19. Wahlperiode

Drucksache **19/4272**

HESSISCHER LANDTAG

05. 12. 2016

Stellungnahme
der Landesregierung
betreffend den Dreiundvierzigsten Tätigkeitsbericht
des Hessischen Datenschutzbeauftragten
Drucksache 19/2334

Eingegangen am 5. Dezember 2016 · Ausgegeben am 20. Dezember 2016
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Inhaltsverzeichnis

Stellungnahme zu:

1. Einführung

1.1 Allgemeines

Zu 1.1.2 National Security Agency
Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.1.3 Europäische Datenschutz-Grundverordnung
Die Europäische Datenschutz-Grundverordnung ist inzwischen im Amtsblatt der Europäischen Union verkündet worden (ABl. L 119 vom 4. Mai 2016, S. 1) und wird ab dem 25. Mai 2018 unmittelbar in allen Mitgliedstaaten der Union gelten. Es ist deshalb erforderlich, die im Landesrecht vorhandenen Vorschriften zum Datenschutz daraufhin zu überprüfen, ob sie mit den Regelungen der Datenschutz-Grundverordnung vereinbar sind, und sie ggf. zu ändern.

Zu 1.1.4 Rechtsprechung
Die Landesregierung nimmt den Bericht des Hessischen Datenschutzbeauftragten über die Entwicklung der Rechtsprechung zur Kenntnis.

Zu 1.1.5 Publikationen
Die Landesregierung nimmt den Bericht des Hessischen Datenschutzbeauftragten über neue Publikationen mit datenschutzrechtlichem Bezug zur Kenntnis.

Zu 1.1.6 Datenschutzbewusstsein
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die Gewährleistung der Privatheit auch angesichts neuer Entwicklungen im Bereich der Informations- und Kommunikationstechnik verfassungsrechtlich geboten ist.

Zu 1.2 Rechtsentwicklung in Europa
Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.3 Rechtsentwicklung in Deutschland
Die Landesregierung nimmt den Bericht des Hessischen Datenschutzbeauftragten über die Rechtsentwicklung in Deutschland zur Kenntnis.

Zu 1.4 Besonderheiten, Arbeitsschwerpunkte und Statistik
Die Landesregierung nimmt den Bericht des Hessischen Datenschutzbeauftragten über seine Wiederwahl und die Arbeitsschwerpunkte seiner Behörde zur Kenntnis.

2. Europa

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

Zu 2.1.1 EU-Datenschutz-Grundverordnungsentwurf
Der Bericht des Hessischen Datenschutzbeauftragten über den Ablauf der Beratungen zur Datenschutz-Grundverordnung ist zutreffend. Inzwischen ist die Datenschutz-Grundverordnung im Amtsblatt der Europäischen Union verkündet worden (ABl. L 119 vom 4. Mai 2016, S. 1) und wird ab dem 25. Mai 2018 gelten.

2.1.2 EU-Richtlinie für Polizei- und Justizbehörden
Nachdem die Verhandlungsführer aus Europäischem Parlament, Europäischem Rat und Europäischer Kommission die Trilog-Verhandlungen abgeschlossen und damit eine Einigung über die mehrjährigen Verhandlungen über eine Reform des EU-Datenschutzrechts erreicht haben, wurde die Richtlinie (EU) 2016/680 am 4. Mai 2016 im Amtsblatt der Europäischen Union (L 119 S. 89) veröffentlicht und ist mittlerweile - mit einer Umsetzungsfrist bis zum 25. Mai 2018 - in Kraft getreten. Aus hessischer Sicht sollte darauf geachtet werden, dass es bei einer Umsetzung in nationales Recht nicht zu einer Beeinträchtigung der Arbeit der Sicherheitsbehörden kommt. Dabei gilt es, einen hohen Datenschutzstandard und die Praxistauglichkeit des Datenschutzes in Ausgleich zu bringen.

2.2 "Smart Borders" - Intelligente Grenzen an den Außengrenzen der EU

Zu 2.2.1 Die Entwicklung des Reformprojekts im Berichtszeitraum
Am 25./26. Juni 2015 besuchten EU-Parlamentarier verschiedene finnische Grenzkontrollstellen. Dabei standen insbesondere Praktikabilitätsfragen bei Straßenverkehrs- und Schifffahrtskontrollen im Vordergrund. Im Hinblick auf die technische Umsetzung des Reformprojekts fanden Tests an den Flughäfen in Amsterdam, Lissabon, Arlanda und Frankfurt statt, u.a. zur automatischen Bilderkennung und zum Iris-Scan sowie Fingerabdrucktests.

