüfung im Einbürgerungsdezernat des Regierungspräsidiums Darmstadt Anlass für Hinweise zu einzelnen Verfahrensabläufen gegeben hat, wurden diese aufgegriffen und den beiden nicht beteiligten Regierungspräsidien mit Erlass vom 26. März 2003 mit der Bitte um Beachtung an die Hand gegeben.

Die Modalitäten der Einbeziehung polizeilicher Erkenntnisse in das Einbürgerungsverfahren stellen sich aus der Sicht der Landesregierung wie folgt dar:

Das Einbürgerungsrecht begründet an mehreren Stellen Aufgaben für die Einbürgerungsbehörde, zu deren Erfüllung sie nicht nur auf die Kenntnis strafrechtlicher Verurteilungen, sondern auch auf sonstige strafrechtliche Erkenntnisse angewiesen ist, die bei der Polizei vorhanden sind.

Dies gilt zunächst für laufende Ermittlungsverfahren. § 88 Abs. 3 Ausländergesetz (AuslG) ordnet für alle Einbürgerungsbegehren nach § 85 AuslG die Aussetzung des Einbürgerungsverfahrens bis zur rechtskräftigen Verurteilung oder dem sonstigen Abschluss des Strafverfahrens an. In gleicher Weise ist bei Ermessenseinbürgerungen nach den §§ 8, 9 Staatsangehörigkeitsgesetz (StAG) zu verfahren; auf Nr. 8.1.1.2 der "Allgemeinen Verwaltungsvorschrift zum Staatsangehörigkeitsrecht - StAR-VwV-" des Bundes vom 13. Dezember 2000 (BAnz. Nr. 21a vom 31. Januar 2001) wird verwiesen. Die Polizei verfügt über entsprechende Erkenntnisse.

Für die Beurteilung der Einbürgerungsvoraussetzung der Straffreiheit in den Einbürgerungstatbeständen des Ausländergesetzes - §§ 85 Abs. 1 Nr. 5, Abs. 2, 88 Abs. 1 - werden Kenntnisse aus dem Bundeszentralregister über noch nicht getilgte Verurteilungen benötigt; diesen Bedarf deckt § 42 Abs. 1 Nr. 6 Bundeszentralregistergesetz (BZRG) ab. Nach § 88 Abs. 1 Satz 2 AuslG muss bei einer Überschreitung der Bagatellgrenzen nach pflichtgemäßem Ermessen entschieden werden, ob Verurteilungen außer Betracht bleiben können. Für diese Ermessensbetätigung sind auch strafrechtliche Ermittlungen von Bedeutung, die ohne eine Verurteilung nach den §§ 153 ff. StPO oder §§ 45, 47 JGG eingestellt worden sind. Die Polizei verfügt über die erforderlichen Erkenntnisse.

Das Nichtvorliegen von Ausweisungsgründen nach den §§ 46 Nr. 1 bis 4, 47 Abs. 1 und 2 AuslG ist Tatbestandsvoraussetzung für Ermessenseinbürgerungen nach §§ 8, 9 StAG.
Während die Ausweisungsgründe nach § 46 Nr. 3 AuslG - Verstoß gegen Rechtsvorschriften oder behördliche Verfügungen im Zusammenhang mit Gewerbsunzucht - und nach § 46 Nr. 4 AuslG - Betäubungsmittelkonsum - relativ selten sind, ist der Verstoß gegen Rechtsvorschriften oder gerichtliche und behördliche Entscheidungen nach § 46 Nr. 2 AuslG von praktischer Bedeutung. Der zuletzt genannte Ausweisungsgrund erfasst nicht nur strafrechtliche Verurteilungen - hierfür genügt die Abfrage des Bundeszentralregisters -, sondern auch bußgeldbewehrte Taten und Einstellungen nach den §§ 153 ff. StPO, die verfahrensmäßig die Feststellung einer rechtswidrigen und schuldhaften Tatbegehung einschließen. Die polizeilichen Erkenntnisse über die Einleitung eines Verfahrens sind danach für die Bearbeitung eines entsprechenden Einbürgerungsvorgangs erforderlich, weil sie die Einbürgerungsbehörde erst in die Lage versetzen, den Verfahrensausgang zu ermitteln, sofern er der Polizei nicht bekannt ist, und an Hand der Ermittlungsergebnisse die in Rede stehende Einbürgerungsvoraussetzung zu prüfen.

Von praktischer Relevanz ist auch die Gefährdung der freiheitlich demokratischen Grundordnung, die Befürwortung von Gewalt bei der Verfolgung politischer Ziele oder die Unterstützung des internationalen Terrors durch Einbürgerungsbewerber. Der darauf aufbauende Ausweisungsgrund des § 46 Nr. 1 AuslG a. F., auf den § 8 Nr. 2 StAG derzeit noch verweist, ist durch Artikel 11 des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002 (BGBl. I S. 361) inhaltlich modifiziert und jetzt in § 47 Abs. 2 Nr. 4 i. V. m. § 81 Abs. 1 Nr. 5 AuslG angesiedelt worden. Da § 8 Nr. 2 StAG auch das Nichtvorliegen von Ausweisungsgründen nach § 47 Abs. 2 AuslG erfasst, ist es für die Rechtsanwendung unerheblich, dass es der Bundesgesetzgeber bisher versäumt hat, die Bestimmung redaktionell anzupassen. Der betreffende Ausweisungsgrund wird tatbestandlich nicht nur durch strafrechtliche Verurteilungen verwirklicht, sondern bereits durch entsprechende nachweisbare Betätigungen der Einbürgerungsbewerber. Diesbezügliche Erkenntnisse der Polizei, insbesondere der Staatsschutzkommissariate, sind daher für eine rechtmäßige Aufgabenerfüllung erforderlich.

Der Ausweisungsgrund nach §§ 47 Abs. 2 Nr. 4, 8 Abs. 1 Nr. 5 AuslG steht auch Einbürgerungsbegehren nach dem Ausländergesetz entgegen; sein tatbestandliches Vorliegen schließt gemäß § 86 Nr. 3 AuslG Einbürgerungen nach § 85 AuslG aus.

Sofern sich Bestrebungen nach §§ 47 Abs. 2 Nr. 4, 8 Abs. 1 Nr. 5 AuslG nicht sicher nachweisen lassen, genügt auch ein auf tatsächliche Anhaltspunkte gestützter Verdacht auf sicherheitsrelevante Betätigungen, um Anspruchs- und Ermessenseinbürgerungen auszuschließen, § 86 Nr. 2 AuslG, Nr. 8.1.2.5, 9.1.2.1 StAR-VwV. Einschlägige Ermittlungsverfahren sind daher - unabhängig von ihrem Ausgang - einbürgerungsrelevant. Von besonderer Bedeutung sind auch hier Verfahrenseinstellungen nach §§ 153 ff. StPO, die alleine oder in einer Zusammenschau mit sonstigen Erkenntnissen tatsächliche Anhaltspunkte i. S. d. § 86 Nr. 2 AuslG darstellen und somit eine Einbürgerung ausschließen können. Der diesbezügliche Erkenntnisstand weicht übrigens bei der Polizei und dem Landesamt für Verfassungsschutz häufig voneinander ab, so dass beide Abfragen zur rechtmäßigen Aufgabenerfüllung der Einbürgerungsbehörde erforderlich sind.

Das vorstehende Aufgabenspektrum belegt, dass die Einbürgerungsbehörden umfassend auf polizeiliche Erkenntnisse angewiesen sind, auch und gerade auf solche, die nicht zu strafrechtlichen Verurteilungen geführt haben. Dementsprechend nennt Nr. 19.2 der Verwaltungsvorschrift über das Verfahren bei Anspruchs- und Ermessenseinbürgerungen - VfVEbg - vom 25. Juni 2001 (StAnz. S. 2479) als Gegenstände des Übermittlungsersuchens die anhängigen Ermittlungsverfahren und sonstige strafrechtlichen Erkenntnisse.

Die Erforderlichkeit der in Rede stehenden Datenerhebung wird durch die Erfahrungen der Praxis gestützt, nach denen ein Großteil der Einbürgerungsbewerber keine Angaben über Bestrafungen und Ermittlungsverfahren macht, obwohl bei der Antragstellung danach gefragt wird. Auch die Loyalitätserklärung nach § 85 Nr. 1 AuslG, die auch bei Einbürgerungen nach §§ 8, 9 StAG gefordert wird (Nr. 8.1.5, 9.1.2.1 StAR-VwV), erweist sich in derartigen Fällen aufgrund der polizeilichen Erkenntnisse als falsch, so dass eine Einbürgerung nicht in Betracht kommt.

Es ist wichtig, dass die insgesamt zu einem bestimmten Einbürgerungsbewerber verfügbaren einbürgerungsrechtlich relevanten Erkenntnisse innerhalb der Polizei gesichtet und die Ergebnisse soweit erforderlich übermittelt werden. Vor diesem Hintergrund hat sich das bisherige, in Nr. 19.2 VfV-Ebg dargestellte Verfahren bewährt. Die polizeiliche Stellungnahme erfolgt grundsätzlich für die hessische Polizei insgesamt durch das Hessische Landeskriminalamt, dem damit auch die Aufgabe obliegt, die Zusammenfassung der polizeilichen Erkenntnisse zu koordinieren. Die generelle Einleitung der Erkenntnisabfrage bei der örtlichen Polizeidienststelle ist sowohl organisatorisch als auch ergebnisbezogen sinnvoll, so dass an dieser Verfahrensweise grundsätzlich festgehalten werden soll.

