16. Wahlperiode

Drucksache **16/4751**

HESSISCHER LANDTAG

05. 12. 2005

Stellungnahme der Landesregierung

betreffend den Dreiunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Drucksache 16/3746

Eingegangen am 5. Dezember 2005 · Ausgegeben am 23. Dezember 2005

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

Inhaltsverzeichnis

Stellungnahme zu

Zum Vorwort

und

Zu 1. Einführung

Die Landesregierung teilt die skeptische Sicht des Hessischen Datenschutzbeauftragten zu den Folgen der technischen Entwicklung für das informationelle Selbstbestimmungsrecht nicht. Die Informations- und Kommunikationstechnik ermöglicht Bürgerinnen und Bürgern heute einen schnellen und unkomplizierten Zugang zu Informationen aller Art, zur Kommunikation mit anderen, ohne dass räumliche Trennung oder Grenzen noch eine Rolle spielten, die Wirtschaft profitiert in vielfältiger Weise von dieser Entwicklung und auch der Staat erhält die Möglichkeit, manche seiner Aufgaben wirtschaftlicher und besser zu erfüllen. Die Entwicklung der Technik birgt auch Gefahren, die nicht verkannt werden, doch überwiegt nach Ansicht der Landesregierung deren Nutzen für die Menschen.

Die Auffassung des Hessischen Datenschutzbeauftragten, der Datenschutz habe zu Beginn der technischen Entwicklung im Brennpunkt des öffentlichen Interesses gestanden und heute, da die damals nur befürchteten Gefahren technisch realisierbar sind, sei der Datenschutz in den Hintergrund gedrängt, scheint an die skeptische Einschätzung über die Folgen der technischen Entwicklung anzuschließen. Es handelt sich bei dieser vermeintlich zu beobachtenden Entwicklung aber vielleicht auch nur um eine Folge des Umstands, dass Bürgerinnen und Bürger heute in der Regel viel mehr Wissen über Informationstechnik besitzen, als zu Beginn des Computer-Zeitalters. Wer täglich mit IT-Systemen umgeht, kann deren Arbeitsweise und Gefahren besser beurteilen und neigt schon deshalb weniger zur Furcht davor. Das sollte jedoch nicht mit einem mangelnden Bewusstsein für die Gefahren der Informationstechnik verwechselt werden. Wer seinen Einkauf mit einer Kundenkarte bezahlt, seinen Kontostand im Internet überprüft und sein Handy-Guthaben Online auflädt, vertraut darauf, dass sich die Unternehmen bei der Verarbeitung seiner Daten an die gesetzlichen Vorgaben und die vertraglichen Vereinbarungen halten. Er hat nicht die Furcht, zum gläsernen Objekt staatlicher Neugier zu werden, weil er aufgrund seiner Erfahrungen im privaten Bereich darauf vertraut, dass sich auch die Behörden an die geltenden Gesetze halten, wenn sie seine Daten für die Aufklärung von Straftaten oder die Verhütung von Verbrechen verarbeiten. Es mangelt ihm nicht an Bewusstsein für die Notwendigkeit des Datenschutzrechts, er sieht es als gewahrt an, wenn sich die mit seinen Daten arbeitenden Stellen an die geltenden Gesetze halten.

Dass z.B. aus Gründen der inneren Sicherheit notwendige Eingriffe in das informationelle Selbstbestimmungsrecht heute möglicherweise weniger aufgeregt diskutiert werden, als vor zwei Jahrzehnten, mag auch an der Erfahrung der Bürgerinnen und Bürger aus dieser Zeit liegen, in denen wenig schwere Verstöße gegen das Datenschutzrecht festgestellt wurden. Zugleich konnten die Bürgerinnen und Bürger eine aufmerksame Datenschutzkontrolle durch den Hessischen Datenschutzbeauftragten und seine Kolleginnen und Kollegen in den anderen Aufsichtsbehörden für den Datenschutz beobachten. Man wird aus der geringeren Aufregung in der Diskussion daher nicht nur auf einen Verlust an Bewusstsein für die Gefahren der Datenverarbeitung schließen können, sondern auch auf das gestiegene Vertrauen in die Rechtstreue der öffentlichen und privaten Stellen und insbesondere auch in die Arbeit der Aufsichtsbehörden für den Datenschutz.

Die Landesregierung wird die Belange des Datenschutzes auch zukünftig bei ihrer Arbeit berücksichtigen und wo dies möglich ist, den Hessischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben unterstützen, damit die Bürgerinnen und Bürger in Hessen auch zukünftig keine Furcht vor der Entwicklung der Informations- und Kommunikationstechnik haben müssen.

Zu 2. Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten
Zu 2.1 Allgemeines
Zu 2.1.1 Öffentlicher Bereich

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zum Hessischen Datenschutzgesetz (HDSG) und Bundesdatenschutzgesetz (BDSG) zu.

Zu 2.1.2 Gerichte

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten, wonach die Gerichte seiner Kontrolle unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden, zu.

Zu 2.1.3 Kontrolle der Kontrolleure?

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass für ihn keine Kontrollbefugnis über das Hessische Ministerium des Innern und für Sport und das Regierungspräsidium Darmstadt hinsichtlich deren Aufgabenwahrnehmung als Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich besteht.

Zu 2.2 Fraport AG

Der Hessische Datenschutzbeauftragte ist der Auffassung, die Fraport AG sei eine öffentliche Stelle nach dem Hessischen Datenschutzgesetz und unterliege seiner Kontrolle. Die Landesregierung kann dieser Auffassung nicht zustimmen.

Es besteht Einigkeit mit dem Hessischen Datenschutzbeauftragten, dass die Fraport AG ein nicht öffentliches Unternehmen ist, das sich in verschiedenen Bereichen ausschließlich marktorientiert betätigt. Ebenso wird dem Hessischen Datenschutzbeauftragten vorbehaltlos darin zugestimmt, dass mit dem Betrieb eines Verkehrsflughafens wie dem in Frankfurt am Main auch öffentliche Zwecke erfüllt werden, zu dessen Gunsten daher auch eine gemeinnützige Planung betrieben werden kann, wie in dem zitierten Urteil des Bundesverwaltungsgerichts vom 7. Juli 1978 (BVerwGE 56, 110, 118f) zur so genannten Startbahn West dargelegt ist. Nicht zugestimmt werden kann dem Hessischen Datenschutzbeauftragten indessen bei seiner Folgerung, weil der Betrieb des Flughafens auch öffentliche Zwecke erfüllt, sei die Fraport AG eine öffentliche Stelle und unterliege seiner Kontrolle.

Für die Entscheidung über die datenschutzrechtliche Zuständigkeit kommt es auf die Auslegung des § 2 Abs. 3 Bundesdatenschutzgesetz (BDSG) an. Nach § 2 Abs. 3 Satz 1 BDSG gelten Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder als öffentliche Stellen, wenn sie "Aufgaben der öffentlichen Verwaltung wahrnehmen". Zweck der Vorschrift ist es, nicht öffentliche Stellen hinsichtlich der datenschutzrechtlichen Kontrollen den öffentlichen Stellen gleichzustellen, wenn sie dieselben Aufgaben erfüllen, die sonst von der Verwaltung wahrgenommen würden. Ein privatrechtliches Unternehmen muss deshalb den spezifischen Zwecken der daran beteiligten öffentlichen Stellen dienen, nur dann nimmt es an der Erfüllung einer Aufgabe der öffentlichen Verwaltung teil, eine reine Finanzbeteiligung der öffentlichen Stellen reicht nicht aus (Dammann in Simitis, Kommentar zum BDSG, Rdnr. 41 zu § 2). Die Beteiligung muss mit anderen Worten der Hebel sein, mit dem die privatrechtliche Vereinigung für die Erfüllung der Aufgabe der beteiligten öffentlichen Stellen instrumentalisiert wird (Dammann a.a.O., Rdnr. 46 zu § 2).

Die Auffassung darüber, was eine Aufgabe der öffentlichen Verwaltung ist, war in den letzten Jahren einem erheblichen Wandel unterworfen. Die inzwischen durchgeführten Privatisierungen, z.B. Post, Telekom, zeigen, dass der Staat in Bereichen, die früher zweifelsfrei der Verwaltung zuzurechnen waren, keine Aufgaben mehr wahrnehmen will. Die entstandenen Unternehmen stehen - wie jedes Privatunternehmen - im Wettbewerb mit der Konkurrenz. Das gilt auch für die Fraport AG.

Die Beteiligung des Bundes an der Fraport AG ist gegenwärtig nur noch als reine Finanzbeteiligung zu bewerten. Der Bundesfinanzminister Hans Eichel hat dies in einem Aufsatz (Hans Eichel, "Im Fluss - Privatisierungspolitik der Bundesregierung" in Unternehmermagazin 6/2004, abrufbar auch von der Internet-Seite des Bundesfinanzministeriums "www.bundesfinanzministerium.de") in aller Deutlichkeit wie folgt zum Ausdruck gebracht:
"Wo der Bund noch Anteile an börsennotierten Unternehmen hält, wird er den Weg einer kapitalmarktgerechten, kursschonenden Platzierung seiner Aktien fortsetzen. Dies gilt vor allem für die Deutsche Telekom AG, die Deutsche Post AG und die Fraport AG…"
Der Verkauf der Anteile an der Fraport AG wäre ausgeschlossen, wenn die Beteiligung des Bundes der Erfüllung von Aufgaben der Bundesverwaltung diente.

Wenn man dennoch der Ansicht wäre, die Fraport AG nehme Aufgaben der öffentlichen Verwaltung wahr, müsste sie nach § 2 Abs. 3 Nr. 1 BDSG als öffentliche Stelle des Bundes - nicht des Landes Hessen - gelten, weil das Unternehmen über die Grenzen des Landes hinaus tätig wird. Die Fraport AG ist beispielsweise an den Flughäfen Frankfurt-Hahn (Rheinland-Pfalz), Saarbrücken (Saarland), Hannover-Langenhagen (Niedersachsen) beteiligt. Aber dann wäre nicht der Hessische Datenschutzbeauftragte sondern der Bundesbeauftragte für den Datenschutz für die Kontrolle bei der Fraport AG zuständig. Der Bundesbeauftragte für den Datenschutz hat jedoch vor Jahren eine Zuständigkeit für die Fraport AG - damals noch die Flughafen AG - gegenüber dem Regierungspräsidium Darmstadt abgelehnt, als die Frage bereits einmal mit dem Hessischen Datenschutzbeauftragten erörtert wurde.

Im Übrigen würde die vom Hessischen Datenschutzbeauftragten vertretene Rechtsauffassung nur zu einer Änderung der zuständigen Aufsichtsbehörde führen, nicht aber zur Anwendung anderer datenschutzrechtlicher Bestimmungen. Nach § 12 Abs. 1 BDSG gelten die besonderen Vorschriften des Gesetzes für öffentliche Stellen nur, soweit sie nicht am Wettbewerb teilnehmen. Für öffentlich-rechtliche Wettbewerbsunternehmen gelten dagegen dieselben Bestimmungen der §§ 27 ff. BDSG wie für nicht öffentliche Stellen. Auch der Hessische Datenschutzbeauftragte erkennt an, dass sich die Fraport AG in verschiedenen Bereichen ausschließlich marktorientiert betätigt und damit als Unternehmen am Wettbewerb teilnimmt. Selbst wenn der Ansicht des Hessischen Datenschutzbeauftragten zu folgen wäre, dass die Fraport AG als öffentliche Stelle des Landes zu behandeln ist, käme man nach § 3 Abs. 6 HDSG zu demselben Ergebnis, mit Ausnahme der zusätzlich geltenden Bestimmungen über den Datenschutz bei Dienst- und Arbeitsverhältnissen (§ 34 HDSG) und das Fernmessen und Fernwirken (§ 36 HDSG). Die Änderung der Zuständigkeit der Aufsichtsbehörde würde sich auf die Rechte der Betroffenen, deren Daten von der Fraport AG verarbeitet werden, daher kaum auswirken; das gilt auch für die Beschäftigten der Fraport AG.

Die Fraport AG betreibt nicht nur den Flughafen Frankfurt am Main nach wirtschaftlichen Gesichtspunkten, sondern ist aufgrund ihrer Beteiligung an mehreren in- und ausländischen Flughäfen und Bodenservicebetrieben auf Flughäfen ein international tätiger Konzern. Die Landesregierung ist deshalb der Auffassung, dass es nicht nur dem Hessischen und dem Bundesdatenschutzgesetz sondern auch dem Gebot der Gleichbehandlung mit anderen Wirtschaftsunternehmen entspricht, wenn die datenschutzrechtliche Aufsicht über dieses Unternehmen weiterhin der für den nicht öffentlichen Bereich zuständigen Behörde - dem Regierungspräsidium Darmstadt - obliegt.