Das Registrierungsprogramm für (Viel-)Reisende (RTP) soll im Vollzug durch die "Kiosk-Lösung" (Grenzabfertigung an einer zusätzlichen Übergangsstelle) vereinfacht werden. Dies wird voraussichtlich zu einer Entlastung der diplomatischen Vertretungen führen, aber den Zeitaufwand bei der Einreise vergrößern.

Zu 2.2.2 Datenschutzrechtliche Bedenken vor dem Hintergrund des Urteils des EuGH zur Vorratsdatenspeicherung

Der neue Vorschlag der Kommission vom 6. April 2016 für eine Verordnung des Europäischen Parlaments und des Rates über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten der Europäischen Union und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung der Verordnung (EG) Nr. 767/2008 und der Verordnung (EU) Nr. 1077/2011 wurde dem Bundesrat von der Bundesregierung zur Stellungnahme zugeleitet.

In seiner Sitzung vom 17. Juni 2016 hat der Bundesrat das mit dem Verordnungsvorschlag verfolgte Ziel, ein Einreise-/Ausreisesystem (EES) zur Erfassung und Speicherung von Informationen über den Zeitpunkt und den Ort der Ein-und der Ausreise von Drittstaatsangehörigen, die die Außengrenzen der Mitgliedstaaten überschreiten, zur Berechnung der Dauer ihres Aufenthalts und zur Erstellung von Warnmeldungen einzurichten, begrüßt. Auch die in Art. 24 des Verordnungsvorschlags enthaltene Möglichkeit für Inlandsbehörden beziehungsweise für die Polizei, eine Abfrage im EES zur Klärung der Frage, ob bei einem Drittstaatsangehörigen die Voraussetzungen für eine Einreise in das Hoheitsgebiet der Mitgliedstaaten oder den dortigen Aufenthalt erfüllt sind, durchzuführen, wurde vom Bundesrat grundsätzlich begrüßt.

Das Urteil des EuGH vom 8. April 2014 zur Ungültigkeit der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, wird im Verordnungsvorschlag vom 6. April 2016 berücksichtigt.

Zu 2.2.3 Zeitlicher Rahmen

Die Landesregierung war bisher mit Fragen der technischen Realisierung des EES nicht befasst, sodass zum zeitlichen Rahmen keine Angaben gemacht werden können.

Zu 2.3 EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

2.4 Koordinierte Kontrollgruppe für das SIS II

Zu 2.4.1 Ausschreibungen von gestohlenen Kraftfahrzeugen im SIS II

Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend. Mit dem Wiederauffinden des Fahrzeugs, der Mitteilung an den ausschreibenden Staat und dessen Möglichkeit, ein Rechtshilfeersuchen zu stellen, entfällt regelmäßig der Grund für die Ausschreibung. Ein polizeilicher Mehrwert durch ein weiteres Aufrechterhalten der SIS-II-Ausschreibung bis zum Abschluss bestimmter prozessualer Schritte ist grundsätzlich nicht erkennbar. Eine Löschung der Ausschreibung erfolgt in diesen Fällen grundsätzlich durch die ausschreibende Stelle. Wenn die ausschreibende Stelle eine hessische Polizeibehörde ist, wird die Löschung auch durch diese vorgenommen. Ein Nachhalten von Daten ("inaktuelle Fahndung") in SIS II erfolgt nicht.

Zu 2.4.2 Leitfaden zum Auskunftsrecht in allen Schengen-Staaten

Die Überarbeitung eines Leitfadens zum Auskunfts- und Löschungsrecht, einschließlich der Erstellung von Adresslisten und standardisierten Vordrucken, ist begrüßenswert, auch wenn die Zahl der Anträge (siehe Nr. 2.4.3 im Tätigkeitsbericht) im Verhältnis zu den gespeicherten Daten gering ist.

Zu 2.4.3 Bericht über die tatsächliche Ausübung der Rechte der Betroffenen

Die Landesregierung war an dem Projekt der Kontrollgruppe nicht beteiligt.

Zu 2.4.4 Abgleich von Meldevordrucken in Hotels mit dem SIS II

Die Ausführungen des Hessischen Datenschutzbeauftragten zu den neuen Rechtsgrundlagen sind zutreffend.

2.5 Gemeinsame Kontrollinstanz für Europol

Zu 2.5.1 Neue Rechtsgrundlage für Europol

Der Änderungsvorschlag der Gemeinsamen Kontrollinstanz (GKI) in deren Stellungnahme zum überarbeiteten Entwurf einer Europol-Verordnung zur Zusammensetzung des Beirats mit bis zu zwei Vertretern der jeweiligen nationalen Kontrollbehörde anstatt mit einem Vertreter wird begrüßt. Die Repräsentation der Bundesländer durch einen Vertreter der Landesdatenschutzbeauf-

tragten neben einem Vertreter der Bundesbeauftragten für Datenschutz im Beirat ist wegen des in Deutschland geltenden Grundsatzes "Polizei ist Ländersache" zu befürworten.

