18. Wahlperiode

Drucksache **18/4568**

HESSISCHER LANDTAG

05. 10. 2010

Stellungnahme der Landesregierung

betreffend den Neununddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten
Drucksache 18/3847

Eingegangen am 5. Oktober 2011 · Ausgegeben am 11. Oktober 2011
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Stellungnahme zu:

1. Einführung

Zu 1.1 Allgemeines

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.
Der Hessische Landtag hat am 19. Mai 2011 das Gesetz zur Neuordnung des Datenschutzes und Wahrung der Unabhängigkeit des Datenschutzbeauftragten in Hessen beschlossen, das am 1. Juli 2011 in Kraft getreten ist (GVBl. I S. 208). Das Gesetz hat dem Hessischen Datenschutzbeauftragten die Aufsicht über den Datenschutz im nicht öffentlichen Bereich übertragen.

1.2 Grundlagen des Datenschutzes

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.3 Rechtsentwicklung

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

2. Europa

Zu 2.1 SWIFT-Abkommen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 2.2 Einheitlicher Rechtsrahmen für den Datenschutz auf europäischer Ebene

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

2.3 Gemeinsame Kontrollinstanz für das Schengener Informationssystem

Zu 2.3.1 Schengener Informationssystem der zweiten Generation (SIS II)

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 2.3.2 Gemeinsame Überprüfung der Ausschreibungen von Drittausländern zur Einreiseverweigerung

Im 37. Tätigkeitsbericht wurde das Verfahren hinsichtlich der Ausschreibungsvoraussetzungen und der Verlängerung der Ausschreibungsfristen im Schengener Informationssystem (SIS) bei den Ausländerbehörden der Stadt Darmstadt und des Kreises Bergstraße in Teilen beanstandet (siehe 37. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten - Drs. 18/106 - Nr. 4.4.1). Beide Ausländerbehörden haben gegenüber dem Hessischen Ministerium des Innern und für Sport versichert, die aufgetretenen Mängel künftig durch geeignete Maßnahmen zu beseitigen (siehe Stellungnahme der Landesregierung zum 37. Tätigkeitsbericht vom 1. September 2009 - Drs. 18/1014 - zu Nr. 4.4.1). Darüber hinaus gehende Hinweise auf eine fehlerhafte Bearbeitung von Ausschreibungsverfahren seitens hessischer Ausländerbehörden liegen dem Hessischen Ministerium des Innern und für Sport nicht vor.

Zu 2.3.3 Gemeinsame Überprüfung der Ausschreibungen zur Auslieferungsfestnahme

Die Landesregierung ist an der Arbeit der Gemeinsamen Kontrollinstanz für das Schengener Informationssystem nicht beteiligt. Über die berichteten Prüfungen ist der Landesregierung nichts bekannt.

Zu 2.3.4 Regelmäßiger Abgleich der Meldevordrucke in Hotels mit dem Schengener Informationssystem

Die Landesregierung stimmt der vom Hessischen Datenschutzbeauftragten vertretenen Auffassung zur Auslegung des § 27 Abs. 3 HMG zu.

Zu 2.4 Gemeinsame Kontrollinstanz für EUROPOL

Die Ausführungen des Hessischen Datenschutzbeauftragten in diesem Abschnitt beruhen auf seinen Kenntnissen aus der Einbindung in die europäische Kontrollinstanz für EUROPOL. Die Tätigkeit der Gemeinsamen Kontrollinstanz für EUROPOL kann durch die Landesregierung nicht bewertet werden.

3. Bund

3.1 Ausbau des Nachrichtendienstlichen Informationssystems NADIS zu einem Wissens- und Informationsmanagementsystem

Zu 3.1.1 NADIS - bisheriges System

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.1.2 Künftiges Konzept - NADIS als Wissensnetz (NADIS-WN)

Die Ausführungen des Hessischen Datenschutzbeauftragten sind in Teilen ergänzungs- bzw. korrekturbedürftig, wie nachfolgend ausgeführt wird. Im Übrigen stimmt die Landesregierung den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.1.2.1 Das System

NADIS WN wird in den geplanten Ausbaustufen kein Dokumentenmanagementsystem (DMS) beinhalten. Im Fachkonzept NADIS WN aus dem Februar 2007 ist die Einbindung eines zentralen DMS nicht vorgesehen. Das Arbeiten mit sogenannten Ursprungsdokumenten kann nur über im System zu hinterlegende Kopien oder per Verlinkung erfolgen. Länder oder das Bundesamt für Verfassungsschutz (BfV), die bereits in der eigenen Amtsdatei mit Verlinkung zu einem DMS die Ursprungsdokumente nutzen, können diese Funktion zukünftig unter Einhaltung datenschutzrechtlicher Vorgaben auch in NADIS WN nutzen.

Das Landesamt für Verfassungsschutz Hessen hinterlegt bisher keine Ursprungsdokumente in der eigenen Amtsdatei. Aufgrund der wesentlichen Arbeitserleichterung wird die Hinterlegung von Ursprungsdokumenten in der Amtsdatei HARIS jedoch - in enger Abstimmung mit dem Hessischen Datenschutzbeauftragten - vorbereitet. Ein DMS ist im Landesamt für Verfassungsschutz Hessen nicht im Einsatz. Das Landesamt beabsichtigt derzeit auch nicht, Ursprungsdokumente in NADIS WN einzubringen.

NADIS WN dient nicht der Optimierung von Arbeitsabläufen. Es ist jedoch die Abbildung von Arbeitsschritten, gerade im Bereich der Massendatenverfahren, zur Unterstützung der Anwender in Bund und Ländern vorgesehen. Diese werden im Fachkonzept oder auch dem Ergebnisbericht der Bund-Länder-Arbeitsgruppe NADIS-neu vom September 2008 als sogenannte Workflows bezeichnet.

Das Bundesministerium des Innern übernimmt die Entwicklung und Bereitstellung der Gesamtprojektleitung bis zur Inbetriebnahme von NADIS WN 1.0. Danach gehen die Aufgaben der fachlichen und technischen Betriebsführung in den Bereich des BfV über. Die Ausbaustufen NADIS WN 2.0 bis 5.0. werden im Rahmen einer derzeit noch in der Abstimmung befindlichen Projektstruktur entwickelt.

3.1.2.2 Rechtliche Probleme

Zu 3.1.2.2.1 Textdatei

Die Landesregierung kann der Auffassung des Hessischen Datenschutzbeauftragten nicht zustimmen. Das bisher im Einsatz befindliche System NADIS stammt noch aus den 70er-Jahren. Es ist inzwischen so veraltet, dass weder Wartung noch Support für Soft- und Hardware geleistet werden können. Zur Aufgabenerfüllung der Sicherheitsbehörden, die im heutigen Zeitalter gezwungenermaßen auf ein modernes, zuverlässiges System angewiesen sind, ist der derzeitige Stand ein nicht mehr tragbares Risiko. Bei der Entwicklung eines neuen Systems wäre es fahrlässig, nicht nach dem neuesten Stand der Erkenntnis und des Wissensmanagements sowie der Erhebung der aktuellen und zukünftigen Bedürfnisse der Verfassungsschutzbehörden zu handeln. Die im alten System NADIS bestehenden technischen Möglichkeiten zur Erfassung von Datensätzen, die nach § 6 Satz 8 BVerfSchG gespeichert werden dürfen, reichen bei weitem nicht mehr aus. Sie bleiben hinter den rechtlichen Möglichkeiten zurück. Das alte NADIS ließ zudem eine enorm hohe Vielzahl an Fehleingaben zu, sodass zuverlässige Aussagen aus diesem System heraus nicht immer möglich waren. Dies wird durch das neue System NADIS WN weitgehend durch die Hinterlegung von Katalogen, Geodaten (einheitliche Straßen-, Stadt- und Ländernamen) und Prüfung von Dateiformaten bei der Eingabe behoben.

Das neue System ist daher bereits jetzt ein unverzichtbarer Bestandteil für zuverlässige Auswertungen und Analysen und auch - auf der Grundlage des geltenden Rechts - sinnvoll nutzbar. Der Gesetzgeber hat seinerzeit erkannt, dass es Entwicklungen geben kann, die es notwendig machen, mehr als nur Daten zu speichern, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen dienen (§ 6 Satz 2 BVerfSchG). Dem ist durch den erweiterten Anwendungsbereich des § 6 Satz 8 BVerfSchG Rechnung getragen worden, wonach das Führen von Textdateien oder Dateien, die weitere als die in Satz 2 genannten Daten enthalten, unter den dort näher beschriebenen Voraussetzungen - sowohl für den Bund als auch für die Länder - zulässig ist.

