19. Wahlperiode

Drucksache **19/1507**

HESSISCHER LANDTAG

21. 01. 2015

Stellungnahme
der Landesregierung
betreffend den Zweiundvierzigsten Tätigkeitsbericht
des Hessischen Datenschutzbeauftragten
Drucksache 19/289

Eingegangen am 21. Januar 2015 · Ausgegeben am 11. Februar 2015
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Inhaltsverzeichnis

Stellungnahme zu:

1. Einführung

Zu 1.1 Allgemeines

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass durch die Präsenz der bekannt gewordenen Abhöraktivitäten ausländischer Nachrichtendienste in den Medien bei vielen Bürgerinnen und Bürgern der Eindruck entstanden sein kann, andere Datenschutzthemen spielten jetzt keine Rolle mehr. Gerade die vom Hessischen Datenschutzbeauftragten angeführten Themen - Soziale Netzwerke, private Videoüberwachungsanlagen - sind Beispiele für alltägliche Vorgänge, die sehr unmittelbare Auswirkungen auf die Privatsphäre des Einzelnen haben und deshalb mindestens dieselbe Aufmerksamkeit verdienen.

Zu 1.2 Abhöraktivitäten ausländischer Nachrichtendienste in Hessen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.3 Europa

Die Landesregierung hat bereits in der Stellungnahme zum 41. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten dessen Kritik zugestimmt, dass die von der Kommission unterbreiteten Vorschläge zur Reform des Datenschutzrechts in der Europäischen Union dringend der Korrektur bedürfen (siehe Drs. 18/7802 Seite 5). Die Beratung der Kommissionsentwürfe im Europäischen Rat ist zurzeit noch nicht abgeschlossen. Die Landesregierung setzt sich weiterhin für die Berücksichtigung der von Bund und Ländern vorgeschlagenen Änderungen ein.

Zu 1.4 Öffentlichkeitsarbeit

Die Landesregierung nimmt den Bericht des Hessischen Datenschutzbeauftragten über seine Öffentlichkeitsarbeit zur Kenntnis.

Zu 1.5 Soziale Netzwerke

Die Landesregierung teilt die Besorgnis des Hessischen Datenschutzbeauftragten, dass sich der Datenfluss in Sozialen Netzwerken von den Datenschutzaufsichtsbehörden gegenwärtig kaum kontrollieren lässt, wenn der Betreiber seinen Hauptsitz außerhalb der Europäischen Union hat.

Zu 1.6 Bundesverfassungsgericht

Mit der Entscheidung des Bundesverfassungsgerichts vom 24. April 2013 - 1 BvR 1215/07 - wurde über eine Verfassungsbeschwerde gegen das Antiterrordateigesetz befunden. Der Beschwerdeführer wandte sich gegen das als Art. 1 des Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz) vom 22. Dezember 2006 (BGBl I S. 3409) erlassene Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz - ATDG). Das Bundesverfassungsgericht befand, dass die Antiterrordatei in ihren Grundstrukturen verfassungsgemäß ist, aber hinsichtlich ihrer Ausgestaltung im Einzelnen nicht den verfassungsrechtlichen Anforderungen genügt.

Die betroffenen Sicherheitsbehörden in Bund und Ländern wurden durch das BMI über die Entscheidung und über erforderliche Maßnahmen zur Umsetzung der darin enthaltenen Maßgaben informiert. Es wurden zunächst Übergangsregelungen (Sofortmaßnahmen) im Sinne der Forderungen des Bundesverfassungsgerichts getroffen, die zum 8. Oktober 2013 abgeschlossen waren.

Hinsichtlich der darüber hinaus beanstandeten Vorschriften im ATDG gab das Bundesverfassungsgericht dem Gesetzgeber bis zum 31. Dezember 2014 eine Neuregelung auf. In enger Zusammenarbeit des Bundesinnenministeriums mit den AK II und AK IV der Innenministerkonferenz wurde ein Bericht zu den Auswirkungen des Urteils auf die Zusammenarbeit und den Austausch von personenbezogenen Daten zwischen der Polizei und dem Verfassungsschutz in den Gremien verabschiedet. Dieser bildete u.a. die Grundlage für den nun vorliegenden und in der Abstimmung befindlichen Gesetzentwurf.

Zu 1.7 Gesetzgebungsanregungen

Der Vorschlag des Hessischen Datenschutzbeauftragten, die Videoüberwachung im Hessischen Datenschutzgesetz zu regeln, wird im Rahmen der Evaluierung des Gesetzes, welche im kommenden Jahr erfolgen soll, in die Prüfung mit einbezogen werden.

1.8 Arbeitsschwerpunkte und Statistik

Zu 1.8.1 Innerbehördliche Konsolidierung

Die Landesregierung nimmt den Bericht des Hessischen Datenschutzbeauftragten über die Arbeitsschwerpunkte und Arbeitsstatistik der Aufsichtsbehörde zur Kenntnis.

2. Übergreifende Themen (öffentlicher und nicht öffentlicher Bereich)

2.1 Querschnittsthemen

Zu 2.1.1 Der Abwesenheitskalender

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass bei der Führung eines Abwesenheitskalenders in öffentlichen Stellen die Einsehbarkeit auf den Umfang beschränkt werden muss, der zur Erreichung des Zwecks, zu dem der Kalender geführt wird, erforderlich ist.

2.1.2 Zentrale Spielersperrdatei nach Glücksspielstaatsvertrag und Hessischem Spielhallengesetz

Zu 2.1.2.1 Protokollierung der Abfragen

Nach § 23 Abs. 4 Glücksspielstaatsvertrag (GlüStV) und § 11 Abs. 4 Hessisches Spielhallengesetz (HSpielhG) sind Zugriffe auf die Sperrdatei und Auskünfte aus der Sperrdatei zu protokollieren. Das Hessische Ministerium des Innern und für Sport hat die ursprünglich vorgesehene Dauer der Speicherung der Protokollierung von vier Jahren aufgrund der Bedenken des Hessischen Datenschutzbeauftragten auf ein Jahr verkürzt.

Um zu verhindern, dass die Protokollierung der Abfragen zu einer personenbezogenen Speicherung des Spielerverhaltens führt, wurde darüber hinaus beim Erzeugen des Protokolleintrags pro Abfrage ein zusätzlicher Mechanismus geschaffen (Hinzunahme eines Zufallswertes vor dem Erzeugen des Hasheintrags für die Protokolldatei), der keinerlei Rückschlüsse auf die angefragten Parameter zulässt. Durch diese beiden Änderungen wurde den Bedenken des Hessischen Datenschutzbeauftragten Rechnung getragen.

Der Hessische Datenschutzbeauftragte hat dem Hessischen Ministerium des Innern und für Sport im März 2014 mitgeteilt, dass gegen das Protokollierungskonzept in dieser aktualisierten Form keine Bedenken mehr bestehen.

Zu 2.1.2.2 Keine Abfragepflicht für Lotterien ohne besonderes Gefährdungspotenzial

Der GlüStV bestimmt, dass Veranstalter von Lotterien mit besonderem Gefährdungspotenzial, Spielbanken und Veranstalter von Sportwetten verpflichtet sind, an einem bundesweiten Spielersperrsystem teilzunehmen (§ 8 Abs. 2 und 4). Über die Auslegung des Begriffs "Lotterien mit besonderem Gefährdungspotenzial" konnte mit dem Hessischen Datenschutzbeauftragten bisher keine Einigung erzielt werden. Der Hessische Datenschutzbeauftragte kommt nach Auslegung des GlüStV zu dem Ergebnis, dass nur solche Lotterien, die mehr als zwei Ziehungen pro Woche veranstalten, als Lotterien mit besonderem Gefährdungspotenzial anzusehen sind. Der GlüStV biete dagegen keine Rechtsgrundlage für eine Sperrabfrage bei Lotterien mit nicht mehr als zwei Ziehungen pro Woche. Dies gelte sowohl für Offline- als auch für Online-Lotterien.

Das Hessische Ministerium des Innern und für Sport hat diese Auffassung dem Glücksspielkollegium mitgeteilt. Das Glücksspielkollegium, dessen Mitglieder von den obersten Glücksspielaufsichten der Länder benannt werden, ist dagegen der Ansicht, jede im Internet veranstaltete Lotterie sei als Lotterie mit besonderem Suchtgefährdungspotenzial anzusehen (§ 4 Abs. 5 GlüStV). Daher habe vor jeder Teilnahme an einer Lotterie im Internet eine Sperrabfrage zu erfolgen. Im Glücksspielkollegium, das durch Mehrheitsbeschluss von mindestens zwei Dritteln der Stimmen der Mitglieder seine Entscheidungen trifft (§ 9a Abs. 8 GlüStV), ist Hessen sowie einige weitere Länder bei der Abstimmung zu dieser Frage überstimmt worden.

Um ein abgestimmtes Meinungsbild zu erhalten, hat der Hessische Datenschutzbeauftragte auf Bitten des Hessischen Ministeriums des Innern und für Sport die Datenschutzbeauftragten der anderen Bundesländer um Stellungnahme zu dieser Rechtsfrage gebeten. Eine Rückfrage ergab, dass dem Hessischen Datenschutzbeauftragten Rückmeldungen von sechs Datenschutzbeauftragten aus anderen Bundesländern vorliegen. Demnach teilen fünf Datenschutzbeauftragte (BW, BY, HH, HB und SL) die Einschätzung des Hessischen Datenschutzbeauftragten. Der Datenschutzbeauftragte aus Nordrhein-Westfalen teilte ohne weitere Begründung mit, er teile die im Glücksspielkollegium mehrheitlich vertretene Auffassung. Nach Ansicht des Hessischen Datenschutzbeauftragten wird von den Datenschutzbeauftragten aus den übrigen Bundesländern keine

Rückmeldung mehr erfolgen, sodass dieser Abstimmungsprozess als abgeschlossen angesehen werden kann.

Nach einer erneuten rechtlichen Prüfung des Sachverhalts ist die Landesregierung der Auffassung, dass der Mehrheitsbeschluss des Glücksspielkollegiums zu Fragen des Betriebs der Sperrdatei nicht bindend ist, da § 9a Abs. 8 GlüStV auf diesen nicht anwendbar ist. Es obliegt vielmehr den zuständigen Glücksspielaufsichten in den einzelnen Bundesländern, in eigener Verantwortung darüber zu entscheiden, ob Lotterien ohne besonderes Gefährdungspotential an OASIS GlüStV anzuschließen sind, wenn sie die Spielteilnahme im Internet ermöglichen. Für eine Überprüfung der durch ein anderes Bundesland getroffenen Entscheidung durch das Land Hessen fehlt es an einer gesetzlichen Grundlage. Eine eigene Rechtmäßigkeitsprüfung eines von einem anderen Bundesland in dessen Zuständigkeit erlassenen Bescheids durch das Hessische Ministerium des Innern und für Sport könnte daher als ein Verstoß gegen das Prinzip der Eigenstaatlichkeit der Bundesländer gewertet werden.