Zu 2.3 Anwendbarkeit des Hessischen Datenschutzgesetzes auf hessische Verkehrsverbünde

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass für die Verkehrsverbünde im Sinn des § 5 Gesetz zur Weiterentwicklung des öffentlichen Personennahverkehrs in Hessen das Hessische Datenschutzgesetz gilt.

Zu 3. Europa
Zu 3.1 Schengener Durchführungsübereinkommen
Zu 3.1.1 Allgemeines

Die Landesregierung kann hierzu keine Stellungnahme abgeben, da ihr keine weitergehenden Informationen über die Tätigkeiten der Gemeinsamen Kontrollinstanz vorliegen.

Zu 3.1.2 Entwicklung des Schengener Informationssystems

Die Ausführungen des Hessischen Datenschutzbeauftragten zur Notwendigkeit der Schaffung einer neuen Generation des Schengener Informationssystems (SIS) sind zutreffend. Das neue SIS soll dabei in technischer Hinsicht weiter entwickelt werden und unter anderem die Aufnahme neuer Kategorien von Ausschreibungen ermöglichen sowie Speicherung, Übertragung und möglicherweise den Abruf biometrischer Daten (z.B. Lichtbilder und Fingerabdrücke) zulassen. Eine Abkehr vom Charakter des SIS als "Treffer/kein Treffer"-System ist in den einschlägigen EU-Ratsarbeitsgruppen allerdings entgegen der Annahme des Hessischen Datenschutzbeauftragten nicht in der Diskussion.

Zu 3.1.2.1 Bereits feststehende Änderungen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.1.2.2 In der Diskussion befindliche Vorschläge

Die Ausführungen geben den aktuellen Stand der Diskussion auf europäischer Ebene zutreffend wieder.

Zu 3.1.3 Gemeinsame Überprüfung der Ausschreibungen zu Drittausländern

Die Landesregierung kann hierzu keine Stellungnahme abgeben, da ihr keine weitergehenden Informationen über die Tätigkeiten der Gemeinsamen Kontrollinstanz vorliegen.

Zu 3.2 Europaweit koordinierte Prüfung von Ausschreibungen zur Einreiseverweigerung in das Schengen-Gebiet

Das Hessische Ministerium des Innern und für Sport war an den Prüfungen des Hessischen Datenschutzbeauftragten nicht beteiligt. Der Hessische Datenschutzbeauftragte hat das Ergebnis seiner Prüfungen dem Ministerium im vergangenen Jahr mitgeteilt und angekündigt, er werde nach Auswertung der Unterlagen auch in anderen Bundesländern erneut auf das Ministerium zukommen. Dies ist bis zum Redaktionsschluss dieser Stellungnahme nicht geschehen.

Zu 4. Bund

Zu 4.1 Die Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff und die Konsequenzen für das Instrumentarium von Strafverfolgungsbehörden

Die Landesregierung stimmt mit dem Hessischen Datenschutzbeauftragten darin überein, dass die Entscheidung des Bundesverfassungsgerichts vom 3. März 2004 einer sorgfältigen Umsetzung durch den Gesetzgeber bedarf. Der Gesetzgeber ist jedoch nicht gehalten, im Rahmen der gesetzlichen Neuregelung über die Vorgaben des Bundesverfassungsgerichts noch hinauszugehen und verfassungsrechtlich nicht gebotene Restriktionen für die Strafverfolgung vorzusehen, wie an einigen Stellen des Gesetzentwurfs der Bundesregierung geschehen. Hessen hatte daher gemeinsam mit anderen Bundesländern im Bundesrat mehrere Änderungsanträge gestellt, die auch in die Stellungnahme des Bundesrates zu dem Regierungsentwurf Eingang fanden. Der Bundestag hat leider nicht alle vorgeschlagenen Änderungen in das am 24. Juni 2005 beschlossene Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 übernommen.

Zu 4.2 Neues Telekommunikationsgesetz

Der Hessische Datenschutzbeauftragte ist der Auffassung, das neue Telekommunikationsgesetz (TKG) bringe keine datenschutzrechtlichen Verbesserungen, sondern führe eher zu einer Absenkung des Datenschutzniveaus.
Die Landesregierung vermag sich den im Tätigkeitsbericht geäußerten Bedenken nicht anzuschließen.

Zu 4.2.1 Vorratsdatenspeicherung

Die Landesregierung sieht in der vom Bundesrat seit langem geforderten Vorratsspeicherung von Verkehrsdaten ein notwendiges Mittel der effektiven Strafverfolgung.

Zu 4.2.2 Vorausbezahlte (Prepaid-)Karten

Die auf Anregung des Bundesrats in das TKG eingefügte Datenerfassung bei Mobiltelefonen mit vorausbezahlter Karte ist nach Auffassung der Landesregierung ebenfalls ein notwendiges Mittel der effektiven Strafverfolgung. Straftäter nutzen nicht selten Mobiltelefone mit Prepaid-Karten zur Kommunikation. Angaben über den Erwerber eines Mobiltelefons können den Strafverfolgungsbehörden deshalb im Einzelfall wichtige Hinweise zur Aufklärung von Straftaten geben. Es besteht aus diesem Grund kein Anlass, für Daten über Erwerber von Mobiltelefonen einen anderen Maßstab anzulegen als bei Mobiltelefonen mit Vertragsbindung.

Zu 4.2.3 Inverssuche

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zur Inverssuche zu.
Die Kontrolle, ob die Regelung zur Inverssuche (§ 105 TKG) eingehalten wurde, obliegt nach § 115 Abs. 4 TKG allerdings dem Bundesbeauftragten für den Datenschutz.

Zu 4.2.4 Überwachung

Nach Ansicht der Landesregierung ist es für eine effektive Strafverfolgung ebenfalls erforderlich in bestimmten Fällen die zu erteilende Auskunft auf Daten, die ihrerseits vor einem Zugriff schützen sollen (Passwörter, PIN und PUK), zu erstrecken. Die schutzwürdigen Belange der von einer solchen erweiterten Auskunft betroffenen Telefonkunden sind dadurch ausreichend gewahrt, dass das Gesetz nur einem begrenzten Kreis von Ermittlungsbehörden unter bestimmten Voraussetzungen ein Auskunftsrecht zubilligt.

Zu 5. Land
Zu 5.1 Polizei und Strafverfolgung
Zu 5.1.1 Novellierung im Polizeirecht
Zu 5.1.1.1 Überblick

Im Rahmen der Sachverständigenanhörung vor dem Innenausschuss des Hessischen Landtags gab es unterschiedliche Auffassungen zu dem Gesetzentwurf der Landesregierung. Dabei wurden auch einzelne Kritikpunkte des Hessischen Datenschutzbeauftragten von anderen Experten aufgegriffen. Überwiegend fanden die Regelungsvorschläge der Landesregierung jedoch Zustimmung.

Zu 5.1.1.2 Konsequenzen aus den Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004

Der Hessische Datenschutzbeauftragte begrüßt es ausdrücklich, dass der hessische Gesetzgeber für das Polizeirecht Konsequenzen aus den Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 (1 BvR 2378/98 und 1 BvR 1084/89) zu heimlichen Überwachungsmaßnahmen nach der Strafprozessordnung und dem Außenwirtschaftsgesetz nicht nur für den Bereich der Wohnraumüberwachung getroffen hat. Dabei fehle zum Teil jedoch eine konsequente Umsetzung und die dafür im Gesetzgebungsverfahren genannten Begründungen seien rechtlich angreifbar.

Nach den Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 stand die hessische Landesregierung vor einem zeitlichen Problem. Es galt sicherzustellen, dass das Achte Änderungsgesetz zum HSOG rechtzeitig zum 1. Januar 2005 in Kraft treten konnte. Daher mussten entweder die sich aus den Entscheidungen ergebenden weit reichenden Folgerungen in diesem Gesetzentwurf unberücksichtigt gelassen oder aber kurzfristig umfangreiche Ergänzungen des Entwurfs vorgenommen werden. Die Landesregierung hat sich für den zweiten Weg entschieden, nicht zuletzt nachdem der Hessische Datenschutzbeauftragte, dessen Rat eingeholt und dessen Verbesserungsvorschläge berücksichtigt worden waren, seine Zustimmung signalisiert hatte. Alle Beteiligten haben dabei Neuland betreten, weil die Entscheidungen des Bundesverfassungsgerichts juristisch noch nicht aufgearbeitet sind und die Aussagen zur Wohnraumüberwachung zudem das Strafverfahren betreffen, mithin auf einer anderen verfassungsrechtlichen Grundlage (Art. 13 Abs. 3 GG) beruhen als Wohnraumüberwachungen nach Polizeirecht (Art. 13 Abs. 4 GG).

Zu 5.1.1.2.1 Straftaten mit erheblicher Bedeutung

Die Kritik des Hessischen Datenschutzbeauftragten an der Neufassung der Definition der Straftaten mit erheblicher Bedeutung ist nicht nachzuvollziehen.

Ein Vergleich der alten mit der neuen Fassung des § 13 Abs. 3 HSOG zeigt, dass die neue Fassung wesentlich präziser ist als die bisherige. Die alte Fassung hatte folgenden Wortlaut:

"Straftaten mit erheblicher Bedeutung sind Straftaten, die auf Grund ihrer Begehungsweise oder ihrer Dauer eine Gefahr für die Allgemeinheit darstellen und geeignet sind, die Rechtssicherheit der Bevölkerung zu beinträchti-

gen; dies gilt insbesondere für Straftaten, die banden-, gewerbs-, gewohnheits- oder serienmäßig begangen werden."

Demgegenüber lautet die neue Fassung:

"Straftaten mit erheblicher Bedeutung im Sinne dieses Gesetzes sind
1. Verbrechen und
2. Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, soweit sie
   a) sich gegen Leib, Leben oder Freiheit einer Person oder bedeutende Sach- oder Vermögenswerte richten,
   b) auf den Gebieten des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- und Wertzeichenfälschung oder des Staatsschutzes (§§ 74a und 120 des Gerichtsverfassungsgesetzes) begangen werden oder
   c) gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangen werden."

Der Hessische Datenschutzbeauftragte kritisiert auch keineswegs einzelne Formulierungen des neuen § 13 Abs. 3 HSOG. Vielmehr stellt er einen Bezug zwischen dieser Vorschrift und der Wohnraumüberwachung nach § 15 Abs. 4 HSOG her, für den es jedoch keinen Anlass gibt. Die Wohnraumüberwachung ist nach § 15 Abs. 4 HSOG ausschließlich zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person zulässig. Die Vorschrift knüpft mithin nicht an eine Straftat mit erheblicher Bedeutung an. Demzufolge ist es für die Wohnraumüberwachung irrelevant, welche Anforderungen das Gesetz an eine Straftat mit erheblicher Bedeutung stellt.

Ebenso ist es nicht erheblich, welche Voraussetzungen Art. 13 Abs. 3 GG für eine Wohnraumüberwachung verlangt, denn die Wohnraumüberwachung nach Polizeirecht richtet sich nicht nach dieser Bestimmung, sondern nach Art. 13 Abs. 4 GG. Es besteht auch kein Anlass, einzelne Elemente aus Abs. 3 in Abs. 4 zu übertragen. Das HSOG lässt eine Wohnraumüberwachung ausschließlich zum Schutz höchster Individualrechtsgüter vor gegenwärtiger Gefahr zu und überschreitet damit die durch Art. 13 Abs. 4 GG gesetzte Schwelle der "dringenden Gefahr für die öffentliche Sicherheit" deutlich.

Zu 5.1.1.2.2 Akustische Wohnraumüberwachung

Zunächst ist darauf hinzuweisen, dass die vom Hessischen Datenschutzbeauftragten gewählte Überschrift missverständlich ist. Die Wohnraumüberwachung nach Polizeirecht ist anders als im Strafverfahren keineswegs nur eine akustische. Der verfassungsändernde Gesetzgeber hat bei der Schaffung der neuen Abs. 3 und 4 des Art. 13 GG durch Gesetz vom 26. März 1996 (BGBl. I S. 610) erkannt, dass den Behörden zur Gefahrenabwehr weiter gehende Möglichkeiten eröffnet sein müssen als zur Strafverfolgung. Er hat deshalb die Wohnraumüberwachung zu Zwecken der Gefahrenabwehr nicht auf akustische Maßnahmen beschränkt. Dementsprechend ermöglicht § 15 Abs. 4 HSOG technische Überwachungsmaßnahmen jeglicher Art, einschließlich der Videoüberwachung.

