18. Wahlperiode

Drucksache **18/1014**

HESSISCHER LANDTAG

01. 09. 2009

Stellungnahme der Landesregierung

betreffend den Siebenunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Drucksache 18/106

Eingegangen am 1. September 2009 · Ausgegeben am 8. September 2009

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

Inhaltsverzeichnis

Seite

Die Stellungnahme der Landesregierung gibt den Sachstand im Mai 2009 wieder.

1. Einführung

1.1 Allgemeines

Der Hessische Datenschutzbeauftragte zitiert in seiner Einführung die Vorbildwirkung Hessens für die Entwicklung des Datenschutzes. Er verbindet den Blick in die Vergangenheit mit der Forderung nach einem neuen Vorbild für das Datenschutzrecht. Es sei gemeinschaftsrechtlich geboten, die Datenschutzaufsicht in institutioneller Unabhängigkeit zu führen. Dazu solle dem Hessischen Datenschutzbeauftragten unter Beibehaltung seiner Unabhängigkeit auch die Aufsicht für den privaten Bereich übertragen werden.

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass Hessen über eine große Tradition des Datenschutzes verfügt. Diese ist durch das Gemeinschaftsrecht keineswegs überholt. Der Europäische Gerichtshof hat noch nicht über die Klage der Kommission gegen die Bundesrepublik Deutschland wegen mangelnder Unabhängigkeit der Aufsichtsbehörden entschieden. Gegenwärtig steht also nicht fest, ob das Recht der Europäischen Union zwingend verlangt, dass die Datenschutzaufsicht im privaten Bereich durch eine institutionell von der Exekutive unabhängige Stelle ausgeübt wird. Damit entspricht die vom Hessischen Datenschutzbeauftragten geforderte Umgestaltung der Aufsicht nur einer der möglichen Interpretationen der EG-Datenschutzrichtlinie.

Zu Recht weist der Hessische Datenschutzbeauftragte auf das verfassungsrechtliche Verbot einer Verwaltung mit Eingriffsbefugnissen im ministerialfreien Raum hin. Darin stimmt ihm die Landesregierung uneingeschränkt zu. Soll dieses Verbot beachtet und zugleich das Gebot der institutionellen Unabhängigkeit der Aufsicht befolgt werden, sofern der Europäischen Gerichtshof die dahingehende Auslegung EG-Datenschutzrichtlinie bestätigt, dürfte eine Lösung, die beiden Forderungen entspricht, nicht leicht zu finden sein. Die vom Hessischen Datenschutzbeauftragten vorgeschlagene Verstärkung der parlamentarischen Verantwortlichkeit seiner Behörde durch ein der G10-Kommission vergleichbares Gremium birgt beispielsweise die Gefahr, deren Unabhängigkeit bei der Kontrolle im öffentlichen Bereich zu beeinträchtigen. Zu den seiner Kontrolle unterliegenden Stellen gehört in gewissem Umfang nämlich auch der Hessische Landtag selbst. Andererseits besteht für die Aufsichtsbehörde im privaten Bereich gegenwärtig keine besondere Kontrolle durch das Parlament, sodass insoweit eine gewisse Einschränkung gegenüber der bestehenden Unabhängigkeit einträte.

Die Entscheidung über eine Umgestaltung der Datenschutzaufsicht für den privaten Bereich, wie sie der Hessische Datenschutzbeauftragte fordert, liegt jedoch nicht bei der Landesregierung sondern bei dem Hessischen Landtag als dem Landesgesetzgeber. Nach Auffassung der Landesregierung wird dessen Gestaltungsfreiheit maßgeblich von der Entscheidung des Europäischen Gerichtshofs bestimmt werden. Womöglich wird er zu gegebener Zeit über den Vorrang des Europarechts gegenüber einem bislang als verbindlich angesehenen Grundsatz des deutschen bzw. hessischen Verfassungsrechts zu entscheiden haben.

1.2 Datenschutz

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die zitierten Entscheidungen richtungweisend für den Datenschutz sind.

Zu 1.2.1 Abwehrkomponente

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.
Der Hessische Datenschutzbeauftragte leitet das Gebot zur Datensparsamkeit zu Recht aus dem Grundsatz der Erforderlichkeit ab, der für öffentliche Stellen in Hessen in § 11 Hessisches Datenschutzgesetz (HDSG) normiert ist. § 11 HDSG verlangt von dem für die Datenverarbeitung Verantwortlichen, die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf das zur Erfüllung der Aufgaben und zur Erreichung des Zwecks erfor-

derliche Maß zu begrenzen. Der Bundesgesetzgeber hat gleichwohl mit der Novelle des Bundesdatenschutzgesetzes im Jahr 2001 das Gebot zur Datensparsamkeit in das Gesetz aufgenommen (§ 3a BDSG).

Zu 1.2.2 Schutzkomponente

Die Landesregierung ist nicht der Auffassung des Hessischen Datenschutzbeauftragten, die angeführten Beispiele lieferten einen Beleg dafür, dass die Trennung von öffentlichem und privatem Bereich im Datenschutz nicht mehr zeitgemäß ist. Die Vorfälle betrafen sowohl Unternehmen, die der Kontrolle durch Aufsichtsbehörden der allgemeinen Verwaltung unterliegen, als auch solche, die durch einen für beide Bereiche zuständigen Datenschutzbeauftragten kontrolliert werden. Insofern ist nicht ersichtlich, dass eine Verbindung beider Bereiche zu einer Erhöhung des Datenschutzniveaus führt. Bei der datenschutzrechtlichen Aufarbeitung der Rechtsverstöße arbeiten die Aufsichtsbehörden für den Datenschutz ohne Ansehung der jeweiligen Organisationsform der Behörden zusammen. Das gilt insbesondere für den vorrangig betroffenen Datenschutz im privaten Bereich und die Arbeit im Düsseldorfer Kreis, dem Abstimmungsgremium der zuständigen Aufsichtsbehörden des Bundes und der Länder.

Zu 1.2.3 Datenzugangsschutz

Die Landesregierung begrüßt die Feststellung des Bundesverwaltungsgerichts im Urteil vom 23. Januar 2008 (6 A 1.07), dass der G10-Kommission bei der Entscheidung, ob eine Mitteilung der Beschränkungsmaßnahmen gegenüber dem Betroffenen nach § 12 G10 erfolgt, ein Beurteilungsspielraum zusteht, welcher die Rechtskontrolle durch die Gerichte beschränkt. Damit wird dem schwierigen und komplexen Abwägungsvorgang angemessen Rechnung getragen, in dessen Rahmen vielfältige Prognoseentscheidungen getroffen werden müssen, insbesondere bezüglich der durch eine Mitteilung entstehenden Gefahr für den Zweck weiterführender Beschränkungsmaßnahmen nach dem G10. Diese Gefahren resultieren nicht zuletzt aus den durch eine Mitteilung offen gelegten Anhaltspunkten für die Arbeitsweisen und technischen Möglichkeiten des Verfassungsschutzes. Hervorzuheben ist ferner die Ausführung des Bundesverfassungsgerichts, dass, wenn die G10-Kommission im Zweifel ist, ob eine Zweckgefährdung nicht mehr besteht, die Mitteilung noch zu unterlassen ist.

1.3 Rechtsentwicklung

Zu 1.3.1 Überblick

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.3.2 Rechtsprechung

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

1.4 Daseinsvorsorge

Zu 1.4.1 Herleitung

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.4.2 Anwendungsbereich

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu, soweit er die Tätigkeit eines Unternehmens in einem der aufgezählten Bereiche nur als Indiz für die Zurechnung zur Daseinsvorsorge versteht.

Zu 1.4.3 Rechtsfolgen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu, soweit er die Möglichkeiten zur Erfüllung der Aufgaben der Daseinsvorsorge beschreibt. Der Schlussfolgerung des Hessischen

Datenschutzbeauftragten, dass die Leistungen der Daseinsvorsorge datenschutzrechtlich zum öffentlichen Bereich zählen, kann die Landesregierung allerdings nicht vorbehaltlos zustimmen. Wie bereits in der Stellungnahme der Landesregierung zum 34. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten ausgeführt (siehe zu Ziffer 2.1.2.3 - Drucks. 16/5891), kommt es nach der einschlägigen Vorschrift des § 2 Abs. 3 und 4 Bundesdatenschutzgesetz für die Zuordnung zum öffentlichen bzw. nicht öffentlichen Bereich auch darauf an, ob an einem Unternehmen eine Stelle oder Körperschaft des öffentlichen Rechts beteiligt ist. Die bloße Tätigkeit in einem Bereich der Daseinsvorsorge führt nach dem geltenden Datenschutzrecht nicht dazu, ein in rein privater Hand befindliches Unternehmen dem öffentlichen Bereich zuzurechnen.

Zu 2. Europa

2.1 Gemeinsame Kontrollinstanzen für das Schengener Informationssystem und für EUROPOL

Die Ausführungen des Hessischen Datenschutzbeauftragten in diesem Abschnitt beruhen auf seinen Kenntnissen aus der Einbindung in die europäischen Kontrollinstanzen für Schengen und EUROPOL. Sie können von der Landesregierung nur in beschränktem Umfang kommentiert werden.

2.1.1 Gemeinsame Kontrollinstanz Schengen

Zu 2.1.1.1 Schengener Informationssystem der zweiten Generation (SIS II)

Anders als angekündigt, konnte das SIS II auch Anfang 2009 nicht in Betrieb gehen. Schon vor Ende des vergangenen Jahres waren Probleme bekannt geworden, die eine zeitliche Verzögerung bei der Realisierung absehbar werden ließen. Die Prognose eines neuen Realisierungstermins erscheint angesichts der bisherigen Verzögerungen nicht angebracht.

Zu 2.1.1.2 Ausschreibungen zur verdeckten Registrierung

Der Austausch von Informationen über so genannte "Troublemakers" wird zutreffend als ein wesentliches Thema auf Ebene der europäischen polizeilichen Zusammenarbeit beschrieben. Nach den der Landesregierung vorliegenden Informationen und Protokollen der Ratsarbeitsgruppen (insbesondere RAG PZ) war es allerdings nicht das Anliegen des Rates, diesen Informationsaustausch auf Art. 99 SDÜ zu stützen; vielmehr sollte die Möglichkeit einer Heranziehung von Art. 99 SDÜ als Rechtsgrundlage für einen derartigen Informationsaustausch geprüft werden.