Mittlerweile ist das Gesetzgebungsverfahren zur Europol-Verordnung abgeschlossen und die Verordnung (EU) 2016/794 wurde am 24. Mai 2016 im Amtsblatt der Europäischen Union (L 135/53) veröffentlicht.

Zu 2.5.2 Europol als Dienstleister (Serviceprovider) für die Mitgliedstaaten
Die Europol-Verordnung stellt eine rechtliche Grundlage für die Funktion von Europol als Serviceprovider dar.

Zu 2.5.3 Zusammenarbeit von Europol mit den zentralen Meldestellen in den Mitgliedstaaten zur Verhinderung der Geldwäsche
Um insbesondere die analytischen Kompetenzen von Europol bei der Bekämpfung und Verhinderung von Geldwäsche nutzen zu können, ist mit der Europol-Verordnung die rechtliche Voraussetzung für eine Zusammenarbeit zwischen den nationalen Meldestellen und Europol geschaffen worden.

2.6 Google-Urteil des EuGH
Die Landesregierung nimmt den Bericht des Hessischen Datenschutzbeauftragten über den Inhalt und die datenschutzrechtlichen Folgen des Google-Urteils des EuGH vom 13. Mai 2014 zur Kenntnis.

3. Übergreifende Themen (öffentlicher und nicht öffentlicher Bereich)

3.1 Querschnittsthemen

Zu 3.1.1 Umgang mit Patientendaten nach Schließung von Krankenhäusern
Die Problemschilderung ist zum Teil zutreffend. Bei der Schließung von Krankenhäusern, z.B. im Falle einer Insolvenz, stellt sich in der Tat die Frage, wie die Patientenakten weiterhin sicher verwahrt werden. Wird ein Krankenhaus oder nur eine einzelne Betriebsstätte eines Krankenhauses geschlossen, ist der bisherige Krankenhausträger verpflichtet, die Aufbewahrung der Patientenakten - auf seine Kosten - sicherzustellen. Erfolgt die Aufbewahrung der Patientenakten in der stillgelegten Betriebsstätte, sind alle erforderlichen und zumutbaren Sicherungsmaßnahmen zu treffen, um einen unbefugten Zugriff zu verhindern.

In Hessen ist bislang nur der unter Nr. 3.1.1.1 geschilderte Fall (Schließung der Betriebsstätte der Asklepios-Klinik in Homberg) bekannt, bei dem die Sicherungsmaßnahmen des Krankenhausträgers offenbar nicht ausreichend waren. Aus diesem Grund kann nicht allgemein behauptet werden, dass "es ein hohes Risiko" gibt, dass Patientenakten nicht sicher verwahrt werden.

Auch im Zusammenhang mit einer Insolvenz eines Krankenhausbetriebes kann ebenfalls nicht allgemein von einem hohen Risiko gesprochen werden, dass nach Abschluss eines Insolvenzverfahrens die Aufbewahrung der Patientenakten nicht sichergestellt werden könnte. Zwar muss der Insolvenzverwalter im Zuge des Verfahrens über den Verbleib der Patientenakten entscheiden. Reicht die Insolvenzmasse nicht zur Deckung der Kosten für eine langfristige Aufbewahrung (z.B. 10 bis 30 Jahre) aus, muss er die Patientenakten "freigeben", d.h. die Akten werden sich selbst überlassen. Die Akten werden dann regelmäßig in den Räumen eingeschlossen, in denen sie sich bereits befinden.

Bislang ist in Hessen erst der unter Nr. 3.1.1.2 geschilderte Fall aufgetreten (ehemalige Reha-Klinik im Urbachtal), für den das Hessische Ministerium für Soziales und Integration jedoch nicht die Rechtsaufsicht inne hat.

Zu 3.1.1.1 Geschlossene Asklepios-Klinik in Homberg (Efze)
Über den geschilderten Sachverhalt wurde das Hessische Ministerium für Soziales und Integration im Frühjahr 2014 informiert. Zutreffend ist, dass die Betriebsstätte der Asklepios-Klinik in Homberg in Abstimmung mit dem Hessischen Ministerium für Soziales und Integration geschlossen wurde.