Der Hessische Datenschutzbeauftragte teilt die Auffassung des hessischen Gesetzgebers, dass der Kernbereich privater Lebensgestaltung nicht betroffen sein kann, soweit der Störer in die geschützte Sphäre eines anderen eingreift. Zu Recht weist er ferner darauf hin, dass sich nicht jede Äußerung bzw. jedes Gespräch während einer laufenden Überwachungsmaßnahme auf die abzuwehrende Gefahr beziehen wird und die Überwachung in solchen Fällen zu unterbrechen wäre, wenn man den Beschluss des Bundesverfassungsgerichts zur Wohnraumüberwachung im Strafverfahren zum Maßstab nimmt. Gerade letzteres ist jedoch nicht zwingend geboten.

Zwar spielt insoweit die unterschiedliche verfassungsrechtliche Verankerung in Art. 13 GG keine Rolle, denn der Kernbereich privater Lebensgestaltung, um den es hier geht, ist Ausfluss der Menschenwürdegarantie des Art. 1 GG. Der Kernbereich privater Lebensgestaltung des polizeirechtlichen Störers ist demnach prinzipiell in gleicher Weise geschützt wie derjenige des Beschuldigten im Strafverfahren. Der Unterschied liegt in der Wertigkeit der gegenläufigen Interessen. Nach der Rechtsprechung des Bundesverfassungsgerichts ist der Kernbereich privater Lebensgestaltung abwägungsresistent, so dass selbst höchste Belange des Gemeinwohls wie die effektive Verfol-

gung schwerster Straftaten nicht zu seiner Schmälerung führen können. Sollen andere Personen vor gegenwärtiger Gefahr für Leib, Leben oder Freiheit geschützt werden, findet eine derartige Abwägung mit öffentlichen Interessen aber nicht statt; vielmehr geht es um den Schutz höchster Individualrechtsgüter anderer Personen. Hier stehen sich die Menschenwürde des Störers und die des Opfers gegenüber. Das erfordert und ermöglicht eine andere Grenzziehung. Der Schutz des Opfers lässt sich durch eine Überwachung, die jedes Mal unterbrochen wird, wenn das Gespräch einen irrelevanten Inhalt betrifft, nicht gewährleisten. Es lässt sich nämlich nicht zuverlässig beurteilen, wann die Überwachung wieder fortgesetzt werden darf. Damit bestünde zulasten des Opfers das erhebliche Risiko, dass bedeutsame Informationen verloren gehen. Der hessische Gesetzgeber hat diese Situation, über die das Bundesverfassungsgericht nicht zu entscheiden hatte, gelöst, indem das HSOG eine Unterbrechung der Überwachung bei Gesprächsinhalten, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, nicht verlangt, jedoch ein mit einer Löschungspflicht gekoppeltes Verwertungsverbot ausspricht.

Zu 5.1.1.2.3 Präventive Telekommunikationsüberwachung

Der Hessische Datenschutzbeauftragte kritisiert das Fehlen von Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung im Falle der präventiven Telekommunikationsüberwachung.
Bei der Schaffung von § 15a HSOG ging man in der Tat davon aus, dass die diesbezüglichen Ausführungen des Bundesverfassungsgerichts im Urteil vom 3. März 2004 zur Wohnraumüberwachung hier nicht anwendbar sind, weil die Nutzung von Telekommunikationseinrichtungen nicht in den Kernbereich privater Lebensgestaltung fällt. Das Gericht hat nämlich in seinem Urteil erklärt, dass die vertrauliche Kommunikation ein "räumliches Substrat" benötige (a.a.O., Rdnr. 120). Die Telekommunikation von einem Festnetzanschluss oder einem Mobiltelefon aus verlässt jedoch den geschützten räumlichen Bereich der Wohnung.

In der Entscheidung zum Niedersächsischen Gesetze über die öffentliche Sicherheit und Ordnung vom 27. Juli 2005 (1 BvR 668/04) hat sich das Bundesverfassungsgericht nunmehr auch zur Beachtung des Kernbereichs privater Lebensgestaltung bei der Telefonüberwachung geäußert. Danach erfordert die nach Art. 1 Abs. 1 Grundgesetz stets garantierte Unantastbarkeit der Menschenwürde auch bei der Telekommunikationsüberwachung grundsätzlich den Schutz des Kernbereichs privater Lebensgestaltung (a.a.O., Rdnr. 163). Verfassungsrechtlich hinzunehmen sei das Risiko einer Verletzung des Schutzbereichs allenfalls bei einem besonders hohen Rang des gefährdeten Rechtsguts (a.a.O., Rdnr. 164). Die Regelung in § 15a HSOG setzt eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person voraus und gilt damit nur im vom Bundesverfassungsgericht genannten Ausnahmefall. Außerdem verlangt das Bundesverfassungsgericht, dass Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet werden, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist. Diese Forderung ist durch § 27 Abs. 2 Satz 1 Nr. 1 in Verbindung mit Abs. 6 Satz 1 Nr. 2 HSOG erfüllt, wonach Daten, die den Kernbereich privater Lebensgestaltung betreffen, zu löschen sind. Nach gegenwärtiger Bewertung genügt die Regelung zur Telekommunikationsüberwachung im HSOG damit auch den vom Bundesverfassungsgericht im Urteil vom 27. Juli 2005 formulierten Anforderungen.

Zu 5.1.1.2.4 Kennzeichnung und weitere Verwendung mittels verdeckter Datenerhebung erlangter Daten

Der Hessische Datenschutzbeauftragte beanstandet, dass Daten, die bei der Wohnraumüberwachung oder der Telekommunikationsüberwachung nur zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erhoben werden dürfen, nach § 20 Abs. 6 Satz 2 HSOG in anderem Kontext zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person übermittelt werden dürfen, selbst wenn diese Gefahr nicht gegenwärtig ist. Die gesetzliche Regelung steht jedoch im Einklang mit der Rechtsprechung des Bundesverfassungsgerichts.

Das Bundesverfassungsgericht lässt die Weiterverwendung von Daten aus der Wohnraum- wie der Telekommunikationsüberwachung grundsätzlich nur für Zwecke zu, die auch als Rechtfertigung für die ursprüngliche Erhebung

ausgereicht hätten (BVerfGE 100, 313 <360, 389>, Urteil vom 3. März 2004 - 1 BvR 2378/98 und 1 BvR 1084/89 -, Rdnr. 333 ff., Beschluss vom 3. März 2004 - 1 BvF 3/92 -, Rdnr. 169). Dabei postuliert es neben der Zweckbindung auch eine Bindung an das konkrete "Ermittlungsverfahren" (Urteil vom 3. März 2004, a.a.O). Eine anderweitige Nutzung soll aber unter den Voraussetzungen des Volkszählungsurteils zulässig sein (Urteil vom 3. März 2004, a.a.O). Überträgt man diese Aussagen auf Gefahrenabwehrsachverhalte, kann es dem Gesetzgeber nicht verwehrt sein, die Nutzung der erhobenen Daten auch zur Abwehr einer bloß konkreten Gefahr von Leib, Leben oder Freiheit einer anderen Person zuzulassen. Es wird sich insbesondere nicht einwenden lassen, dass der veränderte Verwendungszweck mit dem Erhebungszweck unvereinbar ist. Eine Unvereinbarkeit liegt nach der Rechtsprechung des Bundesverfassungsgerichts (Urteil vom 3. März 2004, a.a.O.) dann vor, "wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen". Die zeitliche Nähe des möglichen Schadenseintritts spielt demnach keine Rolle. Ein anderes Ergebnis würde auch keinen Sinn machen, weil die konkrete Gefahr durch bloßen Zeitablauf das Stadium der gegenwärtigen Gefahr erreicht. Die Gefahrenmeldung müsste also lediglich hinausgeschoben werden, um das Stadium der gegenwärtigen Gefahr zu erreichen, was gegebenenfalls wesentlich einschneidendere Abwehrmaßnahmen notwendig machen würde.

Zu 5.1.1.2.5 Rechte der Betroffenen

Der einzige Kritikpunkt des Hessischen Datenschutzbeauftragten bezieht sich darauf, dass die Zurückstellung der Benachrichtigung seiner Behörde zu melden ist und nicht einem Gericht. Der Einwand, das Bundesverfassungsgericht habe für die Zurückstellung der Benachrichtigung eine gerichtliche Kontrolle gefordert, trifft nicht zu. Das Bundesverfassungsgericht hat sich in seinem Urteil zur Wohnraumüberwachung zwar aufgrund der existierenden gesetzlichen Regelung in der Strafprozessordnung mit der Einschaltung von Gerichten in diesem Zusammenhang befasst. Die abstrakt formulierte Forderung des Bundesverfassungsgerichts ist jedoch nicht ausschließlich auf den Richter bezogen. Vielmehr heißt es in der Entscheidung des Bundesverfassungsgerichts (Urteil vom 3. März 2004, a.a.O.) in Randnummer 305 ausdrücklich:

"Die Befassung unabhängiger Stellen auch mit der Überprüfung der Gründe für die weitere Geheimhaltung staatlicher Eingriffe ist ein wesentliches Element des Grundrechtsschutzes, den die Betroffenen selbst nicht wahrnehmen können".

Hätte das Bundesverfassungsgericht in diesem Zusammenhang auf der Einschaltung eines Richters bestehen wollen, hätte es dies konkret zum Ausdruck gebracht und nicht von einer "unabhängigen Stelle" gesprochen.

Zu 5.1.1.3 DNA-Identifizierungsmuster von Kindern

Der Hessische Datenschutzbeauftragte ist der Auffassung, der Gesetzgeber habe bei der Schaffung des neuen § 19 Abs. 3 HSOG "übersehen, dass Kinder - da nicht strafmündig - keine Straftaten begehen können".

An dieser Auffassung ist zutreffend, dass Kinder nicht strafmündig sind. Das Strafgesetzbuch behandelt Kinder als schuldunfähig (§ 19 StGB), was aber nicht bedeutet, dass Kinder keine tatbestandsmäßigen und rechtswidrigen Straftaten begehen könnten. Im Polizeirecht kommt es auf die strafrechtliche Verantwortlichkeit gerade nicht an (u.a. Meixner/Fredrich, HSOG, 10. Aufl. 2005, § 6 Rdnr. 4f.; vgl. auch § 6 Abs. 2 HSOG, der von der polizeirechtlichen Verantwortlichkeit von Kindern ausgeht).

Die Landesregierung ist der Ansicht, dass der Landesgesetzgeber entgegen den Bedenken des Hessischen Datenschutzbeauftragten auch regelungsbefugt ist. Der Bundesgesetzgeber darf zwar im Wege der konkurrierenden Gesetzgebung Maßnahmen zur Vorsorge für die künftige Strafverfolgung selbst regeln und hat dies auch in Bezug auf alle anderen Fallgestaltungen fehlender Schuldfähigkeit im DNA-Identitätsfeststellungsgesetz getan. Dass er dabei die Fälle der Schuldunfähigkeit von Kindern, gegen die ein Strafverfahren überhaupt nicht statthaft ist, mit negativem Ergebnis in seine Überlegungen einbezogen hätte, ist nicht ersichtlich. Es lässt sich deswegen kei-

neswegs behaupten, das Bundesrecht entfalte insoweit eine Sperrwirkung. Zu dieser Frage sei ergänzend auf die Begründung des Gesetzentwurfs sowie auf die ausführlichen Darlegungen des als Sachverständigen angehörten Prof. Dr. Heckmann verwiesen.

Unzutreffend ist die Annahme des Hessischen Datenschutzbeauftragten, die DNA-Analyse nach § 19 Abs. 3 HSOG sei ein Mittel mit generalpräventiver Wirkung. Sie hätte dann das Ziel, andere Personen als den Betroffenen von der Begehung von Straftaten abzuhalten. Tatsächlich verfolgt die Vorschrift jedoch dezidiert spezialpräventive Ziele, d.h. es geht ihr darum, weitere Straftaten gerade derjenigen Person zu verhüten oder zumindest aufzuklären, deren DNA-Profil erfasst worden ist. Die DNA-Analyse ist ein besonders geeignetes Mittel zur Spezialprävention.