Zu 2.1.1.3 Gemeinsame Überprüfung der Ausschreibungen von Dritt-Ausländern zur Einreiseverweigerung

Die Hessen betreffenden Feststellungen befinden sich unter Ziffer 4.4.1 des Tätigkeitsberichts. Die Stellungnahme der Landesregierung hierzu findet sich unter dieser Ziffer.

Zu 2.1.1.4 Gemeinsame Überprüfung der Ausschreibungen zur vorläufigen in Gewahrsamnahme und zur Wohnsitz- und Aufenthaltsermittlung

Hierzu liegen noch keine Hessen betreffenden Rückmeldungen vor.

Zu 2.1.2 Gemeinsame Kontrollinstanz EUROPOL

Es trifft zu, dass eine politische Einigung erfolgt ist und der Ratsbeschluss Anfang 2010 in Kraft treten soll.
Im Übrigen ist der Landesregierung keine Beurteilung der Tätigkeit der Gemeinsamen Kontrollinstanz möglich.

2.2 EURODAC - Koordinierung der Kontrolle

Die deutschen Polizeibehörden haben bislang keinen Zugriff auf EURODAC. Ein solcher Zugriff wird allerdings von den Polizeien des Bundes und der Länder für erforderlich gehalten. Auf deutsche Initiativen hin

hat der Rat für Justiz und Inneres im Juni 2007 Schlussfolgerungen zu EURODAC verabschiedet, in denen er sich für einen Zugang der Polizei- und Strafverfolgungsbehörden ausspricht und die Kommission auffordert, so bald wie möglich einen Vorschlag zur Änderung der EURODAC-Verordnung vorzulegen. Die anstehenden Änderungen der Verordnung beschränken sich laut Auskunft des Bundesinnenministeriums vom Dezember 2008 allerdings auf das Dublin II-Verfahren sowie technische Details. Mit Schreiben vom 9. Oktober 2008 hat der zuständige Kommissar Barrot angekündigt, Ende des 1. Halbjahres 2009 eine Initiative über den Zugang der Polizei- und Strafverfolgungsbehörden zu EURODAC vorlegen zu wollen.

2.3 Auswirkungen des Vertrags von Lissabon auf den Datenschutz

In Übereinstimmung mit den Ausführungen des Hessischen Datenschutzbeauftragten im Tätigkeitsbericht geht die Landesregierung davon aus, dass die Gesetzgebungskompetenz in Art. 16 AEUV gegenüber der Vorgängervorschrift in Art. 286 EG ausgedehnt worden ist. Sie erlaubt nicht mehr nur Regelungen, die die EU selbst verpflichten, sondern auch solche, die die Mitgliedstaaten betreffen. Allerdings sind hierbei zwei Punkte zu bedenken: Datenschutzrechtliche Regelungen, die die Mitgliedstaaten verpflichten, gab es bislang auch schon, allerdings aufgrund der Kompetenzgrundlage zum Binnenmarkt. Zweitens enthält Art. 16 AEUV zumindest nach dem Wortlaut des Vertrages keinen "Gesetzgebungsauftrag", sondern lediglich eine Gesetzgebungsbefugnis.

Es ist ferner zutreffend, dass sich die Kompetenzgrundlage Art. 16 AEUV im Gegensatz zur heutigen Kompetenzgrundlage Art. 286 EG auch auf die polizeiliche und justizielle Zusammenarbeit ("in Strafsachen" (PJZS) - diese begriffliche Unterscheidung zur bereits heute vergemeinschafteten Zusammenarbeit in Zivilsachen sollte berücksichtigt werden) erstrecken wird. Die im Tätigkeitsbericht enthaltene Aussage, dadurch werde möglicherweise der Anwendungsbereich der seit 1995 geltenden Datenschutzrichtlinie auch auf die Bereiche PJZS ausgeweitet, beinhaltet eine rechtlich komplexe Thematik. Inwieweit sich der Anwendungsbereich einer Richtlinie knapp 15 Jahre nach ihrem Erlass ändern kann, ist letztlich eine Frage der Verweisungstechnik. Sollte die Regelung zum Anwendungsbereich der Richtlinie tatsächlich als eine dynamische Verweisung an das jeweils geltende Gemeinschaftsrecht anknüpfen, so ist die Frage, was damit gemeint ist, wenn es keine Gemeinschaft mehr gibt, sondern - wie mit dem Vertrag von Lissabon beabsichtigt - nur noch eine Union. Diese Frage hat weitreichende Auswirkungen und müsste - möglicherweise durch die europäischen Gerichte - langwierig geprüft werden.

In Bezug auf den zitierten Rahmenbeschluss zum Datenschutz in der 3. Säule der EU ist anzumerken, dass er wirksam ist, wenn der Rahmenbeschluss jetzt nach den geltenden Ermächtigungsgrundlagen rechtmäßig erlassen wurde. Er kann nicht am Maßstab eines Vertrags gemessen werden, der noch gar nicht in Kraft ist. Wenn der Vertrag von Lissabon in Kraft treten sollte, stellt sich die Frage, welche Anforderungen Art. 16 AEUV überhaupt stellen soll. Die Tatsache, dass verpflichtende Regelungen für EU und Mitgliedstaaten erlassen werden dürfen, bedeutet nicht unbedingt, dass dies in einem einzigen Rechtsakt geschehen muss, sodass der Inhalt des Rahmenbeschlusses möglicherweise auch nach neuem Recht separat beschlossen werden dürfte.

In Übereinstimmung mit dem Hessischen Datenschutzbeauftragten geht die Landesregierung davon aus, dass in dem Zeitpunkt, in dem die Grundrechte-Charta Verbindlichkeit erlangt, unionsweit ein Grundrecht auf Datenschutz eingeführt wird. Hierdurch wird das deutsche Grundrecht auf informationelle Selbstbestimmung jedoch nicht verdrängt, sondern ergänzt, weil beide Grundrechte unterschiedliche Zielrichtungen haben - europäisches Grundrecht gegenüber EU und Mitgliedstaaten bei der Ausübung von Unionsrecht, deutsches Grundrecht gegenüber deutschen Behörden bei der Ausübung von anderem als Unionsrecht. Soweit im Tätigkeitsbericht in diesem Zusammenhang ausgeführt wird, "der hohe deutsche Datenschutzstandard wird vom Integrationsvorbehalt in Art. 23 Abs. 1 GG erfasst und kann durch EU-Recht nicht abgesenkt werden", erscheint dies hingegen missverständlich. Art. 23 GG besagt, dass die EU, an der Deutschland teilnehmen will, einen "im wesentlichen vergleichbaren Grundrechtsschutz" gewährleisten muss -

gewisse Abweichungen sind also erlaubt. Aufgrund des Anwendungsvorranges kann das EU-Recht den deutschen Datenschutzstandard prinzipiell auch absenken, wenn er sich auf das Gebiet der Umsetzung von Unionsrecht bezieht. Für den restlichen Datenschutzstandard in Deutschland hat die EU hingegen auch nach dem Vertrag von Lissabon keine Kompetenzgrundlage und damit keine Möglichkeit zur Absenkung des deutschen Schutzstandards (vgl. Art. 16 AEUV).

3. Bund

3.1 Grobkonzept zum elektronischen Personalausweis

Die Darstellung des Hessischen Datenschutzbeauftragten zum Grobkonzept und dem Ablauf der Entwicklung bis zur Verabschiedung des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften durch den Deutschen Bundestag am 18. Dezember 2008 ist zutreffend. Der Bundesrat hat in seiner Sitzung am 13. Februar 2009 beschlossen, keinen Antrag auf Anrufung des Vermittlungsausschusses zu stellen. Damit kann das Gesetz in Kraft treten.
Hessen hat im Bundesrat dem Gesetz zugestimmt.

3.2 Neuorganisation der Durchführung des SGB II - Zentren für Arbeit und Grundsicherung

Hinsichtlich der im Tätigkeitsbericht des Hessischen Datenschutzbeauftragten wiedergegebenen Angaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) über die Planungen des Bundesarbeitsministeriums (BMAS) zur Errichtung von Zentren für Arbeit und Grundsicherung (ZAG) hat sich zwischenzeitlich folgender Sachstand ergeben:

Mitte Februar des Jahres hat eine kleine, von der Ministerpräsidentenkonferenz im Dezember 2008 eingesetzte Arbeitsgruppe bestehend aus Bundesminister Scholz und den Ministerpräsidenten Beck und Rüttgers zur Neuorganisation der Trägerschaft im SGB II einen Kompromissvorschlag in Form eines umfangreichen Gesetzespakets vorgelegt. Der Vorschlag sieht - um nach dem Urteil des Bundesverfassungsgerichts vom 20. Dezember 2007 die bisherige Arbeit der ARGEn fortsetzen zu können - deren Verankerung unter dem Namen "Zentrum für Arbeit und Grundsicherung" im Grundgesetz vor.

Die Landesregierung hat sich zu der Grundlinie des Kompromissvorschlages positiv geäußert, gleichzeitig aber noch Verbesserungsbedarf angemeldet.

Ob und ggf. wie der Kompromissvorschlag im Detail umgesetzt werden wird, ist offen. Die Beratungen sind noch nicht abgeschlossen, zurzeit erscheint die erforderliche zweidrittel Mehrheit für eine Verfassungsänderung in Bundestag und Bundesrat nicht gewährleistet.

In der Sache selbst enthält der Gesetzentwurf die von dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beschriebene und von dem Hessischen Datenschutzbeauftragten kritisierte alleinige Zuständigkeit des BfDI. § 50 Abs. 2 bis 4 SGB II lautet im Entwurf wie folgt:

"(2) Das Zentrum für Arbeit und Grundsicherung ist verantwortliche Stelle für die Erhebung, Verarbeitung und Nutzung von Daten nach § 67 Absatz 9 des Zehnten Buches sowie Stelle im Sinne von § 35 Absatz 1 des Ersten Buches.
(3) Das Zentrum für Arbeit und Grundsicherung nutzt zur Erfüllung seiner Aufgaben durch die Bundesagentur zentral verwaltete Verfahren der Informationstechnik. Es ist verpflichtet, auf einen auf dieser Grundlage erstellten gemeinsamen zentralen Datenbestand zuzugreifen. Verantwortliche Stelle für die zentral verwalteten Verfahren der Informationstechnik nach § 67 Absatz 9 des Zehnten Buches ist die Bundesagentur.
(4) Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch das Zentrum für Arbeit und Grundsicherung richtet sich nach dem Datenschutzrecht des Bundes, insbesondere nach dem Zweiten Kapitel des Zehnten Buches. Die Datenschutzkontrolle und die Kontrolle der Einhaltung der Vorschriften über die Informationsfreiheit beim Zentrum für Arbeit und Grundsicherung sowie für die zentralen Verfahren der Informati-

onstechnik obliegt nach § 24 des Bundesdatenschutzgesetzes dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit."