Zu 3.1.2.2.2 Volltext-Recherche

Die Möglichkeit der Aufnahme von Ursprungsdokumenten ist eine technische Anforderung an NADIS WN. Ob und wie die Ursprungsdokumente suchfähig sein werden, ob und wie eine Volltext-Recherche möglich sein soll etc., ist derzeit jedoch sowohl rechtlich als auch in der technischen Umsetzung noch nicht abschließend geklärt. Dementsprechend ist die tatsächliche Nutzung dieser Funktion noch völlig offen und dürfte sich in den einzelnen Ländern unterschiedlich gestalten. Für das Landesamt für Verfassungsschutz Hessen ist eine Volltextrecherche nicht vorgesehen, da das Landesamt für Verfassungsschutz Hessen nicht beabsichtigt, Ursprungsdokumente in NADIS WN einzustellen (s.o. zu 3.1.2.2.1).

3.2 Verordnung zu § 7 Abs. 6 BKA-Gesetz (Rechtsgrundlage für die Inpol-Dateien)

Die Ausführungen des Hessischen Datenschutzbeauftragten zu § 7 Abs. 6 BKAG treffen im Wesentlichen zu. Das Bundesverwaltungsgericht hat den konstitutiven Charakter der Rechtsverordnung festgestellt. Allerdings ist der

Hinweis auf gegenteilige "Entscheidungen von Verwaltungsgerichten" in Verfahren zu Löschungsanträgen präzisierungsbedürftig. Namentlich hat der Hessische Verwaltungsgerichtshof, der auch das für den Sitz des Bundeskriminalamts zuständige Oberverwaltungsgericht ist, die Auffassung vertreten, dass § 7 Abs. 6 BKAG lediglich deklaratorische Bedeutung zukommt (Urteil vom 16.12.2004 - 11 UE 2982/02 -, Abs.-Nr. 40 bei juris).

Der Hessische Datenschutzbeauftragte bemängelt, dass in Falldateien auch solche Personalien aufgenommen worden seien, die bereits im Kriminalaktennachweis (KAN) und in Fahndungsdateien enthalten sind. Es ist jedoch entscheidend, welche Daten in einer Anwendung benötigt werden. Dabei sind auch die unterschiedlichen Speicherungsvoraussetzungen zu beachten. Zum Beispiel können Daten in Fahndungsdateien gleichartige Daten in anderen Dateien nicht überflüssig machen, weil Fahndungsdaten nur während der Dauer einer Fahndung gespeichert bleiben.

3.3 Volkszählung (Zensus) 2011

Die Landesregierung stimmt der Darstellung des Verfahrens und der Rechtsgrundlagen für den Zensus 2011 durch den Hessischen Datenschutzbeauftragten zu. Was das Merkmal Religionszugehörigkeit betrifft, ist darauf hinzuweisen, dass dieses Merkmal zwar nicht zwingend zu den nach der EU-Verordnung vorgeschriebenen Merkmalen gehört. In der Bundesrepublik ist die Religionszugehörigkeit bislang allerdings bei jeder Volkszählung erhoben worden. Dass dies verfassungsrechtlich zulässig ist, steht außer Frage und wird auch vom Hessischen Datenschutzbeauftragten nicht in Zweifel gezogen.

Nach Art. 140 GG in Verbindung mit Art. 136 Abs. 3 Satz 1 der Weimarer Reichsverfassung (WRV) ist es den Behörden nämlich erlaubt, nach der Zugehörigkeit zu einer Religionsgesellschaft zu fragen, wenn davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert. Art. 140 GG in Verbindung mit Art. 136 Abs. 3 Satz 1 WRV erfasst die körperschaftlich organisierten Religionsgemeinschaften. Für solche, denen dieser Status bislang nicht verliehen wurde, zum Beispiel islamische Glaubensgemeinschaften, sind diese Daten aber ebenfalls erforderlich, um Aussagen zur religiösen Zusammensetzung der Bevölkerung zu treffen und den planerischen Bedarf auf diesem Gebiet besser einschätzen zu können. Allerdings ist bei diesen Religionsgemeinschaften die Angabe über die Religionszugehörigkeit freiwillig.

3.4 Der neue Personalausweis

Die Ausführungen des Hessischen Datenschutzbeauftragten sind in Teilen ergänzungs- bzw. korrekturbedürftig, wie nachfolgend ausgeführt wird. Im Übrigen stimmt die Landesregierung den Ausführungen des Hessischen Datenschutzbeauftragten zu.

(Zu 3.4.1.1 Ausweis)
Der RFID-Chip auf dem Ausweis erlaubt nicht nur die Speicherung der gleichen Daten wie auf dem früheren Personalausweis, sondern auf Antrag des Personalausweisbewerbers auch die Speicherung der Fingerabdrücke wie in Nr. 3.4.2.1 dargestellt.

(Zu 3.4.2.2 Der elektronische Identitätsnachweis - eID-Funktion)
Der elektronische Identitätsnachweis, die eID-Funktion, ist bei Personen unter 16 Jahren deaktiviert (vgl. § 10 Abs. 2 PAuswG). Auf Antrag des Ausweisinhabers und unter Vorlage des Personalausweises kann ein ausgeschalteter elektronischer Identitätsnachweis während der Gültigkeitsdauer des Personalausweises eingeschaltet werden, wenn der Ausweisinhaber zum Zeitpunkt der Antragstellung bereits 16 Jahre alt ist (§ 10 Abs. 3 PAuswG). Auf ein Lebensalter von 18 Jahren wird nicht abgestellt.

(Zu 3.4.3.2 Internet, eID-Funktion)
Das Verfahren der nachträglichen Aktivierung der eID-Funktion über den Änderungsdienst der Personalausweisbehörde ist ein sicheres Verfahren. Zur nachträglichen Aktivierung der eID-Funktion ist es erforderlich, dass der Ausweisinhaber persönlich die Personalausweisbehörde aufsucht, wo seine Identität überprüft wird. Dazu stehen auch die auf dem Ausweis gespeicherten biometrischen Daten des Inhabers zur Verfügung. Es ist daher unwahrscheinlich, dass es einem Dieb gelingen könnte, diese Funktion zu aktivieren und dann mit dem gestohlenen Ausweis zu handeln.

3.5 Elektronischer Aufenthaltstitel

Das Gesetz zur Anpassung des deutschen Rechts an die Verordnung (EG) Nr. 380/2008 des Rates vom 18. April 2008 zur Änderung der Verordnung (EG) Nr. 1030/2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatsangehörige vom 12. April 2011 (BGBl I S. 610) wird zum 1. September 2011 in Kraft treten. Das Bundesministerium des Innern hatte den Ländern einen Referentenentwurf des Gesetzes zur Stellungnahme übersandt, den das Hessische Ministerium des Innern und für Sport auch dem Hessischen Datenschutzbeauftragten zugeleitet hat.

Der Hessische Datenschutzbeauftragte hatte an dem ersten Referentenentwurf bemängelt, dass die Speicherung der Irisbilder nicht vorgesehen sei und deshalb auch keine gesetzliche Regelung erfordere. Im weiteren Gesetzgebungsverfahren wurden die Irisbilder als biometrische Daten gestrichen.

Weiter wurde in dem ursprünglichen Gesetzentwurf unter den sichtbar auf dem elektronischen Aufenthaltstitel (eAT) aufzubringenden Feldern das Feld "Anmerkungen" genannt, ohne dass aus dem Gesetzestext selbst oder aus der Begründung hierzu vorherging, welche Art von Anmerkungen damit gemeint waren. In seiner Stellungnahme forderte der Hessische Datenschutzbeauftragte deshalb, dass der Begriff "Anmerkungen" inhaltlich konkreter erläutert werden müsste, um dem Gebot der Normenklarheit gerecht zu werden. Das Hessische Ministerium des Innern und für Sport unterstützte diese Forderung. Die Anregung wurde aufgegriffen und in der Begründung klargestellt, dass unter dem Feld "Anmerkungen" nur aufenthaltsrechtlich relevante Eintragungen vorgenommen werden dürfen. Hierunter fallen zum Beispiel die Rechtsgrundlage für den Aufenthalt, ein Hinweis auf die Gestattung der Erwerbstätigkeit oder sonstige Nebenbestimmungen, die ggf. auf einem Zusatzblatt zum elektronischen Aufenthaltstitel aufgeführt sind.

Der elektronische Aufenthaltstitel soll genau wie der neue Personalausweis mit den Zusatzfunktionen "eID" (elektronischer Identitätsnachweis) sowie einer Möglichkeit zur Erstellung einer qualifizierten elektronischen Signatur (elektronische Unterschrift) ausgestattet werden. Das Gesetz verweist für die näheren Einzelheiten hierzu auf eine noch zu erstellende Aufenthaltsverordnung. In der Diskussion sind allerdings bereits jetzt praktische Fragen aufgetreten, wie zum Beispiel die Frage der Freischaltung der eID-Funktion. Vor allem von den Ausländerbehörden wurde die Frage aufgeworfen, ob die eID-Funktion bei der Auslieferung standardmäßig freigeschaltet sein soll oder dies nur eine Option ist, die auf Antrag freigeschaltet wird. Der Hessische Datenschutzbeauftragte hat die Ansicht vertreten, die eID-Funktion solle generell inaktiv sein und eine Freischaltung nur auf Wunsch des Inhabers des eAT erfolgen. Der Hessische Datenschutzbeauftrage hat darauf hingewiesen, dass das Sperrkennwort, mit dem die eID-Funktion der Karte bei Verlust gesperrt werden kann, standardmäßig und nicht nur auf besonderen Wunsch des Betroffenen ausgegeben werden sollte. Insgesamt erscheine fraglich, ob sämtliche Regelungen, die die Zusatzfunktionen eID und Signaturerstellungseinheit betreffen, überhaupt in einer Verordnung regelbar sind oder vielmehr Gegenstand des Gesetzes sein müssten.