Die im Bericht genannten Gespräche haben stattgefunden. Die Geschäftsleitung der Asklepios Schwalm-Eder-Kliniken hat die genannten Sicherungsmaßnahmen gegenüber dem Hessischen Ministerium für Soziales und Integration bestätigt. Zutreffend ist, dass das Hessische Ministerium für Soziales und Integration dem Hessischen Datenschutzbeauftragten mitgeteilt hat, im Zuge einer weiteren Überarbeitung des Hessischen Krankenhausgesetzes eine Regelung über die Aufbewahrung von Patientenakten im Falle der Schließung eines Krankenhauses/einer Krankenhausbetriebsstätte aufzunehmen.

Richtig ist auch, dass das Hessische Krankenhausgesetz nur Krankenhäuser erfasst und nicht weitere Gesundheitseinrichtungen wie z.B. Reha-Kliniken.

Da die Problematik in der Tat alle Bundesländer betrifft, hat die Arbeitsgemeinschaft der Obersten Landesgesundheitsbehörden (AOLG) bereits beschlossen, dass die Initiative für eine bundesgesetzliche Regelung getroffen werden sollte.

Zu 3.1.1.2 Ehemalige Reha-Klinik im Urbachtal (Neukirchen, Hessen)
Der Hessische Datenschutzbeauftragte hatte das Hessische Ministerium für Soziales und Integration über den Fall der ehemaligen Reha-Klinik in Neukirchen informiert. Das Hessische Ministerium für Soziales und Integration führt jedoch nicht die Rechtsaufsicht über die Reha-Kliniken in Hessen. Gleichwohl wurde aufgrund des Vorfalls in Homberg Ende Oktober 2014 im Hessischen Ministerium für Soziales und Integration das im Datenschutzbericht erwähnte Gespräch geführt.

Zu 3.1.2 Weiter in der Diskussion: Ausgestaltung der Zugriffsberechtigungen in Krankenhausinformationssystemen
Das Hessische Ministerium für Soziales und Integration wurde nicht in die Prüfungen von Krankenhausinformationssystemen einbezogen. An den Gesprächen mit den betroffenen Krankenhäusern hat das Hessische Ministerium für Soziales und Integration nicht teilgenommen.

3.2 Entwicklungen und Empfehlungen im Bereich der Technik

Zu 3.2.1 Technischer Datenschutz und IT-Sicherheit - Aktivitäten in 2014
Die Landesregierung teilt die Bewertung des Hessischen Datenschutzbeauftragten zu den gemeinsamen Anstrengungen zur Verbesserung der organisatorischen und technischen IT-Sicherheit und wird die intensive Zusammenarbeit auch im Jahr 2016 und den Folgejahren fortsetzen.

Zu 3.2.1.1 Aktivitäten der Hessischen Landesverwaltung
Die Landesregierung nimmt den Bericht des Hessischen Datenschutzbeauftragten über ihre Aktivitäten im Bereich Technischer Datenschutz und IT-Sicherheit zur Kenntnis und bedankt sich für die Zusammenarbeit in den gemeinsamen Projekten.

Zu 3.2.1.2 Sonstige Sicherheitsprobleme am Beispiel SSL-Verschlüsselung
Die Landesregierung teilt die Bewertung des Hessischen Datenschutzbeauftragten zur Kritikalität von Schwachstellen im Verschlüsselungssystem SSL/TLS.

SSL/TLS ist der zentrale Schutzmechanismus für die Übertragung vertraulicher Daten im Internet und Gefährdungen dieses Mechanismus wirken unmittelbar auf nahezu alle Internet-Angebote, aber auch auf die Sicherheitsmaßnahmen für IT-Anwendungen der Landesverwaltung. Die Landesregierung erarbeitet deshalb einen Mindeststandard für den Einsatz von SSL/TLS in der Landesverwaltung, dabei werden die Empfehlungen des Hessischen Datenschutzbeauftragten und des BSI berücksichtigt.

Die Bewertungen der vom Hessischen Datenschutzbeauftragten benannten Beispiele sind zutreffend.

Zu 3.2.2 Orientierungshilfe "Cloud Computing"
Die Landesregierung begrüßt die aktualisierte "Orientierungshilfe Cloud Computing" der Datenschutzbeauftragten des Bundes und der Länder. Die Verwendung der Cloud-Technologien kann auch für die öffentliche Verwaltung einen wichtigen Beitrag zum wirtschaftlichen Betrieb der Informationstechnik darstellen. Aufgrund der im Tätigkeitsbericht aufgezeigten datenschutzrechtlichen Probleme sollten jedoch nur Cloud-Dienste verwendet werden, die unter der vollständigen Kontrolle der Verwaltung stehen.

