16. Wahlperiode

Drucksache **16/5891**

HESSISCHER LANDTAG

16. 08. 2006

Stellungnahme der Landesregierung

betreffend den Vierunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Drucksache 16/5359

Eingegangen am 16. August 2006 · Ausgegeben am 24. August 2006
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Die Stellungnahme der Landesregierung gibt den Sachstand im April/Mai 2006 wieder.

Zu 1. Einführung

Der Hessische Datenschutzbeauftragte erläutert in der Einführung zu seinem 34. Tätigkeitsbericht, dass die Wahrnehmung seiner abwehrrechtlichen Befugnisse auch im Jahr 2005 den Schwerpunkt seiner Arbeit bildete. Die Landesregierung begrüßt das positive Gesamturteil des Datenschutzbeauftragten hinsichtlich des Datenschutzes in Hessen. Sie sieht darin eine Bestätigung ihrer Überzeugung, dass die Beschäftigten in den öffentlichen Stellen in Hessen verantwortungsvoll mit den Daten der Bürgerinnen und Bürger umgehen.
Die Landesregierung wird dem Datenschutz auch weiterhin hohe Priorität einräumen.

Der Hessische Datenschutzbeauftragte legt in der Einführung zu seinem Tätigkeitsbericht darüber hinaus die Ansicht dar, der Datenschutz habe nicht nur dem Recht zu dienen, vor rechtswidrigen Datenzugriffen verschont zu werden, sondern auch aktiv dazu beizutragen, dass niemand an der Informationsbeschaffung gehindert wird, weil er zugleich einen Eingriff in die informationelle Selbstbestimmung befürchten muss. Er verbindet damit den Datenschutz und die Informationsfreiheit und schlägt die Erweiterung der Kompetenz seiner Behörde in den Bereich eines Hessischen Informationsfreiheitsgesetzes vor, dessen Erlass er für geboten hält.

Nach Auffassung der Landesregierung ist der Nachweis der Notwendigkeit eines Informationsfreiheitsgesetzes gegenwärtig noch nicht erbracht (vgl. Stellungnahme zu Ziff. 2.1.2.2). Aus diesem Grunde sieht die Landesregierung derzeit keine Notwendigkeit, sich zu der vom Hessischen Datenschutzbeauftragten vorgetragenen Kompetenzregelung eine abschließende Meinung zu bilden.

2. Datenschutzbeauftragte

2.1 Hessischer Datenschutzbeauftragter

Zu 2.1.1 Allgemeines

Die Landesregierung stimmt der Beschreibung der Rechts- und Aufgabenstellung des Hessischen Datenschutzbeauftragten zu.

Zu 2.1.2 Neue Aufgaben

Die Auffassung der Landesregierung zur Forderung des Hessischen Datenschutzbeauftragten nach Erweiterung seiner Aufgabenstellung wird in Zusammenhang mit den Ausführungen zum Umweltinformations- (zu Ziff. 2.1.2.1) bzw. Informationsfreiheitsgesetz (zu Ziff. 2.1.2.2) erläutert.

Zu 2.1.2.1 Hessisches Umweltinformationsgesetz

Der Hessische Datenschutzbeauftragte führt zutreffend aus, dass in dem dem Hessischen Landtag vorgelegten Gesetzentwurf (Drs. 16/5407) die Institution eines Informationsfreiheitsbeauftragten gegenüber einem früheren Entwurf entfallen und statt dessen ein behördliches Überprüfungsverfahren geschaffen worden ist (§ 9 HUIG-Entwurf). Diese mit Kabinettsbeschluss vom 18. Juli 2005 (Freigabe des Gesetzentwurfs zur Verbandsanhörung) getroffene Veränderung des ursprünglichen Referentenentwurfs wird vom Hessischen Datenschutzbeauftragten in seinem Tätigkeitsbericht kritisiert.

Beides, die ursprünglich vorgesehene Einrichtung eines Informationsfreiheitsbeauftragten beim Hessischen Datenschutzbeauftragten und auch das jetzt normierte behördliche Überprüfungsverfahren, dient in erster Linie der Umsetzung der maßgeblichen EG-Richtlinie, die in ihrem Art. 6 Abs. 1 fordert, dass die Behörden ihre Entscheidungen in einem der Verwaltungsgerichtsbarkeit vorgeschalteten Behördenverfahren überprüfen oder per Gesetz eine unabhängige Schiedsstelle geschaffen wird.

Mit dem Regierungsentwurf (Kabinettsbeschluss vom 13. März 2006), wie er in das Gesetzgebungsverfahren gegangen ist, hat sich die Landesregierung bewusst gegen einen Informationsfreiheitsbeauftragten und für ein behördliches Überprüfungsverfahren entschieden. Hintergrund dieser Entscheidung sind die seit Jahren in einem nachhaltigen Reformprozess verfolgten Bemühungen des Landes um Reduzierung des Vorschriftenwesens und um Abbau von Bürokratie. Parallel zu einer ständigen Kontrolle der Normen im Hin-

blick auf deren Erforderlichkeit werden auch die Verwaltungsverfahren auf ihre Effizienz hin untersucht.

Aus diesem Grunde hat das 3. Verwaltungsstrukturreformgesetz in vielen Bereichen die Widerspruchsverfahren abgeschafft. Mit dem jetzt im HUIG-Entwurf festgelegten behördlichen Überprüfungsverfahren, das gerade kein förmliches Widerspruchsverfahren i.S.d. § 68 VwGO darstellt, erfüllt Hessen die Umsetzungsvoraussetzungen der Richtlinie im Maßstab 1:1 und vermeidet zusätzlichen bürokratischen Aufwand.

Sofern der Hessische Datenschutzbeauftragte seine Forderung, einen Beauftragten für den Umweltinformationszugang zu schaffen, weiterverfolgen möchte, müsste er dies im Rahmen der Landtagsberatungen zu dem HUIG-Entwurf zur Geltung bringen.

Zu 2.1.2.2 Hessisches Informationsfreiheitsgesetz
Bestrebungen der Landesregierung, einen Gesetzentwurf für ein Informationsfreiheitsgesetz im Landtag einzubringen, bestehen nicht.

Zur Zeit haben der Bund und die Bundesländer Berlin, Brandenburg, Hamburg, Nordrhein-Westfalen und Schleswig-Holstein ein Informationsfreiheitsgesetz. Das Argument, dass Hessen ähnlich wie der Bund ein Informationsfreiheitsgesetz erlassen sollte, um wieder Anschluss an die Spitzengruppe der Länder zu finden, reicht nicht aus, ein solches Gesetz zu rechtfertigen. Mit Blick auf die verfassungsrechtlich geschützten Grundsätze der Sparsamkeit und Wirtschaftlichkeit der Verwaltung bedarf es vielmehr des Nachweises der Notwendigkeit eines Informationsfreiheitsgesetzes. Dieser Nachweis ist nach Einschätzung der Landesregierung noch nicht erbracht.

Nach jetzigem Erkenntnisstand reichen für die Gewährung von Akteneinsicht die in den verschiedenen Gesetzen ausdrücklich geregelten Akteneinsichtsrechte aus. Außerdem besteht ein allgemeines Akteneinsichtsrecht nach pflichtgemäßem Ermessen der Behörde, wenn Bürgerinnen und Bürger oder Unternehmen ein Interesse an der Akteneinsicht geltend machen. Dieses allgemeine Akteneinsichtsrecht ist in der Vergangenheit kaum in Anspruch genommen worden. Sogar im Umweltbereich, der erfahrungsgemäß auf ein erhebliches Interesse der Allgemeinheit und der Unternehmen stößt, haben sich die Akteneinsichts- und Auskunftsbegehren in Grenzen gehalten.

Es bleibt abzuwarten, in welchem Umfang die bestehenden Informationsfreiheitsgesetze in Anspruch genommen werden und ob sie sich bewähren.

Zu 2.1.2.3 Privater Bereich
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass gegenwärtig eine Übertragung der Zuständigkeit für den Datenschutz im privaten Bereich auf die Behörde des Datenschutzbeauftragten nicht zur Diskussion steht. Nach geltender Rechtslage haben der für den öffentlichen Bereich zuständige Hessische Datenschutzbeauftragte und das für den nicht öffentlichen Bereich zuständige Regierungspräsidium Darmstadt auf der Grundlage des § 3 HDSG sowie § 2 Bundesdatenschutzgesetz (BDSG) jeweils die Zuständigkeit zu prüfen, sofern sie im Einzelfall nicht offensichtlich ist. Diese Prüfung wäre jedoch auch im Falle eine Zusammenführung der Datenschutzaufsicht in einer Behörde erforderlich, weil das deutsche Datenschutzrecht in seinen Bestimmungen öffentliche und nicht öffentliche Stellen unterscheidet. Auch ein unabhängiger Landesdatenschutzbeauftragter ist an diese vom Gesetzgeber getroffene Unterscheidung nach der Art der Stelle gebunden.

Für öffentliche Stellen in Hessen, mit Ausnahme solcher des Bundes, gilt das HDSG, für nicht öffentliche Stellen grundsätzlich das BDSG. Die gesetzliche Definition der nicht öffentlichen Stelle findet sich in § 2 Abs. 4 Satz 1 BDSG; der Bund hat insoweit von seiner Gesetzgebungskompetenz Gebrauch gemacht. Weder der Landesgesetzgeber noch die Landesregierung können eine hiervon abweichende Regelung treffen.

Nach der Systematik des BDSG ist eine Vereinigung des privaten Rechts nur dann als öffentliche Stelle zu behandeln, wenn an dem Unternehmen mindestens eine öffentliche Stelle beteiligt ist und es Aufgaben der öffentlichen Verwaltung wahrnimmt (§ 2 Abs. 3) oder wenn es hoheitliche Aufgaben der öffentlichen Verwaltung wahrnimmt (§ 2 Abs. 4 Satz 2). Wenn hoheitliche

Aufgaben wahrgenommen werden, dann kommt es auf eine Beteiligung der öffentlichen Hand nicht an. Das BDSG unterscheidet also bei der Zuordnung privater Unternehmen zu den öffentlichen Stellen zwischen hoheitlichen Aufgaben und anderen Aufgaben der öffentlichen Verwaltung. Nach Auffassung der Landesregierung darf diese Definition im Bundesrecht nicht durch eine teleologische Extension des Begriffs der hoheitlichen Aufgabe in § 3 Abs. 1 Satz 2 HDSG, wie sie der Hessische Datenschutzbeauftragte vorschlägt, umgangen werden. Private Unternehmen würden sonst, entgegen der Vorschriften des BDSG, dem Landesdatenschutzgesetz unterworfen.

Die Landesregierung sieht es als ihre Aufgabe an, für die korrekte Anwendung des BDSG auf nicht öffentliche Stellen Sorge zu tragen. Damit soll weder einer "Flucht ins Privatrecht" Vorschub geleistet, noch die Aufgabenstellung des Hessischen Datenschutzbeauftragten ausgehöhlt werden. Hier setzt das Bundesrecht der Interpretierbarkeit des Landesrechts jedoch eine Grenze.

Auch innerhalb dieser Grenze bietet die im Datenschutzrecht erforderliche Entscheidung, ob eine Daten verarbeitende Stelle eine öffentliche oder nicht öffentliche ist, in Einzelfällen Anlass zur Interpretation. Insoweit begrüßt die Landesregierung ausdrücklich das Angebot des Hessischen Datenschutzbeauftragten, den Versuch einer gemeinsamen Bestandsaufnahme der im Bereich der Daseinsvorsorge tätigen Branchen zu unternehmen. Das Innenministerium wird dazu Kontakt mit dem Hessischen Datenschutzbeauftragten aufnehmen.

Die vom Hessischen Datenschutzbeauftragten nochmals angesprochene Frage der Aufsicht über die Fraport AG (vgl. 33. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drs. 16/3746, Ziff. 2.2 und Stellungnahme der Landesregierung zu Ziff. 2.2, Drs. 16/4751) ist inzwischen geklärt worden. Der Minister des Innern und für Sport hat entschieden, wegen der negativen Folgen für die Rechtssicherheit auf die Fortführung der Diskussion über die Zuständigkeit zu verzichten und Einvernehmen mit dem Hessischen Datenschutzbeauftragten darüber erzielt, dass dessen Behörde für die Fraport AG zuständig ist, soweit das Unternehmen im Bereich der Daseinsvorsorge tätig ist.