Die Landesregierung ist der Auffassung, dass diese Fragen nicht im Gesetz geregelt werden müssen, sondern eine Rechtsverordnung als Grundlage ausreicht. § 61h des Referentenentwurfs des Bundesministeriums des Innern für eine Siebten Verordnung zur Aufenthaltsverordnung (Stand 28. März 2011) verweist bezüglich des Wahlrechts und der Freischaltung der eID-Funktion auf § 18 Abs. 1 bis 4 der Verordnung über Personalausweise und den elektronischen Identitätsnachweis vom 1. November 2010 (BGBl. I S. 1460). Nach § 18 Abs. 1 der Verordnung ergibt sich das Wahlrecht durch Abgabe einer Negativ-Erklärung.

Auch aus § 45a Abs. 1 des Verordnungsentwurfs in der Fassung vom 28. März 2011 ergibt sich, dass dem Inhaber des Dokuments ein Wahlrecht zusteht, ob er die eID-Funktion bei der Aushändigung des Dokuments eingeschalten belassen möchte oder nicht. Außerdem kann er bei der Ausgabe des Dokuments erklären, die Funktion nicht nutzen zu wollen oder die Erklärung verweigern, den Brief mit dem Sperrkennwort erhalten zu haben. Dadurch ist hinreichend sichergestellt, dass die eID-Funktion dem Betroffenen nicht aufgedrängt wird.

Soweit es die Ausgabe des Sperrkennworts für die elD-Funktion betrifft, stimmt die Landesregierung dem Hessischen Datenschutzbeauftragten grundsätzlich zu. Das Problem dürfte aber durch den Verweis in § 61h des Verordnungsentwurfs auf die §§ 17 und 18 Abs. 1 bis 4 der Verordnung über Personalausweise und den elektronischen Identitätsnachweis gelöst werden. Danach erhält der Betroffene vor der Ausgabe des eAT vom Dokumentenhersteller einen Brief u.a. mit dem Sperrkennwort (§ 17 Abs. 1). Den Erhalt des Briefs hat er bei der Ausgabe des eAT zu bestätigen (§ 17 Abs. 7), andernfalls wird die eID-Funktion nicht freigeschaltet (§ 18 Abs. 2).

Schließlich hatte der Hessische Datenschutzbeauftragte eine Regelung zur Löschung der Fingerabdruckdaten, die zur Erstellung des elektronischen Aufenthaltstitels erhoben und gespeichert werden müssen, gefordert. § 61a Abs. 2 Satz 2 des Verordnungsentwurfs sieht vor, dass die bei der Ausländerbehörde gespeicherten Fingerabdrücke spätestens nach Aushändigung des Dokuments zu löschen sind. Damit wird den Anregungen des Hessischen Datenschutzbeauftragten Rechnung getragen.

4. Land

4.1 Querschnitt

Zu 4.1.1 Die behördlichen Datenschutzbeauftragten als Ansprechpartner für Bürgerinnen und Bürger sowie den Hessischen Datenschutzbeauftragten

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.2 Einsichts- und Auskunftsrecht des Bürgers gegenüber der Verwaltung

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.
Das Hessische Rettungsdienstgesetz (HRDG) hat zwar durch das Gesetz vom 16. Dezember 2010 (GVBl. I S. 646) eine neue Fassung erhalten, die eine § 24 Abs. 1 HRDG a.F. entsprechende Regelung nicht mehr enthält. Gleichwohl bleibt es bei der Anwendung des § 18 Abs. 3 HDSG, da das neue HRDG keine von § 18 HDSG abweichende Regelung trifft, die den Auskunftsanspruch ausschließt.

Zu 4.1.3 Datenschutzrechtliche Anforderungen an Sicherheitspartnerschaften

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Er beschreibt die Problemstellung zutreffend. Unter seiner Mitwirkung wird derzeit für den Bahnhof Heusenstamm zwischen der Gemeinde, der Landespolizei und der Bundespolizei ein Konzept erarbeitet, das als Muster für ähnliche Kooperationen dienen kann.

Zu 4.1.4 eArchiv

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zum Projekt eArchiv zu und dankt ihm für die gute Zusammenarbeit im Rahmen des DMS-Projekts, zuletzt bei dem Teilprojekt eArchiv. Die gemeinsam erarbeiteten Musterpapiere (Verfahrensverzeichnis und Vorabkontrolle) für das Verfahren stehen bei Bedarf allen Landesdienststellen zur Verfügung und sind diesen eine wertvolle Hilfe für die Erstellung der erforderlichen dienststellenbezogenen Dokumente.

Die Aussage des Hessischen Datenschutzbeauftragten, wonach die Umsetzung des eArchivs im Rahmen der DMS-Einführung in der hessischen Landesverwaltung die abschließende Phase des Gesamtprojekts darstellt, trifft aus organisatorischer Sicht nur eingeschränkt zu. Die technische Produktentwicklung kann als abgeschlossen bezeichnet werden. Dementsprechend ist der technische Produktübergang einschließlich eArchiv auf die Hessische Zentrale für Datenverarbeitung (HZD) mit der Einführung des Geschäfts- und Abrechnungsmodells HessenPC erfolgt. Die Ausstattung der Landesverwaltung mit den Produkten des DMS wird jedoch noch fortgesetzt.

Das Hessische Ministerium des Innern und für Sport bleibt weiterhin für das strategische Produktmanagement, für die fachlich-organisatorischen Regelungen sowie für die Weiterentwicklungen des DMS und des eArchivs zuständig.

Zu 4.1.5 Löschung von Daten im SAP R/3 HR System

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Sie begrüßt seine konstruktive Begleitung aller Projektschritte, die einen weiteren Erfolg mit der Löschung von Abwesenheitsdaten in diesem Jahr zeitigen. Mittlerweile wird den Ressorts ein Löschwerkzeug für die Löschung der krankheits- und erholungsurlaubsbedingten Abwesenheitsdaten bis einschließlich zum 31. Dezember 2006 zur Verfügung gestellt. In einem zweiten Schritt können ab Juli 2011 die krankheits- und erholungsurlaubsbedingten Abwesenheitsdaten bis einschließlich zum 31. Dezember 2007 gelöscht werden. Das Werkzeug zum Löschen von Abwesenheitsdaten wird bis Ende des Jahres weiter angepasst, um dann auch diejenigen Abwesenheitsdaten löschen zu können, die aus organisatorischen und technischen Gründen bisher vom Löschen ausgenommen sind. Dies betrifft die Fallkonstellationen Mutterschutz/Elternzeit, Sabbatjahr und Altersteilzeit.

Nach der Sommerpause 2011 wird in einem weiteren Projekt unter Beteiligung des Hessischen Datenschutzbeauftragten das Löschen ganzer Personaldatensätze vorbereitet. In diesem Projekt soll zunächst ein Fachkonzept zur Löschung dieser Daten erarbeitet werden, das u.a. den Anforderungen des Archivwesens und der Statistik Rechnung trägt. Daran anschließend wird in einem Umsetzungsprojekt - Beginn im 1. Quartal 2012 - an der Implementierung des Löschwerkzeugs zur Löschung ganzer Personaldatensätze gearbeitet werden.

Im letzten Schritt werden dann die Voraussetzungen zum Löschen weiterer einzelner Personaldaten geschaffen. Zur Umsetzung dieses Schrittes sind die Ergebnisse aus dem Projekt Löschen ganzer Personaldatensätze vorgreiflich.

Die Landesregierung dankt dem Hessischen Datenschutzbeauftragten für die bisherige Begleitung und Mitarbeit an dem Projekt "Löschen krankheits- und erholungsurlaubsbedingter Abwesenheiten".