Aus Sicht der Landesregierung ist eine Zuständigkeit sowohl des BfDI, als auch der Landesbeauftragten für den Datenschutz denkbar. Sofern sich das eingangs erwähnte Vorhaben einer Verfassungsänderung realisieren lässt, wird die Landesregierung daher anregen, den - von dem BfDI unterstützen - Vorschlag des Hessischen Datenschutzbeauftragten für eine zweigleisige datenschutzrechtliche Zuständigkeit im Zuge der dann erforderlichen weiteren Beratungen des Gesetzespakets zu berücksichtigen.

4. Land

4.1 Querschnitt

4.1.1 Entwicklungen im Bereich Videoüberwachung

Zu 4.1.1.1 Einsatz von Videoüberwachungsanlagen in Fußballstadien

Die Landesregierung begrüßt das Engagement des Hessischen Datenschutzbeauftragten bei der datenschutzkonformen Ausgestaltung der Videoüberwachung in Fußballstadien, namentlich im Fußballstadion von Wiesbaden. Das Polizeipräsidium Frankfurt am Main hatte das Problem für den polizeilichen Teilbereich bereits vor der Fußball-Weltmeisterschaft 2006 in Angriff genommen. Den vom Hessischen Datenschutzbeauftragten skizzierten Grundsätzen wird zugestimmt. Allerdings kann die Videoüberwachung nach Auffassung der Landesregierung heute nicht mehr auf § 14 Abs. 1 HSOG gestützt werden. Die Videoüberwachung ist mittlerweile so umfangreich im HSOG geregelt, dass ein Rückgriff auf allgemeine Datenerhebungsbefugnisse ausscheidet. Nr. 14.1.2 der Verwaltungsvorschrift zur Ausführung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (VVHSOG) ist deshalb durch Erlass vom 4. Mai 2006 (StAnz 21/2006 S. 1126) geändert worden.

Rechtsgrundlage für eine polizeiliche Videoüberwachung in Fußballstadien müsste vielmehr § 14 Abs. 3 HSOG sein, der die Überwachung öffentlich zugänglicher Orte gestattet, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen. Es handelt sich dabei um dieselbe Rechtsgrundlage, auf die zur Überwachung öffentlicher Plätze, wie der Konstabler Wache in Frankfurt am Main, zurückgegriffen wird. Dass im örtlichen und zeitlichen Zusammenhang mit Fußballspielen Straftaten verübt werden, ist bedauerliche Realität.

Zu 4.1.1.2 Videoüberwachung an der Konstablerwache

Nach langwierigen Verhandlungen hat die Stadt Frankfurt am Main die Videoüberwachungsanlage an der Konstablerwache zum 1. August 2008 kostenneutral übernommen und trägt seither für Betrieb und Instandhaltung die entsprechenden Kosten. Zuvor sind die analogen Kameras gegen moderne DOM-Kameras ausgetauscht worden. In die Ausgestaltung der Privatschutzzone ist der Hessische Datenschutzbeauftragte eng eingebunden worden. Seine Ausführungen zum Sachverhalt sind zutreffend. Lediglich die von ihm geäußerte Annahme, die geschilderten Probleme mit der Privatschutzschaltung seien auf eine unzureichende Prüfung bei der Beschaffung der Kameras zurückzuführen, ist unbegründet. Da es nicht um die Neukonzeption einer Anlage ging, sondern um die technische Aktualisierung einer bereits bestehenden Anlage, war man bei der Beschaffung der neuen Kameras an das mit der Errichtung der Anlage beauftragte Unternehmen gebunden. Durch die integrierte Kamerasoftware kommt es nunmehr in bestimmten Zoomeinstellungen zu der bemängelten Übergröße der Privatschutzzone, die weder durch den Hersteller der Kameras noch durch das die Anlage errichtende Unternehmen zu beheben war. In der Gesamtsicht ist die Einschränkung allerdings polizeifachlich tragbar.

Zu 4.1.1.3 Kameras an einer Ampelanlage - Verkehrssteuerung

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu. Auch wenn bei der in Rede stehenden Lichtzeichenanlage keine personenbezogenen Daten erhoben werden, ist es angemessen, die

Bevölkerung über derartige Maßnahmen zu informieren und die Funktionsweise ausreichend zu erläutern.

4.1.1.4 Videokameras in der Frankfurter Verkehrsleitzentrale

Zu 4.1.1.4.1 Verkehrsüberwachung

Die vom Hessischen Datenschutzbeauftragten zu Recht geforderte Dienstanweisung, die die Bediensteten anweist, die Kameras nur im Rahmen der zur Verkehrslenkung notwendigen Anforderungen zu nutzen, befindet sich im stadtinternen Abstimmungsprozess. Sobald die Dienstanweisung vorliegt, wird das Ministerium für Wirtschaft, Verkehr und Landesentwicklung dem Hessischen Datenschutzbeauftragten ein Exemplar zur Kenntnis zuleiten.

Zu 4.1.1.4.2 Übertragung der Bilder ins Internet

Zunächst ist zur Richtigstellung darauf hinzuweisen, dass es im ersten Satz des Textes nicht "Verkehrsleitzentrale Hessen", sondern "Verkehrsleitzentrale der Stadt Frankfurt am Main (www.mainziel.de)" heißen müsste.

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass Bilder, auf denen Personen erkennbar sind, nicht ins Internet gestellt werden dürfen. Dies wird ebenfalls in der oben (Zu 4.1.1.4.1) genannten Dienstanweisung geregelt werden.
Im Hinblick auf die Übernahme der Bilder durch den Hessischen Rundfunk wird eine sog. technische Lösung favorisiert. Dadurch soll gewährleistet werden, dass die Stadt Frankfurt am Main entscheidet, wann bzw. welche Bilder ins Internet gestellt werden. Vom Abschluss einer Vereinbarung zwischen dem Hessischen Rundfunk und der Stadt Frankfurt am Main soll daher Abstand genommen werden.

Zu 4.1.1.4.3 Zugriff der Polizei auf die Kamerasteuerung
Eine Vereinbarung zwischen dem Polizeipräsidium Frankfurt und der Stadt Frankfurt am Main über die polizeiliche Nutzung der Bilder der Verkehrsleitzentrale befindet sich derzeit in der Abstimmung. Sobald die Vereinbarung vorliegt, wird das Ministerium für Wirtschaft, Verkehr und Landesentwicklung dem Hessischen Datenschutzbeauftragten ein Exemplar zur Kenntnis zuleiten.

Hinsichtlich der Nutzung der Anlage durch die Polizei gilt dasselbe wie hinsichtlich der Nutzung von Videoanlagen in Fußballstadien (vgl. zu Ziffer 4.1.1.1). Wenn die Polizei die Anlage steuert und damit durch Heranzoomen personenbezogene Daten erhebt, benötigt sie dafür eine entsprechenden Rechtsgrundlage und trägt die datenschutzrechtliche Verantwortung.

Zu 4.1.2 Datenschutzprobleme bei der Bereitstellung des Staatsanzeigers im Internet

Seit dem Jahr 2003 wird neben den amtlichen Printveröffentlichungen der Staatsanzeiger im Internet unter "www.staatsanzeiger-hessen.de" eingestellt; über die Recherchefunktion "Gehe zu / Seitenzahl eingeben" kann auf Ausgaben ab 1999 zugegriffen werden. Bei der Bekanntmachung im Internet handelt es sich mangels einer gesetzlichen Grundlage nicht um eine amtliche Bekanntmachung, sondern um ein zusätzliches Serviceangebot. Der Online-Staatsanzeiger wird in drei Versionen angeboten. Die kostenpflichtige Abonnentenversion ermöglicht den sofortigen Download und Ausdruck. Darüber hinaus wird eine kostenlose Leseversion des Amtlichen Teils mit einer Verzögerung von zehn Tagen eingestellt, und bis zum 15. Dezember 2008 war noch das Herunterladen und Drucken der kompletten Ausgaben nach sechs Monaten möglich. Seither sind die Ausgaben ohne die Bekanntmachungen der Amtsgerichte abrufbar; die Bereinigung des Altbestandes erfolgte ebenso bis zu dem vorgenannten Zeitpunkt.

Moderne Informations- und Kommunikationstechnologien entwickeln sich rasant weiter, Netzwerke und allen voran das Internet bieten einen leichteren Zugriff zu weitreichenden Informationen und eröffnen stetig neue Nutzungsmöglichkeiten. Zum Zeitpunkt der Bereitstellung des Printmediums Staatsanzeigers im Internet war die Entwicklung, insbesondere die der Suchmaschinen, nicht absehbar.

Nachdem der Hessische Datenschutzbeauftragte in seinem 36. Tätigkeitsbericht (Drucks. 16/8377) auf die Gefahren der Bereitstellung von Daten im Internet hingewiesen hat (siehe dort Ziffer 5.1.2.2), wurden fast zeitgleich drei Einwendungen von Bürgern zu der Problematik bekannt. Die bereits abgeschlossenen Insolvenzverfahren der drei Betroffenen wurden im Online-Staatsanzeiger unmittelbar gelöscht. Neben der relativ einfachen und umgehenden Umsetzung der Forderung nach dem Schutz personenbezogener Daten im Öffentlichen Anzeiger durch deren Löschung wurden im Hinblick auf mögliche ähnliche Fälle darüber hinaus zunächst die Suchmöglichkeiten eingeschränkt. Die Recherche über Suchmaschinen zeigte nur noch Fundstellen auf, ohne jedoch mit der betreffenden Bekanntmachung verlinkt zu sein. Auch wurde die Suchfunktion auf der Internetseite des Staatsanzeigers für Nicht-Abonnenten auf den Amtlichen Teil begrenzt. Anschließend wurden die Bekanntmachungen der Amtsgerichte für den allgemein zugänglichen Kreis abgetrennt und nicht mehr eingestellt sowie die bereits vorhandenen Ausgaben zügig um die Bekanntmachungen der Amtsgerichte bereinigt. Die Online-Abonnenten können nach wie vor ohne Einschränkungen auf den Staatsanzeiger im Internet zugreifen, weil es sich um einen registrierten, eingeschränkten Nutzerkreis handelt und ein Datenmissbrauch nachvollziehbar wäre. Sollten weitere Einwendungen gegen abgeschlossene Insolvenzveröffentlichungen erhoben werden, werden diese Eintragungen unverzüglich gelöscht.