Zu 2.1.3 Unabhängigkeit des Hessischen Datenschutzbeauftragten und Instrumente der Neuen Verwaltungssteuerung

Der Hessische Datenschutzbeauftragte ist nach dem Gesetz als oberste Landesbehörde in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Gleichwohl unterliegt auch der Hessische Datenschutzbeauftragte mit den Ressourcen, die ihm vom Präsidenten des Landtags zur Erfüllung seiner Aufgaben zur Verfügung gestellt und im Einzelplan des Landtags ausgewiesen werden, der Haushaltsgesetzgebung des Landtags. Das bedeutet, dass er auch künftig im Rahmen des vom Landtag beschlossenen Produkthaushalts und den damit verbundenen haushaltsgesetzlichen Regelungen sein Amt zu erfüllen hat.

Der besonderen Stellung und Aufgabenverantwortung des Hessischen Datenschutzbeauftragten ist in Gesprächen mit ihm bei der Ausarbeitung seines Zielsystems und seiner Produkte auf Leitungsebene entsprochen worden. Das Zielsystem ist aufgrund seines Vorschlags vom Kabinett zur Kenntnis genommen worden. Den Ausführungen und Anmerkungen des Hessischen Datenschutzbeauftragten in Bezug auf die Validität seiner Produktplanung und den damit zusammenhängenden Risiken für den Vollzug des Produkthaushalts ist in der Weise Rechnung getragen worden, dass abweichend von der üblicherweise für die Produkthaushalte geltenden 10%igen Korridorregelung für den Produkthaushalt des Hessischen Datenschutzbeauftragten eine 35%ige Deckungsfähigkeit für seine Produkte vorgesehen wird. In das landesweite Controlling-Verfahren wird die Dienststelle des Hessischen Datenschutzbeauftragten nicht einbezogen.

Mit diesen Modifizierungen ist aus Sicht der Landesregierung gewährleistet, dass die durch Gesetz festgelegte Unabhängigkeit des Hessischen Datenschutzbeauftragten auch im Rahmen der Neuen Verwaltungssteuerung unangetastet bleibt.

Mit dem Parlament wird abzustimmen sein, ob die für die Ressorts festgelegten Führungsberichte, die den Vollzug des Produkthaushalts im Wesentli-

chen darstellen, auch in der Dienststelle des Hessischen Datenschutzbeauftragten zu erstellen sind und dem Budgetbüro beim Hessischen Landtag zur Verfügung gestellt werden.

2.2 Behördliche Datenschutzbeauftragte

Zu 2.2.1 Ergebnisse einer Untersuchung zu Rechtsstellung und Aufgaben behördlicher Datenschutzbeauftragter

Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten mit Interesse zur Kenntnis genommen.
Das Merkblatt zu Stellung und Aufgaben des behördlichen Datenschutzbeauftragten, das der Hessische Datenschutzbeauftragte in seinem Internet-Angebot bereit hält, kann Interessierten uneingeschränkt empfohlen werden.

3. Europa

Zu 3.1 Allgemeines

Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten mit Interesse zur Kenntnis genommen.

Zu 3.2 14. Wiesbadener Forum Datenschutz

Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten mit Interesse zur Kenntnis genommen.

Zu 3.3 Gemeinsame Kontrollinstanz für das Schengener Informationssystem

Die Darstellungen des Hessischen Datenschutzbeauftragten sind zutreffend.

Zu 3.4 Gemeinsame Kontrollinstanz für EUROPOL

Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten mit Interesse zur Kenntnis genommen.
Eigene Erkenntnisse über die Tätigkeit der Gemeinsamen Kontrollinstanz liegen der Landesregierung nicht vor.

4. Bund

Zu 4.1 Rechtsprechung des Bundesverfassungsgerichtes zum Kernbereich privater Lebensgestaltung

Der Hessische Datenschutzbeauftragte weist zu Recht darauf hin, dass der Gesetzgeber in Hessen die in den beiden Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 (1 BvR 2378/98, 1 BvR 1084/99) aufgestellten Forderungen zum Schutz des Kernbereichs privater Lebensgestaltung und zur Unterrichtung von Personen, die von verdeckten Maßnahmen betroffen waren, bereits beim Achten Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 15. Dezember 2004 (GVBl. I S. 444) berücksichtigt hat. Das Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 (1 BvR 668/04) zur Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz betrifft Hessen wegen der viel enger begrenzten Befugnis zur Telekommunikationsüberwachung (§ 15a HSOG) nur insoweit, als das Gericht in dieser Entscheidung den Kernbereich privater Lebensgestaltung von der Wohnung als räumlichem Substrat gelöst hat.

Bei der Schaffung von §15a HSOG ist der Gesetzgeber in der Tat davon ausgegangen, dass die Ausführungen des Gerichts zum Kernbereich privater Lebensgestaltung ausschließlich bei der Wohnraumüberwachung anwendbar sind. Das Bundesverfassungsgericht bestätigt auch in seinem Urteil zur polizeirechtlichen Telekommunikationsüberwachung aus dem Jahr 2005 im Prinzip einen Unterschied, fordert aber gleichwohl grundsätzlich, dass die Überwachung zu unterbleiben hat, wenn Inhalte erfasst werden, die den Kernbereich privater Lebensgestaltung betreffen (Absatz-Nr. 162, 163). Es formuliert allerdings eine Ausnahme für den Fall des besonders hohen Ranges eines gefährdeten Rechtsguts (Absatz-Nr. 164). Hier kommt nun ein wesentlicher Unterschied zwischen dem niedersächsischen und dem hessischen Polizeigesetz zum Tragen. Während der niedersächsische Gesetzgeber die Telekommunikationsüberwachung umfassend zur Verhütung von Straftaten und sogar zur Vorsorge für die Strafverfolgung zugelassen hatte, lässt die hessische Regelung einen Eingriff in das Fernmeldegeheimnis ausschließlich dann zu, wenn dies zum Schutz der höchsten Individualrechtsgüter - Leib, Leben oder Freiheit einer Person - vor einer gegenwärtigen Gefahr unerlässlich ist. Damit beschränkt sie sich auf den Bereich, für den das Bundesverfassungsgericht eine Ausnahme zubilligt.

Der Forderung des Bundesverfassungsgerichts, dass Daten, die den Kernbereich betreffen, nicht gespeichert und verwertet, sondern unverzüglich gelöscht werden, trägt das HSOG ohne Bindung an die Wohnraumüberwachung bereits Rechnung. §27 Abs. 6 Satz 1 Nr. 2 HSOG bestimmt, dass Daten, die dem Kernbereich privater Lebensgestaltung unterfallen, selbst dann zu löschen sind, wenn sie im Rahmen einer verdeckten Datenerhebung angefallen sind und die betroffene Person hierüber noch nicht unterrichtet worden ist. Das Löschungsgebot des Gesetzes schließt immer auch zugleich ein Verwertungsverbot für die zu löschende Information mit ein.

Soweit sich der Hessische Datenschutzbeauftragte in diesem Zusammenhang mit der Bestimmung der Straftaten von erheblicher Bedeutung befasst (Ziff. 4.1.1.2), ist klarstellend zu bemerken, dass die Telekommunikationsüberwachung in Hessen nicht zur Verhütung von Straftaten, sondern auf der Grundlage des klassischen Polizeirechts allein zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person zugelassen ist.

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 folgt für den Bereich der Strafverfolgung, namentlich für die Telekommunikationsüberwachung nach §§ 100a, 100b StPO kein gesetzlicher Änderungsbedarf.

§ 100a StPO beinhaltet einen Anlasstatenkatalog, der erkennen lässt, dass der Gesetzgeber ein den Verhältnismäßigkeitsgrundsatz berücksichtigendes Konzept verfolgt hat. Hinsichtlich der vom Bundesverfassungsgericht geforderten Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung ist außerdem zu berücksichtigen, dass sich der Entscheidung vom 27. Juli 2005 eine Abstufung (vgl. Absatz-Nr. 162 und 163 des Urteils) entnehmen lässt, wonach bei der Telekommunikationsüberwachung ein weniger strenger Maßstab anzulegen ist als bei der akustischen Wohnraumüberwachung. Das Bundesverfassungsgericht begründet dies namentlich damit, dass die Bürger zur höchstpersönlichen Kommunikation nicht in gleicher Weise auf Telekommunikation angewiesen sind wie auf eine Wohnung. Diesen Anforderungen werden die §§ 100a, 100b StPO gerecht. Der Katalog der Anlasstaten des § 100a StPO beinhaltet Straftatbestände, die jeweils dem Schutz von besonders hochrangigen Rechtsgütern dienen. Auch enthält die derzeitige Fassung des Gesetzes ausreichende Vorkehrungen hinsichtlich des Umgangs mit Kommunikationsinhalten des höchstpersönlichen Bereichs. Nach § 100b Abs. 6 StPO ist das für die Strafverfolgung nicht oder nicht mehr benötigte Material unverzüglich zu vernichten.

Zu 4.2 Einführung des E-Passes

Die rechtlichen Rahmenbedingungen für die Einführung des neuen biometriegestützten EU-Reisepasses (ePass) mit der Speicherung des Passbildes und der Daten der maschinenlesbaren Zone in einem Chip (erste Stufe) wurden vom Bund durch die Zweite und Dritte Verordnung zur Änderung passrechtlicher Vorschriften (BGBl. I S. 2306 und S. 2980) zum 1. November 2005 geschaffen.

Der Bundesrat hatte das Vorhaben der Bundesregierung, zum 1. November 2005 biometrie-gestützte Reisepässe einzuführen, begrüßt und den Verordnungen zugestimmt. Gleichzeitig hatte der Bundesrat die Bundesregierung gebeten, unverzüglich einen Entwurf zur Änderung des Passgesetzes mit dem Ziel der notwendigen Anpassung an die Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 vorzulegen.

Die gleiche Bitte haben die Innenminister und -senatoren der Länder auf ihrer Sitzung am 4./5. Mai 2006 ausgesprochen. Mit dem Gesetzentwurf sollen insbesondere die erforderlichen Rechtsgrundlagen für die geplante Abnahme der Fingerabdrücke durch die Passbehörden und deren Speicherung im Chip (zweite Stufe) sowie für den Abgleich der biometrischen Merkmale geschaffen werden.

Das Bundesministerium des Innern hat die baldige Vorlage des Gesetzentwurfs zugesagt. Beabsichtigt ist dabei auch die Schaffung einer Ermächtigungsgrundlage zum Erlass einer Verordnung zur Regelung technischer Anforderungen. Im Rahmen des Gesetzgebungsverfahrens werden die datenschutzrechtlichen Fragen zu beantworten und im notwendigen Umfang gesetzlich zu regeln sein.

Die Einführung des ePasses zum 1. November 2005 wurde vom Bund zum Zweck der Erhöhung der Dokumentensicherheit und damit der besseren Bekämpfung des internationalen Terrorismus und der Verhinderung des Missbrauchs von Pässen verfolgt.

Die Einführung des ePasses war aber auch sinnvoll, um die zu diesem Zeitpunkt aktuellen Forderungen der USA für die weitere Teilnahme am Visa-Waiver-Programm (Einreise ohne Visum) zu erfüllen. Die Forderungen waren, dass nach dem 26. Oktober 2005 nur diejenigen Länder an dem Visa-Waiver-Programm teilnehmen können, die zu diesem Stichtag mit der Ausgabe biometriegestützter Reisepässe begonnen haben. Dieses Erfordernis hat die Bundesregierung mit der Einführung des ePasses zum 1. November 2005 erfüllt. Von den USA wurde kurzfristig im Sommer 2005 die ursprüngliche Befristung vom 26. Oktober 2005 auf den 26. Oktober 2006 verlängert.

Zu 4.3 Fußball-Weltmeisterschaft 2006

Die Landesregierung stimmt der Darstellung der datenschutzrechtlichen Fragestellungen im Zusammenhang mit der Fußball WM 2006 zu.
Allerdings ist der Ansicht des Hessischen Datenschutzbeauftragten, dass ein mobiler Einsatz von Videokameras nach der Rechtslage praktisch ausgeschlossen sei (Ziff. 4.3.1), nicht zutreffend. § 14 Abs. 3 HSOG erlaubt eine Videoüberwachung, wenn der Ort öffentlich zugänglich ist und es eine konkrete Gefahr abzuwehren gilt oder tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Straftaten drohen. Sofern sich kurzfristig Hinweise auf eine konkrete Gefahr oder tatsächliche Anhaltspunkte für bevorstehende Straftaten an einem bestimmten Ort ergeben, kann die Polizei darauf zügig reagieren.