Zu 4.1.6 Download-Berechtigungen

Mit dem Hessischen Datenschutzbeauftragten besteht völliges Einvernehmen dahin gehend, dass sowohl die Ausführung von SAP-Berichten als auch deren Speicherung und Weiterverarbeitung nur bei entsprechender Aufgabestellung, also im Rahmen der durch die §§ 7, 11, 12, 13 HDSG bzw. §§ 107 ff. HBG definierten Zweckbestimmung und Erforderlichkeit, zulässig ist. Die gebotene hohe Sensibilität im Umgang mit Personaldaten und vorausgegangene Beanstandungen des Hessischen Datenschutzbeauftragten in früheren Tätigkeitsberichten waren bereits im November 2007 Anlass für das Hessische Ministerium des Innern und für Sport, auf die strikte Einhaltung der Vorgaben des § 7 Abs. 2 der Gemeinsamen Erklärung zur Einführung von SAP R/3 HR in der Landesverwaltung hinzuweisen, in der es heißt:

"Daten, die aus SAP R/3 HR generiert werden, dürfen auch in anderen SAP-Modulen oder Systemen nur nach den in dieser Erklärung genannten Voraussetzungen verarbeitet werden. Es gilt der Grundsatz, dass SAP R/3 HR keine Daten in personenidentifizierender Form an andere Anwendungssysteme, externe Stellen oder in lokale Dateien weitergibt, soweit aufgrund gesetzlicher, tariflicher oder arbeitsvertraglicher Regelungen nichts anderes bestimmt ist oder dieses zur Erfüllung der Aufgaben aus der Abwicklung des Dienst- bzw. Beschäftigungsverhältnisses zwingend erforderlich ist."

Durch entsprechende Ressorterlasse wurde die Beachtung dieser Vorgaben gegenüber den nachgeordneten Dienststellen verbindlich geregelt.

Das erneute Aufgreifen der Thematik durch den Hessischen Datenschutzbeauftragten war zum Teil Anlass, die rechtlichen Rahmenbedingungen für den Umgang mit Personaldaten in den Ressorts nochmals in Erinnerung zu rufen und im Rahmen des dienstlich Vertretbaren auch auf eine weitere Reduzierung der Zahl der downloadberechtigten Personen hinzuwirken.

Auf die Möglichkeit zum Download von Daten aus SAP R/3 HR kann jedoch nicht verzichtet werden. In Einzelfällen bestehen Anforderungen an die Auswertungen, die von den SAP-Berichten nicht vollständig abgedeckt werden können. Zum Beispiel kann die Kombination von Daten aus verschiedenen Berichten erforderlich sein, die systemseitig nicht auf andere Weise verfügbar gemacht werden können. Bei der Anforderung statistischer Daten kann ein Download der personenbezogenen Auswertungen erforderlich werden, um die angeforderten statistischen Daten ermitteln und darstellen zu können. Der im Sozialministerium jährlich zu erstellende Schwerbehindertenbericht wäre ohne den Download aus SAP nicht zu bearbeiten.

Der Hessische Datenschutzbeauftragte hat im Tätigkeitsbericht nicht ausgeführt, inwiefern die Vorgaben des § 10 Abs. 2 HDSG bei Download-Daten nicht eingehalten werden. Der Landesregierung ist eine diesbezügliche Stellungnahme daher nicht möglich.

Abschließend ist in Bezug auf die Darstellung im Tätigkeitsbericht klarzustellen, dass von den angeführten 72 Download-Berechtigungen für Mitarbeiterinnen und Mitarbeiter der Oberfinanzdirektion lediglich vier Personen auf Ebene der OFD Frankfurt/Main angesiedelt waren und es sich bei den übrigen 68 Personen um Mitarbeiterinnen und Mitarbeiter der 35 Finanzämter handelt, die dort mit personalwirtschaftlichen Aufgaben betraut sind.

4.2 Justiz, Strafvollzug und Polizei

Zu 4.2.1 Strafvollzugsgesetze

Die Bewertung der datenschutzrechtlichen Regelungen in den hessischen Vollzugsgesetzen durch den Hessischen Datenschutzbeauftragten ist ganz überwiegend positiv. Dies ist nicht zuletzt auf die frühzeitige Abstimmung mit dem Hessischen Datenschutzbeauftragten zurückzuführen.

Die Kritik des Hessischen Datenschutzbeauftragten an § 58 Abs. 2 HStVollzG ist, soweit es die Erhebung biometrischer Daten angeht, zutreffend, als vorgetragene Bedenken im Gesetzgebungsverfahren vom Gesetzgeber letztlich nicht aufgegriffen wurden. Dies steht in Zusammenhang damit, dass sich entsprechende Regelungen in den Vollzugsgesetzen aller Länder finden, namentlich in Baden-Württemberg (§ 31 Buch 1 BW JVollzG), Bayern (Art. 93 Bay StVollzG), Berlin (§ 45 UVollzG Bln, § 66 JStVollzG Bln), Brandenburg (§ 45 BbgUVollzG, § 66 BbgJStVollzG), Bremen (§ 45 Brem UVollzG, § 66 Brem JSt-VollzG), Hamburg (§ 71 HmbStVollzG, § 51 HmbUVollzG, § 71 HbmJStVollzG), Mecklenburg-Vorpommern (§ 45 UVollzG M-V, § 66 JStVollzG M-V), Niedersachsen (§ 78 NJVollzG), Nordrhein-Westfalen (§ 35 UVollzG NRW, § 76 JStVollzG NRW), Rheinland-Pfalz (§ 66 LJStVollzG RP), Saarland (§ 45 SUVollzG, § 66 SJStVollzG), Sachsen (§ 67 SächsJStVollzG), Sachsen-Anhalt (§ 45 UVollzG LSA, § 67 JSTVollzG LSA), Schleswig-Holstein (§ 66 JStVollzG) und Thüringen (§ 45 ThürUVollzG, § 66 ThürJStVollzG). Auch § 58 Abs. 2 des Hessischen Jugendstrafvollzugsgesetzes enthält eine inhaltsgleiche Regelung, die seinerzeit nicht beanstandet wurde. Insoweit werden die grundsätzlichen Bedenken in Übereinstimmung mit den anderen Bundesländern nicht geteilt.

Zur Klarstellung sei angemerkt, dass eine über die Identifizierung der Person hinausgehende Gewinnung und Verwendung von biometrischen Daten weder beabsichtigt war noch zukünftig beabsichtigt ist. Um Missverständnissen vorzubeugen wird geprüft werden, ob eine klarstellende Ergänzung des Gesetzestextes in Bezug auf zulässige Arten der Erfassung biometrischer Daten - z.B. des Gesichts, der Hände oder der Stimme - und die Unzulässigkeit der Erhebung weiterer Erkenntnisse über die bloße Feststellung der Identität hinaus bei nächster Gelegenheit vorzunehmen ist.

Soweit die Kritik des Hessischen Datenschutzbeauftragten § 62 Abs. 4 HStVollzG betrifft, beruht auch diese Vorschrift auf der Abstimmung mit anderen Bundesländern. Um den datenschutzrechtlichen Anforderungen Rechnung zu tragen, wurden die formalen Anforderungen durch die Vorgabe des Abschlusses eines Staatsvertrages bewusst hoch angesetzt. Im Rahmen dieses Staatsvertrages wären dann in der Tat Erforderlichkeit und Zweck der Datenübermittlung - z.B. denkbar zur Schaffung einer bundesweiten Vollzugsdatei - genau zu beschreiben. Da der Staatsvertrag selbst der Ratifikation durch den Hessischen Landtag bedarf, wird dem Gesetzgebungsvorbehalt mit der Vorschrift ausreichend Rechnung getragen.

Das Hessische Maßregelvollzugsgesetz wurde Anfang dieses Jahres evaluiert, eine Novellierung steht im Jahr 2012 an. Im Rahmen der Evaluierung wurde auch der Hessische Datenschutzbeauftragte beteiligt. In seiner Stellungnahme hat er unter anderem darauf hingewiesen, dass Fragestellungen mit datenschutzrechtlichem Bezug eindeutiger im Gesetz geregelt werden müssen, und angeregt, sich am Hessischen Strafvollzugsgesetz zu orientieren, wo keine unterschiedlichen Regelung zum Strafvollzug erforderlich sind. Im Rahmen der Novellierung werden, soweit es die Behandlungsabläufe im Maßregelvollzug zulassen, die Anregungen des Hessischen Datenschutzbeauftragten berücksichtigt werden.

4.2.2 Hessisches Dolmetscher- und Übersetzergesetz

Zu 4.2.2.1 Beteiligung der Ausländerbehörden bei der Überprüfung der Zuverlässigkeit

§ 2 Abs. 2 des Hessischen Dolmetscher- und Übersetzergesetzes (HessDolmG) regelt, dass derjenige Ausländer, der nicht EU-Bürger ist, seinen ständigen Wohnsitz oder die berufliche Niederlassung im Gebiet des Landes Hessen hat und die sonstigen in § 2 Abs. 1 Nr. 2 bis 4 genannten Voraussetzungen erfüllt, ebenfalls als Dolmetscher allgemein beeidigt werden kann. Für die Überprüfung der Zuverlässigkeit ist in diesen Fällen nach § 2 Abs. 2 Satz 2 HessDolmG eine Stellungnahme der zuständigen Ausländerbehörde einzuholen. Der Hessische Datenschutzbeauftragte ist der Auffassung, dass das Gesetz keine Festlegungen dazu enthalte, wozu genau die Ausländerbehörde Stellung nehmen soll. Das Gesetz entspreche daher nicht dem datenschutzrechtlichen Grundsatz, nachdem Daten nur insoweit zu verarbeiten sind, wie dies für die Erfüllung der Aufgaben der Behörde erforderlich ist. Es sei daher eine Konkretisierung dahin gehend, welche zusätzlichen Informationen der Ausländerbehörde für die Entscheidung über die Zuverlässigkeit erforderlich sein sollen, zwingend notwendig.