Das Hessische Ministerium des Innern und für Sport als Betreiber der Sperrdatei wird die von den zuständigen Glücksspielaufsichten getroffenen Entscheidungen lediglich umsetzen.

Zu 2.1.2.3 Anbindung der Spielhallen an die Spielersperrdatei nach § 23 GlüStV

Der Kritik des Hessischen Datenschutzbeauftragten wurde vom Hessischen Ministerium des Innern und für Sport Rechnung getragen, indem die geforderte Trennung der Spielersperren nach § 8 GlüStV und § 6 HSpielhG in der Sperrdatei OASIS erfolgreich umgesetzt wurde. Die Daten werden jetzt durch das Anfügen eines technischen Attributs getrennt nach den Rechtsgrundlagen GlüStV bzw. HSpielhG vorgehalten. Die Datenbestände der Spielersperren werden dadurch in zwei getrennten Dateien geführt mit dem Ergebnis, dass Spielersperren nach dem GlüStV nur innerhalb des Sperrsystems OASIS GlüStV eingetragen, abgefragt, geändert und aufgehoben werden können. Gleiches gilt für Spielersperren im Sperrsystem OASIS HSpielhG, die aufgrund des HSpielhG erfasst wurden.

Dieser Vorgehensweise hat der Hessische Datenschutzbeauftragte im März 2014 zugestimmt.

Zu 2.1.3 Neues Rahmenkonzept für die vernetzte Forschung

Das Hessische Ministerium für Soziales und Integration beabsichtigt in Fortschreibung der Regionalen Gesundheitsreporte 2014 und in gemeinsamer Erstellung eines im Koalitionsvertrag genannten "Versorgungsatlasses", bestimmte Versorgungsfragen und Morbiditätsentwicklungen wissenschaftlich untersuchen zu lassen. Hierfür wurden 160 000 Euro für den Landeshaushalt 2015 angemeldet.

Bei der Umsetzung dieses Projektes wird darauf geachtet werden, dass die mit entsprechenden Forschungsaufgaben betrauten Organisationen den Leitfaden der Datenschutzbeauftragten des Bundes und der Länder anwenden.

Zu 2.1.4 Akteneinsichtsrecht der Patienten

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zur Umsetzung der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden

Gesundheitsversorgung wurde in Hessen das "Gesetz über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (Patientenmobilitätsgesetz)" verabschiedet. Es trat zum 20. November 2013 in Kraft.

Im Dezember 2013 wurde zudem vom Hessischen Ministerium für Soziales und Integration ein eigenständiges Referat für "Qualitätssicherung und Patientensicherheit" etabliert. Beschwerden von Patientinnen und Patienten und Angehörigen sowie Diskussionen in verschiedenen Gremien machten die Besorgnis deutlich, dass medizinische Entscheidungen immer stärker von wirtschaftlichen Interessen oder Zwängen der Leistungserbringer überlagert werden könnten. Ökonomischen Rahmenbedingungen Priorität einzuräumen, birgt die Gefahr, das Patientenwohl und die Qualität der medizinischen Patientenversorgung zu vernachlässigen. Hier wurde die besondere Verantwortung eines Bundeslandes wie Hessen gesehen, einer solchen Entwicklung frühzeitig zu begegnen, gleichzeitig aber weiter für eine verlässliche Finanzierung von medizinischen Leistungen einzutreten.

Mit der Einrichtung eines eigenständigen Referats wurde ein deutliches Signal dafür gesetzt, dass der Bereich "Qualitätssicherung und Patientensicherheit" als originäre landespolitische Aufgabe gesehen wird.

Die neu geschaffene Bündelung von Aufgaben in einem Referat stellt sicher, dass das - auch im Hessischen Koalitionsvertrag herausgehobene - Thema kompetent und zielgerichtet bearbeitet werden kann.

Zudem ist Hessen im April 2014 als erstes Flächenland dem Aktionsbündnis Patientensicherheit (APS) beigetreten.

Zu 2.1.5 Prüfung der Rollen- und Berechtigungskonzepte für das Klinikinformationssystem in hessischen Krankenhäusern

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 2.1.6 Umgang mit Leichenschauscheinen in Kliniken

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.
Es ergibt sich auch aus dem Friedhofs- und Bestattungsgesetz (FBG), dass der Leichenschauschein vom Arzt nicht offen an den Bestattungsunternehmer übergeben werden darf. Nach § 12 Abs. 4 FBG sind bei der Leichenschau die Bestimmungen der Anlage 1 zum FBG "Durchführung der Leichenschau" zu beachten. In Abs. 5 der Anlage 1 zum FBG ist ausdrücklich geregelt, dass der Leichenschauschein zu verschließen ist.

3. Datenschutz im öffentlichen Bereich

3.1 Europa

3.1.1 Geplante EU-Datenschutz-Grundverordnung und EU-Richtlinie für Polizei- und Justizbehörden

Zu 3.1.1.1 EU-Datenschutz-Grundverordnung

Die Beratung des Entwurfs der EU-Datenschutz-Grundverordnung im Rat der Europäischen Union ist noch nicht abgeschlossen. Der Trialog zwischen dem Parlament, dem Rat und der Kommission wurde noch nicht aufgenommen.

Zu 3.1.1.2 EU-Richtlinie für Datenschutz bei Polizei- und Justizbehörden

Der von der EU-Kommission vorgelegte Entwurf für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr wird gegenwärtig im Europäischen Parlament und im Rat der Europäischen Union beraten. Das Europäische Parlament hat am 12. März 2014 in erster Lesung seinen Standpunkt festgelegt und etliche Änderungsvorschläge unterbreitet. Im Rahmen der Beratungen zur Richtlinie im Rat hat sich gezeigt, dass es noch zahlreiche offene rechtliche Fragen, insbesondere zum Anwendungsbereich der Richtlinie, gibt und die EU-Mitgliedstaaten weiteren erheblichen Prüf- und Erörterungsbedarf sehen.

Aus hessischer Sicht sollte darauf geachtet werden, dass es durch die Datenschutz-Richtlinie nicht zu einer Beeinträchtigung der Arbeit der Sicherheitsbehörden kommt. Dabei gilt es, einen hohen Datenschutzstandard und die Praxistauglichkeit des Datenschutzes in Ausgleich zu bringen.

Zu 3.1.2 Defizite einer EU-Verordnung über die elektronische Identifizierung und Vertrauensdienste

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten insofern zu, als dass bisher tatsächlich keine Vertrauensdienste im Verordnungsentwurf vorgesehen sind. Im Übrigen ist die Kritik an De-Mail und der fehlenden Ende-zu-Ende-Verschlüsselung bekannt und ihr wird insofern seitens der Landesverwaltung Rechnung getragen, dass von jeder Behörde im Rahmen des ihr zustehenden Ermessens von Fall zu Fall zu entscheiden sein wird, ob neben einer Transportverschlüsselung noch zusätzlich eine Ende-zu-Ende-Verschlüsselung durchgeführt werden muss. Allerdings erfolgt in den Bereichen, in denen die technischen Voraussetzungen für De-Mail und einer Ende-zu-Ende-Verschlüsselung nicht gegeben sind, keine Datenübertragung. Im Übrigen sind derzeit nur die Bundesbehörden verpflichtet, ab dem 1. Juli 2015 einen Zugang für De-Mail zu eröffnen.

3.1.3 Gemeinsame Kontrollinstanz für das Schengener Informationssystem

3.1.3.1 Schengener Informationssystem der zweiten Generation (SIS II)

Zu 3.1.3.1.1 Inbetriebnahme des SIS II

SIS II ging entgegen den Ausführungen im Tätigkeitsbericht nicht am 9. März 2013 sondern erst am 9. April 2013 durch die Freischaltung der INPOL-TN-Länder durch das BKA in Betrieb. Im Übrigen ist die Darstellung im Tätigkeitsbericht zutreffend.

Zu 3.1.3.1.2 Rechtsgrundlagen

Die vom Hessischen Datenschutzbeauftragen angeführten Änderungen, insbesondere die Speicherungen biometrischer Merkmale, wurden umgesetzt. Weitere Neuerungen sind:

- andere "Datentiefe", d.h. teilweise mehr Informationen z.B. durch weitere Felder bzw. Attribute in den "alten" Fahndungskategorien gemäß SIS 1+,
- andere erlaubte Zeichen,
- Schengen-Aktivierung des Europäischen Haftbefehls (EAW - European Arrest Warrent) und
- Abfrage neuer Fahndungskategorien (z.B. Flugzeuge, Boote, etc.) mit Binärdaten.

Zu 3.1.3.1.3 Von der GKI zur koordinierten Kontrollgruppe für SIS II

Die Landesregierung hat den Bericht des Hessischen Datenschutzbeauftragten über die Änderung der Zuständigkeit für die Datenschutzkontrolle des SIS II zur Kenntnis genommen.

Zu 3.1.3.2 Gemeinsame Überprüfungen der Ausschreibungen zur Festnahme im Schengener Informationssystem

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend.

Im 41. Tätigkeitsbericht (Drs. 18/7202 Seite 76) hat der Hessische Datenschutzbeauftragte berichtet, dass vor der Ausschreibung im SIS nicht in allen Fällen gemäß Artikel 95 Abs. 2 SDÜ verfahren wird. In manchen Fällen wurde nicht geprüft, ob die Festnahme des Betroffenen nach dem Recht der ersuchten Staaten zulässig ist. Diese Problematik hat sich, wie der Hessische Datenschutzbeauftragte selbst bemerkt, entschärft, da nach der nunmehr einschlägigen Vorschrift des SIS II-Beschlusses eine derartige der Ausschreibung vorangehende Prüfung nicht mehr vorgesehen ist.

Zu 3.1.3.3 Probleme bei der Ausschreibung von Kraftfahrzeugen im Schengener Informationssystem

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zur Problematik bei der Ausschreibung von Kraftfahrzeugen im Schengener Informationssystem zu. Das Land Hessen unterstützte bereits 2010 eine Initiative zum Erlass einer bundesweiten Handlungsempfehlung für Justiz und Polizei.

Zu 3.1.4 Gemeinsame Kontrollinstanz für EUROPOL

Europol verarbeitet eine große Menge sensibler personenbezogener Daten. Daher ist es wichtig, dass Europol bei der Verwendung dieser Daten die Rechte des Einzelnen beachtet. Zur Wahrung dieser Rechte beinhaltet der Europol-Ratsbeschluss, durch den sowohl Europol als auch die GKI ins Leben gerufen wurden, eine Reihe von Bestimmungen zum Datenschutz.