Im Übrigen hat die Landesregierung bereits ausführlich im Achtzehnten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drs. 16/4752) unter Ziffer 11 über das Thema berichtet; auch der Neunzehnte Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden befasst sich unter Ziffer 16 mit der Fußball WM 2006.

5. Land

Zu 5.1 Hessischer Landtag

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

5.2 Justiz

Zu 5.2.1 Moderne Justiz, Datenschutz und richterliche Unabhängigkeit

Die Landesregierung stimmt mit dem Hessischen Datenschutzbeauftragten darin überein, dass die Gerichte seiner Kontrolle unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

Hinsichtlich der im Tätigkeitsbericht angesprochenen Problematik der Notwendigkeit von Sicherheits- und Datenschutzkonzepten am häuslichen Arbeitsplatz von Richterinnen und Richtern entwirft das Ministerium der Justiz derzeit mit der Gemeinsamen IT- Stelle der hessischen Justiz ein Datensicherheitskonzept, welches unter anderem eine Speicherung der dienstlichen Daten am häuslichen Richterarbeitsplatz lediglich auf USB-Stick mit Verschlüsselungssystem und nicht auf der Festplatte oder anderen Medien vorsieht. Der Entwurf des Konzepts soll noch vor der Sommerpause fertig gestellt und dann mit dem Hessischen Datenschutzbeauftragten abgestimmt werden.

Zu 5.2.2 Verwechslungsgefahr bei Insolvenzbekanntmachungen im Internet

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Ergänzend ist anzumerken, dass begleitend zu der im Tätigkeitsbericht erwähnten Empfehlung des Hessischen Ministeriums der Justiz an die Insolvenzgerichte die Angelegenheit auch bundesweit in den entsprechenden Fachgremien (Entwicklerkreise) diskutiert und in das Gesetzgebungsverfahren eingebracht worden ist. Im Rahmen der Neufassung der Insolvenzordnung werden nunmehr künftig zur besseren Unterscheidung bereits im Eröffnungsbeschluss zusätzlich die Bezeichnungen "Geburtsdatum", "Geburtsort", "Handelsregisterbezeichnung" und "Registergericht"

aufgenommen. Eine Neufassung der Insolvenzordnung mit den beschriebenen Änderungen wird noch für 2006 erwartet. Im Anschluss daran wird eine programmtechnische Änderung der Insolvenzsoftware in Erwägung zu ziehen sein. Hierbei erscheint ein bundesweit abgestimmtes Vorgehen sinnvoll, damit eine einheitliche Veröffentlichungspraxis gewährleistet ist.

5.3 Polizei und Strafverfolgung

Zu 5.3.1 Erfahrungen mit der Videoüberwachung, insbesondere in Frankfurt am Main

Die Landesregierung bewertet die Trends der Videoüberwachung in Hessen (Ziff. 5.3.1.1) ebenso wie der Hessische Datenschutzbeauftragte. Hinsichtlich der Ausführungen zu Videoüberwachungsmaßnahmen in Frankfurt am Main (Ziff. 5.3.1.2) ist allerdings Folgendes zu ergänzen:

Zutreffend ist, dass der Erfassungsbereich der Kameras an der Konstablerwache über die Konstablerwache hinaus geht. Die Thematik ist zwischen Vertretern des Polizeipräsidiums Frankfurt am Main und des Hessischen Datenschutzbeauftragten in einer Besprechung im Februar 2006 erörtert worden. Man ist dabei übereingekommen, dass an den Kameras Sichtblenden angebracht werden, die den Erfassungsbereich einschränken.

Die Beschilderung der Anlage wurde noch vor der Fußball-Weltmeisterschaft optimiert. Die Aufstellungsörtlichkeiten der zusätzlichen Schilder waren zuvor einvernehmlich mit dem Hessischen Datenschutzbeauftragten festgelegt worden.

Die vom Hessischen Datenschutzbeauftragten geforderte Dienstanweisung über die Durchführung von Videoüberwachungsmaßnahmen im Bereich der Konstablerwache und des Hauptbahnhofs wurde bereits erlassen. Sie ist seiner Behörde im Januar 2006 zugeleitet worden. Unter Nr. 5.1 der Dienstanweisung ist der Zugriff auf das Überwachungssystem mittels Passwortvergabe geregelt. Nach Nr. 5.8 der Dienstanweisung hat der Dienststellenleiter D 101 oder ein von diesem Beauftragter die Einhaltung der Dienstanweisung zu überwachen. Derzeit wird die Dienstanweisung im Hinblick auf das Besprechungsergebnis vom Februar 2006 weiter verbessert.

Zu 5.3.2 Gelöscht und doch nicht gelöscht - Prüfung von Polizeidatenbeständen

Der Hessische Datenschutzbeauftragte hat das Innenministerium mit Schreiben vom 21. Februar 2006 auf die von ihm festgestellten Mängel hingewiesen. Ihm wurde daraufhin zugesagt, dass den Mängeln mit größtem Nachdruck und höchster Priorität nachgegangen wird. Hierzu wurde ein Workshop mit dem Auftrag eingerichtet, fachliche Vorgaben an das Aussonderungsprüfverfahren festzulegen, damit den gesetzlichen Anforderungen Rechnung getragen wird.

Inzwischen hat ein mehrtägiger Workshop unter Leitung einer erfahrenen Mitarbeiterin des IPCC (INPOL-Land-Polas Competence Center) zusammen mit PTLV und HLKA stattgefunden, in dem die Anforderungen an das Aktenaussonderungsprüfverfahren nochmals zusammengefasst und verifiziert wurden. Das Ergebnis liegt vor und wird derzeit im IPCC hinsichtlich des aktuellen Umsetzungsstandes in der Technik und ggf. notwendiger Anpassungsbedarfe überprüft (Abgleich Anforderung und derzeitige technische Umsetzung).

Ergänzend hat sich Ende April/Anfang Mai 2006 auf Initiative des BKA eine Bund-Länder- Kommission mit den unterschiedlichen Laufzeiten von Aktenaussonderungsprüffristen in den Ländern und Ihren Wirkungen auf das Gesamtsystem INPOL befasst. Die Kommission hat hierzu einen Vorschlag erarbeitet, der noch in den Gremien abgestimmt werden muss. Das Ergebnis und ggf. daraus resultierende Maßnahmen sollen danach ebenfalls in die Abschlussbewertung einfließen.

Zu 5.3.3 Mangelndes Auskunftsverhalten der Staatsanwaltschaft bei dem Landgericht Frankfurt

Nach Auffassung der Landesregierung handelt es sich bei dem im Tätigkeitsbericht aufgeführten, zur Beanstandung nach § 27 HDSG führenden Vorgang der Staatsanwaltschaft Frankfurt um einen außergewöhnlichen Einzelfall, der weder generell auf ein mangelndes Auskunftsverhalten der hessischen Staatsanwaltschaften noch darauf schließen lässt, letzteren sei der

Umfang des Auskunftsrechts nach §§ 491 Abs. 1 StPO, 19 BDSG nicht ausreichend bekannt.

Das Ministerium der Justiz hat auf die Beanstandung hin dafür Sorge getragen, dass dem Antragsteller eine weitergehende Auskunft erteilt worden ist. Überdies ist - entsprechend der dem Hessischen Datenschutzbeauftragten in der Stellungnahme nach § 27 HDSG erteilten Zusage - die Problematik des Umfangs des Auskunftsanspruchs nach §§ 491 Abs. 1 StPO, 19 BDSG auf der Grundlage der Rechtsauffassung des Hessischen Datenschutzbeauftragten im Rahmen der Herbsttagung der Leiterinnen und Leiter der hessischen Staatsanwaltschaften am 29. und 30. November 2005 in Hanau ausführlich erörtert worden. In diesem Zusammenhang wurden die Behördenleiter auch gebeten, eine enge und reibungslose Kommunikation mit dem Hessischen Datenschutzbeauftragten sicherzustellen. Diese Erörterung wird dazu beitragen, Einzelfälle wie den zur Beanstandung führenden künftig trotz der sehr hohen Arbeitsbelastung der Staatsanwaltschaften zu vermeiden.

5.3.4 Mangelnder Informationsaustausch zwischen Polizei und Justiz

Zu 5.3.4.1 Einzelfälle

Die Darstellung der Einzelfälle im Tätigkeitsbericht ist zutreffend.

Nach Auffassung der Landesregierung entbehrt jedoch die Feststellung, die Polizei sei aus unterschiedlichen Gründen "sehr oft" über das Ergebnis der strafrechtlichen Verfolgung der von ihr festgestellten Ermittlungsergebnisse nicht informiert, einer statistischen Erhebung. Das Ministerium der Justiz hat hierzu den Generalstaatsanwalt und die betroffenen Staatsanwaltschaften um Berichte gebeten. Auf Grundlage der Berichte ist davon auszugehen, dass es sich bei den im Tätigkeitsbericht aufgeführten Vorgängen um Einzelfälle handelt, die nicht darauf schließen lassen, die Polizei werde von den hessischen Staatsanwaltschaften entgegen § 482 Abs. 2 StPO häufig oder gar "sehr oft" nicht über den Ausgang des Verfahrens unterrichtet. Bestätigt wird dies durch den Umstand, dass ein Teil der im Tätigkeitsbericht genannten Verfahren bereits mehrere Jahre zurückliegen; im vierten Fall sogar so lange, dass die Akte nach Ablauf der Aufbewahrungsfrist vernichtet worden ist.

Die hessischen Staatsanwaltschaften sind sich ihrer Informationspflicht nach § 482 StPO in vollem Umfang bewusst. Die Thematik ist zuletzt auf der Arbeitsbesprechung der Leiterinnen und Leiter der hessischen Staatsanwaltschaften am 17./18. Juni 2003 in Grünberg erörtert worden. Hierbei bestand Einigkeit darüber, dass den Polizeibehörden ausreichende Grundlagen für die von ihnen zu treffenden Entscheidungen über Löschungen im Register zur Verfügung zu stellen sind.

Überdies ist durch die ausdrückliche Erwähnung des Erfordernisses der Benachrichtigung der Polizei im landeseinheitlichen Vordruck der Staatsanwaltschaften (dort Ziffer 3) dafür Sorge getragen, dass der Benachrichtigungspflicht in der Praxis entsprochen wird.

Zu 5.3.4.2 Lösungsansatz und Fazit

Obwohl die beschriebenen Sachverhalte Einzelfälle darstellen, ist die derzeitige Verfahrensweise auch nach Auffassung der Landesregierung verbesserungsfähig. Es ist deswegen vorgesehen, eine automatisierte Anlieferung der Verfahrensausgänge in das System POLAS zu ermöglichen. Voraussetzung dafür ist die Umstellung der jetzigen TXT-Schnittstelle zum Justizverfahren MESTA auf die künftige Schnittstelle X-Justiz. Entsprechende Abstimmungen zwischen Polizei und Justiz haben bereits stattgefunden. Nach derzeitiger Planung soll noch in diesem Jahr ein Konzept erstellt werden, das dann im Jahre 2007 umgesetzt werden könnte.

5.4 Verfassungsschutz

Zu 5.4.1 Novellierung des Hessischen Verfassungsschutzgesetzes

Der Hessische Datenschutzbeauftragte berichtet zutreffend über mit der zuständigen Fachabteilung des Innenministeriums geführte Vorgespräche zu Überlegungen hinsichtlich einer Anpassung des in Hessen geltenden einfachen Rechts an inzwischen eingetretene Änderungen des Bundesrechts sowie an die neuere Rechtsprechung des Bundesverfassungsgerichts. Die Überlegungen innerhalb der Landesregierung zu den angesprochenen Fragen sind noch nicht abgeschlossen. Da die Rechtsprechung des Bundesverfassungsgerichts auch vom Bund umgesetzt werden muss, erscheint es im Interesse

einer möglichst übereinstimmenden Regelung im Bund und in den Ländern sinnvoll, zunächst die Regelungsentwürfe des Bundes zu kennen, um sie in die hessischen Überlegungen einbeziehen zu können.