Bereits im Gesetzgebungsverfahren hat der Hessische Datenschutzbeauftragte Kritik an der Fassung des § 2 Abs. 2 HessDolmG geäußert. Auf diese Kritik wurde erwidert, dass der Begriff der Zuverlässigkeit durch die Rechtsprechung u.a. im Bereich des Gewerberechts hinreichend bestimmt ist, sodass die Ausländerbehörde sehr wohl in der Lage sei zu erkennen, welche Erkenntnisse erforderlich sind, um über die Frage der Zuverlässigkeit entscheiden zu können. Auch wurde darauf hingewiesen, dass in anderen Gesetzen die Voraussetzungen für die Überprüfung der Zuverlässigkeit ähnlich geregelt sind, z.B. in § 8a Abs. 5 Nr. 5 SprengG. Auch das Luftsicherheitsgesetz (§ 7 Abs. 3 Nr. 4 LuftSiG) und die Hafensicherheitsgesetze mehrerer Länder sähen nicht näher präzisierte Anfragen an die Ausländerbehörde vor. Dies sei auch zweckgemäß, da eine generalisierte Anfrage vor dem Hintergrund der großen Bedeutung der Zuverlässigkeit der Dolmetscher und Übersetzer für das gerichtliche Verfahren nicht ausreichend ist. Dies gilt nach wie vor.

Tatsächlich lässt die große Bedeutung der Zuverlässigkeit der Dolmetscher und Übersetzer in gerichtlichen Verfahren eine normierte Anfrage an die Ausländerbehörde nicht zu. Vielmehr sind alle die Zuverlässigkeit einer Person ausmachenden Gegebenheiten und Umstände - soweit feststellbar - in die Entscheidung über die Zuverlässigkeit einzubeziehen. Die Ausländerbehörde ist daher gehalten, all die von ihr zur Erfüllung ihrer Aufgaben zulässigerweise erfassten und gespeicherten Daten zum Gegenstand ihrer Stellungnahme dazu, ob eine Person, die einen Antrag auf Beeidigung als Dolmetscherin oder Dolmetscher gestellt hat, als zuverlässig anzusehen ist, zu machen. Die vom Datenschutzbeauftragten geforderte Konkretisierung der Informationen, die Gegenstand der von der Ausländerbehörde gegenüber der zuständigen Stelle, der Präsidentin oder dem Präsidenten des Landgerichts, abzugebenden Stellungnahme sein sollen, verbietet sich mithin. Würde eine solche Vorgabe erfolgen, wäre es möglich, dass der Ausländerbehörde Informationen vorliegen, die die Zuverlässigkeit eines Antragstellers ausschließen können, die aber gleichwohl nicht berücksichtigt werden dürften, da sie im Gesetz nicht aufgelistet sind.

Die der Ausländerbehörde zukommende Aufgabe, hinsichtlich der Zuverlässigkeit einer Person, die einen Antrag auf Vereidigung als Dolmetscher oder auf allgemeine Ermächtigung als Übersetzer gestellt hat, eine Stellungnahme zu deren Zuverlässigkeit abzugeben, ist in ausreichendem Maße konkretisiert. Die Behörde weiß damit, dass sie alle ihr vorliegenden Daten zum Gegenstand der Stellungnahme im Sinne des § 2 Abs. 2 Satz 2 HessDolmG zu machen hat, die hinsichtlich der Zuverlässigkeit einer Person Aussagekraft haben.

Schließlich ist darauf hinzuweisen, dass es nicht um die reine Weitergabe von Daten durch die Ausländerbehörden an die zuständigen Landgerichtspräsidentinnen und -präsidenten, sondern um die Fertigung einer Stellungnahme durch die Ausländerbehörde geht. Damit stellt sich die vom Hessischen Datenschutzbeauftragten angesprochene Frage, welche Daten die Ausländerbehörde an die zuständige Präsidentin oder den zuständigen Präsidenten des Landgerichts weiterzuleiten hat, nach Auffassung der Landesregierung nicht. Die Kritik des Hessischen Datenschutzbeauftragten trifft aus den genannten Gründen nicht zu.

Zu 4.2.2.2 Verschwiegenheitspflicht der Dolmetscher und Übersetzer

§ 4 Abs. 2 Nr. 2 HessDolmG regelt die Verschwiegenheitspflicht der Dolmetscher und Übersetzer. Das Gesetz sieht vor, dass die Verschwiegenheitspflicht sich nicht auf Tatsachen erstreckt, die Gegenstand einer öffentlichen Verhandlung waren. Diese Regelung hält der Hessische Datenschutzbeauftragte für nicht "normenklar" und die Begründung für die Ausnahme von der Verschwiegenheitspflicht sei nicht überzeugend. Der Auffassung des Hessischen Datenschutzbeauftragten kann nicht gefolgt werden.

Die Regelung deckt sich mit § 353d StGB, der das Verbot von Mitteilungen über Gerichtsverhandlungen bestimmt. Dieses Verbot betrifft nur Informationen, die Gegenstand einer nichtöffentlichen Gerichtsverhandlung waren. Fragwürdig wäre deshalb eine unbeschränkte Verpflichtung der Dolmetscher und Übersetzer zur Verschwiegenheit und damit die Verpflichtung, keine Angaben über Ereignisse zu machen, an denen Dritte in zulässiger Weise teilgenommen haben oder hätten teilnehmen können.

Soweit der Hessische Datenschutzbeauftragte in diesem Zusammenhang auf die Entscheidung des OLG Frankfurt am Main vom 11. Januar 2005 (3 Ws 1003/04) verweist und ausführt, aus dieser Entscheidung ergebe sich, dass auch Dinge, die Gegenstand einer öffentlichen Verhandlung waren, Geheimnis im Sinn des § 203 StGB sein können, kann dem nicht gefolgt werden. Das Gericht hat in seiner Entscheidung nämlich ausdrücklich darauf abgestellt, dass nicht klar war, ob der Gutachter, um dessen Verschwiegenheitspflicht nach § 203 Abs. 1 Nr. 1 StGB es

ging, bereits alle den Angeklagten betreffenden persönlichkeitsrelevanten Tatsachen zum Gegenstand seiner Ausführungen im Rahmen einer ersten Hauptverhandlung gemacht hatte, wodurch sie ihre Eigenschaft als Geheimnis verloren haben könnten. Dies ließ das Gericht zu dem Ergebnis gelangen, dass sehr wohl noch Tatsachen denkbar seien, die dem Geheimnisbegriff des § 203 StGB unterfielen, eben weil sie noch nicht Gegenstand einer öffentlichen Verhandlung waren. Tatsachen, die Gegenstand einer allgemein zugänglichen Verhandlung waren, verlieren auf diese Weise ihren Geheimnischarakter (vgl. Fischer, Strafgesetzbuch, 57. Auflage, Rn 5 zu § 203 StGB). Ob die Weitergabe derartiger Informationen das Persönlichkeitsrecht einer Person betrifft, das heißt, verletzen könnte und sich ein Dolmetscher hierdurch rechtlichen Angriffen aussetzen kann, ist nicht Gegenstand der vom Hessischen Datenschutzbeauftragten kritisierten Regelung des Gesetzes.

Zu 4.2.3 Ergebnisse der Prüfung des Justizzentrums Wiesbaden

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.2.4 Telefonieren in der Justizvollzugsanstalt

Ergänzend wird hierzu angemerkt, dass die Mitteilung an die Anstaltsleiterinnen und Anstaltsleiter im Rahmen der Dienstbesprechung am 3. August 2010 erfolgt ist.

Zu 4.2.5 Beteiligung freier Träger im Strafvollzug

Ergänzend wird hierzu angemerkt, dass der Aufforderung des Hessischen Datenschutzbeauftragten durch Erlass des Hessischen Ministeriums der Justiz, für Integration und Europa vom 31. März 2010 Rechnung getragen wurde.

Zu 4.2.6 Übermittlung von Informationen der Polizei an Fahrerlaubnisbehörden

Die Landesregierung hat den zutreffenden Ausführungen des Hessischen Datenschutzbeauftragten nichts hinzuzufügen.