Eine POLAS-Abfrage sowohl durch die örtliche Polizeidienststelle als auch durch das HLKA ist in diesem Zusammenhang erforderlich. POLAS ist ein Nachweissystem für sämtliche bei den hessischen Polizeidienststellen geführte Kriminalakten. Daher muss die örtliche Polizeidienststelle in jedem Fall

POLAS abfragen; nur so erhält sie eine vollständige Übersicht über die Erkenntnisse, die bei ihr über den Einbürgerungsbewerber vorliegen.

Dies gilt auch für das HLKA. Die POLAS-Abfrage erfolgt, um ggf. eigene Kriminalakten beiziehen zu können. Diese Abfrage verbindet das HLKA mit einer Abfrage des Kriminalaktennachweises (KAN) des Bundeskriminalamts, durch den auch bedeutsame Erkenntnisse außerhessischer Polizeibehörden erschlossen werden.

Darüber hinaus wird von der sachbearbeitenden Staatsschutzabteilung des HLKA eine Abfrage in der INPOL-Verbunddatei "APIS" ("Arbeitsdatei PIOS Innere Sicherheit") vorgenommen, auf die neben dem Bundeskriminalamt ausschließlich die Landeskriminalämter unmittelbar zugreifen können.

Die vom HLKA selbst sowie von der örtlichen Polizeibehörde festgestellten Erkenntnisse werden der unteren Verwaltungsbehörde durch das HLKA zusammengefasst übermittelt. Eine zusätzliche Übermittlung von Daten durch die örtliche Polizeibehörde findet nicht statt. Redundante Informationen aus dem Polizeibereich sind damit ausgeschlossen.

Zu 9.2 Datenübermittlung aus dem Erziehungsregister

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 10. Finanzwesen

Zu 10.1.1 Zugriff auf Firmen-EDV

Nach § 147 Abs. 6 Satz 1 Abgabenordnung (AO) hat die Finanzbehörde im Rahmen einer Außenprüfung das Recht, Einsicht in die gespeicherten Daten des geprüften Unternehmens zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen. Weiterhin kann die Finanzbehörde im Rahmen der Außenprüfung verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet oder ihr die gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden (§ 147 Abs. 6 Satz 2 AO).

Die Außenprüfung ist nach § 6 Betriebsprüfungsordnung in den Geschäftsräumen des Steuerpflichtigen durchzuführen. Erst wenn ein geeigneter Geschäftsraum nachweislich nicht vorhanden ist und die Außenprüfung nicht in den Wohnräumen des Steuerpflichtigen stattfinden kann, ist an Amtsstelle zu prüfen (vgl. auch § 200 Abs. 2 AO). Der Außenprüfer wird in der überwiegenden Mehrzahl der Fälle im Unternehmen oder zumindest in den Wohnräumen des Steuerpflichtigen die ihm zur Verfügung gestellten Unterlagen bzw. verwertbaren Datenträger prüfen. Der Datenträger wird somit regelmäßig den direkten Einflussbereich des Steuerpflichtigen nicht verlassen. Weiterhin hat der Steuerpflichtige Eigentumsrechte an dem Datenträger, so dass ein Verbringen an einen anderen Ort gegen seinen Willen nicht zulässig ist. Der Prüfer hat einen Anspruch auf Überlassung der Datenträger an Amtsstelle nur, wenn dort der Prüfungsort ist.

Der zur Auswertung überlassene Datenträger ist nach einer innerdienstlichen Anweisung der Oberfinanzdirektion Frankfurt am Main dem Steuerpflichtigen schnellstmöglich wieder zurückzugeben. Dabei wird die im Schreiben des Bundesministeriums der Finanzen vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 - (BStBl. 2001 S. 415) getroffene Regelung beachtet, dass der zur Auswertung überlassene Datenträger spätestens nach Bestandskraft der aufgrund der Außenprüfung ergangenen Bescheide an den Steuerpflichtigen zurückzugeben oder zu löschen ist.

Die Bedenken des Hessischen Datenschutzbeauftragten, die hessische Finanzverwaltung würde "Paralellbuchhaltungen" von geprüften Unternehmen aufbauen, sind deshalb unbegründet.

Zu 10.1.2 Umsatzsteuer-Nachschau

Bereits in der Stellungnahme zum 30. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten wurde darauf hingewiesen, dass die vom Hessischen

Datenschutzbeauftragten geäußerten Bedenken gegen die Umsatzsteuer-Nachschau nicht geteilt werden.

Durch Übernahme der Umsatzsteuer-Nachschau in das Umsatzsteuergesetz (§ 27b) 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 Unternehmens verschaffen. Eine vorherige Anmeldung eröffnet dagegen die Möglichkeit, einen ordnungsgemäßen Geschäftsbetrieb vorzutäuschen, so dass eine effektive Kontrolle erheblich erschwert wird.

Von der neuen Nachprüfungsmöglichkeit wird nicht "ohne Anlass" bzw. "ohne vorausgehendes Fehlverhalten" Gebrauch gemacht. Das neue Instrumentarium gelangt entsprechend dem Gesetzeszweck nur in begründeten Verdachtsfällen zum Einsatz. Steuerehrliche Unternehmer haben nichts zu befürchten.

Zu 10.1.3 Steuernummern auf Rechnungen

Siehe Stellungnahme zu 10.2.1

Zu 10.1.4 Freistellungsbescheinigungen im Internet

Siehe Stellungnahme zu 10.2.2

Zu 10.1.5 Kontenevidenz

Die vom Hessischen Datenschutzbeauftragten beanstandeten Vorhaben zur Streichung des § 30a AO (Schutz von Bankkunden – so genanntes"Bankgeheimnis"), zur Einführung eines einheitlichen Identifikationsmerkmals nach § 139a AO-Entwurf, zur Einführung von Kontrollmitteilungen nach § 23a EStG-Entwurf und zur Einführung von Anzeigen nach § 45d EStG-Entwurf waren zwar im ersten Entwurf eines Steuervergünstigungsabbaugesetzes enthalten, eine Umsetzung ist derzeit jedoch aufgrund der im Vermittlungsausschuss erzielten Ergebnisse nicht vorgesehen. Diese Vorhaben sind in dem Steuervergünstigungsabbaugesetz nicht mehr enthalten. Daher wird von einer weiteren Stellungnahme abgesehen.

Zu 10.1.6 Steuerdatenabrufverordnung

Auf der Grundlage der Stellungnahmen der Landesbeauftragten für den Datenschutz hat der Bundesbeauftragte für den Datenschutz mit Schreiben vom 23. Mai 2003 eine ausführliche Stellungnahme zur Steuerdatenabrufverordnung abgegeben. Dieses Papier wird zunächst innerhalb der Arbeitsgruppe "Datenschutz" zu erörtern sein. Eine Stellungnahme ist deshalb zurzeit nicht möglich.

Zu 10.1.7 Finanzrechtsprechung und Kontrollmitteilungen

Die vom Hessischen Datenschutzbeauftragten beanstandeten Vorhaben zur Streichung des § 30a AO (Schutz von Bankkunden – so genanntes"Bankgeheimnis") sowie zur geplanten Ausweitung der Kontrollbefugnis der Finanzverwaltung (§ 194 Abs. 3 AO-Entwurf) sind im Steuervergünstigungsabbaugesetz nicht mehr enthalten (vgl. Stellungnahme zu Nr. 10.1.5).

In Bezug auf die Forderungen des Hessischen Datenschutzbeauftragten sowie des Bundesbeauftragten für den Datenschutz nach Schaffung einer normenklaren Vorschrift über die Zulässigkeit von Kontrollmitteilungen, wird darauf hingewiesen, dass Kontrollmitteilungen eine ressortinterne spontane Amtshilfe darstellen, die innerhalb der Verwaltungseinheit "Finanzverwaltung" keiner gesetzlichen Grundlage bedarf (vgl. Tipke/Kruse, AO/FGO zu § 194 Tz. 29). Damit sind Kontrollmitteilungen auch außerhalb der speziell geregelten Fälle zulässig. Davon geht auch das Bundesverfassungsgericht in seinem so genannten "Zinsurteil" (Urteil vom 27. Juni 1991, BStBl. 1991 II S. 654, 668) aus. Nach Auffassung des Bundesfinanzhofs dürfen Informationen, die sich eine Dienststelle der Finanzverwaltung rechtmäßig verschafft hat, von allen Dienststellen des Finanzressorts zur Erfüllung ihrer Aufgaben

verwendet werden. Die Finanzverwaltung ist insoweit als Einheit anzusehen (Urteil des Bundesfinanzhofs vom 2. April 1992, BStBl. 1992 II S. 616).

Im Übrigen unterliegt eine Kontrollmitteilung sowohl bei der ausstellenden als auch bei der empfangenden Finanzbehörde dem Steuergeheimnis, so dass eine missbräuchliche Verwendung ausgeschlossen werden kann.

Zu 10.2 Steuernummern von Unternehmern – ein ungeschütztes Datum?

Zu 10.2.1 Steuernummer auf der Rechnung

§ 14 Abs. 1a Umsatzsteuergesetz, der auf Antrag des Bundesrates im Zuge des Steuerverkürzungsgesetzes vom 19. Dezember 2001 (BGBl. 2001 S. 3922) mit Wirkung vom 1. Juli 2002 eingefügt wurde, dient der besseren Kontrolle des Vorsteuerabzugs. Die dem leistenden Unternehmer obliegende Verpflichtung, in seiner Rechnung die Steuernummer anzugeben, erleichtert und beschleunigt die Überprüfung von Lieferketten und stellt somit eine wichtige Maßnahme zur Bekämpfung des Umsatzsteuerbetruges (z.B. bei sogenannten "Karussellgeschäften") dar. Hierdurch wird die Möglichkeit eröffnet, bei Zweifeln an der Ordnungsmäßigkeit einer dem Leistungsempfänger vorliegenden Rechnung, aus der dieser den Vorsteuerabzug geltend macht, ohne zeitraubende Verzögerungen und zusätzliche Ermittlungen das für den Rechnungsaussteller zuständige Finanzamt festzustellen und dort gegebenenfalls ergänzende Rückfragen durchführen zu können.