Vorab kann mitgeteilt werden, dass das erwähnte Urteil des Sächsischen Verfassungsgerichtshofs nach Ansicht der Landesregierung auf Besonderheiten der Sächsischen Landesverfassung und der historischen Tradition in Sachsen beruht, für die es im Verfassungsrecht Hessens keine Entsprechung gibt.

Personenbezogene Daten, die nach § 6 Abs. 6 LfVG zu löschen sind, können, soweit sie sich auch in Sachakten befinden, wegen der Löschung der Daten zu der Person in den nachrichtendienstlichen Informationssystemen im allgemeinen nicht mehr aufgefunden werden. Ihre Löschung ("Schwärzen") in den Sachakten würde das Verständnis dieser Akten erschweren und einen unverhältnismäßigen Arbeitsaufwand erfordern. Jedoch besteht Übereinstimmung mit dem Hessischen Datenschutzbeauftragten, dass bezüglich solcher in Sachakten noch aufgefunden personenbezogener Daten grundsätzlich ein absolutes Verwertungsverbot besteht. Ob insoweit noch eine klarstellende gesetzliche Regelung erforderlich erscheint, wird im Zuge des ausstehenden Gesetzgebungsverfahrens - unter Beteiligung des Hessischen Datenschutzbeauftragten - erneut geprüft werden.

Zu 5.4.2 Gemeinsames Informations- und Analysezentrum für die Polizei und das Landesamt für Verfassungsschutz

Die Angaben zum Gemeinsamen Informations- und Analysezentrum für die Polizei und das Landesamt für Verfassungsschutz sind zutreffend. Die im Tätigkeitsbericht erwähnte Dienstanweisung ist in Kraft gesetzt.

Zu 5.5 Verkehrswesen

Zu 5.5.1 Inhalt von Führerscheinakten - Speicherung im örtlichen Fahrerlaubnisregister

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragen zu, dass nur die zur Bearbeitung des Antrags erforderlichen Daten aus dem örtlichen Fahrerlaubnisregister übermittelt werden dürfen.

Im Rahmen einer Dienstbesprechung "Fahrerlaubniswesen" sind die Regierungspräsidien durch das Ministerium für Wirtschaft, Verkehr und Landesentwicklung auf die Problematik hingewiesen worden. Die Regierungspräsidien haben zeitnah die Fahrerlaubnisbehörden informiert, die zwischenzeitlich entsprechend verfahren.

Zu 5.5.2 Nutzung von Bankverbindungsdaten aus der Kfz-Zulassung

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass Bankverbindungsdaten, die eine Zulassungsstelle anlässlich der Zulassung eines Fahrzeuges zur Sicherung der Kraftfahrzeugsteuer erhebt, nicht zur Vollstreckung anderer Forderungen als in Kraftfahrzeugsteuersachen an die Kreiskassen übermittelt werden dürfen.
Die Rechtslage wurde vom Ministerium für Wirtschaft, Verkehr und Landesentwicklung mit Erlass an die Zulassungsbehörden vom 21. Juni 2005 klargestellt.

5.6 Schulverwaltung

Zu 5.6.1 Neuerungen im Schulgesetz

Die Landesregierung stimmt den Ausführungen im Tätigkeitsbericht zur Evaluierung in der Schule (Ziff. 5.6.1.1) und zu Bild- und Tonaufnahmen des Unterrichts (Ziff. 5.6.1.2.) zu, dass es abzuwarten und zu beobachten gilt, ob die im Hessischen Schulgesetz zu dem Bereich des Datenschutzes getroffenen Regelungen den Anforderungen in der Praxis genügen.

Zu 5.6.1.3 Nutzung privater IT-Geräte für Schulzwecke

Die Landesregierung sieht in der Frage der Nutzung privater lT-Geräte für schulische Zwecke innerhalb und außerhalb der Schulgebäude ebenso wie der Hessische Datenschutzbeauftragte ein nicht zu unterschätzendes Gefahrenpotential für Schulverwaltungsdaten. Die in Vorbereitung befindliche Neufassung der Verordnung über den Datenschutz in der Schule wird hierzu klare Regelungen treffen.

Zu 5.6.2 Folgerungen der IT-Sicherheitsleitlinie für die Schulen

Der vom Hessischen Datenschutzbeauftragten geschilderten mangelnden Kenntnis der IT-Sicherheitsrichtlinie der Landesregierung in den Schulen

wird das Kultusministerium durch eine zusätzliche Veröffentlichung der Richtlinie im Amtsblatt und durch einen Hinweis in den zu der Verordnung über den Datenschutz in Schulen geplanten Handreichungen begegnen. Die Bestellung von IT-Sicherheitsbeauftragten ist nicht in allen Schulen problemlos möglich. Insbesondere an kleineren Schulen ist es oft schwierig Personen zu finden, welche die erforderliche Sachkenntnis besitzen oder bereit sind, sich diese Sachkenntnis anzueignen.

Die Handreichungen zu der Verordnung über den Datenschutz in Schulen werden auch die geplanten Musterkonzepte zur Datensicherheit enthalten. Es wird erwartet, dass diese Muster auch diejenigen Schulen, welche ein IT-Sicherheitskonzept noch nicht erstellt haben, in die Lage versetzen werden, dieser in der IT-Sicherheitsleitlinie des Landes vorgesehenen Verpflichtung nachzukommen.

Da die Datenverarbeitungssysteme in den Schulen eindeutig in den Zuständigkeitsbereich der Schulträger gehören, hat die Richtlinie und ihre Veröffentlichung im Amtsblatt des Kultusministeriums für die Schulleitungen lediglich informatorischen Charakter. Für die Schulen gelten aber unmittelbar die Vorgaben des HDSG und die Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik.

5.7 Bibliotheken

Zu 5.7.1 Speicherung von Lesernamen bei Bibliotheken

Die Landesregierung teil die Auffassung des Hessischen Datenschutzbeauftragten.

5.8 Gesundheitswesen

Zu 5.8.1 Elektronische Speicherung und Langzeitarchivierung von Krankenakten im Krankenhaus

Wie im Tätigkeitsbericht zutreffend ausführt, sind die Krankenhäuser bzw. Ärzte rechtlich verpflichtet, die wesentlichen Abläufe einer Behandlung in der Krankenakte zu do-kumentieren. Da viele Krankenhäuser beabsichtigen, in Zukunft nicht nur ältere, sondern auch aktuelle Krankenakten zu digitalisieren, haben sie den Hessischen Datenschutzbeauftragten um Beratung bei der Entwicklung entsprechender Konzepte für die Führung und Archivierung der Krankenakten gebeten. Die Landesregierung war in die betreffenden Kontakte der Krankenhäuser mit dem Hessischen Datenschutzbeauftragten und auch in die von zahlreichen technischen Einzelheiten geprägten Recherchen nicht eingebunden. Eine weitergehende Stellungnahme ist der Landesregierung daher nicht möglich.

Zu 5.8.2 Aktuelle Entwicklung des Neugeborenen-Screenings

Die Anwendbarkeit der im Tätigkeitsbericht zitierten Kinder-Richtlinie des Gemeinsamen Bundesausschusses der Ärzte und Krankenkassen vom 21. Dezember 2004 auf in Krankenhäusern geborene Kinder ist umstritten. Die Kinderrichtlinie regelt nämlich lediglich die Voraussetzungen für die Kostenübernahme einer Leistung durch die gesetzliche Krankenversicherung.

Da in Hessen ca. 98 % aller Kinder in Krankenhäusern geboren werden, wurde für das Land ein Regelwerk geschaffen, das mit dem Datenschutzbeauftragten, dem Screening-Zentrum Hessen, der Landesärztekammer Hessen und der Kassenärztlichen Vereinigung Hessen einvernehmlich erarbeitet wurde. Darin ist das gesamte Verfahren geregelt.
Eine gesetzliche Regelung wird bisher nicht für notwendig erachtet, da das Verfahren nachvollziehbar dargestellt wird, freiwillig ist und das Einverständnis der Eltern eingeholt und dokumentiert wird. Die Einzelheiten sind in einer Elterninformation dargestellt, die allen Eltern ausgehändigt wird.

Das Regelwerk wurde inzwischen für den vorhandenen Probenstand umgesetzt. Lediglich die Pseudonymisierung ist aus verfahrenstechnischen Gründen noch nicht umgesetzt.

Die Restblutproben bis zum Jahr 1994 sind inzwischen ordnungsgemäß vernichtet. Für die Jahrgänge 1995 und 1996 sind Probeneingang und Stammdaten nicht in einem EDV-System erfasst. Auskunft zu Untersuchungen aus diesem Zeitraum, wozu eine Verpflichtung über zehn Jahre besteht, sind daher nur mit Hilfe der Testkarten möglich. Gemäß diesen Vorgaben wer-

den die Karten aus dem Jahr 1995 im Jahr 2006 vernichtet, die Karten aus dem Jahr 1996 können dann im Jahr 2007 vernichtet werden.

Ab dem Jahrgang 1997 wurde mit der nachträglichen Pseudonymisierung begonnen, was sich als äußerst aufwendig herausgestellt hat. Es wird daher angestrebt, alle weiteren Karten lediglich zu anonymisieren, um allgemeine Forschungsaufgaben zu ermöglichen.

Ab dem Jahrgang 2002 (Uniklinik Gießen) wurden die Karten pseudonymisiert. Allerdings konnte der angestrebte Vertrag (Aufbewahrung der Namensdaten getrennt von den Restblutproben) mit dem Datentreuhänder (Landesärztekammer Hessen) noch nicht abgeschlossen werden, solange die Umstrukturierung der Hochschule bzw. Universitätskliniken Gießen nicht abgeschlossen war. Mit dem baldigen Abschluss eines Vertrags ist zu rechnen.

Zu 5.8.3 Rahmenbedingungen für den Aufbau von Biobanken
Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten mit Interesse zur Kenntnis genommen.

Zu 5.8.4 Unzulässige Verarbeitung von Versichertendaten in Vietnam
Aufgrund der Kritik des Hessischen Datenschutzbeauftragten im Tätigkeitsbericht wurde die AOK Hessen durch das Sozialministerium um eine Stellungnahme gebeten, deren Inhalt nachfolgend wiedergegeben wird.

"Die Datenstelle Systemform unter der Leitung der Fa. GHP war in den dringenden Verdacht geraten, sensible Sozialdaten zur Verarbeitung von Deutschland unzulässigerweise nach Vietnam transferiert zu haben, ohne ein Einverständnis der involvierten Krankenkassen einzuholen und ohne diese Daten geeignet datenschutzkonform zu verschlüsseln. Die Staatsanwaltschaft Bamberg führt derzeit immer noch Ermittlungen durch. Der Verdacht eines Verstoßes gegen rechtliche Bestimmungen des Datenschutzes gegen die Fa. Systemform ist im Rahmen der Ermittlungen noch nicht ausgeräumt worden.

Sofort nach Bekannt werden eines ersten Verdachts fanden mehrere Prüfungen durch den Datenschutzbeauftragten der ARGE-DMP in Abstimmung mit Mitarbeiterinnen und Mitarbeitern des Hessischen Datenschutzbeauftragten statt. Grundlage für nachfolgende Aktivitäten - soweit es die Zuständigkeit der AOK Hessen betraf - waren die Beschlüsse einer Sitzung des Vorstandes, welcher bereits am 31.01.2005 einen umfassenden Zeit-Maßnahmenplan zur Aufklärung der Vorwürfe verabschiedet hatte.

Aufgrund der ersten Erkenntnisse hat die AOK Hessen als Kopfstelle DMP Diabetes mellitus II und Koronare-Herzerkrankung zusammen mit den Arbeitsgemeinschaften der DMPs Diabetes mellitus II, Koronare-Herzerkrankung und Brustkrebs der Datenstelle Systemform verbindliche und verschärfte datenschutzrechtliche Auflagen gemacht. Diese Auflagen werden seither durch den Datenschutzbeauftragten der AOK Hessen (zuständig für die AOK Hessen und die ARGE-DMP) regelmäßig gemeinsam mit dem Datenschutzbeauftragten der AOK Sachsen und ebenfalls zuständig für die ARGE-DMP in Sachsen überprüft.