4.3 Verfassungsschutz

Zu 4.3.1 Neues Datenverarbeitungssystem HARIS beim Hessischen Landesamt für Verfassungsschutz - weitere Entwicklungen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten im Wesentlichen zu. Lediglich die vom Hessischen Datenschutzbeauftragten berichteten "weiteren Probleme" bei der Speicherung von Verstorbenen sind nicht zutreffend. Nach dem Bericht des Landesamts für Verfassungsschutz Hessen gab es weder bei dieser noch bei einer anderen Art von Speicherung Probleme. Der Hessische Datenschutzbeauftragte war im Rahmen der Erstellung eines Arbeitsplanes fortlaufend eingebunden und hatte für die Daten Verstorbener gebeten, die Speicherung alle zwei Jahre auf Erforderlichkeit zu prüfen. Der Bitte des Hessischen Datenschutzbeauftragten wurde entsprochen und eine Wiedervorlageregelung umgesetzt.

4.4 Ausländerwesen

Zu 4.4.1 Verpflichtungserklärung für die Einladung eines Ausländers

Auf Bund-Länder-Ebene wurde im Jahr 2009 ein bundeseinheitliches Merkblatt zur Verwendung des bundeseinheitlichen Formulars der Verpflichtungserklärung (§§ 68, 66 und 67 AufenthG) erarbeitet, das u.a. die Prüfung der Bonität des sich Verpflichtenden für die Ausländerbehörden regelt. Das mit der Allgemeinen Verwaltungsvorschrift zum Aufenthaltsgesetz (AVwV-AufenthG) vom 26. Oktober 2009 (GMBl. 2009, S. 878) zu § 68 in Einklang stehende Merkblatt (siehe insbesondere Nr. 68.1.2 ff. AVwV-AufenthG) wurde den Ausländerbehörden in Hessen zur verbindlichen Anwendung in der aktuell gültigen Fassung vom 15. Dezember 2009 übermittelt. Danach orientiert sich der Prüfungsmaßstab in Umfang und Tiefe an den Erfordernissen des Einzelfalls. Beispielsweise sind der vom Ausländer angegebene Aufenthaltszweck und die Aufenthaltsdauer, aber auch die bereits zum Verpflichtungsgeber bei der Ausländerbehörde bekannten Informationen zu berücksichtigen. Das Merkblatt gibt lediglich ermessenslenkende Hinweise zur Art der Belege, die die Ausländerbehörde mit Blick auf den Individualfall vom Verpflichtungsgeber zum Nachweis seiner Bonität anfordern kann. Eine standardmäßige Vorlage bestimmter Unterlagen widerspräche der flexiblen und einzelfallbezogenen Prüfung.

Zu 4.4.2 Akteneinsicht im Aufenthaltsgenehmigungsverfahren

Zurzeit werden die im Bericht des Hessischen Datenschutzbeauftragten genannten Sicherheitsbefragungen von den Ausländerbehörden durchgeführt. Grundsätzlich hat die Behörde nach § 29 Abs. 1 Satz 1 HVwVfG den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Dies gilt bis zum Abschluss des Verwaltungsverfahrens nicht für Entwürfe zu Entscheidungen sowie die Arbeiten zu ihrer unmittelbaren Vorbereitung. Auf § 29 Abs. 2 HVwVfG soll zukünftig nur noch im Einzelfall abgestellt werden. Das bedeutet, dass das Einsichtsrecht erst dann gewährt wird, wenn die Behörde ihre abschließende Entscheidung getroffen hat, da auch das Protokoll der Sicherheitsbefragung zu den vorbereitenden Maßnahmen zu rechnen ist.

Zurzeit wird der Erlass bezüglich der Sicherheitsanfragen überarbeitet. Der Hessische Datenschutzbeauftragte wird in diesem Rahmen Gelegenheit zur Stellungnahme erhalten. Es ist daher davon auszugehen, dass ein einvernehmliches Ergebnis erzielt werden kann.

4.5 Schulen und Schulverwaltung

Zu 4.5.1 Änderung des Hessischen Schulgesetzes

Es besteht Einvernehmen mit dem Hessischen Datenschutzbeauftragten, soweit er die geplante Regelung zur Zusammenarbeit von Schule und Jugendamt im Interesse des Kindeswohls in § 3 Abs. 10 des Gesetzentwurfs begrüßt und er die erstmalig vorgesehene Definition von Schülerakten in § 83 Abs. 1 Satz 2 des Gesetzentwurfs unterstützt. Auch gegen die Aufnahme einer geplanten Datenübermittlungsregelung für die Schulpsychologinnen und Schulpsychologen zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit (§ 83 Abs. 6) erhebt der Hessische Datenschutzbeauftragte keine grundsätzlichen Einwände. Soweit er jedoch ergänzend die Aufnahme einer "Erheblichkeitsschwelle" in das Gesetz empfiehlt, wird dies aus systematischen Gründen nicht im Gesetz selbst, sondern in einer Verordnung nach § 83 Abs. 9 zu berücksichtigen sein.

Zu 4.5.2 Schwarze Listen über Lehrer

Die Feststellung des Hessischen Datenschutzbeauftragten, er sei vor der Einrichtung der bei der Zentralstelle Personalmanagement Lehrkräfte - ZPM - seit 1. April 2009 geführten "Informationsliste der Schulverwaltung zur Vermeidung der Wiedereinstellung ungeeigneter Lehrkräfte" nicht rechtszeitig beteiligt worden, ist insoweit zutreffend, als eine förmliche Beteiligung nach § 15 Abs. 1 Satz 3 und 4 HDSG zunächst unterblieben war. Jedoch wurde ein Mitarbeiter des Hessischen Datenschutzbeauftragten bereits im Jahr 2008 durch das Hessische Kultusministerium über das Vorhaben informiert. Inhaltlich wurden dabei keine datenschutzrechtlichen Bedenken erhoben, wenn die Einsicht in die Liste nur einem begrenzten Benutzerkreis möglich ist. Das Staatliche Schulamt Darmstadt, bei dem die ZMP angesiedelt ist, hat diesem und den weiteren zunächst erhobenen Einwänden betreffend Transparenz und verfahrensrechtlicher Mängel, wie vom Hessischen Datenschutzbeauftragten zutreffend festgestellt, inzwischen Rechnung getragen.

Zu 4.5.3 Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz von Lehrkräften

Die rechtlichen Vorgaben des Hessischen Kultusministeriums sind in Zusammenarbeit mit dem Hessischen Datenschutzbeauftragten formuliert worden. Die darin geregelte und vom Hessischen Datenschutzbeauftragten für unabdingbar gehaltene Verpflichtung, ihm nach vorheriger Terminvereinbarung Zugang zur häuslichen Arbeitsstätte der Lehrkraft zu gewähren, um die Einhaltung der datenschutzrechtlichen Vorgaben überprüfen zu können, war bereits im Vorgängererlass aus den 90er-Jahren enthalten und ist insofern keine Neuerung.

Zu 4.5.4 Beratung von Schulträgern bei der Einführung von Informationstechnik

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Die Hervorhebung des Main-Kinzig-Kreises als besonders gelungenes Beispiel für ein Gesamtkonzept sowie des Kreises Groß-Gerau für dessen Mustersicherheitskonzept ist ein zu begrüßendes positives Signal für die beiden Schulträger.

4.6 Wissenschaft und Forschung

Zu 4.6.1 Datenschutzkonzept für die Nationale Kohorte

Die Landesregierung teilt die rechtlichen Einschätzungen des Hessischen Datenschutzbeauftragten.

Zu 4.6.2 Zentrale Datenbank für die Erforschung von Lungenerkrankungen

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

Zu 4.6.3 Konzept für ein Nationales Mortalitätsregister

Der Hessische Datenschutzbeauftragte stellt ein Konzept für die Einführung eines Nationalen Mortalitätsregisters vor. Das Hessische Sozialministerium wurde in den bisherigen Dialog nicht eingebunden. Nach dem vorgestellten Konzept sollen die Gesundheitsämter die codierten Todesursachen an das Statistische Landesamt übermitteln. Dies gehört nach der derzeitigen Rechtslage nicht zu den Aufgaben der Gesundheitsämter in Hessen. Das Konzept bedarf im Hinblick auf das Konnexitätsprinzip einer Überprüfung.

4.7 Gesundheitswesen

Zu 4.7.1 Weiterhin in der Diskussion: Die Ausgestaltung der Zugriffe auf Krankenhausinformationssysteme

Der Hessische Datenschutzbeauftragte führt unter anderem aus, dass es selbst mit Einwilligung des Patienten nicht möglich ist, Stammdaten zwischen Medizinischem Versorgungszentrum (MVZ) und Klinik auszutauschen. Diese Einschränkung der informationellen Selbstbestimmung wird von der Rechtsprechung mit der besonderen Ausgestal-

tung der Datenschutzbestimmungen im SGB V begründet (vgl. BSG, Urt. v. 10. Dezember 2008, B 6 KA 37/07 R). Dies erschwert die gesundheitspolitisch erwünschte Verzahnung zwischen ambulantem und stationärem Sektor und kann zu vermeidbaren Doppeluntersuchungen und Behandlungsbrüchen führen. Im Rahmen weiterer Gesundheitsreformen sollte eine Überarbeitung der gesetzlichen Grundlagen erwogen werden.