Der von der EU-Kommission am 27. März 2013 vorgelegte Entwurf einer Europol-Verordnung, der auch Änderungen der Vorschriften zum Datenschutz beinhaltet, wird derzeit noch im Europäischen Parlament und im Rat der Europäischen Union beraten. Das Europäische Parlament hat seinen Standpunkt in erster Lesung zum Entwurf am 25. Februar 2014 festgelegt und auf der Tagung der EU-Justiz- und Innenminister am 5./6. Juni 2014 wurde seitens des Rates eine allgemeine Ausrichtung zur Europol-Verordnung beschlossen. In den entsprechenden Textvorschlägen, die die Grundlage für die weiteren Verhandlungen im Rahmen des Gesetzgebungsverfahrens bilden, sind bereits einige Änderungen im Hinblick auf die vom Hessischen Datenschutzbeauftragten angesprochenen datenschutzrechtlichen Defizite festzustellen, wie etwa die Stärkung der nationalen Kontrollbehörden.

Zu 3.1.5 "Smart Borders" - Intelligente Grenzen im Europäischen Raum

Ziel des Smart Borders Pakets ist es, angesichts wachsender Reiseströme die Grenzabfertigung durch den Einsatz moderner Technologien zu beschleunigen, den Komfort für die Reisenden zu erhöhen und gleichzeitig ein hohes Maß an Sicherheit zu gewährleisten.

Das Smart Borders Paket sieht die Einführung von zwei neuen Instrumenten vor, ein europäisches Ein-/Ausreiseregister (EES) und ein europäisches Registrierungsprogramm für Vielreisende (RTP).

Im EES sollen die Ein- und Ausreisen von Drittstaatsangehörigen elektronisch erfasst werden, die sich zu einem Kurzaufenthalt (max. 90 Tage innerhalb eines Zeitraums von 180 Tagen) in die EU begeben. Auf diese Weise kann die zulässige Aufenthaltsdauer automatisch berechnet und ihre Einhaltung besser kontrolliert werden. Die Kontrolle der zulässigen Aufenthaltsdauer sowohl von visumfrei Einreisenden als auch von Reisenden mit Kurzzeitvisa ist letztlich auch eine Frage der Glaubwürdigkeit der EU-Visumpolitik. Außerdem kann bei einer elektronischen Erfassung der Ein- und Ausreise die manuelle Stempelung der Reisepässe entfallen, was Voraussetzung für eine (Teil-)Automatisierung der Grenzkontrollen ist (sog. "e-gates"). Ob und in welchem Umfang die Mitgliedstaaten automatisierte Grenzkontrollen einführen wollen, bleibt ihnen überlassen. Sinnvoll dürften automatisierte Grenzkontrollen vor allem an viel frequentierten Grenzübergängen, insbesondere an Flughäfen sein. Hier setzt sich diese Technologie bereits heute zunehmend für Unionsbürger durch, die nicht der Stempelungspflicht im Pass unterliegen.

Durch die Verwendung biometrischer Daten soll eine eindeutige Identifizierung der Reisenden sichergestellt werden. Dies erhöht zum einen die Zuverlässigkeit der Ein- und Ausreiseregistrierung, insbesondere wenn ein Drittstaatsangehöriger bei der Einreise einen anderen Pass benutzt als bei der Ausreise. Die Erfassung biometrischer Daten ermöglicht es jedoch insbesondere, "Overstayer" auch dann zu identifizieren, wenn sie nach der Einreise ihren Pass vernichten. Außerdem kann die Erfassung biometrischer Daten zur Aufdeckung von Identitätstäuschungen beitragen.

Derzeit werden Ein- und Ausreisedaten nur durch Abstempeln des Reisedokuments festgehalten. Mit dieser hergebrachten Verfahrensweise lässt sich aber nicht immer zuverlässig die zulässige Aufenthaltsdauer ermitteln, wobei schlechte Qualität oder Lesbarkeit der Stempel, Fälschung von Stempeln, langwierige Berechnung des Aufenthalts die Gründe sind. Dieses Verfahren ist daher fehleranfällig. Auch kann auf elektronischem Wege bislang nicht kontrolliert werden, ob, wo und wann ein Drittstaatsangehöriger in den Schengenraum einreist oder den Schengenraum verlässt.

Vom EES erfasst werden nur die Ein- und Ausreisen über die EU- bzw. Schengenaußengrenzen.

Für den Fall, dass ein Drittstaatsangehöriger von dem EES fälschlicherweise als "Overstayer" registriert wurde, etwa weil es einen Fehler bei der Ausreiseregistrierung gab oder der Betroffene berechtigter Weise über den ursprünglich berechneten Zeitraum der zulässigen Aufenthaltsdauer hinaus im Schengenraum verbleibt, hat er einen Anspruch auf Korrektur der Daten. Im Übrigen sieht der Verordnungsentwurf vor, dass bei Verlängerung der zulässigen Aufenthaltsdauer die Behörde, die die Entscheidung über die Verlängerung getroffen hat, das neue Ablaufdatum im EES eintragen muss.

Zum Zugriff der Polizei- und Strafverfolgungsbehörden enthält der VO-Vorschlag der Kommission bislang lediglich eine Evaluierungsklausel. Danach soll zwei Jahre nach Einführung des EES geprüft werden, ob ein solcher Zugang einen Mehrwert hätte. Die erste Befassung im Rat hat jedoch gezeigt, dass sich die Mehrzahl der Mitgliedstaaten dafür ausspricht, dass die Polizei- und Strafverfolgungsbehörden von Anfang an einen Zugang zur Verhütung und Verfolgung schwerwiegender Straftaten erhalten.

Auf Seiten der hessischen Justiz ist die Meinungsbildung, ob die Strafverfolgungsbehörden Zugang zu der geplanten Datenbank für ein Europäisches Einreise- und Ausreisesystem erhalten sollten oder nicht, bisher nicht abgeschlossen, zumal die Voraussetzungen, unter denen die Strafverfolgungsbehörden möglicherweise Zugang erhalten sollen, noch nicht bekannt sind. Die vorsorgliche Implementierung der technischen Zugangsmöglichkeit zu der Datenbank für die Strafverfolgungsbehörden für den Fall, dass ein solcher Zugang später - nach Auswertung der Evaluierungsergebnisse - rechtlich noch vorgesehen werden sollte, wird grundsätzlich begrüßt, da zu vermuten ist, dass die nachträgliche Implementierung wesentlich teurer wäre.

Das RTP ist ein Programm, das Drittstaatsangehörigen, die nach einer Hintergrundüberprüfung in das RTP aufgenommen wurden, Erleichterungen bei den Kontrollen an den Außengrenzen der EU bietet. Das RTP soll sicherheitsgeprüften Vielreisenden aus Drittstaaten, zum Beispiel Geschäftsreisenden, die Möglichkeit geben, mit vereinfachten Grenzkontrollen in die EU einzureisen. Nach Schätzungen der Europäischen Kommission werden jährlich fünf Millionen Drittstaatsangehörige legal dieses neue Programm bei der Einreise in die EU nutzen. Im Rahmen des

RTP können an wichtigen Grenzübergängen automatische Grenzkontrollsysteme eingesetzt werden, etwa an Flughäfen, die sich diese moderne Technologie zunutze machen. Dadurch könnten registrierte Reisende sehr viel schneller abgefertigt werden als bisher.

Die Einrichtung der neuen Systeme ist unbestritten mit einem gewissen Aufwand verbunden. Die geschätzten Kosten von 1,1 Mrd. Euro beziehen sich nach Angabe der Bundesregierung jedoch nicht nur auf die Entwicklung der neuen Systeme. Die 1,1 Mrd. Euro umfassen vielmehr sowohl die Einrichtung der zentralen als auch der nationalen Komponenten des EES und des RTP für bis zu 30 Mitgliedstaaten sowie die Betriebskosten für die ersten fünf Jahre.

Das EES und das RTP sollen zusammen die Handhabung und Kontrolle des Personenreiseverkehrs an den EU- bzw. Schengenaußengrenzen verbessern. Die Kontrollen sollen sowohl strenger als auch für vorab sicherheitsüberprüfte Vielreisende aus Nicht-EU-Ländern rascher von Statten gehen.

Die Verhältnismäßigkeit der Regelungen im Einzelnen bedarf sicher noch einer eingehenden Prüfung. Im Rahmen der Verhandlungen auf EU-Ebene wird darauf hinzuwirken sein, dass Regelungsdichte und -tiefe nicht über das für die Erreichung des Regelungszwecks erforderliche Maß hinausgehen.

3.2 Bund

Zu 3.2.1 E-Government-Gesetz des Bundes in Kraft getreten

Der Hessische Datenschutzbeauftragte erhielt vom Hessischen Ministerium des Innern und für Sport im Rahmen der Beteiligung der Innenministerien und Senatsverwaltungen für Inneres der Länder durch das Bundesministerium des Innern zu dem Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften Gelegenheit zur Abgabe einer Stellungnahme. Diese Stellungnahme diente der Vorbereitung der Äußerung des Innenministeriums gegenüber dem Bundesinnenministerium.

Zur Kritik des Hessischen Datenschutzbeauftragten an dem EGovG ist Folgendes zu bemerken:

Die Regelungen, die es zulassen, das Schriftformerfordernis neben einem elektronischen Dokument mit einer qualifizierten elektronischen Signatur (§ 3a Abs. 2 Satz 2 des Verwaltungsverfahrensgesetzes des Bundes - VwVfG) durch andere technische Verfahren als die qualifizierte elektronische Signatur zu ersetzen, sind durch eine Änderung des § 3a Abs. 2 VwVfG in Art. 3 des Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften vom 25. Juli 2013 (BGBl. I S. 2749) geschaffen worden. Das Gesetz enthält in Art. 1 das E-Government-Gesetz, das in § 2 Abs. 1 EGovG vorschreibt, dass jede Behörde verpflichtet ist, auch einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen. Die Regelung gilt ab 1. Juli 2014. Für die anderen in § 3a Abs. 2 Satz 4 VwVfG genannten technischen Verfahren zur Ersetzung der Schriftform besteht keine Verpflichtung der Verwaltung, einen Zugang zu eröffnen. Die qualifizierte elektronische Signatur kann aufgrund der Regelung in § 2 Abs. 1 EGovG gegenüber den anderen Verfahren als vorrangig angesehen werden, was der Kritik des Hessischen Datenschutzbeauftragten an den anderen technischen Verfahren zur Ersetzung der Schriftform entgegen kommt.

Die Forderung des Hessischen Datenschutzbeauftragten, die Fälle mit einem Schriftformerfordernis sinnvoll zu reduzieren und nur elektronische Dokumente mit einer qualifizierten elektronischen Signatur zur Ersetzung der Schriftform zuzulassen, steht mit dem gesetzgeberischen Ziel, die elektronische Kommunikation der Bürgerinnen und Bürger mit der Verwaltung durch andere technische Verfahren nach § 3a Abs. 2 Satz 4 VwVfG zu erleichtern sowie nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten, nicht im Einklang. Davon abgesehen hatten sich Bund und Länder in der Nationalen E-Government-Strategie des IT-Planungsrates bereits selbst das Ziel gesetzt, im Rahmen ihrer Zuständigkeit Schriftformerfordernisse zur Vereinfachung der elektronischen Kommunikation mit der Verwaltung, wo immer möglich, abzubauen.