4.2 Justiz und Strafvollzug

Zu 4.2.1 Netzkonzept in der Praxis bei kleinen Gerichten

Die zuständige Fachabteilung des Ministeriums der Justiz, für Integration und Europa hat mit Erlass vom 31. März 2009 die Mittelbehörden gebeten, auf die im Tätigkeitsbericht angesprochenen Interessenkonflikte, das Fehlen von Verfahrensverzeichnissen, mit dem besonderen Aspekt der fehlenden Musterverfahrensverzeichnisse, die mangelnde Aktualität und die möglicherweise zu weiten Zugriffsrechte auf die Abteilungsablage die gerichtliche Praxis zu befragen. Speziell sind die Mittelbehörden darum gebeten worden, hinsichtlich der Einrichtung der Rolle des Systemrevisors, der Nutzung der Möglichkeit der Verschlüsselung mit dem Verschlüsselungsprogramm Chiasmus und der Einrichtung eines "Safe-Ordners" im persönlichen Verzeichnis, des Einsatzes und der Vergabe der Kennung des Recovery-Agents sowie der Einschränkung der Zugriffsrechte auf die Abteilungsablage analog den Zugriffsrechten zu den Fachverfahren Feststellungen zu treffen.

Daneben soll durch stichprobenhafte Prüfungen bei einigen kleinen Gerichten erhoben werden, ob die Vorgaben der Netzbeschreibung eingehalten werden. In die Prüfungen sollen die jeweiligen IT-Referate eingebunden werden.

Einen ersten Zwischenbericht zu den Prüfungsergebnissen hat das Ministerium der Justiz, für Integration und Europa bis zum 1. Juni 2009 erbeten. Soweit sich die Ergebnisse des Prüfungsberichts des Hessischen Datenschutzbeauftragten bestätigen und sich strukturelle Defizite abzeichnen, wurden die Mittelbehörden zugleich um Unterbreitung von Lösungsansätzen ersucht.

Zu 4.2.2 Überwachung des Besuchs in einer Justizvollzugsanstalt durch Videokamera

Die Landesregierung teilt grundsätzlich die Rechtsauffassung des Hessischen Datenschutzbeauftragten, dass das StVollzG derzeit keine ausreichende Rechtsgrundlage für Aufzeichnungen von Besuchen in Justizvollzugsanstalten bereit stellt.

Dem Hessischen Datenschutzbeauftragten wurde mit Schreiben vom 1. Dezember 2008 in Bezug auf die von ihm beanstandeten Aufzeichnungsmöglichkeiten im Besuchraum der JVA Schwalmstadt mitgeteilt, dass die bis dahin nur theoretisch gegebene Möglichkeit von Videoaufzeichnungen zwischenzeitlich beseitigt wurde. Nachdrücklich wird an dieser Stelle nochmals darauf hingewiesen, dass von der Möglichkeit, entsprechende Aufzeichnungen zu erstellen, zu keinem Zeitpunkt Gebrauch gemacht wurde. Mit der in der JVA Schwalmstadt vorhandenen Anlage ist nunmehr lediglich die bloße Übertragung und gleichzeitige Beobachtung möglich.

Hinsichtlich der Möglichkeit zur Aufzeichnung von Besuchen soll eine entsprechende Regelung, wie im Hessischen Jugendstrafvollzugsgesetz vorhanden, in das Hessische Strafvollzugsgesetz aufgenommen werden.

4.3 Polizei und Ordnungsbehörden

Zu 4.3.1 Novellierung des HSOG

Die Fraktionen der CDU und der FDP haben am 30. Juni 2009 gemeinsam einen Entwurf für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und andere Gesetze in den Hessischen Landtag eingebracht (Drucks. 18/861).

Zu 4.3.1.1 Umsetzung des Kernbereichsschutzes

Der Gesetzentwurf enthält in Art. 1 Nr. 6 Buchst. a und b, Nr. 7 Buchst. a und e Doppelbuchst. bb sowie in Nr. 13 Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung.

Zu 4.3.1.2 Kennzeichenerkennung

In Bezug auf die Nutzung von Kennzeichenlesegeräten sieht der Gesetzentwurf in Art. 1 Nr. 5 die Einfügung eines neuen § 14a in das HSOG vor. Die vorgeschlagene Regelung ermöglicht den Einsatz der Geräte durch die Polizei und stellt sicher, dass die Vorgaben der Verfassungsrichter an den Schutz der Betroffenenrechte eingehalten werden. Der flächendeckende Einsatz der Kennzeichenlesegeräte ist nach dem Gesetzentwurf ebenso unzulässig wie die Herstellung von Bewegungsbildern.

Zu 4.3.2 Datenspeicherungen über Teilnehmer an Demonstrationen gegen die Einführung von Studiengebühren

Die zutreffende Darstellung des Hessischen Datenschutzbeauftragten stellt trotz ihres beträchtlichen Umfangs nur eine Zusammenfassung des verwickelten und vielschichtigen Sachverhalts dar. Im Grundsatz teilt die Landesregierung auch die rechtlichen Bewertungen des Hessischen Datenschutzbeauftragten.

Das Landespolizeipräsidium als Fachaufsichtsbehörde hält jedoch die vorzeitige Löschung gerade der zu dem Betroffenen, dessen Fall der Hessische Datenschutzbeauftragte im Tätigkeitsbericht darstellt, gespeicherten Daten für nicht geboten. Bei ihm handelte es sich nicht um einen hessischen Studenten, der gegen die Einführung ihn unmittelbar betreffender Studiengebühren protestieren wollte. Vielmehr war er als Angehöriger einer linken Hochschulgruppe, die sich den bundesweiten Kampf gegen Studiengebühren auf ihre Fahnen geschrieben hatte, eigens aus Hamburg angereist, wo bereits der dortige Staatsschutz zwei Jahre zuvor gegen ihn wegen des Verdachts des politisch motivierten Hausfriedensbruchs ermittelt hatte. In seinem Fall musste von dem Verdacht einer überörtlich begangenen politischen Straftat ausgegangen werden, die die Vergabe des Personengebundenen Hinweises "LIMO" (politisch links motivierter Straftäter), die erkennungsdienstliche Behandlung sowie die Speicherung der Daten für zehn Jahre gerechtfertigt hätte.

Polizeifachlich nicht gerechtfertigt, war die Löschung sämtlicher Unterlagen über den Betroffenen nach einer Speicherungsdauer von lediglich zwei Jahren. Für Fälle geringer Bedeutung sieht § 15 Abs. 1 Satz 2 HSOG-DVO bei Erwachsenen eine Prüffrist zur Aussonderung von drei Jahren vor, die nach der Verwaltungspraxis in Hessen nur in außergewöhnlichen Fällen unterschritten wird. Besonderheiten, die zugunsten des Betroffenen gesprochen hätten, lagen hier jedoch nicht vor. Insbesondere hätte die Tatsache der Einstellung des Strafverfahrens nach dem Grundsatz "im Zweifel für den Angeklagten" nicht zugunsten des Betroffenen berücksichtigt werden dürfen. Wird ein Strafverfahren nach diesem Grundsatz eingestellt, geht es nicht um die Schwere oder andere Aspekte der Tat oder um eine positive Prognose für den Täter, sondern um die Verhinderung einer sachlich unzureichend fundierten strafrechtlichen Verurteilung. § 20 Abs. 4 Satz 2 Halbs. 2 HSOG zeigt deutlich, dass für das Polizeirecht die Stärke des Tatverdachts unerheblich ist. Nur der vollständige Wegfall des Verdachts einer Straftat ist relevant und zieht dann zwingend die sofortige Löschung der Daten nach sich.

Das Landespolizeipräsidium hat dennoch von Weisungen zur Abänderung der getroffenen Entscheidungen abgesehen.

Zu 4.3.3 Auskunft über eigene Daten aus der Vorgangsverwaltungsdatei ComVor der Polizei

Die Landesregierung teilt die Auffassung des Hessischen Datenschutzbeauftragten. Um eine richtige Handhabung des § 29 HSOG sicherzustellen, hat das Landespolizeipräsidium ein Merkblatt entworfen und dem Hessischen Datenschutzbeauftragten Ende des Jahres 2008 zur Abstimmung zugeleitet. Der Hessische Datenschutzbeauftragte hat den vorgesehenen Weg begrüßt und eine Besprechung vorgeschlagen; diese stand bei Redaktionsschluss für die Stellungnahme der Landesregierung noch aus.

Zu 4.3.4 Zugriff auf das Passbild bei der Fahrerfeststellung

Die Darstellung im Tätigkeitsbericht ist zutreffend. Eine Ergänzung durch die Landesregierung ist nicht erforderlich.

4.4 Ausländerrecht

Zu 4.4.1 Prüfung von Ausländerbehörden

Die Ausländerbehörden des Kreises Bergstraße und der Stadt Darmstadt haben dem Ministerium des Innern und für Sport berichtet, dass die notwendigen Maßnahmen zur Beseitigung der aufgetretenen Mängel hinsichtlich der Ausschreibungsvoraussetzungen und der Verlängerung der Ausschreibungsfristen im Schengener Informationssystem (SIS) ergriffen wurde. Demnach ist künftig eine verbesserte Bearbeitung von SIS-Ausschreibungen gewährleistet.

4.5 Schulen und Schulverwaltung

4.5.1 Ergebnisse der Prüfung beim Staatlichen Schulamt Hanau

Zu 4.5.1.1 Bestellung eines stellvertretenden Datenschutzbeauftragten

Die mündliche Bestellung der stellvertretenden Datenschutzbeauftragten erfolgte im Jahr 2005, die schriftliche nach der Prüfung durch den Hessischen Datenschutzbeauftragten. Die erforderliche Sachkenntnis erwirbt die stellvertretende Datenschutzbeauftragte derzeit durch ein Online-Seminar der Lehrerakademie in Kooperation mit dem Hessischen Datenschutzbeauftragten.