Die Ausführungen des Hessischen Datenschutzbeauftragten, nach denen die Regelung des HSOG zur DNA-Analyse für Kinder weiter gehe als die Befugnis des § 81g StPO zur DNA-Analyse von Jugendlichen, beruhen auf einem früheren Entwurfsstand. Der von der Landesregierung in den Landtag eingebrachte Entwurf hat § 19 Abs. 3 HSOG bereits eine Fassung gegeben, die derjenigen des § 81g StPO entspricht.

Schließlich sind auch die praktischen Bedenken des Hessischen Datenschutzbeauftragten nicht gerechtfertigt. Für Speicherung und Löschung der DNA-Formel gelten die allgemeinen Bestimmungen des HSOG (§§ 20, 27) sowie die Prüffristenverordnung. Eine Speicherung der Daten in der DNA-Datei des Bundeskriminalamts kommt demgegenüber derzeit wegen der Fassung der aktuellen Errichtungsanordnung, die nur im Einvernehmen von Bund und Ländern geändert werden kann, nicht in Betracht. Derartige Schwierigkeiten, die mit bescheidenem Aufwand lösbar sind, können jedoch kein Anlass sein, auf eine als richtig erkannte Lösung zu verzichten.

Zu 5.1.1.4 Kennzeichenerfassung

In Hessen wurde eine denkbar enge Variante der automatisierten Kennzeichenerfassung gewählt. Es dürfen nur amtliche Kennzeichen solcher Fahrzeuge automatisiert überprüft werden, die zur Fahndung ausgeschrieben sind. Aus welchen Gründen die Ausschreibung erfolgt ist, z.B. um gestohlene Kennzeichen aufzuspüren oder um eine gesuchte Person festzunehmen, die in ihrem Fahrzeug unterwegs ist, spielt hingegen keine Rolle. Fragen der Verhältnismäßigkeit stellen sich in diesem Zusammenhang nicht. Wenn die Fahndungsausschreibung als solche rechtmäßig, d.h. auch verhältnismäßig ist, kann es der Polizei nicht verwehrt sein, nach den Kennzeichen auf öffentlichem Straßenraum Ausschau zu halten. Der Schutz Unbeteiligter ist dadurch sichergestellt, dass das Gesetz die unverzügliche Löschung aller übrigen Daten vorschreibt.

Zu 5.1.1.5 Online-Zugriff der Gefahrenabwehrbehörden

Der Hessische Datenschutzbeauftragte kritisiert, dass der Hessischen Polizeischule und der Verwaltungsfachhochschule, die mit Aus- und Fortbildung der Polizeibeamten befasst sind, durch die Neufassung des § 24 HSOG ein Online-Zugriff auf die polizeilichen Datenbestände eröffnet wird. Im Gesetz seien "keinerlei Beschränkungen oder Rahmenbedingungen zur Wahrung des Grundsatzes der Erforderlichkeit" formuliert worden. Diese Ansicht ist jedoch unzutreffend.

Zunächst gehört die Benennung der Polizeischule und der Verwaltungsfachhochschule in § 24 HSOG zu denjenigen Änderungen, denen nur eine klarstellende Bedeutung zukommt. Anlass der Änderung war der Wunsch, den im HSOG mit unterschiedlichem Inhalt gebrauchten Begriff der "Polizeibehörde" nur noch einheitlich im engen Sinn des § 91 Abs. 3 Nr. 2 HSOG zu verwenden. Dies hätte beide Bildungseinrichtungen der Polizei vom bislang möglichen
Online-Zugriff ausgeschlossen, ebenso wie außerhessische Polizeibehörden. Daher wurden beide Fälle ohne Einschränkung besonders aufgeführt (§ 24 Abs. 1 Satz 2 Nr. 2 bzw. 3 HSOG).

Darüber hinaus enthält § 24 Abs. 1 Satz 2 HSOG zwar nur eine Voraussetzung für die Zulassung des Verfahrens, doch müssen auch die Voraussetzungen aus Satz 1 der Vorschrift erfüllt sein. Danach ist die Einrichtung eines automatisierten Abrufverfahrens lediglich zulässig, "soweit diese Form

der Datenübermittlung unter Berücksichtigung der schutzwürdigen Belange der betroffenen Personen und der Erfüllung von Aufgaben der beteiligten Stellen angemessen ist". Das HSOG übernimmt damit im Übrigen eine Formulierung für die Zulassung automatisierter Abrufverfahren aus § 15 Abs. 2 HDSG in der bis zum Jahr 1999 geltenden Fassung. Eine gleichartige Beschränkung findet sich im aktuellen Hessischen Datenschutzgesetz nicht mehr.

Zu 5.1.2 Automatisierte Kennzeichenerkennung
Zu 5.1.2.1 Möglichkeiten der Technik

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend.

Zu 5.1.2.2 Eingriff in das Recht auf informationelle Selbstbestimmung
Zu 5.1.2.3 Schaffung einer Rechtsgrundlage im Hessischen Polizeirecht

Es wird auf die Ausführungen zu Ziff. 5.1.1.4 verwiesen.

Zu 5.1.3 Prüfung polizeilicher Datenbestände bei den Polizeipräsidien Südhessen und Frankfurt am Main

Der Hessische Datenschutzbeauftragte hat bei den Polizeipräsidien Südhessen und Frankfurt am Main geprüft, ob Hinweise auf Betäubungsmittelkonsum in den polizeilichen Informationssammlungen rechtmäßig eingetragen wurden. Die Überprüfung ergab keine Beanstandungen. Die Landesregierung hat der Darstellung des Hessischen Datenschutzbeauftragten daher nichts hinzuzufügen.

Zu 5.1.4 Löschung polizeilicher Daten im Einzelfall

Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend.

Zu 5.1.5 Verwechselt: Datenschutzinteresse trotz "weißer Weste"

Der im Tätigkeitsbericht geschilderte Sachverhalt trifft nach einem aus Anlass dieser Stellungnahme eingeholten Bericht des Generalstaatsanwalts im Wesentlichen zu. Danach sind im Anschluss an den im Tätigkeitsbericht des Hessischen Datenschutzbeauftragten erwähnten Fall Maßnahmen ergriffen worden, um derartige Fehler bei Massenverfahren aus dem Bereich der Labormedizin, wie sie bei der "Arbeitsgruppe Ärzte" bearbeitet werden (derzeit mehr als 1.500 offene Ermittlungsverfahren), künftig auszuschließen. Ladungen zu einer Beschuldigtenvernehmung oder Bögen zur schriftlichen Anhörung werden nur noch über bereits bekannte Praxisanschriften, versehen mit dem Zusatz "persönlich" versandt. Die Umsetzung dieser Vorgabe durch die Ermittlungsbeamten wird vom sachbearbeitenden Staatsanwalt überwacht. Daneben ist die Gefahr von Ermittlungsfehlern bei der Feststellung von Personaldaten über sichergestellte Rechnungsunterlagen seit dem im Tätigkeitsbericht beschriebenen Vorfall regelmäßig Gegenstand der Dienstbesprechungen der "Arbeitsgruppe Ärzte". Ein vergleichbarer Vorfall ist bis heute nicht mehr festzustellen gewesen.

Zu 5.2 Justiz
Zu 5.2.1 Auskunftsverhalten der Staatsanwaltschaften

Die Kritik des Hessischen Datenschutzbeauftragten bezieht sich auf die Behandlung von Auskunftsverlangen von Bürgern, die bei den Staatsanwaltschaften Kassel, Marburg und Frankfurt am Main Auskunft über die zu ihrer Person gespeicherten Daten begehrten.

Aus Sicht der Landesregierung handelt es sich bei den im Tätigkeitsbericht aufgeführten Vorgängen um Einzelfälle, die nicht darauf schließen lassen, den hessischen Staatsanwaltschaften sei der Umfang des Auskunftsrechts nach §§ 491 Abs. 1 StPO, 19 BDSG nicht bekannt.

Die Landesregierung stimmt mit dem Hessischen Datenschutzbeauftragten darin überein, dass es auch unter datenschutzrechtlichen Gesichtspunkten akzeptabel ist, wenn eine Behörde in einer besonderen Belastungsphase zur Erfüllung eines Auskunftsverlangens länger als üblich benötigt. Diese Einschätzung steht im Einklang mit der in Nr. 184 der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) enthaltenen Regelung des Vorrangs der Verfahrensbearbeitung vor der Gewährung von Auskünften und Akteneinsicht. Insbesondere wenn eine besondere Belastungsphase der Staatsanwalt-

schaft und ein sehr umfangreiches, nicht ohne Auswertung der Akten zu beantwortendes Auskunftsverlangen zusammentreffen, kann es dem Bürger ausnahmsweise zugemutet werden, auch einen deutlich überdurchschnittlichen Zeitraum bis zur Beantwortung seiner Anfrage hinzunehmen.

Zu 5.3 Ausländerrecht
Zu 5.3.1 Digitales Einbürgerungssystem

Die Darstellung im Tätigkeitsbericht ist zutreffend. Der Hessische Datenschutzbeauftragte war bereits in der Projektentwicklung beteiligt und hat sowohl bei der Erarbeitung der Verfahrensverzeichnisse nach §§ 6, 15 HDSG als auch bei der Formulierung der Rechtsgrundlage für das Digitale Einbürgerungssystem beraten. Letztere ist in § 3 Abs. 2 des "Gesetzes zur Bestimmung der zuständigen Behörden in Staatsangehörigkeitsangelegenheiten" vom 21. März 2005 (GVBI. I S. 234) enthalten; das Gesetz ist am 1. April 2005 in Kraft getreten.

Die Pilotanwendung wurde am 1. April 2005 gestartet. Bis heute sind die Regierungspräsidien Darmstadt, Gießen und Kassel, die Gemeinde Büttelborn, die Stadt Gießen und der Landkreis Schwalm-Eder beteiligt. Das Landeskriminalamt und das Landesamt für Verfassungsschutz wurden integriert, zum Statistischen Landesamt besteht eine Schnittstelle. Es ist beabsichtigt, das Verfahren auch mit der Stadt Frankfurt am Main zu erproben. Die dabei gewonnenen Erfahrungen sowie mögliche Verfahrensanpassungen werden mit dem Hessischen Datenschutzbeauftragten erörtert.

Zu 5.3.2 Auskunftspflicht nur bei tatsächlichen Ausländervereinen

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die Auskunftspflicht nach § 20 der Durchführungsverordnung zum Vereinsgesetz nur besteht, wenn es sich tatsächlich um einen Ausländerverein handelt. Es ist aus der Praxis jedoch bekannt, dass im Einzelfall gerade die Klärung der Frage, ob es sich um einen Ausländerverein handelt, für die Behörde problematisch sein kann. Das ist dann der Fall, wenn der Verein selbst Anhaltspunkte für die Annahme eines Ausländervereins geschaffen hat, z.B. durch eine frühere Meldung, auf eine Nachfrage der Behörde aber bestreitet, dass er die im Gesetz genannten Voraussetzungen erfüllt. In einem entsprechenden Fall hat das Ministerium des Innern und für Sport die zuständige Ordnungsbehörde ebenfalls auf die Rechtslage hingewiesen.

Zu 5.4 Landesplanung und Planfeststellung

Die Landesregierung schließt sich der Auffassung des Hessischen Datenschutzbeauftragten zum Umgang mit den personenbezogenen Daten der Einwender im Planfeststellungsverfahren gegen den Ausbau des Flughafens Frankfurt am Main an.
Das Regierungspräsidium Darmstadt als Anhörungsbehörde wird entsprechend verfahren.

Zu 5.5 Schulverwaltung, Schulen und sonstige Bildungseinrichtungen
Zu 5.5.1 Pilotprojekt EDUNITE

Das Projekt EDUNITE wurde durch den Hessischen Datenschutzbeauftragten selbst datenschutzrechtlich begleitet und dies im Projektverlauf als positiv und hilfreich empfunden. Die Landesregierung geht von einer weiterhin guten Zusammenarbeit im Zusammenhang mit diesem Projekt aus.