Zu dieser Nachprüfungsmöglichkeit gibt es zur Zeit keine Alternativen. Insbesondere ist die Umsatzsteuer-Identifikationsnummer hierfür nicht geeignet, da nicht alle Unternehmer diese Nummer besitzen. Ergänzend ist noch anzumerken, dass Kleinunternehmer sowie Unternehmer, die nicht steuerbare oder steuerfreie Umsätze erbringen (z.B. Ärzte), nicht zur Angabe der Steuernummer in Ihren Rechnungen verpflichtet sind.

Die von der hessischen Finanzverwaltung ergriffenen Maßnahmen, die der Hessische Datenschutzbeauftragte darstellt, werden für ausreichend erachtet. Die zusätzliche Einführung einer PIN ist aus den nachfolgend genannten Gründen nicht sinnvoll.

- Ein Alleingang Hessens ist nicht möglich, alle Länder müssten das gleiche PIN-Verfahren anwenden.
- Die PIN müsste sowohl dem Steuerpflichtigen als auch dem steuerlichen Berater bekannt gegeben werden. Bei einem Beraterwechsel müsste - um dem Gedanken des Datenschutzes gerecht zu werden - eine neue PIN erteilt werden.
- Wenn Auskünfte nur bei Nennung der PIN erteilt werden dürften, würde die PIN im Vergleich zur Steuernummer, die lediglich eine reine "Ordnungskennziffer" der Steuerverwaltung ist, höherrangig behandelt werden. Insofern bedürfte es einer Gesetzesänderung.
- Die Erteilung einer PIN würde einen hohen Programmieraufwand bedingen, der mit großen Kosten verbunden wäre.

Abschließend sei darauf hingewiesen, dass das Hessische Finanzgericht mit Beschluss vom 9. Dezember 2002 (Az. 7 V 3847/02) entschieden hat, dass die Verpflichtung zur Angabe der Steuernummer in der Rechnung keine konkrete unmittelbare Gefährdung der Verletzung des Steuergeheimnisses oder des Datenschutzes enthält.

Zu 10.2.2 Steuerabzug bei Bauleistungen

Wie im Tätigkeitsbericht ausgeführt wird, besteht mit § 48b Abs. 6 Einkommensteuergesetz eine Rechtsgrundlage für die Einrichtung einer Datenbank zur Abfrage der Gültigkeit von Freistellungsbescheinigungen beim Bundesamt für Finanzen. Der Auffassung des Hessischen Datenschutzbeauftragten kann insofern nicht gefolgt werden, als er ausführt, dass dem Steuerpflichtigen die Zustimmung zur Einstellung seiner Daten "faktisch abgenötigt" werde und die Erforderlichkeit der Datenbank fraglich sei, da nur verlässliche Steuerpflichtige eine Freistellungsbescheinigung erhielten.

Die Bedeutung der Datenbank besteht darin, das Haftungsrisiko des Leistungsempfängers zu minimieren, da dieser mittels einer Abfrage erfahren kann, ob die Freistellungsbescheinigung tatsächlich erteilt wurde und noch gültig ist. Diese Datenbank besteht weniger zur Kontrolle der steuerehrlichen Unternehmer, sondern vielmehr zur Aufdeckung sogenannter "schwarzer Schafe", die eine Freistellungsbescheinigung gefälscht, bzw. eine ungültige Freistellungsbescheinigung vorgelegt haben.

Leistungsempfänger erhalten im Rahmen der Abfrage keine Daten, die sie nicht bereits aus der vorgelegten Freistellungsbescheinigung entnehmen konnten.

Nicht jeder, der in den Besitz einer Freistellungsbescheinigung gekommen ist, kann eine Abfrage beim Bundesamt für Finanzen durchführen. Im Rahmen der Abfrage muss - wie der Hessische Datenschutzbeauftragte ausführt - vom Abfragenden u.a. die Steuernummer des leistenden Unternehmers sowie die auf dem Freistellungsbescheid vermerkte Sicherheitsnummer angegeben werden. Selbst wenn der Abfragende, ohne im Besitz des Freistellungsbescheides des leistenden Unternehmers zu sein, Kenntnis von einer Steuernummer erhalten hat, wird er die Sicherheitsnummer nicht kennen, so dass seine Abfrage keinen Erfolg haben wird. Erst wenn er auch die Sicherheitsnummer kennt, die ausschließlich auf dem Freistellungsbescheid vermerkt ist, kann er eine Abfrage tätigen. Dabei ist es der Finanzverwaltung nicht anzulasten, wenn der Abfragende sich z.B. unrechtmäßig Kenntnis von der Sicherheitsnummer verschafft hat.

Es ist der Finanzverwaltung ebenfalls nicht anzulasten, wenn Unternehmer, die nicht im Besitz einer Freistellungserklärung sind, keine Bauaufträge erhalten. Die Freistellungsbescheinigung ist keine "Auszeichnung für steuerehrliche Bauunternehmen", sondern ist lediglich für die Frage von Bedeutung, ob ein Steuerabzug nach § 48d EStG vorzunehmen ist oder nicht.

Zu 10.3 Keine zusätzlichen Kontrollmitteilungen zur geplanten Abgeltungssteuer

Die vom Hessischen Datenschutzbeauftragten angesprochenen Vorhaben sind nicht mehr im Entwurf eines Steuervergünstigungsabbaugesetzes enthalten (vgl. Stellungnahme zu Nr. 10.1.5).

Zu 11. Recht der Presse, Medien- und Teledienste

Zu 11.1 Datenschutzvorschriften für die hessische Presse

Der Hessische Datenschutzbeauftragte hatte im Rahmen der mündlichen Anhörung zum Gesetzentwurf zur Änderung des Hessischen Pressegesetzes im Innenausschuss von seinen Regelungsvorschlägen nur zwei Anregungen aufrechterhalten. Diese Anregungen betrafen seine Forderung nach einer Auffangregelung des Inhalts, dass für die Presseunternehmen, die sich nicht dem Pressekodex unterwerfen, die allgemeinen datenschutzrechtlichen Vorschriften gelten und die Forderung nach einem redaktionsinternen Datenschutzbeauftragten.

Von den übrigen Regelungsvorschlägen, die der Hessische Datenschutzbeauftragte der Landesregierung und dem Landtag vorgelegt hatte, nahm er Abstand, da er diese nicht mehr durchsetzen wolle, um eine gewisse Gleichförmigkeit in den Ländern auch für Hessen zu sichern. Die Konferenz der Datenschutzbeauftragten habe entschieden, dass zunächst einmal zwei Jahre lang beobachtet werden solle, wie die Selbstregulierung durch den Presserat funktioniere, um dann im Zuge der Neuregelung des Bundesdatenschutzgesetzes (BDSG) zu entscheiden, ob diese Selbstregulierungsmaßnahmen ein ausreichendes Konzept zur Sicherung des Datenschutzes sei oder nicht.

Der Hessische Landtag ist den Anregungen des Hessischen Datenschutzbeauftragten nach einer Auffangregelung und einem redaktionsinternen Datenschutzbeauftragten nicht gefolgt, sondern hat den Gesetzentwurf in der von der Landesregierung vorgelegten Fassung beschlossen.

Zu 11.1.1 Auffangregelung

Die vom Hessischen Datenschutzbeauftragten vorgeschlagene Auffangregelung verstößt gegen das Abwägungsgebot des Art. 9 EG-Datenschutzrichtlinie (EG-DSRL) und damit gegen die Pressefreiheit, weil die Besonderheiten der Pressetätigkeit unberücksichtigt bleiben, wenn die allgemeinen Datenschutzbestimmungen in Gänze gelten. Das von Art. 9 EG-DSRL und § 41 Abs. 1 BDSG anerkannte Medienprivileg würde völlig unbeachtet bleiben. Hinzu kommt, dass für die verbandsrechtlich nicht organisierten Presseunternehmen, die keine Selbstverpflichtung eingehen, die Auffangregelung quasi eine Strafnorm darstellen würde, da sie wesentlich schlechter gestellt wären, als die Presseunternehmen, die eine Selbstverpflichtungserklärung abgegeben haben, obwohl sie gegebenenfalls von sich aus den Pressekodex des Deutschen Presserates einhalten, in welchem Regelungen zum Redaktionsdatenschutz aufgenommen worden sind.

Der Deutsche Presserat hatte darauf hingewiesen, dass es lediglich um ca. 15 % der Presseunternehmen ginge, die publizistisch nicht verbandsrechtlich organisiert seien und eine Selbstverpflichtungserklärung nicht ohne weiteres abgeben werden. Es handele sich lediglich um Kleinstunternehmen. Mit diesen wolle der Deutsche Presserat Gespräche führen, um sie zu der Erklärung zu bewegen.

Auch für die Forderung nach einer Auffangregelung gilt somit zunächst das vom Bundesgesetzgeber mit § 41 Abs. 1 BDSG anerkannte Prinzip der Selbstkontrolle der Presse und die von den Datenschutzbeauftragen angesprochene Maßgabe einer Beobachtung, ob die Selbstkontrolle funktioniert.