Zu 4.5.1.2 Verschlüsselung bei der Speicherung der Diagnosedaten des Schulpsychologen

Nachdem sich die Nutzung von DOMEA mit einer Verschlüsselung kurzfristig nicht realisieren ließ, wurde, wie im Bericht dargestellt, eine alternative Lösung implementiert.

Zu 4.5.1.3 Vernichtung und Archivierung des Schriftgutes

Nach der Prüfung durch den Hessischen Datenschutzbeauftragten wurde das Archiv umfassend geprüft und die zur Aussonderung anstehenden Akten in Listen erfasst, sodass nunmehr dem zuständigen Staatsarchiv die Akten angeboten werden können. Zukünftig werden die Aussonderungszeitpunkte erfasst.

Zu 4.5.1.4 Das Schlüsselsystem

Bei der Feststellung, dass in der Zentrale des Staatlichen Schulamts Hanau ein Schlüsselkasten mit zahlreichen Sicherheitsschlüsseln für die meisten Räume des Amts hing, handelt es sich um ein Missverständnis. In dem seinerzeit in der Zentrale hängenden Schlüsselkasten hingen Zweitschlüssel für die Büromöbel des Hauses, sodass bei Abhandenkommen eines solchen Schlüssels das Möbel ohne Beschädigung geöffnet werden kann. Zweitschlüssel für die Eingangstüren und die Türen zu den einzelnen Büros sind hingen zu keinem Zeitpunkt in diesem Schlüsselkasten untergebracht gewesen. Einzig der Schlüssel zum Außenlager befand sich zum Zeitpunkt der

Prüfung im Schlüsselkasten. Im Außenlager wird Archivgut verwahrt, welches mangels räumlicher Möglichkeiten im hauseigenen Archiv nicht untergebracht werden konnte. Der Schlüsselkasten wurde dennoch dauerhaft im Büro des Büroleiters montiert. Im Übrigen ist die Darstellung zutreffend, dass zum Zeitpunkt der Besichtigung die Zentrale offen stand und keine der beiden Mitarbeiterinnen im Raum war. Beide Mitarbeiterinnen wurden in der Folgezeit eindringlich darauf hingewiesen, dass beim Verlassen des Raums dieser zu verschließen ist.

Zu 4.5.2 Panne bei der Datenübermittlung nach § 17 Meldedatenübermittlungsverordnung an Wiesbadener Schulen

Den Wiesbadener Grundschulen wurde mit Verfügung vom 3. April 2009 der betreffende Teilauszug des oben genannten Tätigkeitsberichts übersandt und die Schulleitungen gebeten, die Schülerstammdaten des betroffenen Jahrgangs zu überprüfen und in den Fällen das Datum der Religionszugehörigkeit zu löschen, in denen eine Befreiung vom Religionsunterricht vorlag.

Die Darstellung des Hessischen Datenschutzbeauftragten der fehlerhaften Datenübermittlung durch die Meldebehörde trifft zu. Der Fehler ist auf den Bereich der Wiesbadener Meldebehörde beschränkt geblieben.

4.6 Landwirtschaft

Zu 4.6.1 Unzulässige Datenerhebung der Hessischen Tierseuchenkasse bei Tierpensionen

Die im Tätigkeitsbericht des Hessischen Datenschutzbeauftragten geschilderte Problematik stellt sich jetzt nicht mehr. Der beanstandete § 1 Abs. 6 Satz 3 der Satzung der Hessischen Tierseuchenkasse über die Erhebung von Tierseuchenbeiträgen für das Wirtschaftsjahr 2008 existiert in der aktuellen Satzung des Jahres 2009 nicht mehr. Die entsprechende Bestimmung ist ersatzlos weggefallen. Auf eine Datenerhebung bei Tierpensionen wird wegen der vom Hessischen Datenschutzbeauftragten (HDSB) erhobenen Kritikpunkte seitens der Tierseuchenkasse bis auf Weiteres verzichtet.

Daneben arbeitet das Ministerium Umwelt, Energie, Landwirtschaft und Verbraucherschutz zurzeit an einer Novellierung des Hessischen Ausführungsgesetzes zum Tierseuchengesetz (HAGTierSG), in dem - in Absprache mit dem Hessischen Datenschutzbeauftragten - eine generelle Ermächtigungsgrundlage für die Datenerhebung der Tierseuchenkasse geschaffen werden soll. Der Entwurf zum HAGTierSG enthält dabei eine wortgleiche Datennutzungs- und Datenschutzregelung, wie sie bereits durch den Hessischen Datenschutzbeauftragten bei der Vorlage des Entwurfs eines neuen Hessischen Ausführungsgesetzes zum Tierische Nebenprodukte-Beseitigungsgesetz gebilligt wurde. Die Regelung stellt für die Datenerhebung durch die Tierseuchenkasse allerdings nur auf zuständige Behörden, den Tierhalter und vorhandene Datenbanken auf der Grundlage von Tierhalterdaten ab. Eine Erhebung bei anderen Personen oder Stellen - zum Beispiel Tierpensionen - ist darin nicht vorgesehen.

4.7 Gesundheitswesen

Zu 4.7.1 Aufbau einrichtungsübergreifender elektronischer Fallakten im Gesundheitsbereich

Der Hessische Datenschutzbeauftragte schildert den Aufbau von einrichtungsübergreifenden elektronischen Fallakten (eFA) im Gesundheitsbereich. Er zeigt das Spannungsverhältnis zwischen der ärztlichen Schweigepflicht (§ 203 Abs. 1 StGB, § 9 Berufsordnung für Ärzte) sowie den Vorgaben des Datenschutzgesetzes (HDSG) einerseits und der auch im Patienteninteresse gebotenen Möglichkeit von diversen Behandlern nach schnellem Zugriff auf die Patientendaten andererseits auf. Diese Diskussion wird bereits im Zusammenhang mit der geplanten Einführung der elektronischen Gesundheitskarte (eGK) intensiv geführt.

Die Möglichkeit einer eFA ist gerade im Bereich der integrierten Versorgung nach §§ 140 ff. SGB V, aber auch im Rahmen der Kommunikation zwischen Hausarzt, Facharzt und Klinik im Patienteninteresse als positiv zu

bewerten, soweit im Vorfeld effiziente Regelungen zum Datenschutz getroffen werden.

Da im Tätigkeitsbericht des Hessischen Datenschutzbeauftragten sehr detailliert Vorschläge zur rechtlichen und technischen Ausgestaltung der eFA dargelegt werden, ist dieser Teil des Berichts an die Landesärztekammer und Landeszahnärztekammer mit der Bitte weitergereicht worden, den Inhalt den Kammermitgliedern in geeigneter Form zur Kenntnisnahme zukommen zu lassen.

Zu 4.7.2 Ein Netzwerk für Ärzte und Krankenhäuser

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.7.3 Datenschutzkonzept für das europäische IPF-Register

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.7.4 Prüfung der Datenübermittlungen zwischen Kliniken und Medizinischen Versorgungszentren

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.7.5 Sozialmedizinische Fallberatung des MDK Hessen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.7.6 Weiterleitung von Verdachtsdiagnosen an Dritte gegen den Willen des Betroffenen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

4.8 Sozialwesen

Zu 4.8.1 Hartz IV - Bekämpfung von Leistungsmissbrauch

Eine wichtige Aufgabe aus dem Bereich des SGB II ist die Bekämpfung des Leistungsmissbrauchs, um auf diese Weise dafür zu sorgen, dass nur die tatsächlich Bedürftigen staatliche Unterstützung erfahren. Dabei kommt der Außendiensttätigkeit eine wesentliche Bedeutung zu. Der Gesetzgeber hat deshalb im Rahmen des Gesetzes zur Fortentwicklung der Grundsicherung für Arbeitsuchende vom 20. Juli 2006 die vom Hessischen Datenschutzbeauftragten zitierte Regelung in § 6 Abs. 1 Satz 2 in das SGB II aufgenommen, wonach die Grundsicherungsträger einen Außendienst zur Bekämpfung von Leistungsmissbrauch schaffen sollen. Weitere Einzelheiten hat der SGB II - Gesetzgeber nicht geregelt, sodass insoweit u.a. die von dem Hessischen Datenschutzbeauftragten genannten Bestimmungen des SGB X zum Sozialverwaltungsverfahren und zum Sozialdatenschutz sowie die datenschutzrechtlichen Vorgaben gelten.

Vor diesem Hintergrund kann den grundsätzlichen Ausführungen des Hessischen Datenschutzbeauftragten, insbesondere im Hinblick auf den stets zu beachtenden Grundsatz der Verhältnismäßigkeit ebenso zugestimmt werden, wie der Beurteilung des an ihn herangetragenen Einzelfalls. Auf der Grundlage seiner Schilderung des Sachverhalts unterliegt es keinen Zweifeln, dass der Grundsatz der Verhältnismäßigkeit bei dem beschriebenen Umfang bzw. der Dauer der Beobachtung nicht mehr gewahrt war, weil nichts dafür erkennbar ist, dass eine derart lang andauernde Observierung erforderlich war.

Zu 4.8.2 Hartz IV - Auskunftspflichten von Trägern der freien Wohlfahrtspflege gegenüber Arbeitsagenturen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

§ 17 Abs. 1 SGB II bestimmt, dass die SGB II - Leistungsträger bei den nach dem Gesetz zu erbringenden Eingliederungsleistungen - so auch den von dem Hessischen Datenschutzbeauftragten erwähnten Leistungen nach § 16 Abs. 2 SGB II - möglichst auf bereits vorhandene Einrichtungen und Dienste Dritter zurückgreifen sollen. Dementsprechend müssen diese Dritten den SGB II - Trägern die erforderlichen Auskünfte erteilen. Dies wird rechtlich über die Vorschrift des § 61 Abs. 1 SGB II abgesichert, wonach Träger, die Eingliederungsleistungen erbringen oder erbracht haben, der Agentur für Arbeit in ihrer Eigenschaft als SGB II Träger oder ggf. der betreffenden Optionskommune unverzüglich die erforderlichen Auskünfte zu erteilen haben, damit beurteilt werden kann, ob und inwieweit Leistungen zu Recht erbracht wurden. Dabei findet die Diskretion z.B. einer Sucht- oder einer Schuldnerberatungsstelle immer dann ihre Grenze, wenn die Kenntnis von bestimmten Tatsachen im Einzelfall zur Erledigung der Aufgaben des SGB II - Trägers erforderlich ist.