Zu 5.5.2 Ergebnisse der Prüfung einer Schule

Die vom Hessischen Datenschutzbeauftragten in seinem Bericht dargestellte datenschutzrechtliche Überprüfung einer Schule hat mehrere - teilweise bereits bekannte - Schwachstellen des Datenschutzes in Schulen deutlich gemacht. Die Probleme werden im Zuge der zurzeit laufenden Neufassung der Verordnung über die Verarbeitung personenbezogener Daten in Schulen aufgegriffen. Dabei wird auch auf die den Schulträgern obliegende Ausstattung der Schulen mit Hard- und Software ebenso wie auf die Möglichkeiten der Nutzung freier Software einzugehen sein. Zu einem erheblichen Teil sind die Mängel jedoch nicht auf mangelhafte bzw. fehlende Ausstattungen zurückzuführen. Daher wird bereits jetzt verstärkt, aber in besonderer Weise im Zuge der Novellierung der Verordnung durch das Kultusministerium und die Schulaufsicht auf die vom Hessischen Datenschutzbeauftragten darge-

stellten Mängel und auf die Verpflichtung aller in den Schulen Tätigen zur Einhaltung der datenschutzrechtlichen Vorschriften hingewiesen werden.

Zu 5.6 Hochschulen
Zu 5.6.1 Prüfung der Universität Marburg

Der Hessische Datenschutzbeauftragte sieht noch Probleme in der Umsetzung des seit dem Jahre 1999 geltenden Hessischen Datenschutzgesetz bei verschiedenen Verwaltungsbereichen der Universität Marburg. Er bemängelt vor allem, dass die Anpassung an das neue Recht nicht immer erfolgt ist.
Alle Anregungen und Veränderungsvorschläge des Hessischen Datenschutzbeauftragten hat die Universität Marburg positiv aufgenommen und beabsichtigt diese umzusetzen.

Die Landesregierung gibt jedoch auch zu bedenken, dass es bei entsprechend großen Verwaltungseinheiten, die eine erhebliche Zahl von Prozessen mit Formularen abwickeln, aus wirtschaftlichen Gründen nicht immer zeitnah möglich ist, das Formularwesen an neue gesetzliche Vorschriften anzupassen. Demzufolge kann es vorkommen, dass im Einzelfall auch noch vorhandene ältere Formulare aufgebraucht werden.

Zu 5.6.2 Beratung der Hochschule für Musik und Darstellende Kunst in Frankfurt am Main

Der Hessische Datenschutzbeauftragte bemängelt die Hilfestellung der Hochschul-Informations-System GmbH (HIS).

Die HIS GmbH wird seit dem Jahr 1992 durch Bund und Länder finanziert. Diese Gesellschaft hat nach der Satzung den Zweck, die Hochschulen und die zuständigen Verwaltungen in ihrem Bemühen um eine rationale und wirtschaftliche Erfüllung der Hochschulaufgaben durch

- Entwicklung von Verfahren zur Rationalisierung der Hochschulverwaltung sowie Mitwirkung bei deren Einführung und Anwendung,
- Untersuchungen und Gutachten zur Schaffung von Entscheidungsgrundlagen,
- Entwicklung von Grundlagen für den Hochschulbau,
- Bereitstellung von Informationen und Organisation zum Informationsaustausch

zu unterstützen.

Nach § 6 Abs. 1 der HIS-Satzung stellen die Gesellschafter die zur Erfüllung des Satzungsauftrags erforderlichen Mittel - soweit keine Einnahmen entstehen - als Zuwendungen im Sinne der §§ 23, 44 Bundeshaushaltsordnung bzw. Landeshaushaltsordnungen zur Verfügung. HIS führt sein von den HIS-Organen beschlossenes Arbeitsprogramm überwiegend mit den Mitteln aus der institutionellen Förderung durch. Im Rahmen dieser Tätigkeit ist auch die Unterstützung bei der Erstellung einer Vorabkontrolle nach § 7 Abs. 6 HDSG für einen Informations- und Kommunikationsserver bei der Hochschule für Musik und Darstellende Kunst in Frankfurt am Main zu verstehen.

Der Hessische Datenschutzbeauftragte unterstellt bei seiner Kritik, die HIS GmbH lasse bei der Vorabkontrolle ihre Produkte und Dienstleistungen aus wirtschaftlichem Interesse in einem zu guten Licht erscheinen. Er vermutet eine Interessenkollision. Der Hessische Datenschutzbeauftragte lässt bei seiner Beurteilung jedoch außer Acht, dass gerade eine Einrichtung wie die HIS GmbH, die bundesweit den Einsatz von Verwaltungsverfahren bei den Hochschuleinrichtungen unterstützt, kein eigenes wirtschaftliches Interesse verfolgt und ganz besonderen Wert darauf legt, alle datenschutzrechtlichen Vorschriften einzuhalten. Bisher sind keinerlei Verstöße bekannt geworden, wo durch mangelhafte technische oder organisatorische Maßnahmen der HIS GmbH, als verantwortlich Tätige, die geschützten Rechte der Betroffenen gefährdet waren.

Unabhängig von dieser Bewertung haben die Bedenken des Hessischen Datenschutzbeauftragten bei der Hochschule für Musik und Darstellende Kunst in Frankfurt am Main Beachtung gefunden. Die Hochschule hat die Vorabkontrolle nunmehr selbst konzipiert und ihrem Datenschutzbeauftragten nach § 7 Abs. 6 Satz 3 HDSG zur Prüfung vorgelegt.

Zu 5.7 Forschung und Statistik
Zu 5.7.1 Aufbau eines Forschungsdatenzentrums der Statistischen Landesämter
Zu 5.7.1.1 Aufgabe und Ziel des Forschungsdatenzentrums
Zu 5.7.1.2 Datenschutzkonzept

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Zwischenzeitlich wurde durch die Änderungen des Bundesstatistikgesetzes (Gesetz zur Änderung des Statistikregistergesetzes und sonstiger Statistikgesetze vom 9. Juni 2005, BGBl. I S. 1534) eine Rechtsgrundlage geschaffen.

Zu 5.7.1.3 Ämterübergreifende Aufgabenerledigung

Mit der oben zu Ziff. 5.7.1.1 und 5.7.1.2 erwähnten Rechtsgrundlage ist auch die Rechtsgrundlage für eine Rahmenvereinbarung (Verwaltungsvereinbarung) geschaffen worden.

Hinsichtlich der erwähnten Plausibilitätsprüfungen werden Überprüfungen gegenüber den Auskunftspflichtigen auch künftig von dem unmittelbar zuständigen Statistischen Amt vorgenommen werden. Die Übertragung dieser Aufgabe wird nicht vorgenommen.

Die Ansicht, dass die ämterübergreifende Aufgabenerledigung einer weitergehenden Rechtsgrundlage, als die der verabschiedeten Regelung bedarf, wurde mit den Dienstaufsichtsbehörden der statistischen Ämter der Länder und des Bundes erörtert. Die Dienstaufsichtsbehörden haben dieser Auffassung einvernehmlich nicht zugestimmt.

Zu 5.8 Gesundheitswesen
Zu 5.8.1 Aufbewahrung und Verwendung von Blut- und Gewebeproben in hessischen Krankenhäusern

Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten zur Praxis in den Krankenhäusern zur Kenntnis genommen und sieht dem Ergebnis seiner Gespräche mit den Universitätskliniken mit Interesse entgegen.

Zu 5.8.2 Zusammenarbeit des Medizinischen Dienstes der Krankenversicherung Hessen mit dem Medizinischen Dienst der Krankenversicherung Sachsen-Anhalt

Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten über die Zusammenarbeit der Medizinischen Dienste aus Hessen und Sachsen-Anhalt zur Kenntnis genommen und begrüßt es, dass die beanstandeten datenschutzrechtlichen Defizite bereits behoben wurden.

Zu 5.8.3 Durchführung strukturierter Behandlungsprogramme durch die AOK Hessen

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu. Die AOK Hessen hat mitgeteilt, dass die bemängelten zu weit gehenden Zugriffsberechtigungen bei der Anwendung des DIMAS-Programms auf das erforderliche Maß beschränkt wurden. Die Kritik am Verfahren der Protokollierung der Datenzugriffe wurde an den zuständigen AOK Bundesverband weitergeleitet. Zurzeit ist eine neue Programmversion in der Entwicklungsphase, bei der die Ausgestaltung der Protokollierung berücksichtigt werden soll. Sobald die neue Version des Programms vorliegt wird das Sozialministerium prüfen, ob die Vorgaben des Hessischen Datenschutzbeauftragten berücksichtigt worden sind.

Zu 5.9 Sozialwesen
Zu 5.9.1 Modellprojekt Wiesbaden / Unterhaltsvorschussgesetz

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 5.9.2 Zusammenarbeit Sozialamt und Polizei

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 5.9.3 Unverschlüsselte Sozialdatenübermittlung per E-Mail

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 5.9.4 Datenübermittlung nach Israel

Die jährliche Vorlage von Lebensbescheinigungen durch Bezieher von Renten nach dem Bundesentschädigungsgesetz (BEG) in Israel soll durch einen Abgleich bestimmter Daten des Regierungspräsidiums Darmstadt als Entschädigungsbehörde mit den Meldedaten des israelischen Innenministeriums abgelöst werden. Wegen der dazu erforderlichen Übermittlung personenbezogener Daten in das Ausland war die Einschaltung des Hessischen Datenschutzbeauftragten geboten. Dessen Beurteilung des Sachverhalts und die im Oktober 2003 und Juni 2004 erteilten Verfahrensvorschläge wurden übernommen.

Das Vorhaben befindet sich noch in der Abstimmungsphase zwischen den Ländern und dem Bundesfinanzministerium einerseits und den beteiligten israelischen Stellen andererseits. Dabei geht es um die Festlegung der technischen Einzelheiten des Datentransfers, die Datensicherheit und um Zugriffsrechte. Erst danach wird ein Vertragsabschluss erfolgen. Zur Vermeidung von Missverständnissen und Verunsicherungen bei den Rentenbeziehern ist deren Zustimmung zu dem Verfahren noch nicht eingeholt worden. Hiermit soll noch gewartet werden, bis die technischen Fragen geklärt sind und der Beginn des Datenabgleichs absehbar ist. Sobald in der Sache weitere nennenswerte Verfahrensschritte eingetreten sind, ist ein ergänzender Bericht an den Hessischen Datenschutzbeauftragten beabsichtigt.

Zu 5.9.5 Zusammenarbeit Kindergarten und Schule

Nach Auffassung der Landesregierung ist es aus pädagogischen Gründen sinnvoll und notwendig, dass sich Kindergarten und Schule über die einzuschulenden Kinder austauschen. Gleichwohl haben die Eltern das Entscheidungsrecht über diesen Informationsaustausch. In pädagogisch positiv zu wertendem Bestreben wird dabei offenbar das informationelle Selbstbestimmungsrecht der Kinder bzw. Eltern nicht selten übersehen. Hier wird durch das Kultusministerium und die Schulaufsichtsbehörde verstärkt auf die Notwendigkeit der Einhaltung der datenschutzrechtlichen Bestimmungen hingewiesen werden.

Die Landesregierung stimmt dem Verfahrensvorschlag des Hessischen Datenschutzbeauftragten, künftig auf eine stärkere Einbindung der Eltern in der Kooperation von Kindergarten und Schule zu achten, zu. Die Landesregierung hat die Thematik der Beachtung des Sozialdatenschutzes in den Entwurf des Hessischen Bildungs- und Erziehungsplanes aufgenommen.

Zu 5.10 Finanzwesen

Zu 5.10.1 "FinanzServiceCenter" in hessischen Finanzämtern

Die Feststellungen des Hessischen Datenschutzbeauftragten waren berechtigt. Seine Anregungen zur räumlichen Gestaltung der Finanzservicestellen und den dortigen Geschäftsprozessen unter dem Gesichtspunkt der Diskretion werden aufgenommen und im Rahmen der jeweils bestehenden Möglichkeiten vor Ort berücksichtigt werden.

Zu 5.11 Personalwesen

Zu 5.11.1 Entwurf des Hessischen Disziplinargesetzes

Zur Entwurfsfassung des Hessischen Disziplinargesetzes (HDG-E) sieht der Hessische Datenschutzbeauftragte Klärungsbedarf hinsichtlich des Belassens von Disziplinarvorgängen in der Personalakte nach Eintritt des Verwertungsverbotes (§ 19 Abs. 3 HDG-E). Diese Kritik am Entwurf des HDG wurde im Rahmen der vorgeschriebenen Anhörung im Gesetzgebungsverfahren geltend gemacht, welches noch nicht abgeschlossen ist. Aus diesem Grunde erfolgte keine Beantwortung, wobei die Anregung inhaltlich jedoch Berücksichtigung fand.