Zu 11.1.2 Redaktionsinterner Datenschutzbeauftragter

Die EG-DSRL erwähnt den betrieblichen Datenschutzbeauftragten lediglich in Kapitel II Abschnitt IX Art. 18 und Art. 20. Von beiden Bestimmungen darf nach Art. 9 EG-DSRL abgewichen werden, soweit die Interessenabwägung zwischen der Pressefreiheit und dem informationellen Selbstbestimmungsrecht dies zum Schutze der Pressefreiheit notwendig macht. Ein betrieblicher Datenschutzbeauftragter ist im Rahmen einer solchen Abwägung seitens des Bundesgesetzgebers in § 41 Abs. 1 BDSG nicht vorgesehen worden. Dieses Abwägungsergebnis wurde nach langen Verhandlungen zwischen dem Deutschen Presserat und der Bundesregierung unter Beteiligung des Bundesdatenschutzbeauftragten gefunden. Alle Bundesländer sind dieser Vorgabe gefolgt, insbesondere um die Rechts- und Wirtschaftseinheit zugunsten der Presseunternehmen zu wahren und eine Ungleichbehandlung dieser Unternehmen in der Bundesrepublik Deutschland zu vermeiden. Hessen wäre einen Sonderweg gegangen, wenn ein betrieblicher Datenschutzbeauftragter für den journalistisch-redaktionellen Bereich gesetzlich vorgeschrieben worden wäre. Die Gefahr, dass Presseunternehmen wegen einer solchen Regelung den Medienstandort Hessen verlassen, wäre dann nicht auszuschließen gewesen.

Für die Mediendienste und den Rundfunk ist zwar ein betrieblicher Datenschutzbeauftragter gesetzlich vorgesehen. Diese sind aber mit den Printmedien nicht vergleichbar. Bei den Mediendiensten und dem Rundfunk geht es um das "gesprochene Wort", welches im Gegensatz zu dem "gedruckten Wort" in das informationelle Selbstbestimmungsrecht intensiver eingreift, so dass hierfür auch weiter gehende datenschutzrechtliche Vorschriften als im Bereich der Printmedien erforderlich sind. Beim "gesprochenen Wort" wird von einer stärkeren Verbreitung ausgegangen. Es erfordert eine stärkere Innenkontrolle als das "gedruckte Wort", welches wegen seiner relativen "Haltbarkeit" einer intensiveren nachträglichen Kontrolle durch die Betroffenen unterworfen ist. Vom Hessischen Datenschutzbeauftragten wird für den betrieblichen Datenschutzbeauftragten auch nur eine Kontrolle nach Abschluss der Veröffentlichung gefordert. Diese kann von dem Betroffenen aber selbst aufgrund der Veröffentlichungen (er hat es "schwarz auf weiß") geleistet werden.

Zu 11.1.3 Zusätzliche Privilegierung

Die weit gehende Befreiung der Presse von datenschutzrechtlichen Vorschriften rechtfertigt sich aus dem Medienprivileg, dass von der EG-DSRL anerkannt worden ist. Das Medienprivileg ist auf eine normative Säule aus-

gerichtet, die durch eine Säule der so genannten freiwilligen Selbstkontrolle ergänzt wird. Eine wirksame Selbstkontrolle macht eine Fremdkontrolle überflüssig und sichert die Pressefreiheit gegenüber dem Staat. Der Gedanke der freiwilligen Selbstkontrolle ist der Pressefreiheit immanent. Die Selbstkontrolle wird insbesondere durch den Pressekodex des Deutschen Presserats erreicht. In diesem sind zur Umsetzung der EG-DSRL und des § 41 Abs. 1 BDSG (vgl. oben zu Nr. 11.1.2) ergänzende Regelungen zum Redaktionsdatenschutz getroffen worden, außerdem wurde eine Beschwerdeordnung geschaffen. Die Regelungen über den Redaktionsdatenschutz betreffen u.a. die Dokumentierung von Richtigstellungen, Widerrufen, Gegendarstellungen und Presserügen sowie den Anspruch Betroffener auf Auskunft über die zu ihrer Person gespeicherten Daten.

Zu 11.2 Novelliertes Datenschutzrecht für Tele- und Mediendienste

Die Darstellung des Hessischen Datenschutzbeauftragten zu den Änderungen des Datenschutzrechts für Tele- und Mediendienste ist zutreffend.

Zu 12. Entwicklungen und Empfehlungen im Bereich der Technik

Zu 12.1 Mobile Computing

Zu 12.1.1 Überblick über die Technologien

Die Problematik der Sicherheit von Bluetooth und WirelessLAN wird durch die "Luftschnittstelle" begründet. Die Reichweite von Bluetooth beträgt normalerweise bis ca. 10 m. Die Reichweite von WirelessLAN kann, mit entsprechenden Antennen, auf bis zu 10km erweitert werden. Um für die in den unkontrollierten Strecken ablaufenden Vorgänge einen möglichst hohen Sicherheitsstandard zu bekommen und zu halten, ist immer der Einsatz des höchstmöglichen Sicherheitsmodus zu empfehlen. Für die Übertragung sensibler Daten ist daneben der Einsatz von IPSec-Lösungen (IPSec = Internet Protocol Security) vorzusehen.
Die Kosten für Endgeräte und Infrastruktur für Bluetooth, sowie WirelessLAN, sind nach neuestem Kenntnisstand (Juni 2003) nur noch etwa halb so hoch wie im Tätigkeitsbericht des Hessischen Datenschutzbeauftragten angegeben.
Die Hessische Zentrale für Datenverarbeitung prüft aktuell den Einsatz von WirelessLAN für Landesbehörden unter Berücksichtigung der Anregungen und Ergebnisse des Hessischen Datenschutzbeauftragten.
Dies erscheint notwendig, damit auf Forderungen aus den Dienststellen der hessischen Landesverwaltung nach WirelessLAN kurzfristig und mit entsprechendem Wissenshintergrund beraten und umgesetzt werden kann. Notwendig im Vorfeld des Einsatzes in den Dienststellen sind jedoch die Schaffung der Voraussetzungen im Bereich IT-Sicherheit nach BSI-Standard (BSI = Bundesamt für die Sicherheit in der Informationstechnik) und die unbedingte und stringente Einhaltung der nicht immer "bequemen" Sicherheits-Lösungen.
Bluetooth wird aktuell weder generell genutzt, noch bezüglich zukünftiger Nutzung vorbereitend geprüft. Inwieweit einzelne Behörden z.B. Laptops mit Bluetooth-Kapazität ausgestattet haben, entzieht sich der Kenntnis der Landesregierung.

Das Thema GPRS wird durch die HZD seit 2003 projektspezifisch in Verbindung mit VPN-Techniken für Mobile Computing, jeweils unter Berücksichtigung der Anregungen und Ergebnisse des Hessischen Datenschutzbeauftragten, genutzt und angeboten.

UMTS ist aktuell, außer in dedizierten Testumgebungen, noch nicht verfügbar.

Zu 12.2 Einsatz von Windows 2000 und Active Directory

Der Landesautomationsausschuss (LAA) hat 2002 die HZD mit der Einrichtung der zentralen Geschäftsstelle Active Directory (GAD) beauftragt. Die Beteiligung aller Ressorts ist als Ziel angestrebt. Die HZD spielt mit der GAD eine zentrale Rolle im Aufbau, der Durchführung und dem Ausbau des Active Directory. Die im Tätigkeitsbericht des Hessischen Datenschutzbeauftragten unter Nr. 12.2 aufgeführten Einzelpunkte sind deshalb nachvollziehbar und finden die Zustimmung der Landesregierung. Lediglich der

letzte Spiegelstrich in Nr. 12.2.2, dass ein Benutzer sich bei einer verteilten Domäne an anderen Standorten anmelden kann, wenn sein Konto bereits gesperrt ist, erscheint hinterfragenswert. Auf der Grundlage einer einheitlichen und gut ausgebauten Netzinfrastruktur ist dieser Punkt als marginal anzusehen und stellt kein Problem dar. Eine "Schnelllöschung" kann, sofern notwendig, auch manuell angestoßen werden, damit eine Kontosperrung sofort erfolgt. Eine Anmeldung eines Nutzers in einer Domäne, die schlecht an das Netz angebunden ist, hat dann wenige Auswirkungen, da der Nutzer über diese Sub-Domäne nicht hinauskommt.

Unter dem zweiten Spiegelstrich führt der Hessische Datenschutzbeauftragte aus, dass die Organisationsadministratoren umfassenden Zugriff im gesamten Netzwerk hätten oder sich diesen Zugriff verschaffen könnten.
Dies ist zwar theoretisch richtig. Die Praxis gestaltet sich jedoch so, dass nach der Einrichtung einer Domäne die Organisationsadministratoren nur die für die Ausübung ihrer Tätigkeiten notwendigen Rechte besitzen. Diese erlauben es nicht, z.B. auf File- oder Datenbankserver innerhalb der Domäne zuzugreifen. Die Rechte dienen lediglich dazu die Gesamtstruktur aufrechtzuerhalten, wie z.B. Replikaktionszyklen zu definieren und zu überwachen. Wird den Organisationsadministratoren dieses Recht durch die Domänenadministratoren entzogen, wie bereits geschehen, kommt es zu massiven Problemen innerhalb der Gesamtstruktur. Anders als diese Textstelle vermuten lässt, ist der Organisationsadministrator kein "Superuser", der auf alle Daten innerhalb des Active Directory zugreifen kann.
Die Problematik stand oftmals im Mittelpunkt der Diskussion, wenn es darum ging neue Teilnehmer/Dienststellen für das Active Directory zu gewinnen. Eine klare Definition der Berechtigungen, der Aufgaben und des Personenkreises der die Berechtigung besitzt, ist im Active Directory unabdingbar notwendig, ebenso wie die Protokollierung der Tätigkeiten und die anschließende Kontrolle.