4. Datenschutz im öffentlichen Bereich

4.1 Hessen

4.1.1 Hessen Querschnitt

Zu 4.1.1.1 Funktionaler Stellenbegriff - Datenübermittlung zwischen verschiedenen Ämtern eines Landkreises
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.1.2 Auftragsdatenverarbeitung - Kontrollrechte des Hessischen Datenschutzbeauftragten
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.1.3 Abgrenzung von öffentlicher Auslegung, öffentlicher Bekanntmachung und Internetöffentlichkeit
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

4.1.2 Justiz, Polizei und Verfassungsschutz

Zu 4.1.2.1 Einsatz von Body-Cams bei der hessischen Polizei
Der Einsatz von Body-Cams bei der hessischen Polizei erfolgt auf der Grundlage von § 14 Abs. 6 HSOG und der mit dem Hessischen Datenschutzbeauftragten abgestimmten Handlungsanweisung. Die im Tätigkeitsbericht erwähnten Rahmenbedingungen und Anforderungen an den Ein-

satz der Body-Cam wurden hierbei umgesetzt. Das vom Hessischen Datenschutzbeauftragten im Tätigkeitsbericht mangels Rechtsgrundlage als unzulässig eingestufte Pre-Recording ist mittlerweile durch den Landesgesetzgeber in § 14 Abs. 6 HSOG neben der neu eingeführten Tonaufzeichnung geregelt worden. Der Hessische Datenschutzbeauftragte wurde im Rahmen des Gesetzgebungsverfahrens zur Neufassung des § 14 Abs. 6 HSOG beteiligt und konnte seinen Bedenken Ausdruck verleihen. Eine ursprünglich vorgesehene Herabsenkung der Einsatzschwelle wurde daraufhin wieder rückgängig gemacht.

Landesweit stehen in Hessen aktuell 72 Kameras bei ausgesuchten Brennpunktdienststellen, die von den jeweiligen Präsidien festgelegt wurden, zur Verfügung. Die hessische Polizei achtet im Hinblick auf die Body-Cam insbesondere darauf, dass deren Einsatz als offene Maßnahme erkennbar ist sowie Aufzeichnungen mit der Body-Cam lediglich anlassbezogen erfolgen und auf ein notwendiges Maß beschränkt sind. Die Pre-Recording-Funktion wird daher gegenwärtig unter denselben Voraussetzungen angewendet wie die Aufnahmefunktion.

Zu 4.1.2.2 Verarbeitung der Daten des Landesamtes für Verfassungsschutz durch das Bundesamt

Die Landesregierung begrüßt und unterstützt die Forderung des Hessischen Datenschutzbeauftragten nach konsequenter Einhaltung seiner Kontrollrechte sowie der Rechte der von der Datenverarbeitung Betroffenen.

4.1.2.3 Novelle des Hessischen Sicherheitsüberprüfungsgesetzes

Zu 4.1.2.3.1 Zur Frage der Notwendigkeit einer Sicherheitsüberprüfung des Hessischen Datenschutzbeauftragten

Der Hessische Datenschutzbeauftragte wurde - wie bereits in der Praxis gehandhabt - in den Kreis der nicht zu überprüfenden Personen gemäß § 3 Abs. 4 HSÜG aufgenommen. Damit wurde der herausgehobenen Position, die der Datenschutzbeauftragte in Hessen genießt, Rechnung getragen.

Zu 4.1.2.3.2 Zur Möglichkeit der Anforderung einer Schufa-Auskunft beim Betroffenen

Im ursprünglichen Entwurf des HSÜG war aufgrund fachlicher Anregung des Landesamtes für Verfassungsschutz eine Zustimmung zur generellen Einholung einer SCHUFA-Auskunft von dem Betroffenen im Falle einer Sicherheitsüberprüfung - also eine Regelanfrage - vorgesehen. Aufgrund der Bedenken des Hessischen Datenschutzbeauftragten wurde als Kompromiss nur eine inhaltlich eingeschränkte und kostenfreie Datenauskunft nach § 34 BDSG aufgenommen und dies auch nur für den Einzelfall, dass sich Hinweise für eine mögliche finanzielle Angreifbarkeit ergeben.

Hintergrund einer solchen Auskunft ist, dass für die Beurteilung eines Sicherheitsrisikos eine mögliche finanzielle Angreifbarkeit des Betroffenen immens wichtig ist. Erpressbarkeit und Bestechlichkeit sind mit die größten Risikofaktoren im Bereich der sicherheitsempfindlichen Tätigkeiten. Für die Einschätzung ist eine möglichst umfassende Kenntnis über die Grundlagen der finanziellen Situation des Betroffenen unumgänglich. Durch eine Schufa-Eigenauskunft können weitere Erkenntnisse über Verbindlichkeiten erlangt werden, die beispielsweise aus der Selbstauskunft oder durch etwaige Befragungen nicht ermittelt werden können.