Im ursprünglichen Entwurf des § 19 Abs. 3 in Art. 1 des Gesetzes zur Neuordnung des Disziplinarrechts verblieben der Tenor der eine Kürzung des Ruhegehalts aussprechenden Entscheidung, und der Tenor der eine Zurückstufung aussprechenden Entscheidung nach Eintritt des Verwertungsverbots in der Personalakte. Nach Überarbeitung konnte der Entwurf dahingehend

geändert werden, dass eine Aufbewahrung nur derjenigen Entscheidung weiter notwendig ist, die eine Zurückstufung ausspricht. Das eine Zurückstufung aussprechende Gerichtsurteil stellt einen sich auf das Beamtenverhältnis direkt auswirkenden statusrechtlichen Akt dar, der nicht durch andere Schriftstücke, z.B. eine Urkunde, dokumentiert wird. Späteren besoldungs- und versorgungsrechtlichen Entscheidungen in diesem Beamtenverhältnis würde die Grundlage fehlen. Deshalb müssen Rubrum und Tenor desjenigen Urteils, das die Zurückstufung ausspricht, in der Personalakte verbleiben. Alle übrigen Unterlagen können nach Zeitablauf vernichtet werden.

Die disziplinarrechtliche Entscheidung über eine Ruhegehaltskürzung kann demgegenüber nach Eintritt des Verwertungsverbotes entfernt werden, da gewährleistet ist, dass die Aufbewahrung solange erfolgt wie die Maßnahme vollstreckt wird. Über diesen Zeitraum hinaus ist auch aus kassentechnischer Sicht eine Aufbewahrung nicht mehr erforderlich.

Das Bundesministerium des Innern hat einen Entwurf zur Änderung des Bundesdisziplinargesetzes vorbereitet, in dem die Aufbewahrungsvorschriften entsprechend obiger Darlegung erweitert worden sind.

Zu 5.11.2 Rechtswidrige Aufbewahrung von Lebensläufen

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 5.11.3 Informationsrechte der Schwerbehindertenvertretung

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 6. Kommunen
Zu 6.1 Outsourcing bei der Stadt Wiesbaden

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.
Die vorgeschlagene Ergänzung von § 4 Abs. 3 HDSG wird bei der nächsten Initiative zur Änderung des Gesetzes von der Landesregierung berücksichtigt werden.

Zu 6.2 Prüfung einer Stadtbibliothek

Die Landesregierung nimmt auf die Fassung der Bibliothekssatzungen kommunaler Bibliotheken keinen Einfluss. Es wäre jedoch zu begrüßen, wenn die vom Hessischen Datenschutzbeauftragten in seinem Bericht gegebenen Hinweise auf rechtlich bedenkliche Formulierungen in den Bibliothekssatzungen, die exemplarisch bei einer Stadtbibliothek festgestellt wurden, dazu beitragen, dass solche irreführenden Formulierungen zukünftig auch bei anderen Bibliotheken gestrichen werden.

Zu 6.3 Datenübermittlung des Datums "Lebenspartnerschaft führend" an öffentlich-rechtliche Religionsgesellschaften

Die Landesregierung stimmt den Darlegungen des Hessischen Datenschutzbeauftragten zu. Der Entwurf der Landesregierung für ein Drittes Gesetz zur Änderung des Hessischen Meldegesetzes (Drucks. 16/4067) sieht daher eine Übermittlung der Angaben über das Führen einer Lebenspartnerschaft an Religionsgemeinschaften nicht vor.

Zu 6.4 Datenbankprotokolle im Einwohnerwesen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 6.5 Unzulässige Datenübermittlung eines Ordnungsamtes an das Taxigewerbe im Zusammenhang mit der Rückkehrpflicht von Mietwagen

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass bei Kontrollen zur Rückkehrpflicht von Mietwagenfahrern das Ordnungsamt private Dritte nicht beteiligen sowie Feststellungen von Rechtsverstößen nicht routinemäßig an Dritte übermitteln darf. Es ist zu begrüßen, dass die beanstandeten Mängel in dem behandelten Einzelfall

umgehend von dem Ordnungsamt der entsprechenden Kommune behoben wurden.

Zu 6.6 Erhebung der Steuernummer durch ein Versorgungsunternehmen

Es trifft nicht zu, dass in dem vom Hessischen Datenschutzbeauftragten geschilderten Sachverhalt die Mitteilung der Steuernummer auf freiwilliger Basis erfolgt. Hat sich der Betreiber einer Fotovoltaikanlage dafür entschieden, Umsätze der Umsatzsteuer zu unterwerfen, um damit den Vorsteuerabzug aus den Herstellungskosten geltend machen zu können, und mit dem Versorgungsunternehmen eine Abrechnung im Wege des Gutschriftsverfahrens vereinbart, ist er verpflichtet, dem Aussteller der Gutschrift seine Steuernummer bekannt zu geben. Dies gilt auch, wenn beim leistenden Unternehmer die Umsatzsteuer nach § 19 Abs. 1 UStG nicht erhoben wird (Abschnitt 185 Abs. 7 UStR).

Eine Gutschrift ist eine Rechnung, die vom Leistungsempfänger ausgestellt wird (§ 14 Abs. 2 Satz 2 UStG, Abschnitt 184 Abs. 1 Satz 1 UStR 2005). Damit müssen Gutschriften auch alle für Rechnungen geltenden Pflichtangaben, unter anderem die dem leistenden Unternehmer vom Finanzamt erteilte Steuernummer (§ 14 Abs. 4 Nr. 2 UStG), enthalten. Fehlende Pflichtangaben führen nach § 15 Abs. 1 Satz 1 Nr. 1 Satz 2 UStG zur Versagung des Vorsteuerabzugs beim Leistungsempfänger (Gutschriftsaussteller). Der Gutschriftsaussteller muss sich deshalb die Pflichtangaben, die ihm nicht selbst zugänglich sind, beschaffen, um die Gutschrift korrekt ausstellen zu können. Ansonsten verstößt er gegen § 14 Abs. 4 UStG und darf keinen Vorsteuerabzug aus der Gutschrift vornehmen. Haben die am Leistungsaustausch Beteiligten wirksam die Abrechnung im Gutschriftsverfahren vereinbart, hat der leistende Unternehmer (Gutschriftsempfänger) dem Aussteller der Gutschrift zwingend seine Steuernummer mitzuteilen, da dieser sonst nicht in der Lage ist, alle Pflichtangaben korrekt in die Gutschrift aufzunehmen. Diese Verpflichtung ist in Abschnitt 185 Abs. 4 Satz 7 der nach Art. 108 Abs. 7 GG von der Bundesregierung mit Zustimmung des Bundesrates erlassenen Umsatzsteuer-Richtlinien 2005 festgelegt.

Zu 6.7 Datenspeicherung im Zusammenhang mit dem Kauf einer Dauerkarte für ein Thermalbad

Der Landesregierung ist dieser Sachverhalt erst durch den Bericht des Hessischen Datenschutzbeauftragten bekannt geworden; sie stimmt seiner Bewertung zu.

Zu 7 Sonstige Selbstverwaltungskörperschaften und Kammern

Zu 7.1 Unzulässigkeit der Weitergabe von Daten aus Auskünften von Postdiensteanbietern durch die Industrie- und Handelskammern

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten, dass die Weitergabe von Daten aus Auskünften von Postdiensteanbietern durch die Industrie- und Handelskammern aufgrund des § 13 Abs. 1 Gesetz über Unterlassungserklärungen bei Verbraucherrechts- und anderen Verstößen unzulässig ist, zu.

Zu 8. Entwicklungen und Empfehlungen im Bereich der Technik und Organisation

Der Hessische Datenschutzbeauftragte problematisiert in seinem Tätigkeitsbericht grundlegende Fragen der IT-Strategie der Landesregierung, insbesondere

- die Zentralisierungsstrategie,
- die elektronische Signatur und
- die Verschlüsselung von Informationen.

Die damit zusammenhängenden sicherheitsrelevanten Aspekte sind bereits wichtige Eckpfeiler bei der IT-Strategie der Landesverwaltung. Wie die folgende Aufzählung belegt, werden im Rahmen der E-Government-Initiative erhebliche Anstrengungen unternommen, um die Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit der Informationen sicherzustellen.

- Die Empfehlungen des Hessischen Rechnungshofs im Rahmen der Querschnittsprüfung "IT-Sicherheit" wurden beim Aufbau der E-Government-Organisation und der IT-Architektur berücksichtigt.
- Auf Empfehlung des Hessischen Rechungshofs wurde eine ressortübergreifende Sicherheitsorganisation etabliert, um einen homogenen Sicherheitsstandard in der Hessischen Landesverwaltung zu gewährleisten und die Dienst- und Fachaufsicht in diesem Bereich zu schärfen.
- Sicherheitsrelevante Fragestellungen werden mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) abgestimmt, um die sicherheitstechnische Aufwärtskompatibilität zum Bund und der Europäischen Union sicherzustellen.
- Hessen wird als erstes Bundesland einen verfahrens- und organisationsübergreifenden Verzeichnisdienst mit einer Schnittstelle zu SAP HR aufbauen, um eine tagesaktuelle Benutzerverwaltung und Rechtevergabe sicherzustellen.
- Hessen ist Mitglied im Signaturbündnis und hat als erstes Bundesland eine durchgängige Strategie zur Einführung der elektronischen Signatur.
- Mit Zentralisierung und Professionalisierung soll die Verfahrenssicherheit im Management der IT-Infrastruktur erhöht werden.
- Mit der Standardisierung der IT-Verfahren soll ein homogenes Sicherheitsniveau erreicht werden.

Die genannten Maßnahmen verfolgen alle das Ziel, das Sicherheitsniveau der Informationstechnik in der Landesverwaltung so hoch wie möglich zu halten. Besonderes Augenmerk liegt dabei auf dem jeweils schwächsten Glied eines IT-Verfahrensprozesses. Dabei dürfen jedoch drei Aspekte nicht aus den Augen verloren werden:

- Absolute Sicherheit wird sich nach derzeitigem Kenntnisstand nie erreichen lassen.
- Der Aufwand zur Erhöhung der Sicherheit muss im Sinne von § 10 Abs. 1 Satz 2 HDSG in einem angemessenen Verhältnis zum Schutzzweck stehen.
- Das größte Risiko der IT-Sicherheit ist der Mensch, insbesondere wenn er fahrlässig oder vorsätzlich gegen geltende Normen verstößt oder von der Komplexität des Verfahrens überfordert wird.

Unter Berücksichtigung dieser Aspekte orientiert sich die IT-Sicherheitsstrategie der Landesregierung an folgenden Grundsätzen:

- Die Sicherheit kann nur sukzessive erhöht werden, dabei liegt die Priorität auf den jeweils höchsten Risiken.
- Hessen steht in engem Kontakt zu seinen strategischen Lieferanten, um seine sicherheitsspezifischen Anforderungen in den Produktentwicklungsprozess einzubringen.
- Sicherheitstechnische Maßnahmen werden auf Grundlage am Markt verfügbarer Standardprodukte realisiert. Die Entwicklung eigener Produkte oder die hessenspezifische Änderung von Standardprodukten wird aufgrund der damit zusammenhängenden betrieblichen und finanziellen Risiken grundsätzlich abgelehnt.
- Hessen orientiert sich bei der Entwicklung seiner IT-Strategie an anderen öffentlichen Stellen und großen Wirtschaftsunternehmen und strebt hier eine Positionierung im oberen Bereich an.
- Risiken, die sich aus fahrlässiger oder vorsätzlicher Handlungsweise ergeben, können nach derzeitigem Stand der Technik nur reduziert, nicht jedoch eliminiert werden. Dabei ist zu berücksichtigen, dass Beamte und Angestellte einer besonderen Treuepflicht unterliegen.
- Bei allen Maßnahmen zur Erhöhung der IT-Sicherheit muss der Mensch und sein Verhalten berücksichtigt werden. Hierzu gehört auch die Erfahrung, dass Sicherheitsvorkehrungen umgangen werden, wenn sie aufgrund der Komplexität den Arbeitsablauf behindern.

Vor diesem Hintergrund kann es bei der Entwicklung einer umfassenden IT-Strategie, die rechtlichen, wirtschaftlichen und sicherheitstechnischen Anforderungen genügen muss, naturgemäß zu unterschiedlichen Bewertungen und Prioritäten kommen. Den Bewertungen des Hessischen Datenschutzbe-

auftragten in seinem Tätigkeitsbericht kann die Landesregierung nicht in allen Punkten folgen.