Aufgrund der bisherigen Erfahrungen ist der vom Hessischen Datenschutzbeauftragten am Ende von Nr. 12.2.3 erwähnte Hinweis besonders hervorzuheben. Die Einführung eines Windows2000-Netzwerkes und des dort verfügbaren Active Directory ist mit einem hohen personellen und finanziellen Aufwand verbunden, der qualifiziertes Personal verlangt. Zur Aufrechterhaltung des Betriebes des Active Directory ist eine ständige Anpassung aufgrund neuer und sich ständig ändernder Anforderungen notwendig. Die hierfür benötigten Ressourcen müssen uneingeschränkt zur Verfügung stehen, da auch kurzfristige Versäumnisse nur unter erschwerten Bedingungen und mit großem Aufwand wieder aufgeholt werden können.

Zu 12.3 Software-Sicherheitslücken

Die HZD recherchiert und informiert sich periodisch bei verschiedenen Informationsanbietern wie z.B. CERT über aktuelle Sicherheitslücken in Betriebssystemen und Anwendungsprogrammen und deren Gegenmaßnahmen. Dazu wurden verschiedene Mailing-Newsletter abonniert, z.B. von der Firma Internet Security Systems. Diese Informationen werden von der HZD zeitnah als Servicedienstleistung an die zuständigen Mitarbeiter der Landesverwaltung (IT-Betreuung) weitergegeben. Soweit diese Sicherheitsinformationen den Betrieb der vom Bereich "Neue Technologien" (z.B. Firewall) der HZD zu verantwortenden Systeme und Dienste betrifft, werden sie regelmäßig umgehend umgesetzt und aktiviert.
Die Nutzung unabhängiger Informationsanbieter ist auch aus Sicht der Landesregierung unabdingbar, zumal sich Sicherheitslücken oft erst bei der Nutzung der Software zeigen und das Abstellen der Mängel erhebliche Zeit benötigt.

Zu 12.4 Sichere Internetanbindung über eine Terminalserverlösung (Graphical Firewall – GFW)

Die Vorbereitungen zur technischen Umsetzung der Internetanbindung über Terminalserver wurden in der HZD begonnen. Dabei werden die Anregungen und Ergebnisse des Hessischen Datenschutzbeauftragten berücksichtigt. Sobald erste Erfahrungen insbesondere im Hinblick auf den Service und Betrieb (insb. Pflege- und Wartungsaufwand des Terminalservers) sowie die Abrechung der Nutzung einer solchen Internet-Anbindung vorliegen, wird geprüft, dieses Produkt als Standardleistung in den Leistungskatalog der HZD aufzunehmen.

Die Problematik der für diese Lösung notwendigen Netzinfrastruktur zur Anbindung aller Dienststellen mit adäquaten Kommunikationsleitungen wurde zunächst unberücksichtigt gelassen.

Zu 12.5 Prüfung von Softwareprodukten, die mit Dateiservern eingesetzt werden

Die aufgeführten Beispiele sind nachvollziehbar. Inwieweit innerhalb der Landesverwaltung noch Anwendungen eingesetzt werden, bei denen die geschilderten Probleme auftreten, ist der Landesregierung nicht bekannt. Die Empfehlung des Hessischen Datenschutzbeauftragten bei neuen Produktentwicklungen die Anwendungsdaten innerhalb einer Datenbank zu halten, kann aus Sicht der Landesregierung nachdrücklich unterstützt werden.

Zu 13. Kommunen

Zu 13.1 Briefwahlunterlagen per E-Mail beantragen

Die Erteilung eines Wahlscheines kann schriftlich oder mündlich bei der jeweiligen Wohnsitzgemeinde beantragt werden. Die Schriftform gilt nach dem durch Verordnung vom 12. Februar 2002 (BGBl. I S. 620) geänderten § 27 Abs.1 Bundeswahlordnung (BWO) und den durch Verordnung vom 25. April 2002 (GVBl. I S. 110) geänderten § 13 Abs. 1 Landeswahlordnung (LWO), § 3 Stimmordnung (StO) auch durch E-Mail oder durch sonstige dokumentierbare Übermittlung in elektronischer Form als gewahrt.

Die geänderten Vorschriften eröffnen den Wahlberechtigten einen zusätzlichen Weg für die Beantragung von Briefwahlunterlagen, ohne dass die Anforderungen an den Inhalt des Antrags geändert worden sind. Ausdrückliche Bestimmungen über den Inhalt eines Wahlscheinantrags gibt es nicht, insbesondere ist die Verwendung des auf der Rückseite der Wahlbenachrichtigung abgedruckten Antragsformulares nicht vorgeschrieben. Mindestanforderungen ergeben sich vielmehr aus der Natur der Sache, die darin besteht, dass die Identität des Antragstellers feststellbar ist und die gesetzlichen Voraussetzungen für die Ausstellung eines Wahlscheines erkennbar sind.

Einem Wahlberechtigten ist es daher unbenommen, etwa von seinem weit entfernten Urlaubsort durch eine formlose E-Mail Briefwahlunterlagen bei seiner Gemeinde zu beantragen; bei Zweifeln an der Identität des Antragstellers besteht für die Gemeinde Veranlassung zu einer Rückfrage. Risiken aus der Benutzung dieser Kommunikationsmöglichkeit gehen - wie bei der Verwendung der traditionellen Briefpost - zu Lasten des Wahlberechtigten.

Dies gilt aus wahlrechtlicher Sicht auch dann, wenn Gemeinden als freiwillige Dienstleistung ein elektronisches Antragsformular im Internet bereitstellen. Sofern diese Formulare im Dialogverfahren verwendet werden, ist es nach übereinstimmender Auffassung des Hessischen Datenschutzbeauftragten, des Landeswahlleiters und der Landesregierung aus Datenschutzgründen wünschenswert, dass die Übertragungen durch eine SSL-Verschlüsselung oder Verfahren mit einem vergleichbaren Niveau geschützt werden; andernfalls ist ein ausdrücklicher Hinweis auf die Risiken angezeigt, die der Antragsteller bei einer unverschlüsselten Versendung der Daten eingeht. Der Landeswahlleiter hat eine entsprechende Empfehlung sowohl im Vorfeld der Bundestagswahl als auch der Landtagswahl durch Erlasse vom 21. Juni 2002 (Wahlerlass Nr. B 19) sowie vom 14. November und 20. Dezember 2002 (Wahlerlass Nr. L 13 und L 23) über die Kreiswahlleiter an die Gemeinden gerichtet.

Einer missbräuchlichen Antragstellung stehen die restriktiven Regelungen über die Herausgabe des Wahlscheins und der Briefwahlunterlagen (§ 28 Abs. 4 Satz 1 BWO, § 15 Abs. 4 LWO) entgegen, nach welchen die Unterlagen an einen anderen als den Wahlberechtigten nur mit einer schriftlichen Vollmacht und nur im Falle einer plötzlichen Erkrankung ausgehändigt werden dürfen. Zudem ist die Herausgabe nur möglich, wenn die Unterlagen dem Wahlberechtigten nicht mehr rechtzeitig durch die Post übersandt oder amtlich überbracht werden können. Mit diesen Regelungen ist sichergestellt, dass auch im Falle einer elektronischen Antragstellung unter einem falschen Namen grundsätzlich nur der Antragsteller selbst den Wahlschein und die Briefwahlunterlagen erhalten kann. Um mögliche Missbräuche rechtzeitig zu erkennen, hat der Landeswahlleiter die Gemeinden zusätzlich gebeten, den

in dem Antrag angegebenen Wahlberechtigten in einem gesonderten Schreiben an dessen Wohnanschrift die Übersendung der Briefwahlunterlagen an die im Wahlschein genannte Adresse zu bestätigen und ihn um sofortige Benachrichtigung zu bitten, wenn der Antrag nicht von ihm selbst stammt. Bei der Bundestagswahl sind nach Berichten von 15 der 21 Wahlkreise insgesamt 7.350 Anträge und bei der Landtagswahl nach Berichten von 39 der insgesamt 55 Wahlkreise 5.815 Anträge elektronisch gestellt worden; über möglich Missbräuche ist dabei nur für die Bundestagswahl in zwei Fällen berichtet worden.

Gleichwohl werden sich Landesregierung und Landeswahlleiter auch bei zukünftigen Wahlen dafür einsetzen, dass die Hinweise des Hessischen Datenschutzbeauftragten von den Kommunen berücksichtigt werden.

Zu 13.2 Unzulässige Datenübermittlung durch ein städtisches Frauenbüro

Die kommunale Stelle hat in eigener Verantwortung gehandelt. Der Landesregierung fehlt daher die Grundlage für eine Stellungnahme.

Zu 13.3 Erfassung von Auskunftssperren im Einwohnermelderegister

Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend. Seine Hinweise an die Kommune, dass beim Zusammentreffen von Auskunftssperren nach § 34 Abs. 5 Hessisches Meldegesetz (HMG) und solchen nach § 35 Abs. 5 HMG alle Sperren in das Melderegister einzutragen sind, finden uneingeschränkte Zustimmung.