Die Entscheidung, weitere technische Verfahren zur Ersetzung der Schriftform zuzulassen, wurde vom Bund damit begründet, dass als elektronisches Äquivalent der Schriftform allein die qualifizierte elektronische Signatur zugelassen war, die als wesentliches Hindernis für E-Government-Angebote der öffentlichen Verwaltung gesehen wurde. In der Begründung zum Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften wird ausgeführt, dass es im Gegensatz zum Zivilrecht in den öffentlich-rechtlichen Normen eine große Anzahl von gesetzlichen Schriftformerfordernissen gebe. Während die öffentlich-rechtliche Anordnung der Schriftlichkeit bei der Papierform traditionell weniger formenstreng gehandhabt werde als im Zivilrecht, so sei z.B. nicht stets eine handschriftliche Unterschrift erforderlich, es würden auch Computerfaxe anerkannt, sei als elektronisches Äquivalent der Schriftform ebenso wie im Zivilrecht bisher allein die qualifizierte elektronische

Signatur zugelassen. Die qualifizierte elektronische Signatur habe sich jedoch entgegen ursprünglichen Erwartungen in der Breite der Bevölkerung nicht durchgesetzt und werde nur in wenigen Verfahren für professionelle Anwender in der Praxis genutzt. Die Vielzahl der verwaltungsrechtlichen Schriftformerfordernisse und die Tatsache, dass diese in der elektronischen Welt allein durch die sehr wenig verbreitete qualifizierte elektronische Signatur ersetzt werden könne, führe dazu, dass in schriftformbedürftigen Verwaltungsverfahren letztlich derzeit keine ausreichend praktikable Alternative zur Papierform existiere. Nach Angaben der Bundesnetzagentur seien in den zehn Jahren von 2001 bis 2010 insgesamt 395.072 qualifizierte Zertifikate, auf denen qualifizierte elektronische Signaturen beruhen, ausgestellt worden. Dabei sei zu berücksichtigen, dass ein Wechsel der Signaturalgorithmen 2007 zu einem Austausch des Gesamtbestandes ab 2007 geführt habe. Daher sei davon auszugehen, dass ca. 300.000 Personen in der Lage seien, qualifizierte elektronische Signaturen zu nutzen (vgl. Bundesnetzagentur, "IS informiert" Nr. 48 vom 23. Mai 2011). Zum Vergleich führt die Bundesnetzagentur an, dass seit November 2010 ca. 7 Millionen neue Personalausweise ausgegeben worden seien und ca. 2 Millionen Nutzer die eID-Funktion, also den elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, eingeschaltet hätten. (Vgl. BT-Drs. 17/11473, Begründung Abschn. A Nr. 2, S. 22).

Die vom Bund angeführten Gründe sind nachvollziehbar. Der Bundesrat hat in seiner Stellungnahme vom 2. November 2012 zu Art. 3 des Gesetzentwurfs die Erweiterung der elektronischen Maßnahmen zur Ersetzung der Schriftform begrüßt, weil sich die qualifizierte elektronische Signatur aufgrund ihrer Komplexität und der damit verbundenen Kosten nicht durchsetzen konnte (BR-Drs. 557/12, Nr. 17). In seinem Beschluss vom 7. Juni 2013 hat der Bundesrat dem vom Deutschen Bundestag am 18. April 2013 verabschiedeten Gesetz zugestimmt und ferner eine Entschließung gefasst, mit welcher er unter anderem die Bundesregierung auffordert, bei der Evaluierung des Gesetzes zu untersuchen, ob und inwieweit die im De-Mail-Gesetz fehlende standardisierte Ende-zu-Ende-Verschlüsselung zu verminderter Akzeptanz und Nutzung des Verfahrens durch die Bürgerinnen und Bürger führt (BR-Drs. 356/13, Nr. 15).

Das Gesetzgebungsverfahren hat zu dem Ergebnis geführt, dass das Sicherheitsniveau der weiteren zur elektronischen Ersetzung der Schriftform zugelassenen technischen Verfahren vom Bund und von den Ländern als ausreichend eingestuft worden ist. Ein identisches Sicherheitsniveau ist nicht als erforderlich angesehen worden.

Die Dauer der Überprüfbarkeit der qualifizierten elektronischen Signatur hat mit dem Sicherheitsniveau der elektronischen Ersetzung der Schriftform nach § 3a Abs. 2 VwVfG nichts zu tun. Nach § 3a Abs. 2 Satz 2 VwVfG wird für die Ersetzung der Schriftform durch ein elektronisches Dokument mit einer qualifizierten elektronischen Signatur nicht verlangt, dass diese dauerhaft überprüfbar ist. Bei einer dauerhaft überprüfbaren qualifizierten elektronischen Signatur ist das ihr zugrunde liegende Zertifikat mindestens 30 Jahre nach dem Ende des Gültigkeitszeitraums des Zertifikats überprüfbar (vgl. § 4 Abs. 2 Signaturverordnung). Bei der nach § 3a Abs. 2 Satz 2 VwVfG verlangten Signatur ist dies nicht der Fall.

Die wichtigen Funktionen der Schriftform bestehen darin, die Integrität und Authentizität eines übermittelten Dokuments zu gewährleisten. Diese wichtige Funktionen werden nach der Einschätzung des Hessischen Datenschutzbeauftragten bei dem nach § 3a Abs. 2 Satz 4 Nr. 1 und Satz 5 geregelten elektronischen Verfahren für die unmittelbare Abgabe der Erklärung in einem elektronischen Formular als erfüllt angesehen. Nach Ablage des ausgefüllten Formulars müsse aber sichergestellt werden, dass durch technische Sicherheitsmaßnahmen Änderungen verhindert werden und die Urheberschaft dokumentiert werde. Die Landesregierung sieht dies ebenso. Hierfür sind aber keine gesetzlichen Vorgaben erforderlich. Die entsprechenden technischen Sicherheitsmaßnahmen können durch verwaltungsinterne Vorschriften vorgegeben werden. Dies ergibt sich aus dem nicht gesetzlich normierten Grundsatz ordnungsgemäßer Aktenführung, der die Pflicht der Behörde zur objektiven Dokumentation des bisherigen wesentlichen sachbezogenen Geschehensablaufs umfasst und aus dem Rechtsstaatsprinzip folgt, da nur eine geordnete Aktenführung einen rechtsstaatlichen Verwaltungsvollzug mit der Möglichkeit einer Rechtskontrolle durch Gerichte und Aufsichtsbehörden gewährleistet. Hieraus ergibt sich die Verpflichtung der öffentlichen Verwaltung, Akten zu führen (Gebot der Aktenmäßigkeit), alle wesentlichen Verfahrenshandlungen vollständig und nachvollziehbar abzubilden (Gebot der Vollständigkeit und Nachvollziehbarkeit) und diese wahrheitsgemäß aktenkundig zu machen (Gebot wahrheitsgetreuer Aktenführung). Umgekehrt folgen aus dieser Pflicht das grundsätzliche Verbot der nachträglichen Entfernung und Verfälschung von rechtmäßig erlangten Erkenntnissen und Unterlagen aus den Akten (Sicherung von Authentizität und Integrität) sowie das Gebot, den Aktenbestand langfristig zu sichern. Diese Grundsätze gelten auch für die auf IT gestützte elektronische Aktenführung und die der Behörde zugegangenen elektronischen Dokumente bzw. Formulare, die zu der elektronischen Akte ohne Änderungen zu nehmen sind. Die elektronische Akte ist daher auf Datenträgern zu führen, die ermöglichen, dass ihr Inhalt wegen der besonderen Art der Speicherung nicht unbefugt geändert oder gelöscht werden kann. Die Daten müssen zudem bis zum Ablauf der Aufbewahrungsfrist sicher gespeichert werden.

Auch in den vom Hessischen Datenschutzbeauftragten als kritisch eingestuften Fällen des § 3a Abs. 2 Satz 4 Nr. 2 und 3 VwVfG (De-Mail-Nachricht mit der Versandart nach § 5 Abs. 5 De-Mail-Gesetz) werden die wesentlichen Funktionen der Schriftform durch die sie ersetzende De-Mail erfüllt. Nach § 5 Abs. 3 De-Mail-Gesetz hat der Postfach- und Versanddienst die Vertraulichkeit, die Integrität und die Authentizität der Nachrichten zu gewährleisten. Der Nutzer des Postfach- und Versanddienstes drückt dabei seinen Willen nicht durch eine eigene qualifizierte elektronische Signatur aus, was entgegen der Auffassung des Hessischen Datenschutzbeauftragten auch nicht erforderlich ist, um von einer willentlichen Erklärung auszugehen. Diese erfolgt vielmehr dadurch, dass der Nutzer sich bei seinem De-Mail-Konto sicher anmeldet und über den zur Verfügung gestellten sicheren elektronischen Postfach- und Versanddienst seine Erklärung an den Empfänger übersendet. Die sichere Anmeldung des Nutzers steht der Eingabe einer PIN einer Person zur Erzeugung einer Signatur gleich. Nach § 4 Abs. 1 De-Mail-Gesetz muss der akkreditierte Diensteanbieter dem Nutzer den Zugang zu seinem De-Mail-Konto und den einzelnen Diensten mit einer sicheren Anmeldung ermöglichen. Für die sichere Anmeldung hat der akkreditierte Diensteanbieter sicherzustellen, dass zum Schutz gegen eine unberechtigte Nutzung der Zugang zum De-Mail-Konto nur möglich ist, wenn zwei geeignete und voneinander unabhängige Sicherungsmittel eingesetzt werden. Nach § 5 Abs. 5 De-Mail-Gesetz bestätigt der akkreditierte Diensteanbieter die Verwendung der sicheren Anmeldung, indem er im Auftrag des Senders die Nachricht mit einer dauerhaft nachprüfbaren qualifizierten elektronischen Signatur verbindet. Diese Signatur ist dem Nutzer zuzurechnen, da sie in seinem Auftrag erfolgt.