Zu 4.7.2 Auftragsdatenverarbeitung durch den MDK Sachsen-Anhalt für den MDK Hessen - Fortsetzung der Prüfung

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Der Medizinische Dienst Hessen hat die Erfassung der Daten (§ 301 SBG V) nach § 80 SGB X angezeigt und ist somit seiner Verpflichtung nachgekommen. Mit der Problematik der fehlenden elektronischen Protokollierung der Zugriffe aus Sachsen- Anhalt auf den Server des MDK Hessen befindet sich der MDK Hessen in Abstimmung mit dem Hessischen Datenschutzbeauftragten.

Zu 4.7.3 Umfang und Inhalt amtsärztlicher Gutachten

Die Landesregierung stimmt der Darstellung des Hessischen Datenschutzbeauftragten grundsätzlich zu.

Die Ärztliche Begutachtung in Personalangelegenheiten des öffentlichen Dienstes war ab dem Jahr 2003 durch Erlass des Hessischen Sozialministeriums geregelt (StAnz. 43/2003 S. 4235). Die Frage der Notwendigkeit, des Umfangs, der Zuständigkeit und der Kostenerstattung von amtsärztlichen Gutachten hat in den vergangenen Jahren dennoch immer wieder zu Diskussionen der beteiligten Behörden geführt.

Zuständige Behörde für die Erstellung amtsärztlicher Gutachten sind nach § 14 Hessisches Gesetz über den öffentlichen Gesundheitsdienst (HGöGD) die Gesundheitsämter, allerdings wurden mit der Erstellung von amtsärztlichen Gutachten die Hessischen Ämter für Versorgung und Soziales (HÄVS) beauftragt. Trotz der Klarstellung in den §§ 14, 19 des HGöGD von 2007 ergaben sich immer wieder Zweifelsfragen. Vor diesem Hintergrund hat sich eine Erweiterung und komplette Neufassung des Erlasses als notwendig erwiesen.

In der Vorbereitung des neuen Erlasses hat eine Arbeitsgruppe unter Federführung des Hessischen Sozialministeriums Grundsätze für die amtsärztliche Untersuchung von Beamtinnen und Beamten, Richterinnen und Richtern, Beschäftigten und Versorgungsempfängerinnen und Versorgungsempfängern des öffentlichen Dienstes sowie von Bewerberinnen und Bewerbern für den öffentlichen Dienst und Personen in einem entsprechenden Ausbildungsverhältnis zwecks Ausstellung eines amtsärztlichen Zeugnisses auf Veranlassung von Behörden der Landesverwaltung, der Gemeinden und Gemeindeverbände des Landes Hessen sowie sonstiger der Aufsicht des Landes unterstehender Körperschaften, Anstalten oder Stiftungen des öffentlichen Rechts erarbeitet. Zu diesen Grundsätzen wurden von der Arbeitsgruppe auch strukturierte Vorlagen (Checklisten) für die Untersuchungen ausgearbeitet und dem Erlassentwurf als Anlagen angehängt. Gegenwärtig befindet sich der Erlassentwurf zur Überprüfung bei der AVV, anschließend wird er in die Ressortabstimmung gehen.

Das HGöGD steht zurzeit zur Novellierung an. Im einschlägigen § 18 HGöGD ist ausschließlich eine redaktionelle Änderung vorgesehen.

Zu 4.7.4 Patientenlisten auf dem Gehweg

Das Klinikum Kassel hat, wie der Hessische Datenschutzbeauftragte ausführt, die erforderlichen Maßnahmen getroffen, um zukünftig einen vergleichbaren Vorfall zu vermeiden. Weiterer Handlungsbedarf besteht nicht.

Zu 4.7.5 Auskunftsanspruch gegenüber einer Unfallversicherung

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zum Auskunftsanspruch gegenüber einer Unfallversicherung zu.

4.8 Sozialwesen

Zu 4.8.1 Datenschutzvorrang im Sozialverwaltungsverfahren

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zum Vorrang des Sozialdatenschutzes gegenüber dem Sozialverwaltungsverfahrensrecht in den Fällen, in denen es um personenbezogene Daten geht, zu. Das Hessische Sozialministerium nimmt die Ausführungen im Tätigkeitsbericht zum Anlass, die Vorschriften und den damit verbundenen Vorrang des Sozialdatenschutzrechts im Verhältnis zum Sozialverfahrensrecht in den Gremien anzusprechen.

Zu 4.8.2 Abruf von Konteninformationen eines "Doppelgängers" durch eine Sozialbehörde

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu. Wie im Tätigkeitsbericht aufgezeigt, besteht das Problem nicht bei den anfragenden Stellen, den Sozialleistungsträgern, sondern vielmehr bei dem Bundeszentralamt für Steuern. Die Fehleranfälligkeit des weiteren Verfahrens liegt darin begründet, dass das Bundeszentralamt die Kontenerklärung ohne Nutzen der Anschrift durchführt. Insoweit wird der Forderung des Hessischen Datenschutzbeauftragten zugestimmt.
Das Hessische Sozialministerium wird das Thema zur Information in den Gremien ansprechen.

Zu 4.8.3 Fehldrucke mit Sozialdaten als Malpapier für Kinder

Der Vorfall ist dem Hessischen Sozialministerium erst durch den Tätigkeitsbericht bekannt geworden. Die Aufgaben nach SGB VIII (Kinder- und Jugendhilfegesetz) werden in kommunaler Selbstverwaltung durchgeführt. Im Übrigen wurden nach dem Bericht des Hessischen Datenschutzbeauftragten vor Ort die notwendigen Maßnahmen ergriffen, um einen weiteren solchen Vorfall zukünftig auszuschließen.

Zu 4.8.4 Ausgestaltung des Formulars zur Einwilligung des Sozialleistungsempfängers in eine amtsärztliche Untersuchung

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Grundsätzlich bedarf es zur Einholung von Auskünften über medizinische Unterlagen (Befunde, Diagnosen) einer Einwilligung des Betroffenen und einer Schweigepflichtentbindung. Bei der Abfrage und Erhebung von Gesundheitsdaten ist eine Klarstellung gegenüber dem Betroffenen, welche Daten zu welchem Zweck benötigt werden, unbedingt erforderlich.
Das Hessische Sozialministerium wird das Thema auf der nächsten Sitzung der Arbeitsgruppe Eingliederung beim Arbeitskreis Option des Hessischen Landkreistages ansprechen und auf die vom Hessischen Datenschutzbeauftragten formulierten Erfordernisse hinweisen.

Zu 4.8.5 Informationsanspruch des Personalrats beim betrieblichen Eingliederungsmanagement

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.8.6 Hessische Familienkarte

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Der Hessische Datenschutzbeauftragte hat die Landesregierung konstruktiv bei der Konzeption und datenschutzrechtlichen Umsetzung des Projekts Familienkarte Hessen unterstützt. Dafür dankt die Landesregierung dem Hessischen Datenschutzbeauftragten und seinen Mitarbeiterinnen und Mitarbeitern ausdrücklich.

Die Zuständigkeit für die Familienkarte Hessen hat zum 1. Januar 2011 von der Hessischen Staatskanzlei zum Hessischen Sozialministerium gewechselt. Für die Inhaber der Familienkarte Hessen änderte sich durch den Wechsel nichts, alle Angebote sowie die Möglichkeiten der Beantragung und die Verarbeitung der Anträge wurden unverändert beibehalten. Auftraggeber ist in allen Fällen nun jedoch das Hessische Sozialministerium. Eine kleine Änderung gab es lediglich bei den Serviceleistungen. Hier werden neben Babysittern, Kinderferienbetreuung und Au-Pairs nun nicht mehr Tagesmütter vermittelt, sondern haushaltsnahe Dienstleistungen. Dies verändert das Procedere jedoch nicht.

Der Versand der Familienkarte Hessen erfolgt, wie bereits im Tätigkeitsbericht erwähnt, nicht mehr durch das Land, sondern durch einen Dienstleister. Hierbei gelten die gleichen Anforderungen nach § 4 HDSG wie für den Druck der Karten. Alle im Tätigkeitsbericht aufgeführten Punkte zur Verarbeitung personenbezogener Daten haben weiterhin Bestand und werden vom Hessischen Sozialministerium in der verlangten und mit dem Hessischen Datenschutzbeauftragten abgestimmten Form behandelt.