Zu 14. Hochschulen

Der Arbeitsansatz regelmäßiger Treffen von mehreren behördlichen Beauftragten für den Datenschutz hat sich besonders im Hochschulbereich bewährt. Es hat sich ein Arbeitskreis "Datenschutz" gebildet, in dem in regelmäßig stattfindenden Gesprächen, bei denen immer auch ein Vertreter oder eine Vertreterin des Hessischen Datenschutzbeauftragten anwesend ist, die anstehenden datenschutzrechtlichen Fachfragen auf kollegialer Ebene besprochen werden. Auf diese Weise hat der Hessische Datenschutzbeauftragte bereits im Vorfeld mit seinem besonderen Sach- und Fachverstand gemeinsame Lösungsansätze begleitet und deren Umsetzung mit beschleunigt.

Zu 14.1 Evaluation der Lehre an hessischen Hochschulen

Mit dem neuen Hochschulgesetz kommen einige völlig neue Aufgaben auf die Hochschulen zu. So müssen nach §§ 3 Abs. 8, 27 Abs. 4 und 92 Abs. 2 Hessisches Hochschulgesetz (HHG) regelmäßig von der Hochschule ihre Leistungen u.a. in Forschung und Lehre dargestellt sowie die Qualität und der Erfolg ermittelt und bewertet werden. Dabei müssen die erbrachten Leistungen durch Verfahren der Leistungsbewertung (Evaluation) regelmäßig überprüft werden. Die Grundzüge dieses Bewertungsverfahrens und das Zusammenwirken der Hochschulen untereinander wird zwischen Hochschulen und dem Ministerium für Wissenschaft und Kunst vereinbart.

In diesem Zusammenhang wird vom jeweiligen Präsidium einer Hochschule eine Satzung erlassen, die angibt, welche personenbezogenen Daten für die Leistungsbeschreibung in Forschung und Lehre, bei der Förderung des wissenschaftlichen Nachwuchses und zur Durchsetzung der Gleichberechtigung von Frauen und Männern erforderlich sind. Mit der Satzung soll gleichzeitig die Verarbeitung der personenbezogenen Daten auch im Sinne des Hessischen Datenschutzbeauftragten geregelt und die Formen ihrer Veröffentlichung festgelegt werden.

Für diesen Zweck haben der Hessische Datenschutzbeauftragte und das Ministerium für Wissenschaft und Kunst jeweils einen Entwurf einer Mustersatzung erarbeitet, die den Hochschulen als allgemeine Orientierungshilfe dienen kann. Die Hochschulen wurden per Erlass darauf hingewiesen, dass mit diesem Satzungsentwurf nicht die nach §§ 27 Abs. 4, 92 Abs. 3 HHG zu treffenden Vereinbarungen und Festlegungen präjudiziert werden sollen. Die Mustersatzung sollte nämlich nicht Vorgaben machen, welche möglichen statistischen Auswertungen, welche empirischen Untersuchungen usw. für Evaluationszwecke herangezogen werden sollen, sondern die Satzung findet

ihre Beschränkung in der Festsetzung, welche personenbezogenen Daten herangezogen und wie diese verarbeitet werden dürfen. Das eigentliche Evaluationsverfahren und damit die gesamte Fragestellung nach statistischen Ergebnissen wurde noch nicht festgelegt; es wird im Laufe der Zeit erarbeitet.

Die beiden Mustersatzungen weichen formal nur darin voneinander ab, dass der Hessische Datenschutzbeauftragte einen detaillierten Katalog von einzelnen Datenmerkmalen enumerativ aufführt, während der Entwurf des Ministeriums für Wissenschaft und Kunst diesen Katalog allgemeiner und offener fasst.

Im Übrigen hat der Hessische Datenschutzbeauftragte u.a. das Pilotprojekt der Einführung einer multifunktionalen Chipkarte mit elektronischer Signatur bei der Universität Gießen begleitet. Diese frühzeitige und vor allem umfassende Beratung vor Ort durch den Hessischen Datenschutzbeauftragten hat sich sehr bewährt. So konnten für diesen sehr komplexen Vorgang, der nicht nur die Hardware-Ausstattung, die Ablauforganisation sowie die Datenverarbeitung unmittelbar (z.B. den Datenaustausch) besonders beeinflusst hat, schon sehr frühzeitig auch alle notwendigen datenschutzrechtlichen Rahmenbedingen (z.B. Erlass einer Satzung, umfassende Information der Betroffen) geschaffen werden. Diese Erfahrung zeigt, dass es gerade beim Einsatz komplexerer neuer Technologien bei der Verarbeitung personenbezogener Daten geboten erscheint, ein Arbeitsteam zu bilden, in das auch immer der Hessische Datenschutzbeauftragte einbezogen ist.

Der Hessische Datenschutzbeauftragte plant in diesem Jahr eine Prüfung, ob alle von ihm vorgeschlagenen Maßnahmen auch umgesetzt sind. In diesem Zusammenhang bietet es sich jedoch an, dass von den Betroffenen schriftlich bestätigt wird, dass alle Maßnahmen aufgrund einer Checkliste umgesetzt und verwirklicht wurden. Damit wird von den für den Datenschutz Verantwortlichen ummittelbar ihre Verpflichtung angenommen und ihre Umsetzung auch im Sinne einer Qualitätskontrolle verbindlich garantiert. Weitere Kontrollen bleiben natürlich davon unberührt.

Zu 15. Schulverwaltung und Schulen

Die vom Hessischen Datenschutzbeauftragten festgestellten Mängel im Staatlichen Schulamt Fulda - fehlen der Vorabkontrolle und Verfahrensverzeichnis - bei Programmen zur Kontrolle der Arbeitszeit und Abrechnung von Telefonkosten werden in Kürze behoben.
Der Hessische Datenschutzbeauftragte wurde entsprechend unterrichtet.

Die Anregungen und Vorgaben hinsichtlich der Informationspflicht, der Aufbewahrungsfristen, der Aufbewahrung von Personalakten und der Datensicherungsmaßnahmen werden beachtet.

Zu 16. Archivwesen

Die vom Hessischen Datenschutzbeauftragten durchgeführten exemplarischen Prüfungen vor Ort in den einzelnen Dienststellen werden positiv bewertet. Solche unmittelbaren Prüfungen vor Ort tragen dazu bei, dafür Verständnis zu wecken, dass die teilweise sehr konkreten Probleme am einzelnen Arbeitsplatz meist nicht auf der mangelnden Bereitschaft der Mitarbeiterinnen und Mitarbeiter, für einen befriedigenden Datenschutz zu sorgen, beruhen, sondern dass räumliche und sachliche Gegebenheiten zu besonderen Erschwernissen führen (z.B. die vom Hessischen Datenschutzbeauftragten angeführte potentielle Einbruchgefahr). Auf diese Weise tragen solche Begegnungen unmittelbar auch dazu bei, der Arbeitsebene zu einem besseren Verständnis der tatsächlichen Situation und Probleme zu verhelfen und die tägliche Arbeitsroutine zu überdenken. Auch ist damit meist eine neue Bewertung und Sicht auf die eigenen Möglichkeiten innerhalb der Verwaltungen verbunden. Teilweise lassen sich problemlos, z.B. mit der Neugestaltung eines Erhebungsbogens, die Belange des Datenschutzes schnell und einfach verwirklichen, ohne dass dazu ein aufwendiger Schriftverkehr geführt wird. Der Hessische Datenschutzbeauftragte sollte solche Vorortprüfungen ausweiten.

Der Hessische Datenschutzbeauftragte hat exemplarisch die Einhaltung der datenschutzrechtlichen Vorschriften beim Hessischen Staatsarchiv Marburg

geprüft und festgestellt, dass diese Behörde, der u.a. die besondere Sicherheit des Archivgutes obliegt, korrekt die datenschutzrechtlichen Vorschriften beachtet.

Bei drei automatisierten DV-Verfahren wurden aus Termingründen die nach § 7 Abs. 6 HDSG erforderlichen Vorabkontrollen versäumt. Diese Kontrolle wird derzeit nachgeholt und die fraglichen Verfahren werden überprüft.

Bei der Erhebung der Benutzerdaten wurden die Nutzer des Archivs nicht förmlich über ihre Rechte nach § 12 Abs. 4 HDSG informiert. Diese fehlenden schriftlichen Hinweise werden in das neue Erhebungsformular aufgenommen.

Aufgrund der bisherigen räumlichen Gegebenheiten wird vom Hessischen Datenschutzbeauftragten ein gewisses theoretisches Sicherheitsrisiko beim Gebäude gesehen. Da das Archiv in Marburg einer allgemeinen größeren baulichen Sanierung unterliegt, werden im Rahmen dieser Maßnahme auch Lösungswege gesucht, wie am besten auf dieses gewisse Sicherheitsrisiko eingegangen werden kann.

Zu 17. Gesundheitswesen

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 18. Sozialwesen

Zu 18.1 "Offensiv-Gesetz"

Die Bezugnahme in dem Gesetzentwurf auf das Bundesdatenschutzgesetz ist in der Tat nicht sachgerecht, da es einen datenschutzrechtlichen Systembruch darstellt. Die Landesregierung stimmt daher den Ausführungen des Hessischen Datenschutzbeauftragten im Tätigkeitsbericht zu. Es bestehen keine Bedenken, im Zuge eines weiteren Gesetzgebungsverfahrens die datenschutzrechtliche Bezugnahme im gewünschten Sinne zu verändern.

Bei den Pilotprojekten zum Job-Offensivcenter ist in den mit den beteiligten Trägern abgeschlossenen Vereinbarungen ausdrücklich festgelegt, dass der wechselseitige kontinuierliche Austausch notwendiger personenbezogener Daten ausschließlich unter Beachtung der geltenden Bestimmungen (§ 421d Abs. 3 SGB III und § 18a BSHG) erfolgen soll.