Zu der vom Hessischen Datenschutzbeauftragten geäußerten Kritik an der De-Mail wegen des Fehlens einer Ende-zu-Ende-Verschlüsselung ist zu bemerken, dass auch der Bundesrat im Gesetzgebungsverfahren betr. den Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften die De-Mail aus den gleichen Gründen kritisiert hatte (vgl. BT-Drs. 17/4145, S. 2, Nr. 2). Die Bundesregierung hatte darauf erwidert, dass eine Ende-zu-Ende-Verschlüsselung nicht in Betracht komme, weil sie das Ziel von De-Mail gefährde, eine einfache und ohne spezielle Softwareinstallation mögliche Nutzbarkeit durch die Bürgerinnen und Bürger anzubieten (vgl. BT-Drs. 17/4145, S. 9, zu Nr. 2). Der Bundestag hatte sich sodann gegen das Erfordernis einer Ende-zu-Ende-Verschlüsselung entschieden (vgl. BT-Drs. 17/4893, S. 14 zu Nr. 5). Auf die von der Bundesregierung und dem Bundestag angeführten Gründe wird verwiesen. Im Gesetzgebungsverfahren betr. den Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften war das Problem vom Bundesrat bei § 3a Abs. 2 Satz 4 VwVfG-E nicht mehr angesprochen worden (vgl. BT-Drs. 17/11473, S. 70 f., Nr. 16 bis 18)). Das Fehlen einer Ende-zu-Ende-Verschlüsselung wurde bzw. wird nunmehr akzeptiert, was vertretbar ist, da bei der Ersetzung der Schriftform durch De-Mail nach § 3a Abs. 2 Satz 4 Nr. 2 und 3 VwVfG weder für die Bürgerinnen und Bürger noch für die Verwaltung eine Verpflichtung besteht, elektronische Dokumente mit einer De-Mail zu versenden. Die Verwaltung hat hierüber nach pflichtgemäßem Ermessen zu entscheiden, so dass bei besonders sensiblen Daten, wie beispielsweise bei Gesundheitsdaten, die Ermessensentscheidung nur den Inhalt haben kann, die Versandart einer De-Mail nicht zu wählen oder aber eine Ende-zu-Ende-Verschlüsselung mit einer hierfür erforderlichen Mail-Software vorzunehmen. Letzteres setzt voraus, dass auch der Empfänger eine entsprechende Kryptografiesoftware besitzt.

Zu der Kritik des Hessischen Datenschutzbeauftragten an § 15 EGovG, wonach eine durch Rechtsvorschrift des Bundes bestimmte Pflicht zur Publikation in einem amtlichen Mitteilungs- oder Verkündungsblatt des Bundes, eines Landes oder einer Gemeinde unbeschadet des Art. 82 Abs. 1 des Grundgesetzes zusätzlich oder ausschließlich durch eine elektronische Ausgabe erfüllt werden kann, wenn diese über öffentlich zugängliche Netze angeboten wird, ist zu bemerken, dass bereits der Bundesanzeiger ausschließlich elektronisch veröffentlicht wird und auch im kommunalen Bereich die Möglichkeit geregelt ist, die öffentlichen oder ortsüblichen Bekanntmachungen der Gemeinde oder des Landkreises ausschließlich im Internet (auf ihrer Homepage) zu veröffentlichen. Der vom Bundesrat mit Beschluss vom 2. November 2012 gestellte Antrag, eine Regelung zur Begrenzung der Dauer der Veröffentlichung in der elektronischen Ausgabe zum Schutze des Persönlichkeitsrechts Betroffener zu schaffen (BT-Drs. 557/12, Nr. 14), war ohne Erfolg. Seitens der Bundesregierung wurde gegen ihn eingewandt, dass datenschutzrechtliche Regelungen ohnehin zu beachten seien. Es bleibt abzuwarten, ob dies in der Verwaltungspraxis der Fall sein wird.

Das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften ist innerhalb von fünf Jahren zu evaluieren.

3.3 Hessen

3.3.1 Querschnitt

Zu 3.3.1.1 Die behördlichen Datenschutzbeauftragten als interne und externe Ansprechpartner

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.1.2 Löschen im Dokumentenmanagementsystem der hessischen Landesverwaltung

Die Landesregierung stimmt der einleitenden Feststellung des Hessischen Datenschutzbeauftragten, dass in der hessischen Landesverwaltung die elektronischen Dokumente aus dem eingesetzten Dokumentenmanagementsystem (DMS) am Ende der Aufbewahrungsfristen dem Hessischen Staatsarchiv angeboten werden müssen, grundsätzlich zu. Darauf hingewiesen wird, dass dies auf Bereiche mit führender elektronischer Aktenführung bzw. Hybridakten, im Falle von führenden Papierakten, zutrifft.

Die Landesregierung stimmt ebenfalls zu, dass als nicht archivwürdig eingestufte Dokumente im DMS gelöscht werden müssen. Die vom Hessischen Datenschutzbeauftragten getroffene Aussage, dass die technischen Voraussetzungen für das Löschen von Dokumenten nicht vorliegen und hier zeitnah Abhilfe geschaffen werden muss, kann nicht nachvollzogen werden.

Das Löschen von elektronischen Dokumenten stellt eine bestehende Basisfunktion im DMS dar, die z.B. bei Umressortierungen, Bereinigung von Testdaten oder auch für den hier dargestellten spezifischen Fachprozess des Löschens von nicht archivwürdigen Dokumenten Anwendung findet. Entgegen der Darstellung des Hessischen Datenschutzbeauftragten liegen die technischen Voraussetzungen für das Löschen von elektronischen Dokumenten im DMS vor und werden seit geraumer Zeit in verschiedenen Bereichen in der Praxis genutzt (näheres unter Ziffer 3.3.1.2.1.).

Zu 3.3.1.2.1 Sachstand des Einsatzes des Dokumentenmanagementsystems

Die Landesregierung stimmt dem Hessischen Datenschutzbeauftragten zu, dass die Einführung eines DMS (in der Ausprägung HeDok) eines der Ziele der E-Government-Strategie des Landes Hessen ist und die Umsetzung in den beschriebenen Stufen erfolgt ist.

Zu ergänzen ist, dass die führende eAkte ab 2010 in einem Ministerium und mit paralleler Papieraktenführung und dann ab 2012 in zwei weiteren Häusern flächendeckend ohne zusätzliche Papieraktenführung eingeführt wurde. In vier Ministerien wurde die führende eAkte bis heute in einzelnen Teilbereichen, teilweise mit paralleler Papierakte, eingeführt. In zwei Ministerien befindet sich die vollständige Umstellung auf die eAkte in Planung.

Der Hessische Datenschutzbeauftragte führt ferner aus, dass ein weiterer Schritt, nämlich Dokumente dem Staatsarchiv elektronisch anbieten und endgültig löschen zu können, noch aussteht und dafür als technische Voraussetzung eine Aussonderungsschnittstelle für HeDok zu programmieren ist. Dazu ist anzumerken, dass ein einfacher manueller Anbieteprozess der Dokumente in einem archivtauglichen Format und ein endgültiges Löschen grundsätzlich auch derzeit möglich sind. Das Löschen erfolgt hier nach dem Vier-Augen-Prinzip und anschließender Beauftragung der Hessischen Zentrale für Datenverarbeitung (HZD) zur Umsetzung im System. Die geforderte Aussonderungsschnittstelle für HeDok soll den Anbiete- und Aussonderungsprozess sowohl für HeDok als auch für die auf HeDok basierenden Fachanwendungen, wie z.B. eEinbürgerung, automatisieren und damit komfortabler und effizienter gestalten.

Zu 3.3.1.2.2 Sachstand DIMAG und Aussonderungsschnittstelle für HeDok

Der Hessische Datenschutzbeauftragte weist auf ein Projekt hin, das zum Ziel hat, ein einheitliches Aussonderungsverfahren aus dem eingesetzten DMS zu definieren. Das Projekt und vor allem die Anforderungen an das Aussonderungsmodul für HeDok wurden im Rahmen der Anwenderkonferenz DOMEA zwischen Verwaltungen, Archiven und IT-Stellen mehrerer Bundesländer unter Federführung von Hessen abgestimmt.

Der Hessische Datenschutzbeauftragte stellt dar, dass seit Ende des Jahres 2012 ein Angebot der Herstellerfirma zur Umsetzung vorliege und nach Erteilung des Programmierauftrags das Aussonderungsverfahren im folgenden Jahr umgesetzt und hätte in Betrieb genommen werden können. Dazu ist anzumerken, dass ein abschließendes Angebot erst Anfang 2013 vorlag und eine direkte Beauftragung, wie vom Hessischen Datenschutzbeauftragten angesprochen, aufgrund des

Kostenvolumens nicht möglich war. Für eine Beauftragung sind die in der Hessischen Landesverwaltung geltenden Regelungen zur Mittelbereitstellung und Vergabe zu berücksichtigen. Die hier notwendigen Klärungen wurden seitens des Hessischen Ministeriums des Innern und für Sport nach Vorliegen des Angebots umgehend initiiert.

Die Planung sah außerdem vor, dass sich an den Kosten neben Hessen die beiden Bundesländer Nordrhein-Westfalen und Mecklenburg-Vorpommern beteiligen. Aufgrund von Schwierigkeiten bei der Bereitstellung der Mittel hatten sich die Länder darauf geeinigt, die Durchführung eines Umsetzungsprojektes erst in 2014 anzugehen mit dem Ziel einer Lösungsbereitstellung ab 2015. Die hessischen Mittel für die Umsetzung der Aussonderungskomponente werden entsprechend der Planung durch das Hessische Ministerium des Innern und für Sport bereitgestellt.

Die Ressorts wurden im Mai 2013 um Stellungnahme gebeten, inwieweit in 2014 dringende Bedarfe bzw. rechtliche Anforderungen für eine kurzfristige Aussonderung vorliegen. Dies war nicht der Fall. Die Ressorts haben vor diesem Hintergrund der zeitlichen Planung mit Beginn der Aussonderung ab 2015 zugestimmt.

Eine im Mai 2014 erneut durchgeführte Ressortabfrage hat dies bestätigt und gezeigt, dass umfangreiche elektronische Aussonderungsbedarfe voraussichtlich erst ab 2017 anstehen. Für in Teilbereichen anstehende Bedarfe wird eine Übergangslösung im Hessischen Ministerium für Soziales und Integration in Abstimmung mit dem Hessischen Hauptstaatsarchiv erprobt.

Zu 3.3.1.2.3 Rechtslage

Die Landesregierung stimmt den Rechtsausführungen des Hessischen Datenschutzbeauftragten zur Aktenführung in vollem Umfang zu. Dies beinhaltet auch die Darstellung, dass Akten, die nicht archivwürdig sind, zu vernichten sind, was im Falle von elektronischen Dokumenten bedeutet, dass diese im System zu löschen sind. Wie an verschiedenen Stellen aufgeführt, ist das hier geforderte Löschen von Dokumenten und Metadaten im DMS durch Beauftragung der HZD als Routineprozess etabliert. Es wird darauf hingewiesen, dass die o.g. Anforderung des Löschens auch für Umressortierungen relevant ist und im DMS seit geraumer Zeit von verschiedenen Ressorts genutzt wird.

Die Darstellung, dass sich die Hessische Landesverwaltung derzeit damit behelfe, elektronische Akten bestenfalls in die Langzeitspeicherung in HeDok zu übernehmen, die damit weder ausgesondert noch gelöscht werden und dies so einen Verstoß gegen das Hessische Datenschutzgesetz bedeute, kann daher nicht nachvollzogen werden.

Es wird darauf hingewiesen, dass die Überführung in die Langzeitspeicherung und die damit verbundene Wandlung der Dokumente in das archivtaugliche Langzeitformat PDF/A eine Anforderung der elektronischen Aktenführung und wesentliche Voraussetzung für eine Aussonderung darstellt. Das Löschen von Dokumenten im DMS, z.B. im Rahmen der Aussonderung, wird unabhängig davon im System angewandt.