Eine Auflage ist zum Beispiel die Teilnahme und Mitwirkung an einem externen TÜV-Audit zu den technischen und organisatorischen Maßnahmen nach § 78 SGB X gewesen, um den Vorgang zum Abschluss zu bringen. Nach den bisherigen Prüfergebnissen der beteiligten Datenschutzbeauftragten und der unverzüglichen Intervention gegenüber dem Vertragspartner ist aktuell von einer datenschutzkonformen Datenverarbeitung auszugehen.

Von Seiten der involvierten Krankenkassen wurden die Vorwürfe von Beginn an sehr ernst genommen und alles in deren rechtlich möglichen Rahmen getan, um die Vorwürfe aufzuklären und der Datenstelle Bamberg u.a. über die Einschaltung eines Fachanwaltes stringente und für die weitere Zusammenarbeit nachhaltige Auflagen für Datenschutz und Datentransfer zu machen. Im Übrigen wurde der verantwortliche Geschäftsführer der Datenstelle seinerzeit fristlos entlassen. Ferner erfolgte eine rechtliche und organisatorische Trennung der Fa. Systemform von der Fa. GHP unter anderer Leitung und Verantwortlichkeiten."

Im Rahmen der Rechtsaufsicht wird die AOK Hessen aufgefordert werden, dem Sozialministerium regelmäßig über die Gespräche mit dem Hessischen Datenschutzbeauftragten zu berichten.

Zu 5.8.5 Schuleingangsuntersuchungen - Der Informationsbedarf der Gesundheitsämter kommt einem Wildwuchs gleich

Der nun von den Gesundheitsämtern verwendete Anamnesebogen zur Schuleingangsuntersuchung enthält im wesentlichen die mit dem Hessischen Datenschutzbeauftragten abgestimmten Inhalte. Die Fragen sind zur Beurteilung des Gesundheitszustands eines Kindes notwendig, um medizinische Diagnosen stellen zu können. Die vom Hessischen Datenschutzbeauftragten angeführten Beispiele sind - bis auf den Beruf des Vaters - notwendige medizinische Fragen. Fragen nach dem Sozialstatus/ Migrationshintergrund sind wichtig für die Auswertung der Daten. Die Auswertung ermöglicht eine gezielte Steuerung von Maßnahmen. Ein Beispiel ist die Feststellung von erhöhten Sprachentwicklungsdefiziten bei Kindern.
Weitere Fragen sollen gemeinsam mit dem Hessischen Datenschutzbeauftragten in einer Arbeitsgruppe mit den Schulärzten erörtert werden.

Zu 5.8.6. Neue Datenverarbeitungsprojekte des Medizinischen Dienstes der Krankenversicherung Hessen

Der MDK in Hessen erklärte in seiner Stellungnahme gegenüber dem Sozialministerium, dass wegen der datenschutzrechtlichen Anforderungen verschiedener neuer Datenverarbeitungsprojekte ständiger Kontakt mit dem Hessischen Datenschutzbeauftragten besteht.

Zu 5.8.6.1 Einsatz von Laptops durch die Gutachter des MDK

Der MDK in Hessen hat die vom Hessischen Datenschutzbeauftragten empfohlenen Maßnahmen zur Problematik "Diebstahlsrisiko" umgesetzt. Die Laptops sind jetzt nicht nur durch Kennwörter und das Programm "Safeguard easy" gesichert, sondern zusätzlich auch noch mechanisch durch so genannte "Kensington locks" gegen Diebstahl am Arbeitsplatz geschützt. Hierüber wird der MDK in Hessen den Hessischen Datenschutzbeauftragten noch abschließend informieren.

Zu 5.8.6.2 Übermittlung der Gutachten per E-Mail an den MDK

Hier ist darauf hinzuweisen, dass die Aussage im Tätigkeitsbericht, das Verfahren basiere technisch auf dem mit der AOK Hessen bereits seit Jahren praktizierten elektronischen Austausch von Pflegegutachten, so nicht zutreffend ist. Richtig ist, dass das Verfahren technisch dem Austausch von Notes-Ismed-Datenbanken vergleichbar ist, wie es seit Jahren zwischen den MDK-Beratungsstellen praktiziert wird.

Zu 5.8.6.3 Projekt "Sicherer E-Mail-Verkehr mit externen Gutachtern"

Das Projekt "Sicherer E-Mail-Verkehr mit externen Gutachtern" ist beim MDK in Hessen im Jahre 2005 initiiert worden. Unter Berücksichtigung der datenschutzrechtlichen Problematiken, wie sie der Hessische Datenschutzbeauftragte anspricht, wurde die Testphase beim MDK in Hessen eingeleitet, die jedoch noch nicht abgeschlossen ist. Der MDK in Hessen wird dem Hessischen Datenschutzbeauftragten nach Abschluss der Testphase die Ergebnisse zur Abstimmung vorlegen.

Zu 5.8.6.4 Einsatz des Programms KQP II

Die datenschutzrechtlichen Probleme, die möglicherweise bereits bei dem Einsatz des Programms KQP I bestanden, wurden vom MDK Hessen mit dem Hessischen Datenschutzbeauftragten im Mai 2005 in einem gemeinsamen Termin erörtert.

Aufgrund der datenschutzrechtlich relevanten Belange beim Einsatz des Programms KQP II wurde vorab eine Einigungsstelle einberufen, deren Ziel die Klärung bzw. Lösung der datenschutzrechtlichen Probleme war. Der Einigungsstellenspruch wird den datenschutzrechtlichen Belangen gerecht. Wegen technischer Umsetzungsprobleme konnte das Verfahren KQP II nicht zum geplanten Termin 1. Januar 2006 eingeführt werden. Bei absichtsgemäßem Verlauf wird KQP II bei Erscheinen dieser Stellungnahme bereits beim MDK in Hessen angewendet. Über den aktuellen Verfahrensstand wird der MDK in Hessen den Hessischen Datenschutzbeauftragten umfassend informieren.

Zu 5.8.7 Datenschutzrechtliche Probleme der Auftragsdatenverarbeitung für die Erfassung von ärztlichen Gutachten des Medizinischen Dienstes der Krankenversicherung Hessen

Das Verfahren befindet sich noch in der Testphase. Der MDK in Hessen arbeitet gegenwärtig an einer den Anforderungen des Datenschutzes und der Praxis gerechten Lösung.

Zu 5.8.7.1 Das Verfahren

Grundsätzlich ist die vom Hessischen Datenschutzbeauftragen dargestellte Verfahrensweise richtig wiedergegeben. Allerdings ist fest zu halten, dass sich das Projekt "Schreibdienstleistung", das die Auftragsvergabe zwischen dem MDK in Hessen und dem MDK in Sachsen-Anhalt beinhaltet, noch in der Testphase befindet.

Zu 5.8.7.2 Vertragliche Aspekte der Auftragsdatenverarbeitung und Rechtsverhältnisse der Auftragnehmer untereinander

Die vom Hessischen Datenschutzbeauftragten aufgeführten Kritikpunkte werden bzw. sind zum Teil bereits an den MDK Sachsen-Anhalt weitergeleitet worden. Hier wird nach Möglichkeiten gesucht, um den vom Hessischen Datenschutzbeauftragten gestellten Anforderungen gerecht zu werden.

Zu 5.8.7.3 Vertraglich vorgesehene Pseudonymisierung findet nicht statt

Zwischen dem MDK in Hessen und dem MDK in Sachsen-Anhalt wurde ein neuer Vertrag vereinbart. Inhalt des neuen Mustervertrags ist nunmehr, dass auf eine Pseudonymisierung der Gutachten verzichtet wird, da nur so eine praktikable Handhabung im Massenbetrieb gewährleistet werden kann. Dem Hessischen Datenschutzbeauftragten ist der entsprechend geänderte Mustervertrag (Dienstleistungsvertrag/Datenschutzvertrag) im Februar 2006 zur Kenntnis gegeben worden.

Zu 5.8.7.4 Bewertung des Verfahrens und datenschutzrechtliche Defizite

Seitens des MDK in Hessen sind bereits die ersten Schritte zur Beseitigung der datenschutzrechtlichen Defizite in der laufenden Testphase eingeleitet worden.

Zu 5.8.7.5 Konsequenzen

Die vom Hessischen Datenschutzbeauftragten geforderten Konsequenzen sind bereits gezogen worden bzw. dies wird noch geschehen. Über die noch offenen, sich zum Teil noch in der Testphase befindlichen Punkte wird der MDK in Hessen den Hessischen Datenschutzbeauftragten umfassend informieren.

Insbesondere die angesprochene Unerlässlichkeit der klaren Zuordnung der Verantwortlichkeiten im Innenverhältnis MDK in Hessen / MDK in Sachsen-Anhalt / MedFlex wird einer Lösung zugeführt werden, die auch den Ansprüchen des Hessischen Datenschutzbeauftragten genügen soll.

Im Rahmen der Rechtsaufsicht wird der Medizinische Dienst der Krankenversicherung in Hessen aufgefordert werden, dem Sozialministerium regelmäßig über die Gespräche mit dem Hessischen Datenschutzbeauftragten zu berichten.

Zu 5.9 Sozialwesen

Zu 5.9.1 Hartz IV - Vorlage von Kontoauszügen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten in vollem Umfang zu. Das gilt insbesondere für die Auffassung, wonach das Vorgehen der zuständigen Leistungsträger nach dem SGB II, von den Antragstellern Kontoauszüge der letzten drei bis sechs Monate anzufordern, als bisher auch schon im Sozialhilferecht übliche Standardmaßnahme bei der Entscheidung über die Gewährung von Leistungen nach dem SGB II zulässig ist. In Übereinstimmung mit dem Hessischen Datenschutzbeauftragten ist daher die anders lautende Entscheidung des Hessischen Landessozialgerichts abzulehnen, wonach die Beiziehung von Kontoauszügen der letzten Monate rechtswidrig sei.

Im Übrigen ist dem Hessische Datenschutzbeauftragten auch darin zuzustimmen, dass Kopien der Kontoauszüge zu den Akten genommen werden dürfen, dann aber nach der Überprüfung der Kontoauszüge die nicht relevanten Angaben geschwärzt werden müssen.

Das Sozialministerium wird die Leistungsträger nach dem SGB II, insbesondere angesichts der zitierten Entscheidung des Hessischen Landessozialgerichts, auf die abweichende Auffassung des Hessischen Datenschutzbeauftragten hinweisen.

Zu 5.9.2 Unzulässiger Inhalt von Wohngeld-Antragsformularen

Aus der Darstellung im Tätigkeitsbericht ist nicht zu entnehmen, ob der beanstandete Vordruck, bei dem es sich nicht um ein amtlich durch das Land vorgeschriebenes Formular handelt, regelmäßig zusammen mit den Antragsvordrucken ausgehändigt wurde. Eine solche von den Umständen des Einzelfalls unabhängige Verfahrensweise würde auch nach Auffassung der Landesregierung nicht den maßgeblichen Regelungen des Wohngeldgesetzes und des SGB X entsprechen.

Ob und ggf. in welcher Höhe die Sozialleistung Wohngeld gewährt werden kann, hängt u.a. vom wohngeldrechtlich relevanten Einkommen ab. Nach Nr. 11.0 der Allgemeinen Verwaltungsvorschrift zur Durchführung des Wohngeldgesetzes, die für die Wohngeldstelle bindend ist, sind die Angaben des Antragstellers besonders sorgfältig auf Glaubhaftigkeit und Vollständigkeit zu überprüfen, wenn sich bei der Ermittlung des Jahreseinkommens unter dem sozialhilferechtlichen Bedarf liegende Einnahmen ergeben. Zur Einschätzung der Plausibilität kann es in solchen Fällen erforderlich sein, den Sachverhalt, den die Wohngeldstelle nach § 20 SGB X nach Art und Umfang von Amts wegen ermittelt, auch hinsichtlich des Aufwands für den Lebensunterhalt und seiner Deckung zu beleuchten. Dazu diente offenbar der beanstandete Vordruck.

Es ist beabsichtigt, die Wohngeldstellen nochmals auf die einschlägige Rechtslage hinzuweisen.

Zu 5.9.3 Datenschutzrechtliche Rahmenbedingungen im Bereich der Jugendgerichtshilfe

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zur Rechtslage nach den §38 Abs. 2 und §43 Abs. 1 und 2 JGG zu. Wie ausgeführt ist, hat sich der Datenschutz in diesem Aufgabenfeld verbessert, weil das Sozialdatenschutzrecht des SGB VIII nunmehr auch in diesem Bereich gilt.