Zu 18.2 Dienstaufsicht und Sozialdatenschutz

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 18.3 Auskunftsansprüche im Kinder- und Jugendhilferecht

Die Ausführungen des Hessischen Datenschutzbeauftragten im Tätigkeitsbericht beziehen sich auf ein Schreiben des Sozialministeriums an den Hessischen Datenschutzbeauftragten vom 9. April 2002 auf eine Anfrage zu Auskunftsrechten einer nicht sorgeberechtigten leiblichen Mutter. Im Schreiben des Ressorts wurde u.a. ausgeführt, dass ein Auskunftsrecht eines nicht sorgeberechtigten Elternteils unter Umständen seine Grenzen an den Persönlichkeitsrechten Dritter findet. Da es hier auch um die informationelle Selbstbestimmung dieser Dritten gehen kann, erstaunt es, dass sich der Hessische Datenschutzbeauftragte nicht auf diesen Hinweis bezieht. Eine gemeinsame Richtschnur für die Jugendämter sollte neben der Orientierung am Kindeswohl auch diesen Aspekt berücksichtigen.

Zu 18.4 Datenschutz im Adoptionsvermittlungsverfahren

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 19. Personalwesen

Zu 19.1 Weitergabe dienstlicher Unterlagen bei der Anrufung des Hessischen Datenschutzbeauftragten durch einen Personalrat

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 19.2 Übertragung der Zuständigkeiten für Untersuchungen zur Dienstfähigkeit von Beamtinnen und Beamten in der hessischen Landesverwaltung auf die Versorgungsämter

Die Rechtsgrundlage für die Datenerhebung durch die untersuchenden Ärzte der Hessischen Ämter für Versorgung und Soziales ist entgegen der im Tätigkeitsbericht vertretenen Ansicht nicht zweifelhaft. Die Ausführungen des Hessischen Datenschutzbeauftragten zu § 51 Hessisches Beamtengesetz (HBG) gehen von einem unzutreffenden Verständnis dieser Bestimmung aus. § 51 Abs. 1 Satz 3 HBG enthält keine Zuständigkeitsregelung für Ärzte, sondern die Verpflichtung des Beamten gegenüber seinem Dienstherrn, sich bei Zweifeln über seine Dienstfähigkeit ärztlich untersuchen zu lassen. Durch welchen Arzt dies erfolgen soll, entscheidet die Behörde ("nach Weisung der Behörde"). Sie kann, muss aber nicht, ein amtsärztliches Gutachten verlangen. Die Beteiligung eines Amtsarztes ist lediglich zur Anordnung einer ärztlichen Beobachtung erforderlich. Für alle weiteren sich aus § 51 HBG ergebenden Maßnahmen ist die Einschaltung eines freiberuflich tätigen Arztes ausreichend. Diese Rolle kann ohne weitere Regelungen von den Ämtern für Gesundheit und Soziales übernommen werden.

Des Weiteren enthält die im Tätigkeitsbericht nicht zitierte Vorschrift des § 51 Abs. 1 Satz 4 HBG die Ermächtigung, dass der die Untersuchung vornehmende Arzt der Behörde sein Gutachten sowie "in entsprechender Anwendung der für Amtsärzte geltenden Rechtsvorschriften" auch die Angaben zur Vorgeschichte und den Untersuchungsbefund mitteilt. Diese Ermächtigung gilt auch für die Ärzte der Versorgungsverwaltung. Aus dieser Regelung wird zugleich deutlich, dass die Untersuchung nach § 51 Abs. 1 Satz 3 HBG nicht zwingend von Amtsärzten zu leisten ist.

Um in der Landesverwaltung die Dienstunfähigkeitsuntersuchungen stärker zu vereinheitlichen hat die Landesregierung am 8. Mai 2001 beschlossen, dass mit diesen Untersuchungen in der Regel die Ärzte der hessischen Versorgungsverwaltung zu beauftragen sind. Bereits aus dem Wortlaut des Kabinettsbeschlusses geht unzweideutig hervor, dass keinesfalls die Funktion des Amtsarztes auf die Ärzte der hessischen Versorgungsverwaltung übertragen wurde. Kommt eine Beobachtung des Beamten nach § 51 Abs. 1 Satz 3 HBG in Betracht, kann diese selbstverständlich nur durch den Amtsarzt des Gesundheitsamtes veranlasst werden. Einer im Tätigkeitsbericht unter Nr. 19.2.3 angeregten Änderung oder Ergänzung des § 51 HBG bedarf es daher nicht. Auch § 18a der Dienstordnung war nicht zu ändern, weil dieser lediglich amtsärztliche Untersuchungen zum Gegenstand hat. Es handelt sich bei den von den Ärzten der hessischen Versorgungsverwaltung vorzunehmenden Untersuchungen ausdrücklich nicht um amtsärztliche Untersuchungen. Darüber hinaus gilt auch für diese Untersuchungen der Erlass des Hessischen Ministers des Innern und für Landwirtschaft, Forsten und Naturschutz vom 6. Dezember 1996 (StAnz. S. 4280) betr. "Inhalt ärztlicher Gutachten und Zeugnisse in dienst- oder arbeitsrechtlichen Angelegenheiten".

Das Sozialministerium hat den Entwurf eines neu gefassten Erlasses betr. "Ärztliche Begutachtung in Personalangelegenheiten des öffentlichen Dienstes; hier: Ausstellung ärztlicher/amtsärztlicher Zeugnisse" den betroffenen Ressorts und auch dem Hessischen Datenschutzbeauftragten zur Stellungnahme zugeleitet. Er soll an die Stelle des im Rahmen der Erlassbereinigung außer Kraft getretenen Erlasses über die Ausstellung amtsärztlicher Zeugnisse vom 24. Juli 1990 (StAnz. S. 1655) treten. Dieser Erlassentwurf soll auch nähere Regelungen für die vom ärztlichen Dienst der hessischen Versorgungsverwaltung durchgeführten Dienstunfähigkeitsuntersuchungen enthalten. Zudem soll versucht werden, den o.g. Erlass vom 6. Dezember 1996 in den beabsichtigten Erlass zu integrieren.

Im Übrigen werden in der hessischen Versorgungsverwaltung gegenwärtig die Einwilligungserklärungen für die Datenanforderung bei Drittstellen vereinheitlicht und datenschutzgerecht gestaltet, die Unterrichtung und Erklärung auf dem Anamnesebogen voneinander getrennt und entsprechend neu formuliert sowie der Annahmebogen vereinheitlicht.

Zu 20. Verkehrswesen

Die Landesregierung hat die Ausführungen des Hessischen Datenschutzbeauftragten zur Kenntnis genommen.

Zu 21. Vermessungswesen

Die Verfahren nach der Novellierung des Hessischen Vermessungsgesetzes haben sich bewährt.

Zu 22. Kammern

Die vom Hessischen Datenschutzbeauftragten angesprochenen Änderungen wurden bereits durchgeführt.

Zu 23. Bilanz

Zu 23.1 Einsatz des so genannten IMSI-Catchers durch Strafverfolgungsbehörden und Polizei (30. Tätigkeitsbericht, Nr. 13.2)

Auch die Landesregierung begrüßt grundsätzlich die in der Strafprozessordnung vorgenommene gesetzliche Klarstellung zum Einsatz des IMSI-Catchers im Strafverfahren. Sie ist allerdings der Auffassung, dass die Anknüpfung der Zulässigkeit der Maßnahme an die engen Voraussetzungen des § 100a StPO deutlich überzogen ist. Dabei ist zu sehen, dass der Einsatz des IMSI-Catchers ausschließlich zur Feststellung von Verbindungsdaten der Telekommunikation dient und anders als die in Bezug genommene Regelung des § 100a StPO gerade nicht zu einer Überwachung der Kommunikationsinhalte ermächtigt.

Die Ausführungen des Hessischen Datenschutzbeauftragten zu der neuen strafprozessualen Rechtslage sind zutreffend, nicht jedoch seine Darlegungen zu den praktischen Auswirkungen des Einsatzes eines IMSI-Catchers. Der IMSI-Catcher unterbricht keine bestehenden Telefonverbindungen. Bei sich aufbauenden Verbindungen werden die anrufenden Mobiltelefone lediglich kurzzeitig blockiert, bevor die Anrufe in das öffentliche Netz abgegeben werden. Aus diesen Umständen ist ersichtlich, dass den betroffenen Bürgern durch die Maßnahme keine Kosten entstehen.

Zu 23.2 Neue Informationssysteme für die Polizei (30. Tätigkeitsbericht, Nr. 8.1)

Erfreulich ist die Feststellung des Hessischen Datenschutzbeauftragten, dass ihm aus der polizeilichen Praxis keine datenschutzrechtlichen Probleme mit dem neuen polizeilichen Informationssystem bekannt geworden sind.

Mit Aufsetzen des Projektes POLAS Hessen ist das Präsidium für Technik, Logistik und Verwaltung (PTLV) mit der Erstellung eines ganzheitlichen Sicherheitskonzeptes beauftragt worden. Die Erarbeitung des Sicherheitskonzeptes orientierte sich an den Empfehlungen und Standards des Bundesamts für die Sicherheit in der Informationstechnik (BSI), die u.a. im IT-Grundschutzhandbuch und im IT-Sicherheitshandbuch dokumentiert sind. Die polizeilichen Anforderungen decken sich damit grundsätzlich mit den in den Handlungsleitfäden dokumentierten Empfehlungen/Anforderungen und gehen in den spezifischen polizeilichen Schutzbedürfnissen über die Anforderungen für die allgemeine Verwaltung hinaus.