Zu 3.3.1.2.4 Forderungen

Aus Sicht der Landesregierung ist der Hinweis wesentlich, dass das durch den Hessischen Datenschutzbeauftragten angemahnte rechtzeitige Löschen nicht mehr erforderlicher Daten in HeDok, unabhängig von der Verfügbarkeit einer Aussonderungsschnittstelle, derzeit möglich ist (siehe dazu zu Ziffer 3.3.1.2.1). Nach Auffassung der Landesregierung liegt daher kein Verstoß gegen das Hessische Datenschutzgesetz vor.

Entgegen der Darstellung des Hessischen Datenschutzbeauftragten werden finanzielle Mittel für die Aussonderungsschnittstelle durch das Hessische Ministerium des Innern und für Sport bereitgestellt, so dass entsprechend der mit den Ressorts abgestimmten Bedarfsplanungen auf Basis von Regelaufbewahrungsfristen derzeit die Verfügbarkeit einer elektronischen Aussonderungslösung, die einen automatisierten Löschprozess umfasst, ab 2015 vorgesehen ist. Es wird darauf hingewiesen, dass umfangreiche Aussonderungen in den obersten Landesbehörden voraussichtlich erst ab dem Jahr 2017 anstehen.

3.3.2 Justiz, Strafvollzug und Ordnungswidrigkeiten

Zu 3.3.2.1 Umsetzung der Neuregelungen des Telekommunikationsgesetzes zur Bestandsdatenauskunft in Landesrecht

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.2.2 Prüfung der HZD Hünfeld

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.2.3 Akteneinsicht im Justizvollzug

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.2.4 OWi21 - Neue Komponenten

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.
Die Regelung zur Ausgestaltung der elektronischen Einreichung von Dokumenten durch Betroffene (Online-Anhörung) soll durch eine Minister-Verordnung erfolgen. Dies setzt eine entsprechende Ermächtigung durch die Landesregierung voraus, die durch eine Änderung der Delegationsverordnung geschaffen werden soll. Sobald diese Änderung beschlossen worden ist, wird die Minister-Verordnung auf den Weg gebracht werden.

3.3.3 Verfassungsschutz

Zu 3.3.3.1 Neuordnung der parlamentarischen Kontrolle des Verfassungsschutzes

Die Darstellung des Verlaufs der Beratungen zur Neugestaltung der parlamentarischen Kontrolle des Verfassungsschutzes ist zutreffend. Die Bewertung der Vorschläge des Hessischen Datenschutzbeauftragten bleibt der Gesetzesberatung vorbehalten.

3.3.4 Ausländerwesen

Zu 3.3.4.1 Ausschreibung im Schengener Informationssystem zur Einreiseverweigerung und Befristung der Wirkung der Ausweisung

Die Entscheidung des Bundesverwaltungsgerichts vom 10. Juli 2012 (1 C 19/11) wurde den Ausländerbehörden in Hessen bekannt gegeben. Nach dieser Rechtsprechung kann ein Ausländer, der ausgewiesen wird, beanspruchen, dass die Wirkung der Ausweisung bereits mit dem Erlass der Ausweisungsverfügung befristet wird. Hat die Ausländerbehörde - entsprechend der früheren Rechtslage - keine Befristung verfügt und erweist sich die Ausweisung ansonsten als rechtmäßig, ist über den Befristungsanspruch im gerichtlichen Verfahren gegen die Ausweisung mit zu entscheiden

Wie der Hessische Datenschutzbeauftragte zu Recht feststellt, darf die Dauer der Ausschreibung im Schengener Informationssystem (SIS II) zeitlich nicht über die nach § 11 Abs. 1 des Aufenthaltsgesetzes (AufenthG) bestehende Sperrwirkung einer Ausweisungsverfügung hinausgehen.

Zu 3.3.4.2 Einverständniserklärung im Einbürgerungsverfahren - Anforderungen an Verständlichkeit und Vollständigkeit

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.4.3 Übermittlung von Lichtbildern durch Ausländerbehörden an Bußgeldstellen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

3.3.5 Schulen, Schulverwaltung, Hochschulen

Zu 3.3.5.1 Online-Bewerbungsverfahren für Wohnraum des Studentenwerks Darmstadt

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zum Abstimmungsprozess zu.

3.3.5.2 Videoüberwachung an Schulen bleibt ein Dauerthema

Zu 3.3.5.2.1 Videoüberwachung an Schulen im Landkreis Hersfeld-Rotenburg

Die im Tätigkeitsbericht des Hessischen Datenschutzbeauftragten beschriebene Praxis der Videoüberwachung im Landkreis Hersfeld-Rotenburg ist korrekt dargestellt. Zum einen entspricht die Bestandsaufnahme der Videoüberwachung im Frühjahr 2013 der damaligen Sachlage, zum anderen ist die Beschreibung der mittlerweile erfolgten Konsequenzen der Realität entsprechend. An den Schulen gibt es lediglich eine Videoüberwachung im Außenbereich zwischen 16:00 Uhr und 07:00 Uhr sowie an Wochenenden. An der Brüder-Grimm-Gesamtschule Bebra findet überhaupt keine Videoüberwachung mehr statt. Zudem wird darauf hingewiesen, dass der Schulleiter der Gesamtschule Schenklengsfeld erst nach Abschluss der Sanierungsmaßnahmen an der Schule über die Installation der Videoüberwachung durch den Schulträger informiert wurde.

Im Übrigen stimmt die Landesregierung der Rechtsauffassung des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.5.2.2 Weitere Fälle der Videoüberwachung in Schulen

Die Darstellung des Hessischen Datenschutzbeauftragten betreffend der beabsichtigten Installation von Kameras an zwei Schulen im Landkreis Schwalm-Eder-Kreis ist zutreffend.

Der Kreisausschuss des Schwalm-Eder-Kreises hat als zuständiger Schulträger den Hessischen Datenschutzbeauftragten bei zwei Anträgen auf Videoüberwachung von Schulen beteiligt. Die Bundespräsident-Theodor-Heuss-Schule in Homberg (Efze) und die Gustav-Heinemann-Schule in Borken (Hessen) hatten entsprechende Anträge gestellt.

Auf die Videoüberwachung an der Bundespräsident-Theodor-Heuss-Schule wurde - wie auch schon im Tätigkeitsbericht angeführt - verzichtet, da das Problem (Alkoholeinnahme auf dem Schulgelände und die daraus resultierenden Verunreinigungen) hierdurch nicht gelöst werden kann.

Der Schulträger hat sich jedoch entschlossen, an der Gustav-Heinemann-Schule eine Videoüberwachung zu installieren. Der Hessische Datenschutzbeauftragte hat dem zugestimmt. Hierdurch soll Vandalismus, Einbrüchen und Diebstählen vorgebeugt werden. Die Videoüberwachung soll mit einer Einbruchmeldeanlage gekoppelt und nur während der unterrichtsfreien Zeit (auch nicht während VHS-Kursen etc.) aktiv sein.

Diese Videoüberwachung wird vom Kreisausschuss als ein Pilotprojekt angesehen. Über die Erfahrungen muss dem Kreistag berichtet werden und sie sollen bei zukünftigen Anfragen von Schulen berücksichtigt werden.

Zu 3.3.5.2.3 Notwendigkeit einer Regelung der Videoüberwachung im HDSG

Der Vorschlag des Hessischen Datenschutzbeauftragten, die Videoüberwachung im Hessischen Datenschutzgesetz zu regeln, wird im Rahmen der Evaluierung des Gesetzes in die Prüfung einbezogen werden.

Zu 3.3.5.3 Einführung von elektronischen Klassenbüchern in Schulen

Die Einführung von elektronischen Klassenbüchern in Verbindung mit der LUSD ist aus Gründen der Datensicherheit und auch aus fachlichen Gründen kritisch zu sehen.

Die LUSD enthält datenschutzrechtlich relevante Daten von Schülerinnen und Schülern (Personal- und Adressdaten, Leistungsdaten, Abschlussdaten, Prüfungsdaten), von Ansprechpartnern (Personal- und Adressdaten) und von Schulpersonal (Personal- und Adressdaten, Unterrichtsdaten, dienstliche Daten).

Der Zugang zur LUSD ist deshalb bisher nur für einen in der Regel stark eingeschränkten Personenkreis (Schulleitung und Sekretariat) in den Schulen möglich. Es kann nur von stationären Rechnern in festgelegten Räumen über die gesicherten Router und das gesicherte Netz auf die LUSD zugegriffen werden.

Die Nutzung der LUSD im Rahmen von elektronischen Klassenbüchern würde bedeuten, den Personenkreis der User erheblich auszuweiten (Lehrkräfte und pädagogisches Personal, ggf. auch Eltern) und die Nutzung in den verschiedensten Räumen und mit mobilen Geräten über das offene Internet zu ermöglichen, ggf. auch von zu Hause aus.

Dagegen sind erhebliche Sicherheitsbedenken auf Seiten der LUSD anzumelden, sofern es um einen direkten Datenzugriff auf die LUSD geht. Dieser sollte auf keinen Fall in dem oben beschriebenen Ausmaß ermöglicht werden. Denkbar ist dagegen, dass über eine Schnittstelle aus der LUSD ein definierter, eng begrenzter Datensatz zu Schülern (z.B. Name, Geburtsdatum, Schule, Klasse) ähnlich wie bei der Schnittstelle zu Stundenplanprogrammen übergeben wird, mit dem zertifizierte Anbieter anderer Anwendungen dann weiterarbeiten können. Bereits die Übergabe von Daten zu Kursen und Lehrern der Schüler wäre genau zu prüfen.

Fachlich gesehen gibt die Einführung elektronischer Klassenbücher nur einen Sinn, wenn zumindest in einer Schule alle Lehrkräfte die Funktionen auch nutzen, da die Angabe von und ggf. Einsicht von Eltern in Anwesenheiten/Abwesenheiten von Schülerinnen und Schülern oder Noten oder Hausaufgaben für Eltern wie für die interne Schulverwaltung nur einen Sinn ergibt, wenn diese Daten auch vollständig und verbindlich von allen Betroffenen gepflegt werden. Einzelne Daten einzelner Lehrkräfte zu einzelnen Schülern oder Klassen wären hier eher kontra-

produktiv, würden zu Ansprüchen und Streitigkeiten und ggf. zu rechtlichen Problemen führen, wenn Eltern sich auf Daten verlassen, die dann doch nicht zuverlässig geliefert werden.

Eine rechtsverbindliche Setzung der Zulässigkeit wie auch der Verbindlichkeit der Datenpflege erscheint in diesem Zusammenhang unausweichlich.

Fachlich sind Bedenken gegen eine Entscheidung für die Einführung einer solchen Verbindlichkeit anzumelden. Es ist mit Widerständen in den Schulen und bei den Lehrkräften gegen die Verbindlichkeit der elektronischen Pflege solcher Daten zu rechnen.