Zu 5.10 Personalwesen

Zu 5.10.1 E-Beihilfe

Die Darstellung des Sachverhalts im Tätigkeitsbericht ist an einigen Stellen zu ergänzen.

Der Pilotbetrieb des Systems eBeihilfe beim Regierungspräsidium Kassel ist am 1. Januar 2005 nicht, wie unter Ziff. 5.10.1.2 im Tätigkeitsbericht angegeben, mit den Buchstabengruppen K und L, sondern zunächst mit der Buchstabengruppe T – Z umgesetzt worden.
Die Entwicklungsdatenbank ist mit Zustimmung des Hessischen Datenschutzbeauftragten Mitte Dezember 2005 in das Rechenzentrum Hünfeld verlegt worden.

Zu einer Inanspruchnahme des eBehilfe-Verfahrens durch Dritte, wie im Tätigkeitsbericht unter Ziff. 5.10.1.3 in Bezug auf die Beamtenversorgungskassen Kassel und Darmstadt sowie die Städte Frankfurt am Main und Darmstadt angegeben, ist es nicht gekommen. Das zunächst bekundete Interesse an einer Nutzung des Systems eBeihilfe besteht dort nicht mehr.
Im Übrigen stimmt die Landesregierung der Darstellung im Tätigkeitsbericht zu.

Zu 5.10.2 Datenschutzrechtliche Begleitung der Einführung der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung

Der Hessische Datenschutzbeauftragte schildert in seinem Bericht, dass er in der Einführungsphase und zu Beginn des Einsatzes der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung u. a. aufgrund der Komplexität des Systems eine Vielzahl datenschutzrechtlicher Fragestellungen und Probleme festgestellt hat. Im Hinblick darauf hat die Landesregierung den Hessischen Datenschutzbeauftragten von Anfang an beteiligt, um datenschutzrechtliche Fragen von Beginn an mit seiner Behörde zu erörtern.

Die festgestellten Probleme konnten inzwischen weitestgehend behoben werden.

Zu 5.10.2.1 Personaldaten im landesweiten Zugriff
Das zunächst bestehende Problem, dass bei bestimmten Konstellationen, zum Beispiel Versetzungen, ein landesweiter Zugriff auf Personaldaten bestand, konnte in Abstimmung mit dem Hessischen Datenschutzbeauftragten gelöst werden. Die erarbeitete Lösung ist bereits im Tätigkeitsbericht zutreffend beschrieben.

Zu 5.10.2.2 Nicht genutzte Berechtigungen (inaktive User)
Dem kritisierten Umstand, dass eine nicht unerhebliche Anzahl von Personen mit Zugangsberechtigungen für das SAP-System dieses zum Zeitpunkt der Überprüfung durch den Hessischen Datenschutzbeauftragten seit mehr als 90 Tagen nicht mehr genutzt hatten, ist abgeholfen worden.

Der Forderung des Hessischen Datenschutzbeauftragten, dass User, die eine andere Aufgabe übernehmen, versetzt werden oder ausscheiden, sofort als Zugangsberechtigte aus der Berechtigungsdatei gelöscht werden, wird dadurch Rechnung getragen, dass eine entsprechende Anweisung in das Zugriffsberechtigungsrahmenkonzept aufgenommen wird und bei der Beantragung einer neuen Berechtigung die Sperrung der alten erfolgt. Darüber hinaus wird ein Report zur dezentralen Identifikation inaktiver User zur Verfügung gestellt.

Zu 5.10.2.3 Standardsuchhilfe
Im Bereich des Veranstaltungsmanagements war es den Bearbeitern zunächst möglich, auf den gesamten Personaldatenbestand der Landesverwaltung zuzugreifen. Diese Problematik ist inzwischen weitgehend behoben worden.

Die Zugriffsberechtigten im Bereich Veranstaltungsmanagement haben nach dem Buchen einer Person auf eine Veranstaltung Zugriff auf die Anschrift und die organisatorische Zuordnung. Bei Teilnehmern aus den sicherheitsrelevanten Bereichen wird als Korrespondenzadresse nicht die private Anschrift, sondern die Anschrift der Dienststelle ausgegeben. Auf weitergehende Daten zur Person ist kein Zugriff möglich. Die Standardsuchhilfen sind in den Anwendermenüs für die Zugriffsberechtigten deaktiviert und durch eine Suchmaske ersetzt worden, durch die nur Datensätze einzelner, für konkrete Veranstaltungen angemeldeter Personen aufgerufen werden können. Allerdings wurde nach der Erstellung des Datenschutzberichts festgestellt, dass Zugriffsberechtigte über im Allgemeinen nicht bekannte Umwege die Standardsuchhilfen in anderen Transaktionen des Veranstaltungsmanagements theoretisch noch aufrufen könnten. Die mit dem Projekt befassten Mitarbeiter des Hessischen Datenschutzbeauftragten sind darüber informiert worden. Die Problematik wird derzeit analysiert und soll in Abstimmung mit dem Hessischen Datenschutzbeauftragten behoben werden.

Zu 5.10.2.4 Zugriff auf Personaldaten von Bediensteten nachgeordneter Behörden
Der Hessische Datenschutzbeauftragte hat die unterschiedliche Festlegung des Zugriffs auf Personaldaten von Bediensteten nachgeordneter Behörden in manchen Ressorts kritisiert, zum Beispiel die Zugriffsberechtigung von Mitarbeitern eines Ministeriums auf Daten aller Bediensteten des nachgeordneten Bereichs. Um dauerhaft eine datenschutzgerechte Zugriffssteuerung zu gewährleisten, hat der Hessische Datenschutzbeauftragte gefordert, ein entsprechendes Merkmal im SAP-System zu hinterlegen.

Der Kabinettsausschuss "Verwaltungsreform und Verwaltungsinformatik" hat am 14. September 2005 als ersten Schritt die unverzügliche Umsetzung einer organisatorisch-technischen Lösung beschlossen. Dem ist durch die Entwicklung des sog. "Merkmals Z" (Zentrale Zugriffe) Rechnung getragen worden. Es erlaubt eine zusätzliche Differenzierung, um innerhalb eines Ressorts die Zugriffsmöglichkeiten auf Personaldaten in SAP R/3 HR zwischen verschiedenen Ebenen (zum Beispiel Ministerium und nachgeordnete Dienststelle) zu steuern. Das "Merkmal Z" ist entwickelt und befindet sich zurzeit in der Testphase. Die technische Möglichkeit zum Einsatz des Merkmals wird ab Juni 2006 allen Ressorts zur Verfügung stehen.

Bei der Vergabe des "Merkmals Z" haben die Ressorts gewisse Vorgaben zu beachten. Diese Rahmenbedingungen für das "Merkmal Z" wurden den

Ressorts bereits mitgeteilt. Die festgelegten Vorgaben wurden unmittelbar zur Produktivsetzung Anfang Juni 2006 wirksam. Ab diesem Zeitpunkt liegt es in der Verantwortung der jeweiligen Ressorts, über den Einsatz des "Merkmals Z" zu entscheiden.

Weiterhin soll zur Umsetzung des Beschlusses des Kabinettsausschusses "Verwaltungsreform und Veraltungsinformatik" vom 14. September 2005 eine Anpassung der Zuständigkeitsanordnungen im Personalwesen erfolgen. Eine standardisierte Zuständigkeitsanordnung für alle Ressort ist aufgrund der Unterschiede im Aufbau des nachgeordneten Bereichs sowie des Umfangs der delegierten Befugnisse jedoch nicht möglich. Das Ministerium des Innern und für Sport erarbeitet deshalb zurzeit eine Zuständigkeitsverordnung für den eigenen Ressortbereich. Diese soll um Regelungen zur Übertragung von Befugnissen, Daten der Beschäftigten im System zu bearbeiten, sowie zur Berechtigung, in SAP HR verarbeitete Personaldaten der Beschäftigten einzusehen und auszuwerten (lesende Berechtigung), ergänzt werden. Dem Kabinettausschuss soll vorgeschlagen werden, die Zuständigkeitsverordnung des Ministers des Innern und für Sport den anderen Ressorts als "Muster" für die Anpassung ihrer Zuständigkeitsanordnungen zur Verfügung zu stellen.

Zu 5.10.2.5 Fazit und Ausblick
Die meisten der in der Anfangsphase fast zwangsläufig auftretenden Probleme konnten inzwischen, wie sich bereits aus dem Tätigkeitsbericht ergibt, behoben werden. Es ist auch weiterhin das Interesse und das Bestreben der Landesregierung, in engem Zusammenwirken mit dem Hessischen Datenschutzbeauftragten die noch offenen bzw. eventuell noch auftretenden datenschutzrechtlichen Fragestellungen einer sachgerechten Lösung zuzuführen.

Zu 5.10.3 Bekanntgabe von Bediensteten, die Altersteilzeit beantragt haben, an den Personalrat
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 5.10.4 Datenübermittlung durch den Polizeiärztlichen Dienst an die Polizeiverwaltung
Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend. Anzumerken ist lediglich, dass sich die Nr. 2.5.1 der Polizeidienstverordnung 300, auf die der Bericht in Ziff. 5.10.4.3 Bezug nimmt, allein auf die Beurteilung der Polizeidiensttauglichkeit bezieht. Für die polizeiärztlichen Gutachten zur Bewertung der Polizeidienstfähigkeit ist die im Abschnitt 3 der Polizeidienstverordnung 300 ("Bestimmungen zur Beurteilung der Polizeidienstfähigkeit") befindliche Nr. 3.1.4 einschlägig.

Zu 5.11 Finanzwesen
5.11.1 Darf das Finanzamt Geschäftspost an die Privatanschrift des Einzelunternehmers versenden?
Die Darstellung im Tätigkeitsbericht entspricht den Gegebenheiten und war in dem obligatorischen Jahresgespräch zwischen dem Hessischen Datenschutzbeauftragten und dem Ministerium der Finanzen Gegenstand der Erörterung.

Es ist darauf hinzuweisen, dass die Zustellung der geschäftlichen Korrespondenz in der geschilderten Form im Einklang mit den geltenden bundeseinheitlichen Bekanntgabevorschriften der Abgabenordnung steht. Der Grund, dass alle steuerliche Korrespondenz an eine Adresse geht, liegt im Grundinformationsdienst, der Zustelladressen nicht nach Steuerarten getrennt speichern kann. Dies wird sich mit der Einführung des neuen Informationsdiensts "GINSTER" ändern.
Bis zur Einführung des neuen Informationsdiensts sind die Finanzämter angewiesen, in vergleichbaren Fällen die maschinelle Anschrift zu unterdrücken und persönliche und geschäftliche Steuerkorrespondenz personenbezogen zu adressieren.

6. Kommunen
6.1 Forderungsmanagement von Kommunen
Zu 6.1.1 Einbeziehung von Inkassobüros und Übertragung von Forderungen
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu. Der Verkauf von öffentlich-rechtlichen Forderungen an Inkas-

so-Unternehmen und die hierfür erforderliche Abtretung sind ohne eine entsprechende gesetzliche Regelung nicht zulässig. Sie würden gegen die im Hessischen Verwaltungsvollstreckungsgesetz festgelegte Verfahrens- und Zuständigkeitsordnung verstoßen.

Zu 6.1.2 Vereinbarung mit der SCHUFA

Die Landesregierung hat die Auffassung des Hessischen Datenschutzbeauftragten mit Interesse zur Kenntnis genommen. Sie wird vom Regierungspräsidium Darmstadt, als für die SCHUFA zuständige Aufsichtsbehörde, bei der Prüfungspraxis berücksichtigt werden.

Zu 6.2 Prüfung des Online-Abrufs von Privaten aus dem Liegenschaftskataster

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die Vorgaben des Landesamts für Bodenmanagement und Geoinformation nur unzureichend umgesetzt waren.

Informationen aus dem Liegenschaftskataster und der Landesvermessung sind seit geraumer Zeit flächendeckend in digitaler Form für jedermann verfügbar. Über ein internetbasiertes Shop-System und entsprechend automatisierte Abrufverfahren werden sie den Bürgerinnen und Bürgern, der Wirtschaft und der Verwaltung in zeitgemäßer Form angeboten. Die personenbezogenen Daten des Liegenschaftskatasters stehen jedoch unter besonderem datenschutzrechtlichen Vorbehalt und dürfen von einem dafür besonders zugelassenen Personenkreis nur unter Auflagen Online abgerufen werden. Deren Einhaltung sowie die Rechtmäßigkeit der einzelnen Datenabrufe werden vom Landesamt für Bodenmanagement und Geoinformation als zuständige Behörde stichprobenweise überprüft.