Die neugefasste gesetzliche Vorschrift sieht ein Einholen der Einwilligung zu einer Schufa-Auskunft nicht in jedem Falle vor. Nur wenn bei der Sicherheitsüberprüfung konkrete Hinweise auf eine mögliche finanzielle Angreifbarkeit des Betroffenen auftreten, wird eine solche Einwilligung erbeten. Da es sich um eine Einzelfallbetrachtung handelt, die bei jeder Sicherheitsüberprüfung aufs Neue durchgeführt wird, kann die Vorschrift nicht konkreter gefasst werden. Die Schufa-Auskunft stellt in diesem Fall eine zusätzliche Quelle dar, um das Ausmaß finanzieller Verpflichtungen möglichst genau zu erfassen. Sie hat in vielen Fällen einen speziell orientierten Erkenntnisgewinn, der mit anderen Quellen wie z.B. dem Schuldnerverzeichnis nicht in gleichem Maße erreicht werden kann. Die Datenauskunft wird dabei nicht getrennt gesehen und führt nicht sofort zu einer entsprechenden Bewertung, sondern ist ein Mosaikstein der Sicherheitsüberprüfung. Dabei wird sie - auch in Anbetracht der vielfach geäußerten Kritik an der Institution Schufa - sorgsam verwendet, um Fehlbewertungen auszuschließen.

Die Einholung der Datenauskunft kann auch im Sinne des Betroffenen sein, weil so mögliche Zweifel an der finanziellen Stabilität ausgeräumt werden können. Bestehen Anhaltspunkte für finanzielle Probleme, ist der zu überprüfenden Person regelmäßig ein solches Mittel recht, um jeglichen Verdacht aus dem Weg zu schaffen. Denn bleiben Zweifel bestehen, ist stets der Sicherheit des Staates Vorrang zu gewähren. Das Risiko, eine sicherheitsempfindliche Tätigkeit zu übertragen, kann sodann im Zweifelsfall zu groß sein. Die über die Schufa erlangten Angaben bleiben grundsächlich im geschützten Bereich des LfV. Sie werden allenfalls in einer Zusammenfassung im Rahmen der Mitteilung des Überprüfungsergebnisses an die zuständige Stelle weitergegeben. Eine mögliche Beeinträchtigung des Rechts auf informationelle Selbstbestimmung bleibt dadurch gering und ist keinesfalls unverhältnismäßig zu dem möglichen Erkenntnisgewinn.

Durch die vorgenommene Gesetzesergänzung wird die in der Praxis bereits etablierte und für notwendig erachtete Vorgehensweise gesetzlich niedergelegt. Dies dient auch der Transparenz und Vorhersehbarkeit des Verfahrens für den Betroffenen und zwar bereits im Vorfeld und nicht erst im Laufe dessen.

Zu 4.1.2.3.3 Zur Notwendigkeit der Angabe einer allgemein zugänglichen eigenen Internetseite und Teilnahme in sozialen Netzwerken im Rahmen der Sicherheitserklärung

Wie bereits in der Gesetzesbegründung näher ausgeführt, hat diese Überprüfungsmaßnahme vor allem den Sinn, das Auftreten des zu Überprüfenden in der virtuellen Öffentlichkeit einzuschätzen. Dies ist eine der wenigen Möglichkeiten, um festzustellen, wie der Betreffende mit sensiblen Daten umzugehen pflegt. Selbstverständlich sind die Äußerungen in sozialen Netzwerken regelmäßig vom Grundrecht auf Meinungsfreiheit gedeckt. Aus der Art der Nutzung ergeben sich im Vergleich zum gesprochenen Wort allerdings einige wesentliche und beachtenswerte Unterschiede. Es ist wichtig, dass Personen, die mit Verschlusssachen in Kontakt kommen, dafür ein besonderes Gespür haben oder entwickeln können. Die Kommunikation in sozialen Netzwerken ist verschriftlicht und im Gegensatz zum gesprochenen Wort nicht flüchtig. Mitteilungen im Internet sind kontinuierlich bis zur Löschung für den jeweiligen Adressatenkreis nachlesbar. Mit der Zugänglichmachung von Einträgen im Internet wird die Kontrolle über diese Inhalte abgegeben, da diese in der Regel zeitlich unbegrenzt abrufbar sind und grenzenlos kopiert werden können. Äußerungen im Internet bergen des Weiteren die Gefahr einer hohen und schnellen Verbreitung. Kommentare können damit ein Gewicht erlangen, das bei einer mündlichen Äußerung, z.B. unter Kollegen, nie erreicht worden wäre. Darüber hinaus werden die Auftritte in sozialen Netzwerken erfahrungsgemäß gerade von ausländischen Nachrichtendiensten genutzt, um im Rahmen des sogenannten "social engineering" Informationen für Anbahnungs- oder Ausforschungsaktivitäten zu gewinnen.