Zu 3.3.5.4 Änderung des Kandidatenverfahrens der LUSD

Die Ausführungen zum aktuellen Stand des Kandidatenverfahrens und zu den damit verbundenen Problemen sind zutreffend beschrieben.

Hinzuzufügen ist, dass sich die Suche einer aufzunehmenden Schülerin bzw. eines aufzunehmenden Schülers durch die aufnehmende Schule mit dem zusätzlich notwendigen Kriterium der Straßeneingabe als Suchfeld in der Praxis insbesondere der Berufsschulen und Schulen für Erwachsene in hoher Anzahl als schwierig bis unmöglich erweist. Schülerinnen und Schüler oder Eltern wissen nach längerer Zeit nicht mehr, wie die damalige Straße hieß, oder die damals aktive Schule hat möglicherweise den Straßennamen falsch geschrieben oder abgekürzt. In solchen Fällen ist es oft unmöglich, die Schülerin bzw. den Schüler unter ihrem/ seinem Namen über das Kandidatenverfahren aufzunehmen und Schulen müssen ggf. die Schülerin/den Schüler neu in die Datenbank aufnehmen, wobei sie an Name, Vorname oder Geburtsdatum eine Änderung vornehmen müssen, um das tun zu können. Im Ergebnis sind Schülerinnen und Schüler dann doppelt in der Datenbank vorhanden, was nach Möglichkeit verhindert werden sollte.

Das vom Hessischen Datenschutzbeauftragten als Sicherheitskriterium vorgeschlagene Feld des Geburtsortes ist in diesem Zusammenhang als ebenso kritisch zu sehen, da es für dieses Feld keine Schreibkonventionen gibt und insbesondere die Schreibweise ausländischer Geburtsorte oft völlig unklar ist. Damit wären die praktischen Probleme also nicht lösbar.

Zur Lösung des Problems ist deshalb vom LUSD-Anforderungsmanagement in Absprache mit dem Hessischen Datenschutzbeauftragten folgender Vorschlag für ein sicheres und praktikables Verfahren der alternativen Schülersuche in der LUSD entwickelt worden:

Wird eine Schülerin oder ein Schüler nach Eingabe von Nachname, Vorname und Geburtsdatum in die LUSD-Suchmaske zur Schüleraufnahme als in der Datenbank vorhanden gekennzeichnet und die Schule kennt nicht die bei der Schülerin bzw. dem Schüler eingetragene Straße als 4. Kriterium, um fortfahren zu können, kann sie folgendermaßen vorgehen: Ein Sicherheitsdialog wird geöffnet oder ist von vornherein als Alternative zur Straßeneingabe sichtbar. In diesem sind die Informationen über den Benutzer und das Datum sichtbar und eine Autorisierung und Begründung für den Zugriff ist einzugeben. Diese Daten werden gespeichert. Erst wenn diese Informationen gepflegt wurden, kann ein Zugriff auf die Schülerdaten ohne Anzeige der Adresse der Schülerin oder des Schülers und der aktuellen oder letzten Schule erfolgen, sofern Name, Vorname und Geburtsdatum der Schülerin/ des Schülers eingegeben und gefunden wurden. Es muss nun, um weiterarbeiten zu können, eine neue Adresse der Schülerin/ des Schülers eingegeben werden, die farbig (rot) hervorgehoben wird, und es muss ein Kandidatenverhältnis der Schülerin/ des Schülers zur aufnehmenden Schule angelegt und angenommen werden. Dieses Kandidatenverhältnis wird, sofern die Schülerin oder der Schüler noch aktiv an einer anderen Schule ist, bei dieser Schule sichtbar.

Erst danach kann die aufnehmende Schule mit den Daten der Schülerin oder des Schülers weiterarbeiten, ihn z.B. in der Planung für das nächste Schuljahr in einer Klasse verplanen. Wird die Schülerin oder der Schüler später von der aufnehmenden Schule als tatsächlich aufgenommene Schülerin oder aufgenommener Schüler aktiviert (d.h. diese Schule wird zur stammdatenführenden Schule der Schülerin/ des Schülers), wird die rote Adresse als tatsächliche Adresse der Schülerin/ des Schülers gespeichert und wird schwarz.

Mit diesem Verfahren ist ausgeschlossen, dass eine Schule an Adressdaten von fremden Schülerinnen und Schülern herankommt, deren Namen und Geburtsdatum sie kennt. Gleichzeitig ist aber auch die Aufnahme von Schülerinnen und Schülern an einer Schule in Fällen möglich, bei denen sich der in der LUSD hinterlegte Straßenname der Schülerin bzw. des Schülers nicht rekonstruieren lässt. In der überwiegenden Zahl der Fälle bei aktiven Schülern wird es bei dem bisherigen Verfahren der Eingabe des Straßennamens als 4. Kriterium bleiben.

Diese Änderung des Kandidatenverfahrens der LUSD wird voraussichtlich im Jahr 2015 umgesetzt.

3.3.6 Gesundheitswesen

Zu 3.3.6.1 Aufbau klinischer Krebsregister in Hessen

Die Ausführungen des Hessischen Datenschutzbeauftragten bilden den aktuellen Sachverhalt zutreffend ab.
Der Hessische Landtag hat das neue Hessische Krebsregistergesetz inzwischen verabschiedet, es wurde am 24. Oktober 2014 verkündet (GVBl. S. 241). Der Hessische Datenschutzbeauftragte wurde sowohl durch seine Teilnahme im Hessischen Krebsregisterbeirat, als auch durch intensive Kontakte während des Gesetzgebungsverfahrens von Beginn an eng eingebunden.

Zu 3.3.6.2 Notwendigkeit der Eingrenzung der Datenübermittlungen vom Medizinischen Dienst der Krankenversicherung an die Krankenkasse

Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend.

Der Hessische Datenschutzbeauftragte hat bereits mit dem MDK Hessen Gespräche geführt, die dazu geführt haben, dass der MDK Hessen zugesagt hat, zukünftig verstärkt darauf zu achten, dass nur die Teile des Gutachtens an die Krankenkasse übermittelt werden, die notwendige, den Befund untermauernde medizinische Angaben mit Bedeutung für die Leistungsgewährung enthalten.
Das Hessische Ministerium für Soziales und Integration war mit diesem Sachverhalt bislang nicht befasst, wird jedoch darauf achten, dass der MDK Hessen seine Zusage einhält.

Zu 3.3.6.3 Voraussetzungen einer zulässigen Verwendung von Selbstauskunftsbogen durch die Krankenkassen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.6.4 Ungesicherte Krankenakten im Universitätsklinikum

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

3.3.7 Sozialwesen

Zu 3.3.7.1 Kooperation im Sozialwesen: Zur Bedeutung des Sozialdatenschutzes

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.7.2 Fonds "Heimerziehung in der Bundesrepublik Deutschland in den Jahren 1949 bis 1975"

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.7.3 Dauerbrenner bei Hartz IV: Übermittlung von Sozialdaten an Vermieter

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.7.4 Eigeninitiierte Sozialdatenübermittlung eines Jobcenters an die Polizei

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Die vom Hessischen Datenschutzbeauftragten in seiner ausführlichen Stellung dargelegte Rechtslage ist in die Seminarinhalte der Polizeiakademie Hessen eingeflossen. Die aktuelle Darstellung des Hessischen Datenschutzbeauftragten im 42. Tätigkeitsbericht war zudem bereits Anlass für erste positive Rückmeldungen anderer hessischer Jobcenter, da dort dieselben Fragestellungen vorhanden sind.

Zu 3.3.7.5 Vorlage eines ärztlichen Attestes bei der Erteilung einer Erlaubnis zur Vollzeitpflege in der Kinder- und Jugendhilfe

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

§ 44 des Achten Buches Sozialgesetzbuch gibt den Jugendämtern die Befugnis, von den Antragstellern die Vorlage eines ärztlichen Attests zu verlangen. Hierbei ist jedoch der Grundsatz der Datenerforderlichkeit in der Kinder- und Jugendhilfe nach § 62 Abs. 1 des Achten Buches Sozialgesetzbuch zu beachten, der besagt, dass Sozialdaten nur erhoben werden dürfen, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. Der Schlussfolgerung des Hessischen Datenschutzbeauftragten, dass der Umfang des ärztlichen Attests zu begrenzen ist, kann daher zugestimmt werden. Es genügt, wenn die Jugendämter zunächst die Information er-

halten, dass die Bewerber "geeignet" sind oder "Bedenken bestehen". Sollten Bedenken bestehen, können diese mit den Antragsstellern besprochen werden und erst in einem nächsten Schritt ggfs. eine freiwillige Schweigepflichterklärung in Betracht gezogen werden. Für die Bescheinigung "geeignet" reicht eine aktuelle Erklärung des Hausarztes aus, einer Untersuchung durch das Gesundheitsamt bedarf es aus Erforderlichkeitsgrundsätzen nicht.

Gleiches gilt im Übrigen auch für die Untersuchung von im selben Haushalt lebenden Personen über 16 Jahren im Zusammenhang mit der Erteilung einer Erlaubnis zur Vollzeitpflege nach § 44 des Achten Buches Sozialgesetzbuch. Eine anlasslose Untersuchungspflicht in einem bestimmten (engen) Zeitraum wird ebenfalls für nicht erforderlich gehalten.

Zu 3.3.7.6 Videoaufnahmen von Kindern im Kindergarten oder in einer Kindertagesstätte

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Eine Befassung des Hessischen Ministeriums für Soziales und Integration mit den geprüften Fällen war nicht gegeben. Da das sog. Videocoaching für Erzieherinnen jedoch zunehmend als Instrument der Fortbildung, z.B. im Bereich der sprachlichen Bildung, und zur Verbesserung der Qualität pädagogischen Handelns in Kindertageseinrichtungen eingesetzt wird, würde die Erarbeitung eines Mustertextes für die Einwilligung der Eltern mit Hilfe des Hessischen Datenschutzbeauftragten begrüßt werden, um die Verletzung von datenschutzrechtlichen Vorschriften bereits im Vorfeld zu vermeiden.

3.3.8 Personalwesen

Zu 3.3.8.1 Begleitung des Projekts "Optimierung der Personalverwaltung"

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

3.3.9 Kommunale Selbstverwaltungskörperschaften

Zu 3.3.9.1 Gesetzentwurf der Fraktionen von CDU und FDP zur Änderung des Brand- und Katastrophenschutzgesetzes - Einführung einer "Bevölkerungswarndatei"

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Die vom Hessischen Datenschutzbeauftragten geforderte Verordnung wird vorbereitet.