Die Realisierung und Umsetzung des ganzheitlichen Sicherheitskonzeptes für Hessen wird stufenweise, einhergehend zum Projektverlauf POLAS/ComVor vorgenommen. Begonnen wurde zur Jahresmitte 2002, nachdem Anfang des Jahres ein IT-Sicherheitsmanagement etabliert worden war.

Entsprechend dem IT-Sicherheitskonzept ist die IT-Sicherheitsorganisation eingerichtet, mit einem Landessicherheitsbeauftragen beim PTLV und IT-Sicherheitsbeauftragten bei den Präsidien. Die Umsetzung der jährlich fortzuschreibenden Maßnahmen ist sichergestellt. Durch den Landessicherheitsbeauftragten erfolgt eine jährliche Berichterstattung.

Die Auditierung mit den Inhalten
- IT-Sicherheitsmanagement
- Räumliche Infrastruktur (Rechenzentrum, Zugangsregelungen, etc.)
- Technische Infrastruktur (Netz, Server, etc.)
- Netz-Administration, -Schnittstellen, -Benutzerverwaltung
- IT-Anwendungen (Datenbanken, Zugriffsserver, INPOL-Anwendung)

wird bereits umgesetzt bzw. ist im Jahresverlauf eingeplant.

Zu den technischen Möglichkeiten von ComVor trägt der Hessische Datenschutzbeauftragte vor, das Verfahren sei so konstruiert, dass immer nur ein konkreter Vorgang erschließbar ist und es demzufolge nicht möglich ist, hessenweit zu suchen, ob und in welcher Rolle eine Person in verschiedenen Ermittlungsverfahren auftaucht. Diese Aussage trifft auf das der Vorgangsbearbeitung dienende eigentliche ComVor-System zu. Der Vollständigkeit halber ist jedoch darauf hinzuweisen, dass das Suchsystem ComVor-Index weitergehende Recherchemöglichkeiten bietet. Einzelheiten beider Komponenten sind seinerzeit von der mittlerweile aufgelösten Projektgruppe mit dem Hessischen Datenschutzbeauftragten erörtert worden.

Zu 23.3 Projekt "Elektronische Fußfessel" (28. Tätigkeitsbericht, Nr. 6; 29. Tätigkeitsbericht, Nr. 20.2)

Zu dem das Modellprojekt "elektronische Fußfessel" begleitenden Forschungsvorhaben liegt mittlerweile ein Zwischenbericht vor, der dem Hessischen Datenschutzbeauftragten mit Schreiben des Ministeriums der Justiz vom 26. Mai 2003 übermittelt worden ist. Im Übrigen wird die Begleituntersuchung weiter fortgeführt.

Der Annahme des Hessischen Datenschutzbeauftragten, der Einsatz der elektronischen Fußfessel bedürfe als Eingriff in das Recht auf informationelle Selbstbestimmung einer gesetzlichen Grundlage, vermag sich die Landesregierung nicht anzuschließen. Insoweit ist zu sehen, dass die Maßnahme in Hessen ausschließlich auf der Grundlage einer Einwilligung des Betroffenen durchgeführt wird und daher gerade nicht als Eingriff in das Recht auf informationelle Selbstbestimmung ohne oder gegen den Willen des Betroffenen anzusehen ist. Einer gesetzlichen Eingriffsbefugnis bedarf es daher insoweit nicht.

Zu 23.4 Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen (30. Tätigkeitsbericht, Nr. 8.4)

Die Unterschiede zur Auffassung des Hessischen Datenschutzbeauftragten sind geringfügiger, als es die Darstellung im Tätigkeitsbericht vermuten lässt.

Erkennungsdienstliche Behandlungen in einem Strafverfahren können nach § 81b StPO aus zwei Gründen erfolgen. Zum einen kann die Maßnahme zur Aufklärung der aktuellen Straftat erforderlich sein, z.B. um festzustellen, ob die am Tatort gesicherten Fingerspuren vom Beschuldigten stammen. Sie ist dann nach § 81b 1. Alternative StPO ohne zusätzliche Voraussetzungen gestattet.

Eine ed-Behandlung kann aber auch geboten sein, wenn sie zwar für das anhängige Strafverfahren unerheblich ist, die Polizei aber annimmt, dass gegen den Beschuldigten in der Zukunft wegen anderer Straftaten erneut zu ermitteln sein wird und die Unterlagen dabei von Nutzen sein könnten. Dieser die Vorsorge für die künftige Strafverfolgung betreffende Fall ist in § 81b 2. Alternative StPO geregelt. Nach der ständigen Rechtsprechung des Bundesverwaltungsgerichts setzt eine ed-Behandlung nach der zweiten Alternative voraus, dass für den Betroffenen aufgrund einer Gesamtabwägung aller Umstände eine so genannte Negativprognose zu erstellen ist. Dieselben Anforderungen gelten für die weitere Aufbewahrung der Unterlagen.

Erkennungsdienstliche Unterlagen, die von vornherein zur Vorsorge für die künftige Strafverfolgung angefertigt werden, dürfen demnach nur unter strengeren Voraussetzungen gespeichert werden als sonstige kriminalpolizeiliche Unterlagen, für die § 20 Abs. 4 HSOG gilt, der auf die Negativprognose verzichtet. Die Aufbewahrung von erkennungsdienstlichen Unterlagen nach § 81b 1. Alternative StPO ist an keine zusätzlichen Anforderungen gebunden.

Für die auf die Grundlage der ersten Alternative angefertigten ed-Unterlagen gilt § 481 StPO, wonach die Polizeibehörden personenbezogene Informationen aus Strafverfahren nach Maßgabe der Polizeigesetze verwenden dürfen. Die polizeirechtliche Grundlage für die Speicherung ergibt sich für Hessen aus § 20 Abs. 4 H Eine Negativprognose wird deshalb von Gesetzes wegen nicht verlangt. Auch insoweit besteht Einvernehmen mit dem Hessischen Datenschutzbeauftragten.

Die Bedenken des Hessischen Datenschutzbeauftragten richten sich darauf, dass der in der Aufbewahrung der erkennungsdienstlichen Unterlagen liegende Eingriff schwerer wiege als der mit der Speicherung der übrigen Daten verbundene Eingriff und dass deswegen der Verhältnismäßigkeitsgrundsatz verletzt sein könnte.

Dieser Einwand ist beachtlich, erfordert aber keine ausdrückliche Behandlung in den Richtlinien. Die Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen (KPS-Richtlinien) sehen bereits in Nr. 20 die Bereinigung von KPS abweichend von den zuvor aufgestellten Regelungen vor, wenn die weitere Speicherung für die polizeiliche Aufgabenerfüllung nicht mehr erforderlich ist oder die Daten unzulässigerweise gespeichert sind. Die Missachtung des Verhältnismäßigkeitsgrundsatzes würde zu einer unzulässigen Speicherung führen.

Die Erfahrung spricht dafür, dass der ganz überwiegende Teil der ed-Maßnahmen ausschließlich zur Vorsorge für die künftige Strafverfolgung erfolgt. In fast allen verbleibenden Fällen werden zugleich die Voraussetzungen der zweiten Alternative vorliegen, auch wenn die Maßnahme nicht darauf gestützt ist. Der Grund ist darin zu sehen, dass die Polizei zur Aufklärung bloßer Bagatellstraftaten keine erkennungsdienstliche Behandlung durchführt. Aus den jeweils vorliegenden Umständen (Schwere der Straftat, Art der Tatbegehung), die eine ed-Behandlung zur Aufklärung erfordert, wird sich deshalb in der Regel auch eine Negativprognose herleiten lassen.

Für eine ausdrückliche Behandlung dieser Problemstellung in den KPS-Richtlinien besteht kein Anlass.

Zu 23.5 Modellprojekt Mammographie-Screening (30. Tätigkeitsbericht, Nr. 11.1)

Die Tatsache, dass am Anfang noch nicht genügend Personal eingestellt war und damit eine Abweichung vom Datenschutzkonzept vorlag, war nicht bekannt. Durch weitere Personaleinstellungen konnte diese Frage inzwischen geklärt werden. Unterschiedliche Personen sind in getrennten Bereichen (zwei Etagen) für die Administration der beiden Datenbanken zuständig.
Das wartungsbedingte Abschalten des Passwortes unmittelbar vor der Visite der Datenschutzmitarbeiter war nicht bekannt und ist inzwischen korrigiert.

Zu 23.6 Datenschutz in der Abgabenordnung (30. Tätigkeitsbericht, Nr. 10.2 und 27.7)

In den Novellierungsprozess der Abgabenordnung unter datenschutzrechtlichen Gesichtspunkten ist zwischenzeitlich Bewegung gekommen.

Beide Seiten haben jeweils vor dem Hintergrund ihres Verfassungsauftrages (Gleichmäßigkeit und Vollständigkeit der Besteuerung beziehungsweise Wahrung des Rechts auf informationelle Selbstbestimmung) ihre Standpunkte verdeutlicht; eine gemeinsame Zielrichtung soll erarbeitet werden. Die Fortsetzung der Koordinierungsgespräche ist in nächster Zeit vorgesehen.

Zu 23.7 Zusammenarbeit bei der Produktion von Fernsehsendungen - Reality TV (30. Tätigkeitsbericht, Nr. 8.2)

Die Bestätigung des Hessischen Datenschutzbeauftragten, dass die Richtlinien in der Praxis Beachtung finden, nimmt die Landesregierung mit Genugtuung zur Kenntnis.

Wiesbaden, 9. Dezember 2003

Der Hessische Ministerpräsident:
Koch

Der Minister des Innern und für Sport:
Bouffier