Zu 4.8.3 Zusammenarbeit zwischen Arbeitsschutzbehörden und Unfallversicherungsträgern

Die Stellungnahme des Hessischen Datenschutzbeauftragten zu einer Anfrage betreffend den Datenaustausch und die Zusammenarbeit von Arbeitsschutzbehörden und Trägern der Gesetzlichen Unfallversicherung bestätigt die Auffassung der Landesregierung, dass der Datenaustausch zum Zwecke der Erfüllung gesetzlich vorgeschriebener Aufgaben zulässig ist. Aus Sicht des Hessischen Datenschutzbeauftragten bestanden gegen das vorgesehene Pilotprojekt keine Bedenken.

Das in Rede stehende Pilotprojekt hatte seinen Ursprung in den Erfahrungen der Aufsichtsdienste der Arbeitsschutzbehörden und der Unfallversicherungsträger, dass der Arbeitsschutz in der Zeitarbeitsbranche ohne besonderen Austausch der entsprechenden Betriebsdaten nicht verbessert werden kann. Das Projekt wurde konzipiert als noch nicht abzusehen war, dass im Rahmen der gesetzlichen Verankerung der "Gemeinsamen Deutschen Arbeitsschutzstrategie" sowohl der Datenaustausch eine neue Rechtsgrundlage erhalten als auch das Thema "Zeitarbeit" zu einem bundesweit durchzuführenden Schwerpunktprogramm aller Länderbehörden und Unfallversicherungsträger werden würde.

Mit dem Inkrafttreten des § 21 Abs. 3 neu ArbSchG im Rahmen des Unfallversicherungsmodernisieriungsgesetzes (UVMG) im Oktober 2008 und den Beschlüssen der Nationalen Arbeitsschutzkonferenz zu Handlungsfeldern und Arbeitsprogrammen ist das Erfordernis eines gesonderten Pilotprojekts zur Verbesserung des Arbeitsschutzes bei der Zeitarbeit nicht mehr gegeben. Das Modellprojekt wurde daher nicht durchgeführt.

Die Fragen des Daten- und Informationsaustausches werden im Rahmen der Gesamtevaluierung der "Gemeinsamen Deutschen Arbeitsschutzstrategie" und ihrer Arbeitsprogramme zu evaluieren sein.

4.9 Personalwesen

Zu 4.9.1 Informationsrecht des Personalrats

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu den Informationsrechten des Personalrats zu. Die §§ 107ff Hessisches Beamtengesetz (HBG) und das Hessische Personalvertretungsgesetz (HPVG) enthalten keine gesetzliche Regelung in Form einer Befugnis, die der Personalvertretung die im Tätigkeitsbericht genannten anlassfreien Aufstellungen und Leserechte gewähren würde.

Bereits im neunten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Landtagsdrucksache 9/4032) wurde unter Ziffer 4.1.4 (1. Spiegelstrich) ausgeführt:
"Die Personalvertretungen sind Teil der "speichernden Stelle", nicht aber "Dritte" im Sinne der Datenschutzgesetze. Die Frage, welche personenbezogenen Daten der Personalrat von der Dienststellenleitung verlangen kann, richtet sich ausschließlich nach den Bestimmungen des Hessischen Personalvertretungsgesetzes (HPVG) und den dort abschließend umschriebenen Aufgaben der Personalvertretung; nicht aber sind die datenschutzrechtlichen

Vorschriften über die Übermittlung (§ 3 HDSG i. V. m. § 24 BDSG) heranzuziehen".

Nach alledem ist die Verarbeitung in Form der Übermittlung personenbezogener Daten dann - datenschutzrechtlich - unzulässig, wenn, wie ausgeführt, keine personalvertretungsrechtliche Rechtsgrundlage vorliegt.

Die Vorlage eines Berichts über Qualifizierungsmaßnahmen mit namentlicher Auflistung der Bediensteten an den Personalrat könnte aber zum Beispiel im Zusammenhang mit dem Beteiligungstatbestand des § 74 Abs. 1 Nr. 8 HPVG (Grundsätze der Berufsausbildung und Fortbildung der Beschäftigten) zulässig sein, wenn diese anlässlich der mitbestimmungspflichtigen Einführung oder Fortschreibung eines "Fortbildungskonzepts" bzw. eines "Fortbildungskatasters" erfolgt.

Zu 4.9.2 Amtsbezeichnungen im Intranet der Finanzverwaltung

Die Landesregierung teilt die Auffassung des Hessischen Datenschutzbeauftragten.

Die Veröffentlichung von Amtsbezeichnungen der Bediensteten im Intranet der Finanzverwaltung ist nur dann zulässig, wenn die Veröffentlichung im Hinblick auf den verfolgten Zweck erforderlich ist. Aus der Tatsache, dass die Oberfinanzdirektion Frankfurt am Main die Entscheidung über die Veröffentlichung der Amtsbezeichnungen den einzelnen Dienststellen überlassen hat, war in der Tat zu schließen, dass die Veröffentlichung für die Durchführung von innerdienstlichen Maßnahmen nicht erforderlich ist. Die Daten wurden dementsprechend aus dem Intranet der Finanzverwaltung entfernt.

Die Veröffentlichung der Amtsbezeichnung von Bediensteten im Landesintranet richtet sich nach § 34 HDSG. An die Erforderlichkeit einer Veröffentlichung der Amtsbezeichnung im Landesintranet sollten jedoch keine allzu hohen Anforderungen gestellt werden.

Die Beamtin oder der Beamte führt nach § 97 Abs. 2 Satz 1 HBG im Dienst die Amtsbezeichnung des ihr oder ihm übertragenen Amts. Die Vorschrift gibt der Beamtin oder dem Beamten keinen Anspruch auf Verwendung der Amtsbezeichnung durch den Dienstherrn oder etwa darauf, von anderen Beschäftigten oder dem Publikum mit der Amtsbezeichnung angeredet zu werden, da dies lediglich eine Frage der Übung oder des Takts ist. Es lässt sich aus dieser Vorschrift auch nicht ableiten, dass sich die Beamtin oder der Beamte im Dienst immer ihrer oder seiner Amtsbezeichnung zu bedienen hätte. Vielmehr ist auch dies eine Frage der Übung. Die Amtsbezeichnung hat im Wesentlichen organisatorische Bedeutung. Die Beamtin oder der Beamte hat ihre oder seine Amtsbezeichnung zumindest dann anzugeben, wenn dies für bestimmte dienstliche Anlässe allgemein oder im Einzelfall angeordnet ist (vgl. Plog/ Wiedow/ Lemhöfer/ Bayer, Kommentar zum Bundesbeamtengesetz, BBG, Bd. 1, § 81 Rn. 10; von Roetteken/ Rothländer, Hessisches Bedienstetenrecht, HBR, IV Beamtenrecht, Bd. 4, § 97 Rn. 7). Die Qualität von Personalaktendaten im Sinn der §§ 107ff. HBG besitzt daher zwar der Vorgang zur Ernennung nach § 9 HBG, das heißt zur ersten Verleihung eines Amtes oder eines anderen Amtes im dort genannten Sinne; die Amtsbezeichnung selbst ist aber wegen § 97 HBG im Dienst als bekannte Information über die betroffene Person anzusehen, so wie der Name selbst.

4.10 Finanzwesen

Zu 4.10.1 Auskunftspflicht der Finanzämter gegenüber Sozialleistungsbehörden für die Bearbeitung von Arbeitslosengeld II-Anträgen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Leistungen der Grundsicherung für Arbeitssuchende nach dem SGB II werden in Form von Dienstleistungen, Geldleistungen (z.B. Arbeitslosengeld II) und Sachleistungen erbracht. Träger der Leistungen sind die Bundesagentur für Arbeit und die kreisfreien Städte und Kreise. Nach § 40 Abs. 1 Satz 1 SGB II gilt § 21 Abs. 4 SGB X auch für das Verfahren nach dem SGB II, sodass die Finanzbehörden, soweit es im Verfahren nach diesem Gesetzbuch

erforderlich ist, grundsätzlich Auskunft zu erteilen haben. Die Auskunft durch die Finanzbehörden ist dabei nur erforderlich, wenn die erbetenen Angaben nicht mit Hilfe der nach dem SGB auskunftspflichtigen Personen festgestellt werden können.

Nach § 30 Abs. 4 Nr. 2 der Abgabenordnung ist die Offenbarung steuerlicher Kenntnisse nur zulässig, soweit sie durch Gesetz ausdrücklich zugelassen ist. Die um Auskunft ersuchende Behörde hat deshalb im Einzelfall unter Angabe der einschlägigen gesetzlichen Vorschriften darzulegen, dass die erbetene Auskunft zulässig ist. Bestehen hierüber Zweifel, müssen diese durch Rückfrage geklärt werden. Die Offenbarungsbefugnis besteht gegenüber Behörden, die eine öffentlich-rechtliche Verwaltungstätigkeit nach dem SGB ausüben. Als Verwaltungstätigkeit im Sinn dieser Vorschrift ist insbesondere die Gewährung und Rückforderung von Sozialleistungen sowie die Inanspruchnahme Dritter wegen Sozialleistungen anzusehen.

Die Auskunft erstreckt sich nur auf die den Finanzämtern bekannten Verhältnisse. Weitere Ermittlungen brauchen nicht durchgeführt zu werden, es sei denn, sie bieten sich aus steuerlichen Gründen an.

Es dürfen nur Auskünfte über die Einkommens- und Vermögensverhältnisse der betroffenen Personen erteilt werden. Dazu gehört auch die Einkommensquelle und damit zum Beispiel Name und Anschrift des Arbeitgebers des Unterhaltsschuldners.

§ 60 SGB II sieht für die Gewährung von Arbeitslosengeld II in bestimmten Fällen auch eine Auskunftsverpflichtung des Unterhaltspflichtigen vor. Da - wie vom Hessischen Datenschutzbeauftragten ausgeführt - die Gewährung von Arbeitslosengeld II jedoch nicht von der Frage abhängt, ob die Unterhaltspflichtigen behauptete Mieteinnahmen versteuert haben, hat die Finanzbehörde die erbetene Auskunft zu Recht verweigert.

5. Kommunen

Zu 5.1 Ergebnisse der Prüfung von Kommunen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

5.2 Ergebnisse der Prüfung von Passbehörden

Zu 5.2.1 Die Einführung des ePass

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

5.2.2 Wesentliche Ergebnisse der Prüfung in Passämtern

Zu 5.2.2.1 Abläufe

Nach Kenntnis der Landesregierung sind die Abläufe in den Passämtern zutreffend dargestellt.