Nachdem bei Stichproben festgestellt worden war, dass die datenschutzrechtlichen Bestimmungen von den geprüften Personen nicht im erforderlich Maße eingehalten wurden, hat das Landesamt für Bodenmanagement und Geoinformation die Betroffenen nochmals über die ihnen obliegenden Verpflichtungen belehrt und konkrete Maßnahmen zur Abhilfe vereinbart. Im April 2006 wurde die Umsetzung dieser Maßnahmen überprüft. Über diese Einzelfälle hinaus wurden präventiv sämtliche bereits zum Direktabruf von personenbezogenen Daten des Liegenschaftsregisters zugelassenen Personen angeschrieben und nachdrücklich auf die Einhaltung der datenschutzrechtlichen Bestimmungen und die sich aus Verstößen ergebenden Konsequenzen aufmerksam gemacht. Neu zugelassene Abrufer von personenbezogenen Daten des Liegenschaftskatasters erhalten seit Anfang 2006 einen überarbeiteten Genehmigungsbescheid, in dem noch deutlicher als bislang auf die Einhaltung der mit der Genehmigung verbundenen Verpflichtungen und deren Überprüfung durch die Genehmigungsbehörde hingewiesen wird.

Das Landesamt für Bodenmanagement und Geoinformation wird die Einhaltung der datenschutzrechtlichen Bestimmungen auch weiterhin durch regelmäßige Stichproben bei den zugelassenen Abrufern überwachen.

Zu 6.3 Wahlstatistik

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

7. Sonstige Selbstverwaltungskörperschaften

7.1 Hochschulen

Zu 7.1.1 Datenschutzrechtliche Fragen bei der Privatisierung des Universitätsklinikums Gießen und Marburg

Bei der Erstellung des Datenraumes haben die von der Landesregierung Beauftragten in Ab-stimmung mit den örtlichen Datenschutzbeauftragten der Universitätskliniken in Gießen und Marburg frühzeitig die Festlegung getroffen, keine personenbezogenen Daten zugänglich zu machen, sondern Aufstellungen und Listen zu anonymisieren. Anlässlich der Begehung durch den Hessischen Datenschutzbeauftragten wurden in geringfügigem Umfang Unterlagen auf-gefunden, die nicht vollständig anonymisiert waren und bei denen die Erforderlichkeit, in die Daten Einsicht zu geben, nicht oder nicht eindeutig vorlag. Bei der Ausgestaltung der Daten-räume sind die behördlichen Datenschutzbeauftragten beteiligt worden; eine Beteiligung des Hessischen Datenschutzbeauftragten unterblieb zunächst, da die Beteiligten der Ansicht wa-ren, die Beteiligung der behördlichen Datenschutzbeauftragten entspreche den getroffenen Vereinbarungen. Nachdem im Rahmen der Kontrolle am 31. August deutlich wurde, dass eine

unmittelbare Beteiligung des Hessischen Datenschutzbeauftragten notwendig ist, wurde die-sem am 1. September die Möglichkeit zur Kontrolle des erweiterten Datenraums vor seiner Eröffnung eingeräumt.

Ein Anlass für die weitere Beteiligung des Hessischen Datenschutzbeauftragten wurde nicht gesehen, da Bietern nach Schließung des zweiten Datenraums keine Unterlagen mehr zugäng-lich gemacht wurden. Im Verfahren zur Änderung des Gesetzes für die hessischen Universi-tätskliniken wurde er beteiligt, insbesondere als sich im Gesetzgebungsverfahrens die Notwendigkeit der speziellen datenschutzrechtlichen Bestimmung des § 25a Abs. 6 UniKlinG ergab.
Das Schreiben des Hessischen Datenschutzbeauftragten vom 6. September 2005, in welchem die Vorkommnisse im Zusammenhang mit den Datenräumen aufgegriffen wurden, enthielt eine Aufforderung, künftig die Information des Hessischen Datenschutzbeauftragten sicherzu-stellen und die Verfahren datenschutzrechtskonform auszugestalten. Eine Aufforderung zur Stellungnahme war jedoch nicht enthalten.

Entgegen der Darstellung im Tätigkeitsbericht handelt es sich bei der Privatisierung des Uni-versitätsklinikums Gießen und Marburg nicht nur um eine Teilprivatisierung. Die Verantwor-tung für die Belange von Forschung und Lehre lag auch vor der Privatisierung bei den Fach-bereichen Medizin der beiden Universitäten und damit beim Land Hessen und nicht beim Universitätsklinikum. Ausweislich § 5 des Gesetzes über die hessischen Universitätskliniken ist Aufgabe eines Universitätsklinikum nicht Forschung und Lehre selbst, sondern deren Unter-stützung und im Übrigen maßgeblich die Krankenversorgung und andere Aufgaben des öf-fentlichen Gesundheitswesens. Dieses Aufgabenspektrum wurde vollständig auf den privaten Betreiber übertragen, wobei die Unterstützung der Universitäten und ihrer Medizinfachberei-che bei der Erfüllung der Aufgaben in Forschung und Lehre im Wege der Beleihung von der Universitätsklinikum GmbH als öffentliche Aufgabe wahrgenommen wird.

Die Zuständigkeit des Hessischen Datenschutzbeauftragten ergibt sich somit aus dem Umfang der Beleihung und im Übrigen aus seinem Prüfauftrag für privatrechtlich ge führte Kranken-häuser im Land Hessen. Soweit Aufgaben des öffentlichen Gesundheitswesens wahrgenom-men werden, erfolgt seine Beteiligung, zum Beispiel im Bereich des Neugeborenen-Sreenings.

Zu 7.1.2 Anwendung der IT-Sicherheitsrichtlinie des Landes auf die Hochschulen

Die Landesregierung hat den Bericht des Hessischen Danteschutzbeauftragten mit Interesse zur Kenntnis genommen.

Zu 7.2 Sparkassen

Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten mit Interesse zur Kenntnis genommen.

8. Entwicklungen und Empfehlungen im Bereich der Technik und Organisation

Zu 8.1 Sachstand zur Zentralisierung der IT

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass es in dem erwähnten Workshop weitgehend gelungen ist, für beide Seiten akzeptable Lösungswege zu finden.

Zu 8.1.1 Übergreifende Aspekte

Die Landesregierung hat die Gründe, die für eine zentrale IT sprechen, ausführlich in ihrer Stellungnahme zum 33. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Drs. 16/4751) dargelegt (dort zu Ziff. 8).

Zu 8.1.2 Verschlüsselung

Als Ergebnis des Workshops wurde ein Auftrag an das Fraunhofer Institut für Sichere Informationstechnologie (SIT) erteilt, Softwaresysteme zu finden, die eine verschlüsselte Speicherung auf einem Fileserver und im Dokumentenmanagementsystem für solche Daten gewährleisten, die aus datenschutzrechtlichen oder aus fachlichen Gründen besonders zu schützen sind. Wichtige Randbedingung dabei ist, dass ein Zugriff auf diese Daten für eine Gruppe Berechtigter möglich sein muss, deren Zusammensetzung sich ändern kann. Zwischenergebnisse des SIT liegen nunmehr vor. Danach sind einige Systeme auf dem Markt verfügbar, die die gestellten Voraussetzungen

für eine Speicherung auf einem Fileserver erfüllen. Dagegen wurden nur wenige Systeme gefunden, die eine verschlüsselte Speicherung im DMS-Umfeld ermöglichen. Die Systeme werden zurzeit geprüft. Der Hessische Datenschutzbeauftragte begleitet die Prüfung.

Zu 8.1.3 Signatur
Gesetzeskonforme Signatur
Wie im Workshop abgesprochen, sind Vorstöße in Richtung Hersteller mit dem Ziel unternommen worden, eine gesetzeskonforme Lösung bereitzustellen, die sowohl für die Anmeldung am Windows-Betriebssystem (Windows-Logon) als auch für die fortgeschrittene Signatur nutzbar ist. In einer Besprechung mit der Firma Microsoft (Hersteller des Betriebssystems) und der Firma Kobil (Hersteller von Signaturkartenlesern) wurden drei mögliche Lösungsansätze diskutiert und bewertet.

1. Eingabe der zum Windows-Logon erforderlichen PIN über einen externen Kartenleser mit Tastatur.
2. Anpassung oder Austausch der für die Anmeldung verantwortlichen Komponente "msgina.dll" in den Installationen der Landesverwaltung Hessen. Es würde eine hessenspezifische Variante des Windows-Betriebssystems erstellt.
3. Schutz der auf der Karte implementierten fortgeschrittenen Signatur durch eine eigene PIN.

Die Bewertung durch die Hersteller Microsoft und Kobil ergab folgende Aussagen:
Zu 1: Es ist nicht möglich, die PIN-Eingabe über eine externe Anmeldung zu erzwingen. Als Begründung gab Microsoft an, zu dem für die Anmeldung relevanten Zeitpunkt seien die Softwarekomponenten noch nicht geladen, die für eine PIN-Eingabe über den externen Kartenleser erforderlich sind.
Zu 2: Eine Anpassung oder gar ein Austausch der Komponente "msgina.dll" wird von Microsoft wegen der zu erwartenden Instabilität des Betriebsystems und der zu erwartenden Schwierigkeiten beim Update- und Patchmanagement (Beseitigung von Betriebssystemsfehlern) abgelehnt.
Auch die Firma Kobil rät von einer Anpassung bzw. von einem Austausch ab.
Zu 3: Die Datenstruktur der im Handel befindlichen Chipkarten lässt einen separaten Schutz der implementierten fortgeschrittenen Signaturen durch eine eigene PIN nicht zu.
Außerdem würde nach Angaben des Herstellers Kobil die Einführung einer weiteren PIN für diesen Zweck von den Anwendern abgelehnt werden, da sie sich eine weitere PIN zu merken hätten.

Zur Anpassung der rechtlichen Rahmenbedingungen ist eine Bundesratsinitiative geplant. Die dafür erforderlichen Entwürfe werden im Innenministerium zurzeit erarbeitet.

Signatur im Terminal-Server-Umfeld
Um eine gesetzeskonforme Signatur im Terminal-Server-Umfeld zu erreichen, ist geplant, eine zertifizierte Signatursoftware einzusetzen. Die gesetzeskonforme Anbringung und Überprüfung der Signaturen wird dann durch die Signatursoftware sichergestellt. Es wird geprüft, mit welchen Maßnahmen gewährleistet werden kann, dass die Signatursoftware im Betrieb nicht manipuliert wurde und damit die ordnungsgemäße Funktionsweise gewährleistet werden kann. Die Ausschreibung wurde durch die Stabsstelle eGovernment veranlasst, durch die HZD erarbeitet und ist veröffentlicht. Sie ist mit dem Hessischen Datenschutzbeauftragten abgestimmt.

Zu 8.1.4 Dokumentenmanagementsystem
Die Dienststellen definieren jeweils Dokumententypen, die komplett von der Verarbeitung im Dokumentenmanagementsystem (DMS) ausgenommen werden. Dies wird in der zur Vorabkontrolle gehörenden Negativliste festgelegt und dokumentiert.

Auf die Bearbeitung von Dokumenten, Akten, Vorgängen und Postmappen, die im Grundsatz unkritisch sind, z. B. Antrag auf Förderung, die im Einzelfall aber besonders schützenswerte Daten beinhalten, z. B. sehr sensible personenbezogene Daten des Antragstellers und seiner Familie, wird in den Anwenderschulungen eingegangen. Vertieft wird diese Fragestellung im

entsprechenden Modul des "E-Learning-Kurs DMS", das Hilfestellungen gibt.

Zu 8.1.5 Stand Ende des Jahres
Der Auftrag an das Fraunhofer Institut für Sichere Informationstechnologie (SIT) wurde erteilt (siehe oben zu Ziff. 8.1.2).