Thema Zentralisierung
Nach Ansicht des Hessischen Rechnungshofs können die baulichen und organisatorischen Anforderungen an eine sichere E-Government-Architektur nur durch einen zentralen Betrieb mit der erforderlichen Professionalität erfüllt werden. Das vom Hessischen Datenschutzbeauftragten angeführte Risiko des Eintritts eines Super-GAUs als mögliche Folge der Zentralisierung, ist grundsätzlich nicht von der Hand zu weisen. Es wurden jedoch bereits Maßnahmen ergriffen, die das Risiko eines vollständigen Datenverlusts auf ein Minimum reduzieren.

Die Daten können an zwei Standorten (Wiesbaden und Hünfeld) gespeichert und ständig synchronisiert werden. Im Falle einer Störung wird der Anwender automatisch auf das intakte System geleitet. Darüber hinaus wird mit der doppelten Speicherung das Risiko eines Totalverlusts im Katastrophenfall minimiert.

Die gespeicherten Daten werden automatisch als dritte Kopie archiviert. Diese Archive unterliegen einem automatischen Refreshzyklus, um eine dauerhafte Speicherung sicherzustellen.

Der zentrale Betrieb der IT-Anwendungen geschieht auf einem hohen professionellen Niveau. Die entsprechenden Service-Prozesse entsprechen internationalen IT-Standards. Dieses Niveau kann wirtschaftlich nur dann erreicht werden, wenn der Betrieb auf möglichst wenige Stellen konzentriert wird, also zentral erfolgt.

Bereits heute findet eine sichere zentrale Verarbeitung von Informationen mit mindestens gleichem Schutzbedarf erfolgreich statt. Die Daten der Polizei, die zum Teil Leben und Unversehrtheit von Personen betreffen, werden ebenso wie Daten der Justiz- und Steuerverwaltung in der HZD, also an zentraler Stelle, verarbeitet und vorgehalten. Die Erfahrung zeigt, dass mit diesen Daten sorgfältig umgegangen wird und keine Vorkommnisse bekannt geworden sind, die die vom Hessischen Datenschutzbeauftragten geäußerten Bedenken begründen würden. Gründe bei der Einführung eines Dokumenten-Managementsystems einen höheren Schutzbedarf festzustellen, als für die bereits zentral betriebenen IT-Verfahren der Polizei und der Steuerverwaltung, sind für die Landesregierung nicht erkennbar.

Zwingende Voraussetzung für einen gleichermaßen wirtschaftlichen wie sicheren Betrieb der IT-Infrastruktur der Landesverwaltung ist eine einheitliche Konfiguration der Endgeräte. Die derzeit vorhandene Infrastruktur ist historisch in Folge einer nicht vorhandenen IT-Strategie heterogen gewachsen und teilweise bis heute noch ständigen Anpassungen unterworfen. In dieser Situation sind drei technisch grundsätzlich unterschiedliche Lösungsansätze denkbar, nämlich die Client-Server-Lösung, die Web-basierte Lösung und die Terminal-Server Lösung.

Alle Lösungen haben ihre spezifischen Vor- und Nachteile, die nur in direktem Zusammenhang mit der infrage kommenden Applikation und der zugehörigen Organisation in der Landesverwaltung abschließend bewertet werden können. Die grundsätzlichen Unterschiede der technischen Alternativen lassen sich folgendermaßen beschreiben:

Bei der Client-Server-Lösung sind die regelmäßig vorzunehmenden Anpassungen der Software (Releases, Sicherheitspatche, Bugfixe etc.) besonders komplex, da die Konfiguration der Server und der Clients häufig voneinander abhängen und eine heterogene Client-Server-Landschaft existiert. Die Anpassungen der Clients können in dieser Architekturkonstellation nicht zentral vorgenommen werden, sondern müssen dezentral in der Fläche erfolgen und sind damit in höchstem Maße ineffizient und fehleranfällig.

Diese Lösung kommt nicht nur wegen des hohen Administrationsaufwands, sondern insbesondere durch den damit verbundenem Zeitverzug bei sicherheitsrelevanten Maßnahmen nicht in Betracht. Nach vorherrschender Meinung der IT-Architekten entspricht diese Lösung nicht mehr dem Stand heutiger Technik.

Bei einer Web-basierten Lösung müssen sämtliche Dateninhalte vom Server zum Client transferiert werden. In direktem Vergleich zu den anderen Lösungen erhöht dies die Netzlast und damit die Übertragungskosten nicht unerheblich. Des Weiteren unterstützen Web-basierte Lösungen applikationsspezifisch aktive Web-Inhalte wie Active-X und Java, die bisher allgemein als Sicherheitsrisiko eingestuft wurden, da eine Zertifizierung und Verifizierung dieser aktiven Web-Inhalte technisch nur unzureichend möglich war. Zum Zeitpunkt der Einführung der meisten in Hessen genutzten Querschnittsverfahren waren diese Applikationen, z.B. SAP-GUI und DOMEA 3.x, zudem nicht Web-fähig.

Aus den vorgenannten Gründen wurde bis heute eine Web-basierte Lösung in der Regel abgelehnt. Die neuesten Entwicklungen zeigen jedoch, dass es einen neuen Trend zu Web-basierten Lösungen gibt. Die neuen Releases SAP ECC 5.0 und DOMEA 4.x ermöglichen im Rahmen ihrer technischen Weiterentwicklung Lösungen für die genannten Risiken, die früher nicht zur Verfügung standen. Die Einführung Web-basierter Lösungen ist deshalb zukünftig eine ernstzunehmende Alternative, die im Einzelfall zu prüfen ist.

Bei einer Terminal-Server Lösung wird lediglich der Bildschirminhalt von einem Terminalserver zum PC übertragen. Ein mögliches Sicherheitsrisiko besteht jedoch in einer technisch nicht umsetzbaren Ende-zu-Ende Verschlüsselung der Daten, weil diese im Klartext in dem Terminalserver verarbeitet werden müssen. Das Risiko einer unberechtigten Dateneinsichtnahme auf der Übertragungsstrecke zwischen PC und Terminalserver wird jedoch durch eine Citrix-Verschlüsselung minimiert. Im Rahmen der Einführung der digitalen Signatur kommt es zu neuen Fragestellungen, was z.B. den Speicherort und Zugriffsmöglichkeiten auf persönliche Zertifikate betrifft. Bei der Terminal-Server Lösung handelt es sich derzeit um die am weitesten verbreitete Lösung, weil die Wirtschaftlichkeit des Betriebes in einem angemessenen Verhältnis zur IT-Sicherheit steht.

Das Risiko des unberechtigten Zugriffs an zentraler Stelle auf Daten und Programme kann, wie oben beschrieben, nicht grundsätzlich ausgeschlossen werden. Die Landesregierung sorgt im Rahmen ihrer IT-Strategie sowie insbesondere auch in der Organisation und Fach- und Dienstaufsicht der HZD für einen verantwortungsvollen Umgang mit diesem Risiko. Dezentrale ressortspezifische Lösungen würden bei erheblich höheren Kosten das Sicherheitsproblem nicht lösen, weil dann zum einen eine wesentlich größere Anzahl vertrauenswürdiger Mitarbeiter zum Betrieb erforderlich wäre und zum anderen trotzdem weiterhin die gleichen Lieferanten der eingesetzten Produkte wie bei der zentralen Lösung benötigt würden. Das Know-how um diese Lösung wäre im Land auf viele Stellen bei erheblich niedrigerem Niveau verteilt und läge zentral auf Seiten der Lieferanten und Dienstleister außerhalb der Landesverwaltung.

Die Landesregierung ist deshalb überzeugt, dass eine dezentrale Lösung bei erheblich höheren Kosten keinen signifikanten Sicherheitsgewinn erbringen würde.

Abschließend soll zum Thema Zentralisierung das Beispiel der Datenzentrale "Dataport" angeführt werden. In dieser Datenzentrale betreiben die Bundesländer Hamburg und Schleswig-Holstein ihre IT-Dienstleistung gemeinsam an einer Stelle.
Im Bereich der Steuerdaten planen die Bundesländer Hamburg, Schleswig-Holstein und Mecklenburg-Vorpommern einen gemeinsamen Betrieb der Anwendungen und eine zentrale Bereitstellung der Daten.
Die Beispiele zeigen, dass auch andere Länder bei der Modernisierung ihrer IT-Verfahren auf die Zentralisierung setzen.

Thema elektronische Signatur
Hessen gehört zu den Bundesländern, die sich im Unterschied zu anderen bereits in hohem Maße auf den Einsatz der elektronischen Signatur vorbereiten. Auf die Einrichtung eines übergreifenden Verzeichnisdienstes, die PKI-Pilotierung und die Mitgliedschaft im Signaturbündnis wird an dieser Stelle verwiesen. Allerdings ist anzumerken, dass die Technologie noch in den Kinderschuhen steckt, was die Verfügbarkeit von praktisch einsetzbaren Produkten und die Integration in Anwendungen angeht.

Hessen steht in besonders engem Kontakt zu den Unternehmen Microsoft, Open Text und SAP, um seine konkreten Anforderungen in die Produktentwicklungen einfließen zu lassen. Im Gegenzug wird Hessen von den Unternehmen als kompetenter Partner akzeptiert. Die Unternehmen müssen aber auch stets die Interessen des Gesamtmarkts im Auge behalten. Es verbleibt letzten Endes in deren Verantwortung, inwieweit sie die hessischen Anforderungen in den Standardprodukten berücksichtigen.

Die Entwicklung eigener Produkte oder die hessenspezifische Änderung von Standardprodukten wird aufgrund der damit zusammenhängenden betrieblichen und finanziellen Risiken grundsätzlich abgelehnt. Es werden, wie oben bereits erläutert, nur Standardprodukte eingesetzt.

Die Standardprodukte erfüllen zurzeit noch nicht alle Anforderungen der Landesverwaltung und des HDSB. Als Beispiel hierfür sei die Restriktion der verwendeten NetkeyE4-Karte genannt. Auf der Karte sind zwei Container für die Speicherung von PINs vorgesehen. Die PIN im ersten Container wird gemeinsam für die Freischaltung der Windows-Logon-Funktion, der Signatur und der Verschlüsselung verwendet. Die PIN im zweiten Container ist aus rechtlichen Gründen für die Freischaltung einer später zu installierenden qualifizierten Signatur vorgesehen. Bis zur Einführung der qualifizierten Signatur bleibt der zweite Container hierfür verbindlich reserviert.

Der Hessische Datenschutzbeauftragte weist mit Recht darauf hin, dass bei dieser Architektur die Signatur im ersten Container keine fortgeschrittene Signatur im Sinn des Signaturgesetzes sein kann, sondern nur eine elektronische Signatur.

Der Einsatz der Signatur wird dort angestrebt, wo es rechtlich vorgeschrieben ist oder die Verfahrenssicherheit erfordert.

Die Strategie zur Einführung der Signatur wird in enger Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) abgestimmt. Das BSI trägt Strategie und Lösungsansätze mit und hält sie für zielführend. Darüber hinaus wird die Landesregierung weiter den Markt beobachten und neue Produkte übernehmen, wenn dadurch die Sicherheit erhöht werden kann.

Thema Verschlüsselung bei der Dokumentenverwaltung
Grundsätzlich ist die Verschlüsselung ein geeignetes Mittel, um unbefugte Kenntnisnahme von Informationen durch Dritte deutlich zu erschweren. Bei Anwendung einer Verschlüsselung sind weitere Gesichtspunkte zu berücksichtigen.

Verschlüsselung bietet nur eine zeitlich begrenzte Sicherheit, da die heute bekannten Algorithmen mit zukünftiger Rechnerleistung und zukünftigem Erkenntnisfortschritt zu brechen sind. Die jahrtausende alte Geschichte der Kryptographie zeigt, dass bislang jede Verschlüsselung gebrochen wurde. Es ist nicht abzusehen, dass dieses allgemeingültige Gesetz der Kryptographie in der Zukunft außer Kraft gesetzt wird.

Verschlüsselung wird aufgrund der damit verbundenen Aufwände in der Regel nur dort angewendet, wo Geheimhaltungsvorschriften dies erfordern. In diesem Zusammenhang ist festzustellen, dass die IT-Infrastruktur der Landesverwaltung kein VS-System darstellt, d.h. dass Verschlusssachen ab VS-Vertraulich im Sinne der einschlägigen Verschlusssachenanweisung nicht in der betrachteten Infrastruktur verarbeitet und gespeichert werden dürfen.