5.2.2.2 Problempunkte und Lösungsansätze

Zu 5.2.2.2.1 Anspruch auf Löschung auch bei Datensicherungen

Nach § 16 Abs. 2 Satz 3 PassG soll die Speicherung des biometrischen Merkmals "Fingerabdruck" bei den Passbehörden auf die unbedingt notwendige Dauer beschränkt bleiben. Maßgebender Zeitpunkt für die Löschung ist die Aushändigung des Passes an den Passbewerber. Durch die Speicherung bis zur Aushändigung wird verhindert, dass im Falle eines Produktionsfehlers, der unter Umständen erst bei Aushändigung des Passes vom Passbewerber festgestellt werden kann, die Fingerabdrücke erneut abgenommen werden müssen. Dies dient der Kundenfreundlichkeit, da eine erneute Abnahme des Fingerabdrucks ein für den Passbewerber - auch zeitlich - belastender Akt wäre. Zugleich wird dadurch eine Minimierung des Verwaltungs- und Kostenaufwandes erzielt.

Nach Auskunft der ekom21 KGRZ Hessen, die den größten Teil der hessischen Kommunen betreut, gibt es in Hessen zurzeit zwei unterschiedliche Passverfahren. Bei dem einen Verfahren verbleiben die Passantragsdaten auf dem Server der Kommune bis zur Aushändigung des Passes. Die Sicherungskopien werden von der Kommune in selbst festgesetzten Intervallen vorgenommen. Dies kann bedeuten, dass die Daten im Produktivsystem gelöscht werden, jedoch wie vom Hessischen Datenschutzbeauftragten beschrieben, bis zum nächsten Sicherungsintervall weiter vorhanden sind.

Im anderen Verfahren bedienen sich die Kommunen über das Verfahren CITRIX einer sog. "Serverfarm" der ekom21 KGRZ Hessen zur Speicherung der Daten. Die Sicherungsintervalle sind von der ekom21 KGRZ Hessen festgelegt und betragen laut Auskunft der ekom21 KGRZ Hessen 35 Tage. Die Sicherung erfolgt auf Basis einer SQL-Datenbank (Sicherung des gesamten Datensatzes), sodass es aus Sicht der ekom21 KGRZ Hessen nicht möglich ist, Teile des Antragsdatensatzes, wie die biometrischen Merkmale der Fingerabdrücke, zu "isolieren" und mit kürzerer Frist zu löschen.

Zu 5.2.2.2.2 Signatur

Der Hessische Datenschutzbeauftragte berichtet, dass eine Passbehörde auf Anregung der Bundesdruckerei GmbH eine Signaturersatzkarte einer Nachbarkommune für die Datenübermittlung der Passantragsdaten an den Passproduzenten verwendet hat, ohne damit Rückfragen oder Probleme zu verursachen. Er schließt daraus, dass die Signatur durch die Bundesdruckerei GmbH nicht geprüft wird.

In dem beschriebenen Einzelfall ist die betroffene Passbehörde der Landesregierung nicht bekannt und daher nur eine allgemeine Stellungnahme möglich.

Zum Verständnis des Sachverhalts ist zunächst das Verfahren der Datenübermittlung von der Passbehörde an den Passproduzenten (Bundesdruckerei GmbH) zu skizzieren.

Kapitel 7 der Anlage zu Artikel 1 der Verordnung über die Erfassung und Übermittlung von Passdaten sowie zur Änderung der Zweiten Bundesmeldedatenübermittlungsverordnung vom 9. Oktober 2007 (BGBl. I S. 2312 und G 5702) enthält die Regelungen zur Datensicherheit bei der Übermittlung der Produktionsdaten und der Rückantworten. Danach sind als Signatur- und Verschlüsselungskomponenten solche einzusetzen, die den Anforderungen der qualifizierten elektronischen Signatur genügen. Um die Integrität der Daten zu gewährleisten, werden Signaturzertifikate bei den Passbehörden und beim Passproduzenten benutzt. Jede Passbehörde sowie der Passproduzent besitzen ein eigenes, eindeutiges Signaturzertifikat. Der jeweilige Erzeuger der Daten (Passbehörde oder Passproduzent) bildet mit dem privaten Schlüssel seines Signaturzertifikates über die zu übertragenden Daten eine sog. XML-Signatur. Der jeweilige Empfänger der Daten (Passproduzent oder Passbehörde) überprüft mit dem öffentlichen Schlüssel des Signaturzertifikates des Erzeugers die erhaltenen signierten Daten.

In dem vom Hessischen Datenschutzbeauftragten berichteten Fall wurde die Signaturersatzkarte mit Kenntnis der Beteiligten - passausstellende Behörde, Passbehörde der Nachbarkommune und der Bundesdruckerei GmbH als Passproduzent - mit den entsprechenden Berechtigungsdaten, also des privaten Schlüssels, weitergegeben. Die übermittelten Daten wurden offenbar mit der Ersatzkarte nach § 3 der PassDEÜV ordnungsgemäß elektronisch signiert und verschlüsselt und mit dem öffentlichen Schlüssel des Passproduzenten überprüft. Die gesetzlichen Anforderungen an die Sicherheit der Datenübermittlung wurden damit von den beteiligten Behörden mit den eingesetzten Verfahren erfüllt.

Die im Tätigkeitsbericht zitierte Aussage des Bundesinnenministeriums, dass die Bundesdruckerei GmbH die Signatur der Clearingstellen prüfe und nicht die der Kommunen, kann nicht nachvollzogen werden. Nach Ziffer 5.2.2 der Anlage V 1.2 zur PassDEÜV erstellt die Passbehörde ihre Bestellungen bzw. Aufträge, authentisiert (signiert) sie elektronisch und verschlüsselt sie anschließend. Dann werden die Daten an die Vermittlungsstelle (Clearingstelle) übergeben. Die Vermittlungsstelle benutzt den Webservice XPassTransportService zum Übertragen der gelieferten Daten. Der Passpro-

duzent entschlüsselt die angelieferten Daten, prüft die angehängte Signatur und speichert Bestellungen bzw. Aufträge zur weiteren Prüfung und Bearbeitung im Passproduktionssystem.

Den Kommunen wurde bei der Anschaffung der Hardware durch das Bundesinnenministerium und die Bundesdruckerei GmbH angeraten, eine Ersatzkarte anzuschaffen (Kosten unter 100 €). Im Fall einer Beschädigung der Signaturkarte kann nämlich eine Zeit von ein bis zwei Wochen bis zur Zusendung einer neuen Karte durch die Bundesdruckerei GmbH verstreichen, in der keine Passanträge entgegengenommen werden könnten.

Zu 5.2.2.2.3 Datenprüfung bei der Ausgabe

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend. Die Passbehörden haben keine Möglichkeit einen sogenannten 1:1 Abgleich der Fingerabdruckdaten vor Ort vorzunehmen. Nach Auffassung des Bundesinnenministeriums wird dem Transparenzgebot durch die Möglichkeit zur Visualisierung der im elektronischen Chip gespeicherten Daten Rechnung getragen.

Zu 5.2.2.3 Ergebnisse

Die Landesregierung erachtet die Anregung des Hessischen Datenschutzbeauftragten, die Intervalle der Sicherungskopien auf ein Minimum zu verkürzen, für sinnvoll und wird die Problematik mit dem Bund und den Ländern erörtern.

Zu 5.3 Melderegisterauskünfte an Adresshändler

Der Hessische Datenschutzbeauftragte schlägt Änderungen im Melderecht vor, damit dem Missbrauch von erteilten Sammelauskünften durch Adresshändler besser begegnet werden kann. Die unterbreiteten Vorschläge sind erwägenswert, erfolgen aber zu einer Zeit, in sich das Melderecht im Umbruch befindet. Seit der Änderung der Gesetzgebungszuständigkeiten im Zuge der Föderalismusreform liegt die ausschließliche Befugnis zur Gesetzgebung für das Meldewesen beim Bund. Ein Bundesmeldegesetz kann erst in der nächsten Legislaturperiode erwartet werden.
Eine Änderung des Hessischen Meldegesetzes erscheint zum gegenwärtigen Zeitpunkt unangebracht.

Zu 5.4 Weitergabe von Daten durch eine Stadträtin

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 5.5 Vorlage von Scheidungsurteilen bei erneuter Eheschließung

Zu den Pflichten des Standesamtes bei der Vorbereitung einer Eheschließung gehört auch die Prüfung des Verbots der Doppelehe (§ 1306 BGB). Eheschließende, die schon einmal verheiratet waren, müssen aus diesem Grund die Auflösung der Vorehe nachweisen. In dem bis zum 31. Dezember 2008 geltenden Personenstandsgesetz war dies generell in dem Auftrag zur Prüfung der Ehefähigkeit angelegt (§ 5 Abs. 2 Satz 1 PStG a.F.), während die Konkretisierung in § 159 Abs. 2 Satz 2 der Allgemeinen Verwaltungsvorschrift zum Personenstandsgesetz, der so genannten Dienstanweisung (DA), geregelt war. Weitergehend enthält § 159 Abs. 2 Satz 4 DA eine Beschreibung der Nachweismöglichkeiten, darunter in Nr. 2 "*…eine mit dem Zeugnis der Rechtskraft versehene Ausfertigung der Entscheidung eines deutschen Gerichts über die Scheidung…*".

Diese Wortwahl ließ die Deutung zu, dass das komplette Scheidungsurteil vorzulegen ist, Gleichwohl genügte mit Blick auf die nachzuweisende Tatsache, die Auflösung der Ehe, eine Ausfertigung des Urteilstenors dieser Anforderung (Hepting/Gaaz Personenstandrecht Band I § 5, Randnr. 44); den vollständigen Entscheidungstext benötigt das Standesamt nicht.

Diese Rechtslage gilt auch nach dem Inkrafttreten der Personenstandsnovelle - Personenstandsgesetz vom 19. Februar 2007 (BGBl. I S. 122) und Personenstandsverordnung vom 22. November 2008 (BGBl. I S. 2263) - am 1. Januar 2009 weiter. Die Verpflichtung, die Auflösung einer Vorehe durch

eine öffentliche Urkunde nachzuweisen, ist in das Gesetz selbst aufgenommen worden (§ 12 Abs. 2 Nr. 4 PStG). In dem Entwurf einer neuen Allgemeine Verwaltungsvorschrift zum PStG (PStG-VwV) - Stand 3. April 2009 -, die die bisherige Dienstanweisung ablösen soll, wird - abweichend von § 159 Abs. 4 DA - darauf verzichtet, die Nachweismodalitäten konkret aufzuzeigen. Damit wird die Möglichkeit zur Missdeutung vermieden, die im zugrundeliegenden Sachverhalt offensichtlich zu der Eingabe an den Hessischen Datenschutzbeauftragten geführt hat.