Auch wenn das Zurückhaltungsgebot grundsätzlich nur für Verfassungsschutzmitarbeiter gilt, besteht bezüglich Verschlusssachen (VS) eine allgemeine Dienstpflicht der Zurückhaltung, die sich z.B. in § 13 der VS-Anweisung widerspiegelt und Erörterungen über VS in der Öffentlichkeit untersagt. Zudem besteht auch für Beamte gemäß § 34 Satz 3 BeamtStG eine allgemeine Wohlverhaltenspflicht. Beamtinnen und Beamte trifft hiernach die Pflicht, ihr Verhalten innerhalb und außerhalb des Dienstes so einzurichten, dass es der Achtung und dem Vertrauen gerecht wird, die die berufliche Tätigkeit erfordern. Dies gilt insbesondere im Hinblick auf die Darstellung der eigenen Person in sozialen Netzwerken und ggf. damit verbundene Hinweise auf die Tätigkeit als Landesbeamtin oder -beamter. Diese Grundsätze müssen erst recht für Beamte gelten, die mit besonders sensiblen Daten wie Verschlusssachen umgehen.

Es kann aus diesen Gründen durchaus bedenklich sein, einer Person, die im Netz allzu sorglos mit ihren eigenen persönlichen Daten umgeht, sensible Verschlusssachen anzuvertrauen. Dabei wird dieser Eindruck - wie bereits ausführlich zu Nr. 4.1.2.3.2 ausgeführt - immer nur einen kleinen Baustein in einer Gesamtschau aller Angaben darstellen. Aber er hilft der überprüfenden Behörde, sich ein möglichst vollständiges Bild vom zu Überprüfenden zu machen.

Da der Betroffene seine Daten durch die Veröffentlichung im Netz sozusagen selbst allgemein zugänglich gemacht und damit zugestimmt hat, dass jedermann diese einsehen kann, ist der Eingriff in das Recht auf informationelle Selbstbestimmung in jedem Fall gering und sachlich gerechtfertigt.

Die Aufnahme der Regelung in das Gesetz dient zum einen der Transparenz und dem Kenntlichmachen der Quellen im Vorhinein einer Überprüfung. Zum anderen soll dem Betroffenen noch einmal ausdrücklich bewusst gemacht werden, dass jeder Bereich, in dem er mit anderen in Kontakt tritt - nicht nur der häusliche oder familiäre -, für die Tätigkeit mit Verschlusssachen bedeutsam sein kann und Risiken birgt. Dies wird ihm durch die ausdrückliche Abfrage eigener Internetseiten und Mitgliedschaft oder Teilnahme in sozialen Netzwerken noch einmal explizit vor Augen geführt.

4.1.3 Sozialwesen

Zu 4.1.3.1 Fehlbelegungsabgabe (Wohnungswesen) - Datenschutzrechtliche Aspekte der sozialen Wohnraumförderung

Das Hessische Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz hat dem Hessischen Datenschutzbeauftragten Ende 2014 den Referentenentwurf für ein Gesetz über die Erhebung einer Fehlbelegungsabgabe in der öffentlichen Wohnraumförderung (Fehlbelegungsabgabe-Gesetz - FBAG) mit der Gelegenheit zu einer datenschutzrechtliche Überprüfung vorgelegt.

Im Januar 2015 übermittelte der Hessische Datenschutzbeauftragte dem Hessischen Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz seine datenschutzrechtliche Bewertung hierzu. Die in der Bewertung enthaltenen Anregungen zu dem Gesetzentwurf wurden durch das Hessische Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz umgesetzt. Der Hessische Landtag hat das Gesetz mit diesen Änderungen beschlossen.

Zu 4.1.3.2 Kooperation von Jobcentern und anderen Stellen in der Grundsicherung für Arbeitsuchende

Der Sachverhalt und die rechtliche Bewertung sind zutreffend wiedergegeben. Der Hessische Datenschutzbeauftragte hat das Hessische Ministerium für Soziales und Integration über sein Verständnis der Rechtslage informiert.