Zu 3.3.9.2 Veröffentlichung von Einwenderdaten im Bebauungsplanverfahren unter anderem gegenüber der Presse

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.9.3 Erteilung von Personenstandsurkunden

Der Hessische Datenschutzbeauftragte hat den Vorschlag unterbreitet, in den Fällen des § 63 Abs. 2 Satz 1 PStG bei nicht persönlicher Beantragung einer Geburtsurkunde zur Identitätsfeststellung des Antragstellers eine Kopie des Personalausweises einzureichen. Aufgrund dieses Hinweises wurde den Standesämtern im Ergebnis empfohlen, dass bei der elektronischen Beantragung von Geburtsurkunden nach § 63 Abs. 2 Satz 1 PStG die Identität des Antragstellers mittels des elektronischen Identitätsnachweises nach § 18 Personalausweisgesetz (eID-Funktion des Personalausweises) belegt werden sollte. Sofern die technischen Voraussetzungen hierfür in einem Standesamt nicht vorliegen, kann der Identitätsnachweis auf andere Weise erfolgen. Geeignet ist zum Beispiel die Vorlage einer beglaubigten Kopie des Personalausweises. Die entsprechende Empfehlung wurde mit dem Hessischen Datenschutzbeauftragten vorab abgestimmt. Wegen der besonderen Stellung des Standesbeamten als Urkundsperson wurde allerdings von dem Vorschlag des Hessischen Datenschutzbeauftragten abgesehen, einen Erlass zu fertigen. Denn nach § 2 Abs. 2 PStG sind die Standesbeamten bei der Wahrnehmung ihrer Aufgaben als Urkundspersonen nicht an Weisungen gebunden. Ein verbindlicher Erlass konnte daher nicht ergehen.

Der Vollständigkeit halber sei darauf hingewiesen, dass Geschwister nach § 62 Abs. 1 PStG nicht per se berechtigt sind, eine Geburtsurkunde zu beantragen. Sie müssen ein berechtigtes Interesse glaubhaft machen.

Zu 3.3.9.4 Meldescheine in Beherbergungsstätten

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.9.5 Erweiterte Melderegisterauskünfte an Rechtsanwälte

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.3.9.6 Angabe der Dienstbezeichnung bzw. Gehaltsgruppe auf Zahlungsanordnungen

Der Hessische Datenschutzbeauftragte weist zutreffend darauf hin, dass im Landesbereich die Rechtsgrundlage für die Angabe der Dienstbezeichnung bzw. Gehaltsgruppe derjenigen Personen, die Zahlungsanordnungen unterzeichnen, weggefallen ist. Im Zuge der Einführung der doppelten Buchführung im Land Hessen wurden die Verwaltungsvorschriften für Zahlungen, Buchführung und Rechnungslegung zu den §§ 70 bis 72 und 74 bis 80 LHO 2007 erneuert. Die Vorschrift zur Nennung von Dienstbezeichnung bzw. Vergütungsgruppe auf einer Zahlungsanordnung für die hessische Landesverwaltung ist somit entfallen. Dies gilt sowohl für automatisierte Verfahren als auch für die papiergebundene Form.

In Nr. 3 der Verwaltungsvorschriften zu § 11 Gemeindekassenverordnung (GemKVO) war in der Anlage 1 dazu bestimmt, dass die Feststellung der sachlichen und rechnerischen Richtigkeit durch Unterschrift "mit Angabe der Amtsbezeichnung oder der Vergütungsgruppe" zu bescheinigen ist. Diese Bestimmung ist mit den anderen Verwaltungsvorschriften zur GemKVO nach den Regeln über die Erlassbereinigung mit Ablauf des 31. Dezember 1997 außer Kraft getreten. Seit dem 1. Januar 1998 gibt es keine Regelung des Hessischen Ministeriums des Innern und für Sport, wie die Feststellung der sachlichen und rechnerischen Richtigkeit örtlich zu bestimmen ist. Nach § 11 Abs. 3 GemKVO obliegt dies der Bürgermeisterin- oder dem Bürgermeister bzw. der Landrätin oder dem Landrat. Dabei haben sie die datenschutzrechtlichen Regelungen zu beachten.

Nach der Neufassung der GemKVO, die am 1. Januar 2012 in Kraft getreten ist, wurde aus dem Kommunalbereich die Herausgabe neuer Verwaltungsvorschriften dazu angeregt. Die Entwicklung dieser Verwaltungsvorschriften konnte bisher nicht abgeschlossen werden. Es ist vorgesehen, in den Verwaltungsvorschriften auf die zu beachtenden datenschutzrechtlichen Regelungen hinzuweisen.

Zu 3.3.9.7 Stichprobenerhebung zum Einsatz von Videoüberwachung in Kommunen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

3.3.10 Wirtschaftsverwaltung

Zu 3.3.10.1 Zulässigkeit massenhafter Abfragen von Eigentümerdaten aus dem Liegenschaftskataster durch Makler

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass massenhafte Auskünfte über Grundstückseigentümerinnen und Grundstückseigentümer an Makler bzw. Unternehmen der Immobilienvermittlung und -verwertung über ganze Straßenzüge oder Ortsteile zu reinen Akquisezwecken datenschutzrechtlich nicht zulässig sind.

3.3.11 Rundfunk

Zu 3.3.11.1 Einmaliger Meldedatenabgleich durch den ARD ZDF Deutschlandradio Beitragsservice (vormals GEZ)

Aus Sicht der Landesregierung ist es sehr zu begrüßen, dass sich die Beschwerden gegen den ehemaligen Meldedatenabgleich des Beitragsservices von ARD, ZDF und Deutschlandradio als unbegründet erwiesen haben. Der einmalige Meldedatenabgleich bezieht sich auf genau den Datensatz, den die Meldeämter ohnehin seit vielen Jahren an die GEZ bzw. den Beitragsservice weiterleiten. Er hat sich als effektives Mittel erwiesen, bundesweit die Zahl der Schwarz-Hörer und –Seher deutlich zu reduzieren. Dies liegt im vitalen Interesse aller Rundfunk-Beitragszahler. Die jedenfalls auch durch den einmaligen Meldedatenabgleich erzielten Mehrerträge an Rundfunkbeiträgen (sie belaufen sich nach derzeitigen Prognosen der Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten für die aktuelle Beitragsperiode auf 1,15 Mrd. €) setzen die Länder nun erstmals in die Lage, im 16. Rundfunkänderungsstaatsvertrag sogar eine Senkung des Rundfunkbeitrages staatsvertraglich zu verankern.

Soweit der Beitragsservice von ARD, ZDF und Deutschlandradio als Einrichtung bezeichnet wird, die "Zwangsbeiträge" einziehe, bleibt anzumerken, dass sämtliche öffentlich-rechtlichen Abgaben, seien es Steuern, Gebühren oder Beiträge, auf nicht-freiwilliger Basis erhoben werden, ihnen mithin naturgemäß ein gewisser Zwangscharakter innewohnt.

4. Aufsichtsbehörde nach § 38 BDSG

Nach § 30 Abs. 2 HDSG ist die Landesregierung nicht verpflichtet, zur Tätigkeit des Hessischen Datenschutzbeauftragten als Aufsichtsbehörde nach § 38 BDSG Stellung zu nehmen. Unabhängig von dieser gesetzlichen Verpflichtung zur Stellungnahme äußert die Landesregierung nachfolgend ihre Auffassung zu Ausführungen im Tätigkeitsbericht, wenn Sachverhalte mit einem konkreten Bezug zum Datenschutz im öffentlichen Bereich angesprochen werden und eine fachliche Stellungnahme geboten erscheint.

Zu 4.3.4 Vorlage von Ausweiskopien bei Auskunfteien zur Erlangung einer Selbstauskunft

Die Landesregierung stimmt der vom Hessischen Datenschutzbeauftragten vorgenommenen Bewertung zur Einreichung bzw. Anforderung von Ausweiskopien zu.

Zu 4.7.2 Datenschutzgerechtes Verfahren beim Online-Weiterverkauf personalisierter Konzerttickets

Die Landesregierung stimmt der vom Hessischen Datenschutzbeauftragten vorgenommenen Bewertung der elektronischen Vorlage bzw. Übermittlung von Ausweiskopien zu.

Zu 4.9.1 Datenschutz in der Arztpraxis

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.9.2 Neues Merkblatt der Landespsychotherapeutenkammer für Hinterbliebene verstorbener Mitglieder

Am Verfahren zur Erstellung des Merkblattes war das Hessische Ministerium für Soziales und Integration nicht beteiligt.

Unter Ziffer 4.9.2.3 - Alternative Regelungsmöglichkeiten - macht der Hessische Datenschutzbeauftragte auf ein alternatives Konzept der Psychotherapeutenkammer Niedersachsen aufmerksam, das sich für die Hessischen Heilberufskammern empfehlen könnte. Ein abschließendes Fazit konnte der Hessische Datenschutzbeauftragte zu dem neuen Verfahren noch nicht ziehen, weshalb Niedersachsen im nächsten Jahr noch einmal um einen kurzen Erfahrungsbericht gebeten werden soll.

Diesbezügliche Anregungen wird das Hessische Ministerium für Soziales und Integration zusammen mit den Heilberufskammern sehr gerne prüfen und ggfs. umsetzen.

5. Bilanz

5.1 Löschen von Daten im SAP R/3 HR-System (41. Tätigkeitsbericht, Ziff. 3.3.6.1)

Zu 5.1.1 Löschung von Abwesenheiten (Urlaubs- und Krankheitsdaten)

Die Gründe, die einer Löschung der Daten entgegenstehen bzw. die in den Auswertungen des Hessischen Datenschutzbeauftragten zu einer größeren Anzahl nicht gelöschter Daten führen können, wurden von der Landesregierung in ihrer Stellungnahme zum 41. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Drs. 18/7802 zu Ziffer 3.3.6.1) ausführlich dargelegt; auf diese Ausführungen wird verwiesen.

Aufgrund der Anmerkungen des Hessischen Datenschutzbeauftragten im 42. Tätigkeitsbericht wurde die Einhaltung der Löschfristen nochmals überprüft. Die erforderlichen Korrekturen bzw. Datenlöschungen wurden in allen im Tätigkeitsbericht angeführten Buchungskreisen mit dem Löschlauf im 1. Quartal 2014 durchgeführt.

Im Bereich der Polizeipräsidien wurde in sechs der 107 im Tätigkeitsbericht angeführten Fälle erneut eine Vernichtungssperre gesetzt.

Zu 5.1.2 Löschung ganzer Datensätze

Die Landesregierung begrüßt die Feststellung des Hessischen Datenschutzbeauftragten, dass die personalführenden Stellen die Löschung zeitnah und konsequent durchgeführt haben.

Es ist darauf hinzuweisen, dass im Bereich des Hessischen Ministeriums der Justiz einige Ausnahmetatbestände bzw. weitere Fristen zum Tragen kommen, die eine Löschung der Personaldatensätze hinausschieben. So hat man sich nach einem Erfahrungsaustausch im September 2013 darauf verständigt, den Rechtsreferendaren, die in einem öffentlich-rechtlichen Dienstverhältnis stehen, eine weitere Löschfrist aufgrund ihrer ruhegehaltsfähigen Vordienstzeiten (Versorgungsanspruch nach § 6 HBeamtVG) einzuräumen.

Wiesbaden, 19. Januar 2015

Der Hessische Ministerpräsident
Bouffier

Der Hessische Minister des Innern und für Sport
Beuth