Auch hinsichtlich der Prüfung durch die Partner, ob es sich bei der angegeben Familienkarte um eine gültige Karte handelt, wird allen Forderungen des Hessischen Datenschutzbeauftragten Rechnung getragen. Der Partner erfährt durch Eingabe der Kartennummer und des Nachnamens, der ihm von der jeweiligen Familie genannt wird, lediglich, ob es sich bei dieser Karte um eine gültige Familienkarte Hessen handelt oder nicht. Weitere Informationen werden hierbei nicht übermittelt. Gleiches gilt für die Versicherung. Hier müssen die Familien im Schadensfall jedoch auf dem Schadensformular weitere Angaben machen. Zu diesem Zweck fragt die Versicherung die Daten direkt bei der Familie an.

Die Angaben zum Erhalt des Neugeborenenpakets stellen sich wie beschrieben dar. Die Weitergabe von Daten im Falle der Bestellung erfolgt auf freiwilliger Basis und bedarf nochmals einer gesonderten Einwilligung. Die Bestellung des Neugeborenenpakets erfolgt unabhängig von der Beantragung der Familienkarte Hessen. Durch das Einlesen der Familienkarte Hessen an den Kassenscannern kann lediglich erkannt werden, ob es sich hierbei um eine gültige Familienkarte Hessen handelt. Weitere Daten werden nicht erhoben.

Wird die Familienkarte Hessen an der Kasse in Verbindung mit einer EC-Karte eingesetzt, kann hierdurch nicht - wie bei anderen Kundenkarten - ein unmittelbares Käuferprofil durch das Unternehmen entwickelt werden. Es kann lediglich geschlussfolgert werden, dass im Haushalt des Käufers mindestens ein Kind unter 18 Jahren lebt und er in Hessen wohnhaft ist, da dies die Bedingungen für die Nutzung der Familienkarte sind. Mit der EC-Karte selbst findet lediglich eine Verrechnung mit dem Konto des Nutzers statt. Weder bei der Benutzung der Familienkarte Hessen noch der EC-Karte werden Daten wie Name oder Wohnort bei der Akzeptanzstelle unmittelbar elektronisch erfasst. Die Entwicklung eines Kundenprofils ist damit nicht möglich. Hierzu bedürfte es eines weiteren Schrittes von Seiten des Unternehmens, beispielsweise in dem es sich Daten bei Dritten zu der Kontoverbindung des Nutzers beschafft. Nur durch diesen zusätzlichen Schritt wäre eine Verknüpfung von Familienkartennummer und Anschrift des Kunden möglich.

5. Kommunale Selbstverwaltungskörperschaften

Zu 5.1 Feststellungen aus Prüfungen von Kommunen

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 5.2 Aktion "Gelbe Karte"

Die Landesregierung teilt die Auffassung des Hessischen Datenschutzbeauftragten, dass eine Aufbewahrung von drei Jahren notwendig, aber auch ausreichend ist.

Der Pilotversuch "Gelbe Karte" wurde im April 2010 vom Hessischen Ministerium des Innern und für Sport gemeinsam mit der Stadt Wiesbaden gestartet. Für die Datenspeicherung griff der Pilotanwender mangels einer besonderen Regelung auf die 10-Jahres-Frist des § 29 StVG, der die Tilgung der im Verkehrszentralregister eingetragenen rechtskräftigen Entscheidungen betrifft, zurück. Es ist beabsichtigt, die vom Hessischen Datenschutzbeauftragten empfohlene Speicherfrist den Fahrerlaubnisbehörden für den Fall einer möglichen Teilnahme am Pilotversuch verbindlich vorzugeben.

Darüber hinaus teilt die Landesregierung die Auffassung des Hessischen Datenschutzbeauftragten, dass für den Fall einer landesweiten Übernahme eine eigenständige Rechtsgrundlage notwendig ist. Da davon auszugehen ist, dass auch andere Bundesländer das Verfahren erproben werden, ist die Schaffung einer Rechtsgrundlage im Bundesrecht anzustreben. Der Hessische Datenschutzbeauftragte wurde gebeten, die Thematik mit den Datenschutzbeauftragten der anderen Bundesländern zu erörtern.

Zu 5.3 Beanstandung wegen unzulässiger Datenübermittlung an den Lahn-Dill-Kreis

Der Vorgang wurde vom Hessischen Ministerium für Wirtschaft, Verkehr und Landesentwicklung in enger Abstimmung mit dem Hessischen Datenschutzbeauftragten aufgearbeitet. Seitens des Hessischen Ministeriums für Wirtschaft, Verkehr und Landesentwicklung wurde im Juli 2010 gegenüber dem Landrat des Lahn-Dill-Kreises abschließend festgestellt, dass die Übermittlung personenbezogener Daten im besagten Falle ohne gesetzliche Ermächtigung und ohne Einwilligung des Betroffenen erfolgte. Der Landrat des Lahn-Dill-Kreises wurde gleichzeitig angewiesen, durch interne Maßnahmen dafür Sorge zu tragen, dass künftig die Beachtung der datenschutzrechtlichen Vorschriften durch die Fahrerlaubnisbehörde des Landkreises sichergestellt wird. Der Hessische Datenschutzbeauftragte wurde über die Erteilung der Weisung informiert.

Zu 5.4 Übermittlung von Bürgerdaten durch einen Bürgermeister an das Kreisgesundheitsamt

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.
Der beschriebene Einzelfall, bei dem Defizite bei der Umsetzung der Vorgaben des HGöGD und HDSG aufgetreten sind, wurde von der betroffenen Stelle in eigener Zuständigkeit geregelt, das Hessische Sozialministerium war nicht eingebunden. Das HGöGD steht momentan zur Novellierung an. Im einschlägigen § 18 HGöGD ist ausschließlich eine redaktionelle Änderung vorgesehen.

Zu 5.5 Neue Saisonkarten für Schwimmbäder

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 5.6 Abgleich von Fahrzeughalterdaten mit der Hundesteuerdatei einer Kommune

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 5.7 Datenübermittlung zur Nachwuchswerbung der Freiwilligen Feuerwehren

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

6. Sonstige Selbstverwaltungskörperschaften

6.1 Kreditinstitute

Zu 6.1.1 Auskunftsanspruch des Kunden bei Aufzeichnung von Telefongesprächen durch Kreditinstitute

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 6.1.2 Auskunftsanspruch des Erben gegenüber Kreditinstituten bei angeordneter Testamentsvollstreckung

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

7. Entwicklungen und Empfehlungen im Bereich der Technik

Zu 7.1 Sicherheit von Web-Anwendungen

Die Landesregierung nimmt die Anregung aus dem Tätigkeitsbericht auf und plant die Erstellung eines Maßnahmenkatalogs für die Entwicklung sicherer Webanwendungen. Dieser Maßnahmenkatalog wird im Auftrag des Arbeitskreises IT-Sicherheit des Landes Hessen erarbeitet und verabschiedet werden.

8. Bilanz

Zu 8.1 De-Mail: Sachstand (38. Tätigkeitsbericht, Nr. 3.1)

Die Landesregierung dankt dem Hessischen Datenschutzbeauftragten für die konstruktiven Anregungen bei der Erarbeitung der Stellungnahmen zum Gesetzentwurf. Hessen hat im Bundesrat gemeinsam mit den Ländern Bayern, Baden-Württemberg und Rheinland-Pfalz vielfältige Verbesserungen am Gesetzentwurf erreichen können, insbesondere zu datenschutzrechtlichen Fragen. Allerdings fand das Anliegen, eine Ende-zu-Ende-Verschlüsselung sicherzustellen, keine Mehrheit im Bundesrat. Die Landesregierung hat aber in intensiven Gesprächen mit dem Bund und den Regierungsfraktionen u.a. erwirkt, dass die sichere Anmeldung bei den De-Mail-Diensten das vorrangige Anmeldeverfahren ist und der Nutzer für den Fall der nicht sicheren Anmeldung über die Rechtsfolgen informiert werden muss.

Die Landesregierung wird die Entwicklung nach Inkrafttreten des Gesetzes weiter kritisch verfolgen und lädt den Hessischen Datenschutzbeauftragten ein, sich bei der Umsetzung in Hessen zu beteiligen.

Zu 8.2 Novellierung des HSOG - Regelung zur Videoüberwachung (38. Tätigkeitsbericht, Nr. 4.2.1.2)

Die Gesetzesänderung hat keine grundlegend neue Kennzeichnungspflicht für Polizei- und Gefahrenabwehrbehörden eingeführt. Vielmehr hat bereits die Verwaltungsvorschrift zum HSOG (VVHSOG) vom 3. Januar 2005 (StAnz. S. 218) in Nr. 14.3.2 für § 14 Abs. 3 und 4 HSOG auf das Erfordernis hingewiesen, dass der betroffene Personenkreis "zum Beispiel durch ein Hinweisschild" die Möglichkeit zur Kenntnisnahme von der Überwachungsmaßnahme erhalten muss.

Zu 8.3 Einsatz von Videotechnik zur Verkehrsüberwachung (38. Tätigkeitsbericht, Nr. 4.1.3)

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Wiesbaden, 26. September 2011

Der Hessische Ministerpräsident:
Bouffier

Der Hessische Minister des Innern und für Sport:
Rhein