Ein Hauptmerkmal eines Verschlüsselungsverfahrens ist, dass Informationen mit dem öffentlichen Schlüssel der möglichen Empfänger verschlüsselt werden müssen. Dies bedeutet, dass bereits zum Zeitpunkt der Verschlüsselung bekannt sein muss, wer diese Informationen später lesen soll.

Ein Verschlüsselungsverfahren hat eine begrenzte Gültigkeitsdauer. Zum einen werden die derzeitigen Signaturkarten und damit zwangsläufig auch das Verschlüsselungszertifikat mit einem Gültigkeitszeitraum von drei Jahren ausgegeben. Zum anderen kann ein solches Verfahren jederzeit durch die technische Weiterentwicklung als unsicher eingestuft werden. In beiden Fällen müssten alle betroffenen Dokumente mit dem alten ablaufenden Verfahren entschlüsselt und mit einem neuen, nach dem Stand der Technik si-

cheren Verfahren neu verschlüsselt werden. Dieser Aufwand ist für das Datenvolumen eines Dokumentenmanagementsystems (DMS) und eines Archivs schlichtweg weder handhabbar noch vertretbar.

Bei der Einführung von DOMEA sind weitere technische und funktionale Aspekte zu berücksichtigen. Ein wesentliches Merkmal eines DMS ist es, dass Dokumente anhand von Schlagworten oder mit Hilfe der Freitext recherche gesucht werden können. Eine Verschlüsselung würde die dafür erforderliche Indizierung technisch unmöglich machen. Die Zielsetzung des DMS würde verfehlt werden.

Die geplante langfristige Archivierung von Dokumenten würde stark behindert, weil es unmöglich ist, zum Zeitpunkt der Verschlüsselung zu wissen, wer die Dokumente bis zum Ablauf der vorgeschriebenen Aufbewahrungsfrist lesen darf. Hinzu kommt, dass die Verschlüsselung an natürliche Personen gebunden ist, die grundsätzlich zu jedem Zeitpunkt aus dem aktiven Dienst ausscheiden können.

In einer Dienststelle muss jederzeit die Möglichkeit bestehen, ein Dokument zu entschlüsseln und damit für den zuständigen Sachbearbeiter zugänglich zu machen, unabhängig von der Verfügbarkeit des Erstellers des Dokuments oder Bearbeiters der Akte, zu der es gehört. Theoretisch ließe sich das Problem mit einem Dienststellenschlüssel umgehen, der allen Mitarbeitern einer Dienststelle zugeordnet ist. Eine derartige Strategie würde dem Prinzip der Verschlüsselung jedoch zuwiderlaufen, weil in der Kryptographie der Grundsatz gilt: *"Ein verteilter Schlüssel ist ein offener Schlüssel."*

Die Landesregierung lehnt die grundsätzlich verschlüsselte Speicherung von Dokumenten im DMS deshalb ab. Die Dienststellen erhalten aber die Möglichkeit, die aus ihrer Sicht sensiblen Daten oder Daten, die aufgrund des Datenschutzrechts besonders schutzbedürftig sind, unter einen besonderen Zugriffsschutz zu stellen, zu verschlüsseln oder lokal zu speichern. Dazu werden am Markt verfügbare neue Produkte zur Verschlüsselung geprüft.

Thema Verschlüsselung bei der Kommunikation
Die Landesregierung wird den Dienststellen die Möglichkeit eröffnen, E-Mails, die aus Sicht der Dienststelle besonders zu schützende Daten enthalten oder Daten, die aus Gründen des Datenschutzrechts ein höheres Schutzbedürfnis aufweisen, durch Verschlüsselung zu sichern.

Zu 8.1 Probleme des E-Governments-Konzepts des Landes

Die Landesregierung erachtet ihr E-Government-Konzept als geeignet, die Anforderungen des Datenschutzrechts in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit zu erfüllen.

Zu 8.1.1 Anforderungen an zentrale IT-Verfahren und Strukturen

Vertraulichkeit
Die Landesregierung lehnt eine grundsätzlich verschlüsselte Speicherung aller Daten ab. Die bisherige Praxis bei der Verarbeitung der Daten von Polizei, Justiz und Steuerverwaltung durch die HZD zeigt, dass mit deren sensiblen Daten sorgfältig umgegangen wird, ohne dass bislang eine Verschlüsselung für erforderlich gehalten wurde.

Die Gemeinsame Geschäftsordnung der Ministerien des Landes Hessen (GGO) vom 14. Juli 1998 (StAnz. S. 2498) sieht bei der Behandlung von Posteingängen einschließlich E-Mails nur Einschränkungen für Verschlusssachen ab VS-Vertraulich vor (vgl. § 12). Für den Informationsaustausch mittels Papierdokumenten gibt es also ein Standardverfahren und ein besonders sicheres Verfahren für Dokumente mit höherer Schutzbedürftigkeit. Dieses bewährte Prinzip soll bei der Einführung der landesweiten IT-Verfahren beibehalten werden.

Die Landesregierung wird den Dienststellen die Möglichkeit eröffnen, Dokumente und E-Mails, die aus Sicht der Dienststelle sensible Daten enthalten oder Daten, die aus Gründen des Datenschutzrechts ein höheres Schutzbedürfnis aufweisen, durch Verschlüsselung zu sichern.

Integrität und Verbindlichkeit
Für die vom Hessischen Datenschutzbeauftragten als Beispiel genannte Anwendung DOMEA wird die Integrität der Daten durch eine entsprechende Schutztechnik der Software selbst und das Berechtigungsmanagement gewährleistet. Dieser Schutz verhindert, dass unautorisierte Dritte (z.B. Administratoren) Informationen manipulieren können. Darüber hinaus können Dokumente signiert abgelegt werden. Das Signieren von Dokumenten ist auch im Terminal-Server-Umfeld möglich. Die DATEV eG, Softwarehaus und der IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte, setzt mit ihrem System GERVA seit einiger Zeit eine entsprechende vom TÜVIT zertifizierte Lösung bei ihren Kunden ein.

Verfügbarkeit
Wie schon zur Zentralisierung ausgeführt, werden eine Reihe von Maßnahmen ergriffen, damit es nicht zu einem Super-GAU kommt und zudem eine sehr hohe Verfügbarkeit der Daten durch redundante Netze und entsprechende Back-Up-Konzepte sichergestellt wird.

Zu 8.1.2 Rechtliche Probleme beim vollständigen Übergang auf elektronische Dokumente

Das Einführungskonzept DOMEA sieht nicht vor, dass automatisch alle eingehenden Papierdokumente eingescannt und dann vernichtet werden sollen. Die Dienststellen, die DOMEA einführen, erstellen im Rahmen der Vorabkontrolle so genannte Negativlisten, in denen die Dokumenttypen aufgelistet sind, die nicht eingescannt werden, sondern in Papierform weiterbearbeitet werden.

Zu 8.2 Arbeitskreis "Zentrale IT-Security"

Die Landesregierung hat den Entwurf einer Schutzbedarfsfeststellung zur Kenntnis genommen und wird ihn nach Möglichkeit bei den weiteren E-Government-Projekten berücksichtigen.

Bei den E-Government-Projekten wurde im Bereich der IT-Sicherheit zunächst ein niedriger bis mittlerer Schutzbedarf unterstellt und die Maßnahmen auf dieses Niveau abgestellt. Für dieses Vorgehen sprach, dass schnell und ohne langwierige Schutzbedarfsanalysen übergreifend ein einheitliches und definiertes Sicherheitsniveau erreicht werden sollte. Außerdem sind Maßnahmen, die auf dieser Basis ergriffen wurden, in jedem Fall erforderlich und auch bei einer geänderten Schutzbedarfseinordnung nicht verloren. Dieser Weg wird auch vom BSI als angemessene Vorgehensweise beurteilt.

Zu 8.3 Problemfall "Organisations-Administrator"

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend. Mitarbeiter der Landesverwaltung haben den Hessischen Datenschutzbeauftragten maßgeblich dabei unterstützt, die Defizite des beschriebenen Verfahrens transparent zu machen. Teile der beschriebenen Prüfung wurden auf Anregung und unter Mitwirkung von Mitarbeitern der Landesverwaltung durchgeführt.

Das Konzept Active-Directory wurde im Rahmen des Projekts HCN-2004 grundlegend überarbeitet. In dieser Überarbeitung ist ein auf Delegation beruhendes abgestuftes Administrationskonzept enthalten.

Zu 8.4 Radio Frequency Identification (RFID)

Im Bereich E-Government der Hessischen Landesregierung ist der Einsatz der RFID-Technik nicht vorgesehen.

Die grundsätzlichen Ausführungen des Hessischen Datenschutzbeauftragten zu den Risiken dieser neuen Technik wurden zur Kenntnis genommen und werden berücksichtigt, falls die RFID-Technik einmal in einem Automationsprojekt eingesetzt werden sollte.

Zu 8.5 Anforderungen an die Ausgestaltung eines Meta-Directory

Die Landesregierung hat der Kritik des Hessischen Datenschutzbeauftragten bereits Rechnung getragen. Ein Konzept wurde in Abstimmung mit dem Hessischen Datenschutzbeauftragten entwickelt und die Freigabe durch den Hessischen Datenschutzbeauftragten ist erfolgt.

Zu 8.6 Hinterlegen von Passwörtern

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 9. Bilanz

Zu 9.1 Auftragsdatenverarbeitung durch die HZD im Bereich der Justiz (31. Tätigkeitsbericht, Ziff. 5.1)

Der Hessische Datenschutzbeauftragte hatte in seinem 31. Tätigkeitsbericht die Auffassung vertreten, eine von der HZD betriebene Systembetreuung greife in den Kernbereich der richterlichen Unabhängigkeit ein. Der derzeitige Hessische Datenschutzbeauftragte, Prof. Dr. Ronellenfitsch, folgt dieser Auffassung nicht. Er vertritt die Ansicht, solange Aufsichtsrechte der Justiz über die HZD gewährleistet sind, sei die organisatorische Zuordnung der HZD zur Exekutive verfassungsrechtlich unproblematisch.
Die Landesregierung stimmt der nunmehr vom Hessischen Datenschutzbeauftragten vertretenen Auffassung zu.

Zu 9.2 Vermeidung von Doppelanfragen polizeilicher Datenbestände bei Einbürgerungen und bei ausländerrechtlichen Entscheidungen

Die vom Hessischen Datenschutzbeauftragten angeregte Koordinierung der Abfragen polizeilicher Erkenntnisse vor Einbürgerungen ist - wie von ihm berichtet - inzwischen realisiert. Zentrale Stelle für die Entgegennahme entsprechender Anfragen ist das Hessische Landeskriminalamt (HLKA).

Im Zuge der Realisierung des Digitalen Einbürgerungssystems in Hessen (eEinbürgerung) wird das Verfahren insofern weiter vereinfacht, dass nicht mehr die unteren Verwaltungsbehörden, sondern nur noch die Regierungspräsidien als Einbürgerungsbehörden die Anfrage an das HLKA richten. In einer weiteren Ausbaustufe ist beabsichtigt, von der in § 24 Abs. 1 Satz 2 Nr. 6 HSOG vorgesehenen Möglichkeit eines automatisierten Abrufverfahrens Gebrauch zu machen. Der Online-Zugriff ist auf Negativauskünfte beschränkt, vorhandene Erkenntnisse werden weiter konventionell übermittelt.

Zu 9.3 Rasterfahndung (32. Tätigkeitsbericht, Ziff. 5.1)

Der Hessische Datenschutzbeauftragte hat in seinem Tätigkeitsbericht zutreffend beschrieben, dass inzwischen die in den Prüffällen angelegten Akten vernichtet, der Eintrag in der Crime-Datenbank und im Index des ComVor-Systems gelöscht sowie die Betroffenen nach § 26 Abs. 5 HSOG benachrichtigt wurden.

Zu 9.4 Datensicherheitsmaßnahmen beim Landratsamt Marburg-Biedenkopf (32. Tätigkeitsbericht, Ziff. 6.2)

Die Landesregierung nimmt mit Befriedigung zur Kenntnis, dass die vom Hessischen Datenschutzbeauftragten festgestellten Mängel bei der Datensicherheit inzwischen vom Landratsamt Marburg-Biedenkopf abgestellt wurden.

Wiesbaden, 30. November 2005

Der Hessische Ministerpräsident:
Koch

Der Hessische Minister des Innern und für Sport:
Bouffier