Zu 8.2 Sachstand zur Einführung eines Dokumentenmanagementsystems in der Hessischen Landesverwaltung
Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zur Einführung des Dokumentenmanagementsystems zu. In Bezug auf das im Tätigkeitsbericht beschriebene Rollen- und Berechtigungskonzept (Ziff. 8.2.4.2) ist zu ergänzen, dass die Anpassung des Musterberechtigungskonzepts an den Organisationsplan von den pilotierenden Dienststellen durchgeführt wird. Diese Berechtigungskonzepte und die darin enthaltenen organisatorischen Regelungen werden in den Schulungen behandelt.
Die Ausführungen zur Recherchefunktionalität (Ziff. 8.2.4.2) sind zutreffend. Die Überlegungen zu einer Erweiterung der Recherchefunktionalität sind noch nicht abgeschlossen.

Zu 8.3 Probleme der Passwortverwaltung in Rechenzentren
Wie im Bericht des Hessischen Datenschutzbeauftragten zutreffend dargestellt ist, entsteht das Problem bei der zentralen Administration der Benutzerkonten. Diese Zentralisierung hat in der Landesverwaltung Ende des Jahres 2005 begonnen und wird im Jahre 2006 fortgesetzt.
Das zuständige Projekt wird sich der Fragestellung annehmen. Dabei werden Prozesse, die andere zentral administrierte Organisationen, z.B. Banken, eingeführt haben, analysiert und auf dieser Basis wird eine sichere, aber auch in der Praxis handhabbare Lösung eingesetzt werden. Die Hinweise im E-Government-Handbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) werden dabei berücksichtigt.

Zu 8.4 Telearbeitsplätze in der Hessischen Landesverwaltung
Der Hessische Datenschutzbeauftragte hat auf der Grundlage des vorgegebenen Kriterien-Katalogs für die Nutzung von Telearbeitsplätzen (StAnz. 2003, S. 2748) deren korrekte Umsetzung geprüft.

Sofern Telearbeitsplätze über Laptops realisiert und diese Geräte zwischen dem heimischen Arbeitsplatz und der Dienststelle transportiert werden, verlangt der Hessische Datenschutzbeauftragte eine Festplattenverschlüsselung. Er empfiehlt darüber hinaus, die Mitarbeiterinnen und Mitarbeiter mit Telearbeitsplatz schriftlich darauf hinzuweisen, dass nicht mehr benötigte bzw. gelöschte Dateien nicht unbeabsichtigt im Papierkorb des Rechners zu speichern, sondern endgültig zu löschen sind.

Das Ministerium des Innern und für Sport wird den Empfehlungen des Hessischen Datenschutzbeauftragten entsprechen und über die IT-Sicherheitsbeauftragten der Ministerien und der nachgeordneten Behörden schriftliche Hinweise zur endgültigen Datenlöschung bei Telearbeitsplätzen sowie die Festplattenverschlüsselung von Laptops veranlassen.

Zu 8.5 Orientierungshilfe "Datenschutz in drahtlosen Netzen"
Die Landesregierung begrüßt die Ausführungen des Hessischen Datenschutzbeauftragten. Sofern die Möglichkeit der Nutzung eines Access Points von der Landesverwaltung angeboten wird, soll dies nur für dienstliche Zwecke möglich sein. Eine Vorschrift, die nur eine dienstliche Nutzung erlaubt, wird vorbereitet.

Zu 8.6 Voice over IP (VoIP) - weit mehr als Internet-Telefonie
Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Sie hält in diesem Zusammenhang nicht die Technik, über die kommuniziert wird, sondern das Gesamtkonzept für die Gestaltung des Telekommunikationsbetriebs für entscheidend. Zur Erstellung eines modernen und geeigneten Konzepts wurde Mitte 2005 ein Interessenbekundungsverfahren eingeleitet, bei dem die Telekommunikationswirtschaft aufgefordert wurde, die aus ihrer Sicht für die Landesverwaltung geeigneten Konzepte anzubieten. Voice Over IP ist ein Teil des technischen Konzepts. Ziel ist ein Betreibermodel, dass durch die Nutzung von neuen Techniken eine effizientere und wirtschaftlichere Form der Kommunikation ermöglicht. Die besonderen Bedin-

gungen des Datenschutzes und der Datensicherheit werden berücksichtigt. Der Hessische Datenschutzbeauftragte wird mit einbezogen.

Zu 8.7 Kein Kopierschutz bei Internetveröffentlichungen

Die Landesregierung stimmt dem Hessischen Datenschutzbeauftragten zu, dass ein im beschriebenen Sinne wirksamer Kopierschutz zurzeit technisch nicht realisierbar ist.

9. Bilanz

Zu 9.1 Vorratsdatenspeicherung durch Telekommunikations-, Tele- und Mediendiensteanbieter

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zum Sachstand uneingeschränkt zu.

Hinsichtlich der in Bezug genommenen Entschließung der Datenschutzbeauftragten (Ziff. 10.6) ist jedoch Folgendes anzumerken:

Die Einführung einer Mindestspeicherfrist für Verkehrsdaten - es geht nicht um Kommunikationsinhalte - ist zur Wahrung wichtiger Belange notwendig. Eine Auswertung von Verkehrsdaten ist oftmals der einzig verbleibende, Erfolg versprechende Ermittlungsansatz bei der Aufklärung von bedeutsamen, auch terroristischen Straftaten. Ihre Durchführbarkeit kann nur auf diese Weise sichergestellt werden.

Beispiele, die eine derartige Verpflichtung zur Speicherung untermauern, sind insbesondere die Bombenanschläge vom 11. März 2004 in Madrid und vom 7. und 21. Juli 2005 in London. Die Auswertung von Verkehrsdaten der z. T. weltweit agierenden Tätergruppen führte nach bislang vorliegenden Informationen zu weiteren Ermittlungsansätzen und letztlich gerade in Madrid auch zu Täterermittlungen.

In Großbritannien ergaben Erhebungen zur Speicherungsdauer durch eine gemeinsame Arbeitsgruppe von Polizei und Diensteanbietern, dass insbesondere bei terroristischen Verbrechen und bei Straftaten gegen das Leben ein erhöhtes Datenabfragebedürfnis auch hinsichtlich solcher Verkehrsdaten bestand, die älter als sechs Monate sind.

Bereits in der Vergangenheit haben die Polizeien des Bundes und der Länder der Rechtstatsa-chensammelstelle des Bundeskriminalamts zahlreiche Fälle benannt, die in den Bereichen Internet, Festnetz- und Mobiltelefonie einen entsprechenden Bedarf eindrucksvoll belegt haben. In vielen Fällen konnte der Täter nicht oder nicht rechtzeitig ermittelt werden. So war in dem vom Bundeskriminalamt bearbeiteten Verfahrenskomplex "MELIANI" (Terrorzelle in Frankfurt am Main, die einen Anschlag auf den Straßburger Weihnachtsmarkt plante) die Ermittlung weiterer Kontaktpersonen und möglicher Hintermänner der Gruppierung nicht möglich, weil die Verbindungsdaten nur für wenige Monate zur Verfügung standen.

Seit Mai 2005 erhebt das Bundeskriminalamt zudem im Auftrag der Kommission "Einsatz und Ermittlungsunterstützung" der AG Kripo systematisch Fälle bei den Polizeien des Bundes und der Länder, die konkret Defizite wegen fehlender Verbindungsdaten aufzeigen. Bis Oktober 2005 wurden dem BKA so 381 Fallschilderungen übermittelt, in denen der oder die Täter nicht oder nur unter erschwerten Voraussetzungen ermittelt werden konnten, weil Verbindungsdaten im Bereich Internet, Festnetz oder Mobilfunk nicht verfügbar waren. Schwerpunkte liegen im Bereich der Straftaten gegen die sexuelle Selbstbestimmung, Betrugsdelikten und Straftaten gegen das Eigentum. Ersichtlich ist aber auch, dass Verkehrsdaten bei fast jeder Straftat relevant sein können. Die Zulieferungen belegen zudem, dass Verbindungsdaten nicht nur zum Tatnachweis, sondern gerade auch im Rahmen von Strukturermittlungen das Beziehungsgeflecht auf Täterseite näher beleuchten können.

Dass Anfragen von Strafverfolgungsbehörden nach Verkehrsdaten in der Regel binnen der ersten zwei bis drei Monate gestellt werden, hängt mit der bislang fehlenden Pflicht zur Speicherung der Verkehrsdaten zusammen. Im Wissen, dass die Diensteanbieter die Daten zu Abrechnungszwecken nur für einen kurzen Zeitraum speichern, werden Anfragen erst gar nicht gestellt. Im Übrigen unterscheiden sich die Speicherzeiträume von Anbieter zu Anbieter. Sie liegen zwischen 72 Stunden und sechs Monaten. Selbst wenn eine Auskunft erteilt werden kann, ist diese außerdem häufig für die Ermitt-

lungen nutzlos, weil die angerufene Telefonnummer zuvor in den letzten drei Stellen anonymisiert worden war.

Der Richtlinienvorschlag trägt dem Grundsatz der Verhältnismäßigkeit Rechnung. Die Auswirkungen auf die Rechte des Einzelnen und der Wirtschaftsteilnehmer sind infolge der Beschränkung auf einige wenige Arten von Verkehrsdaten begrenzt und angesichts der Bedeutung der Maßnahme für die Verhütung und Bekämpfung von schweren Straftaten einschließlich des Terrorismus als verhältnismäßig anzusehen. Das vom Bundesverfassungsgericht in Zusammenhang mit dem Grundrecht auf informationelle Selbstbestimmung postulierte Verbot der Vorratsdatenspeicherung wird nicht verletzt. Das Bundesverfassungsgericht hat im Volkszählungsurteil nämlich nur die Speicherung personenbezogener Daten "auf Vorrat zu unbestimmten oder noch nicht bestimmten Zwecken" für verfassungsrechtlich unzulässig erklärt.

Zu 9.2 Datenübermittlungen an Parteien zu Wahlwerbezwecken aus dem Einwohnermelderegister

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend.

Zu 9.3 Videoüberwachung in öffentlichen Verkehrsmitteln

Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten mit Interesse zur Kenntnis genommen.

Zu 9.4 Datenbankprotokolle im Einwohnerwesen

Die Landesregierung hat den Ausführungen des Hessischen Datenschutzbeauftragten nichts hinzuzufügen.

Zu 9.5 Neue Rechtsgrundlagen zur DNA-Analyse im Strafverfahren

Aus Sicht der Landesregierung berücksichtigt das am 1. November 2005 in Kraft getretene Gesetz zur Novellierung der forensischen DNA-Analyse die Belange des Datenschutzes vollumfänglich. Neben einer geringfügigen Ausdehnung des Anwendungsbereichs hat der Gesetzgeber nunmehr auch ausdrücklich auf eine richterliche Anordnung in dem Fall verzichtet, dass eine betroffene Person ihr Einverständnis erteilt. Dies war schon bisher Praxis in Hessen.
Weder die Frage der Freiwilligkeit der Einwilligung noch die gesetzliche Regelung des Reihengentests geben Anlass zu Bedenken.

In Hessen werden die Betroffenen vor der Abgabe einer Einwilligungserklärung ausführlich und in verständlicher Form über die rechtlichen Voraussetzungen und die Folgen der Maßnahme aufgeklärt. Durch die von den hessischen Polizeibehörden benutzten aktuellen Hinweise zur Einverständniserklärung wird jeder Betroffene in die Lage versetzt, den Gegenstand und die Folgen einer möglichen Einwilligung zu erkennen und auf dieser Grundlage eine freie Entscheidung zu treffen.

Der Gesetzgeber hat durch die in § 81h StPO enthaltene besonders ausgestaltete Verhältnismäßigkeitsregelung den Ausnahmecharakter des Reihengentests unterstrichen, so dass es der zusätzlichen Aufnahme einer ultima-ratio-Regel in das Gesetz nicht bedurfte. Hinzu kommt, dass der mit der Vorbereitung und Durchführung eines Reihengentests in jedem Fall verbundene ganz erhebliche organisatorische, personelle und finanzielle Aufwand eine Beschränkung des Einsatzes von Reihengentests auf schwere Straftaten bewirken wird, bei denen weniger aufwendige kriminalpolizeiliche Mittel nicht zum Erfolg geführt haben.

Wiesbaden, 7. August 2006

Der Hessische Ministerpräsident: **Koch**

Der Hessische Minister des Innern und für Sport: **Bouffier**