6. Stiftungsaufsicht

Zu 6.1 Hessisches Stiftungsverzeichnis

Der Hessische Datenschutzbeauftragte hat das Ministerium des Innern und für Sport bei der Entwicklung der Portal-Fachanwendung "Hessisches Stiftungsverzeichnis" beratend begleitet. Seine Anregungen, zuletzt die Einschränkung der Zugriffsrechte, wurden aufgenommen; das Verfahren läuft mit den Umsetzungen seit dem 18. Dezember 2008 produktiv. Eine Klarstellung der Befugnisse der Stadt Frankfurt am Main wird spätestens im Rahmen der Evaluation des Hessischen Stiftungsgesetzes erfolgen.

7. Sonstige Selbstverwaltungskörperschaften

7.1 Rundfunk

Zu 7.1.1 Verbesserter Datenschutz bei der Befreiung von der Rundfunkgebührenpflicht

Den Anliegen des Datenschutzes wurde durch die Regelung im Zehnten Rundfunkänderungsstaatsvertrag Rechnung getragen.

Zu 7.1.2 Änderung der "Impressumspflicht" für Beiträge im Offenen Kanal

Der entsprechend den Empfehlungen des Hessischen Datenschutzbeauftragten geänderte § 39 Abs. 2 des Gesetzes über den privaten Rundfunk in Hessen (Hessisches Privatrundfunkgesetz - HPRG) ist am 1. September 2008 in Kraft getreten.

8. Entwicklungen und Empfehlungen im Bereich der Technik

Zu 8.1 Orientierungshilfe Internet

Die Landesregierung begrüßt die Fortschreibung und Aktualisierung der Orientierungshilfe Internet. Das Dokument ist eine wertvolle Arbeitshilfe für die Dienststellen der Landesverwaltung.

9. Bilanz

Zu 9.1 Online-Durchsuchungen (36. Tätigkeitsbericht, Ziff. 1.3.3 und 4.1)

Ausweislich der Koalitionsvereinbarung für die Legislaturperiode 2009 - 2014 (Kapitel "Innen und Recht" Ziffer 7) konnte zwischen den die Regierung tragenden Parteien kein Konsens zur Online-Durchsuchung gefunden werden. Deshalb wird es eine derartige Befugnis für die hessische Polizei nicht geben.

Zu 9.2 Änderungen im Personenstandswesen (36. Tätigkeitsbericht, Ziff. 4.3)

Auch im Berichtsjahr 2008 hat der Hessische Datenschutzbeauftragte das Ministerium des Innern und für Sport bei der Umsetzung der Personenstandsnovelle beratend begleitet. Schwerpunktmäßig ging es dabei um die Verankerung der Anforderungen an das elektronische Verfahren zur Führung der Personenstands- und Sicherungsregister in der Verordnung zur Ausführung des Personenstandsgesetzes vom 22. November 2008 (BGBl. I S. 2263), sowie die Realisierung der elektronischen Registerführung in hessischen Standesämtern.

In der fachlichen Bewertung des zweckmäßigsten Speicherkonzepts für Personenstandsdokumente, das in der Personenstandsverordnung zu regeln war, gab es eine uneingeschränkte Übereinstimmung zwischen dem Hessischen Datenschutzbeauftragten und dem Ministerium des Innern und für Sport; das Bundesministerium des Innern hat die hessische Position allerdings nicht übernommen. Um den im Personenstandsgesetz für den 1. Januar 2009 zugelassenen Beginn der elektronischen Registerführung nicht zu gefährden, ist das Ergebnis von hessischer Seite hingenommen worden.

Parallel zu den Arbeiten am Regelwerk hat sich in Hessen eine auf Anregung des Ministeriums des Innern und für Sport gebildete Arbeitsgruppe mit der technischen Realisierung der elektronischen Registerführung befasst. Neben dem Hessischen Datenschutzbeauftragen und dem Ministerium waren dort der Fachverband der Hessischen Standesbeamtinnen und Standesbeamten, die ekom21 KGRZ Hessen sowie der Verlag für Standesamtswesen mit der Fachhochschule Gießen/Friedberg vertreten. Auf der Grundlage der in der Arbeitsgruppe geleisteten Vorarbeiten hat die ekom21 KGRZ Hessen ein mandantenfähiges Registerverfahren bereitgestellt, mit dem die standesamtlichen Fachverfahren über die von der Fachhochschule Gießen/Friedberg entwickelte Schnittstelle kommunizieren. Hinsichtlich des Verfahrens AutiSta des Verlags für Standesamtswesen ist diese Zusammenarbeit zum 1. Januar 2009 realisiert worden. Das Standesamt Frankfurt am Main hat mit Jahresbeginn als erstes Standesamt in Deutschland mit der elektronischen Führung der Personenstandsregister begonnen. Zum 1. März 2009 haben sich 282 weitere hessische Standesämter angeschlossen; im Wochendurchschnitt werden gegenwärtig in Hessen ca. 2000 Personenstandsfälle elektronisch beurkundet. Derzeit finden Gespräche zwischen der ekom21 KGRZ Hessen und dem Hersteller des zweiten standesamtlichen Fachverfahrens Open ELViS, der PROFI AG mit dem Ziel statt, die Schnittstelle noch im Laufe dieses Jahres in das Verfahren zu implementieren, sodass die Anwender von Open ELViS ab dem 1. Januar 2010 ebenfalls die Möglichkeit haben, die Personenstands- und Sicherungsregister elektronisch zu führen.

Die Absicht des Hessischen Datenschutzbeauftragten, die weitere Realisierung des Vorhabens zu begleiten, wird von der Landesregierung uneingeschränkt begrüßt

Zu 9.3 Räumliche Situation der Ausländerbehörde in Fulda (36. Tätigkeitsbericht, Ziff. 5.4.1.3)

Nach dem Bericht der Stadt Fulda an das Ministerium des Innern und für Sport wurden durch die Zusammenlegung der Ausländerbehörden des Landkreises Fulda und der Stadt Fulda neue Räumlichkeiten im Gebäude des Landkreises Fulda bezogen. Die früher festgestellten Mängel im Hinblick auf datenschutzrechtliche Belange wurden dadurch ausgeräumt.

Zu 9.4 LUSD - Zentrale Lehrer- und Schülerdatenbank (36. Tätigkeitsbericht, Ziff. 5.6.1)

Die Darstellung der Entwicklung und des Sachstands ist zutreffend.

Zu 9.5 Löschung von Daten im SAP R/3 HR-System (36. Tätigkeitsbericht, Ziff. 5.10.3.2)

Seit dem Releasewechsel 2007/2008 wird in Hessen SAP ERP 6.0 eingesetzt. Insofern wird darauf hingewiesen, dass die Bezeichnung SAP R/3 nicht mehr korrekt ist. Die Landesregierung hält die Kritik des Hessischen Datenschutzbeauftragten gegenüber der noch nicht erfolgten Produktivsetzung des Löschkonzepts für berechtigt. Grund für die Verzögerung ist der bis Mitte März 2009 dauernde Test des Konzepts für die Löschung von Bewerberdaten durch das Kultusministeriums, der nicht fehlerfrei verlief. Dem Hessischen Competence Center wurden im Anschluss die noch bestehenden Fehler und Probleme gemeldet. Laut dem Hessischen Competence Center sind nunmehr sämtliche gemeldeten Fehler behoben worden. Bis Ende Mai 2009 müssen weitere Tests durchgeführt werden. Die Freigabe des Löschkonzeptes wird dann erfolgen, wenn das Programm zur Löschung der Bewerberdaten nachweislich fehlerfrei arbeitet. Andernfalls wäre das Risiko zu groß, dass entweder Bewerberdaten gelöscht würden, die sich noch in laufenden Verfahren befinden oder dass Daten von Bewerbern weiterhin im Verfahren blieben, die zu löschen sind. Diese Fehler würden auch

dazu führen, dass Auswertungen, zum Beispiel der Einstellungsbericht, fehlerhafte Daten lieferten bzw. Bewerber aus laufenden Verfahren verschwänden. Diese Bewerber würden dann ggf. nicht mehr berücksichtigt werden und falsche Entscheidungen und Gerichtsverfahren könnten die Folge sein.

Zwar ist derzeit im SAP-Standard die Löschung ganzer Personalnummern noch nicht möglich - worauf der Hessische Datenschutzbeauftragte zu Recht hinweist. Die ersten Ergebnisse der vom Hessischen Datenschutzbeauftragten angesprochenen Arbeitsgruppe geben der Landesregierung aber Anlass zur Hoffnung, dass rasch eine neu entwickelte Lösung im Landesreferenzmodell Personalwesen implementiert werden kann.

Zu 9.6 Business-Warehouse-HR (HEPISneu) (36. Tätigkeitsbericht, Ziff. 5.10.3.5

Die Erkenntnisse aus dem Projekt "HEPISneu" wurden in die Aufgabe der Regelorganisation übertragen. Im HMdIS wird eine Auswertestelle eingerichtet, die sich der vorhandenen Systeme bedient, um die für die Landesverwaltung notwendigen Personaldaten zur Verfügung zu stellen, sodass statistische Auswertungen vorgenommen werden können.

Zu 9.7 Personalkostenhochrechnung (35. Tätigkeitsbericht, Ziff. 5.9.1.3 und 36. Tätigkeitsbericht, Ziff. 5.10.3.4)

Die Landesregierung verweist zunächst auf die ausführliche Stellungnahme zum 36. Tätigkeitsbericht (zu Ziffer 5.10.3.4 - Drucks. 17/662). An den dort skizzierten Notwendigkeiten, insbesondere im Bereich des Kultusministeriums hat sich nichts geändert. Gleichwohl wird die Landesregierung prüfen, ob eine für alle Seiten akzeptable rechtliche Lösung gefunden werden kann. Diese könnte dann ggf. im Rahmen der anstehenden Dienstrechtsreform umgesetzt werden.

Wiesbaden, 28. August 2009

Der Hessische Ministerpräsident:
Koch

Der Hessische Minister des Innern und für Sport:
Bouffier