Zu 4.1.3.3 Sozialdatenschutz und Überwachung der Kommunalverwaltung durch die Stadtverordnetenversammlung

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.3.4 Löschung von Gesundheitsdaten beim Jobcenter

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.3.5 Datenerhebung in der Grundsicherung für Arbeitsuchende

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.3.6 Verantwortlichkeit für Datenübermittlungen an die Sozialverwaltung

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

4.1.4 Gesundheit

Zu 4.1.4.1 Ausgestaltung von Schweigepflichtentbindungserklärungen der Gutachter- und Schlichtungsstelle bei der Landesärztekammer Hessen

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.5 Kommunale Selbstverwaltung

Zu 4.1.5.1 Ausstattung von Bürgerbüros

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.5.2 Übermittlung von Meldedaten an die Bundeswehr

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Auch nach § 36 Abs. 2 des am 1. November 2015 in Kraft getretenen Bundesmeldegesetzes ist die Datenübermittlung an das Bundesamt für das Personalmanagement der Bundeswehr nur zulässig, soweit die betroffene Person nicht widersprochen hat. Die Meldebehörden haben bei der Anmeldung und einmal jährlich, spätestens im Oktober, durch ortsübliche Bekanntmachung auf das Widerspruchsrecht hinzuweisen.

Zu 4.1.5.3 Keine Speicherung von Dissertationsurkunden und Scheidungsurteilen in Meldebehörden

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Die von der Meldebehörde zu speichernden Daten werden nunmehr durch § 3 des Bundesmeldegesetzes bestimmt. Die Ausführungen des Hessischen Datenschutzbeauftragten sind auch in Bezug auf diese neue Rechtsgrundlage für die Datenspeicherung zutreffend.

Zu 4.1.5.4 Fragebogen zur Anmeldung einer Nebenwohnung

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Wie die Hauptwohnung zu bestimmen ist, regeln nunmehr §§ 21, 22 Bundesmeldegesetz. Die Ausführungen des Hessischen Datenschutzbeauftragten sind auch in Bezug auf diese neue Rechtsgrundlage zutreffend.

Zu 4.1.5.5 Gebührenfreie Auskunft durch Standesämter

Die Auffassung des Hessischen Datenschutzbeauftragten, dass Standesämter verpflichtet sind, Bürgern schriftlich gebührenfrei Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen, wird im Ergebnis geteilt.

Nach § 62 Abs. 1 PStG sind Personenstandsurkunden auf Antrag den Personen zu erteilen, auf die sich der Registereintrag bezieht, sowie deren Ehegatten, Lebenspartnern, Vorfahren und Abkömmlingen. Andere Personen haben ein Recht auf Erteilung von Personenstandsurkunden, wenn sie ein rechtliches Interesse glaubhaft machen. Beim Geburtenregister oder Sterberegister reicht die Glaubhaftmachung eines berechtigten Interesses aus, wenn der Antrag von einem Geschwister des Kindes oder des Verstorbenen gestellt wird. Antragsbefugt sind über 16 Jahre alte Personen.

Nach § 62 Abs. 2 PStG gilt dies entsprechend für die Auskunft aus einem und Einsicht in einen Registereintrag sowie Auskunft aus den und Einsicht in die Sammelakten. § 61 Abs. 1 PStG bestimmt, dass die §§ 62 bis 66 für die Benutzung der bei den Standesämtern geführten Personenstandsregister und Sammelakten bis zum Ablauf der in § 5 Abs. 5 festgelegten Fristen gelten. Benutzung wird dabei definiert als Erteilung von Personenstandsurkunden aus einem Register-

eintrag, die Auskunft aus einem und die Einsicht in einen Registereintrag sowie die Durchsicht mehrerer Registereinträge einschließlich der entsprechenden Verwendung der Sammelakten.

Nach § 18 Abs. 3 HDSG haben datenverarbeitende Stellen, die personenbezogene Daten automatisiert speichern, dem Betroffenen auf Antrag gebührenfrei Auskunft zu erteilen über die zu seiner Person gespeicherten Daten. Auskünfte aus einem Registereintrag an Personen, auf die sich die Registereinträge beziehen, sind vom allgemeinen Auskunftsanspruch nach dieser Vorschrift umfasst, soweit die personenbezogenen Daten des Auskunftssuchenden selbst betroffen sind. Von § 18 Abs. 3 HDSG sind dagegen nicht erfasst die Erteilung von Personenstandsurkunden und die Auskunft an andere Personen als die, auf die sich der Registereintrag bezieht, sowie die Auskunft aus und die Einsicht in die Sammelakten.

Der Gesetzgeber hat mit § 62 i.V.m. § 61 und §§ 55 ff PStG eine abschließende spezifische datenschutzrechtliche Regelung betreffend die Erteilung von Personenstandsurkunden, Auskunfts- und Einsichtsrechte in Bezug auf die Registereinträge und Sammelakten erlassen, deren Regelungsgehalt über den in § 18 Abs. 3 HDSG normierten allgemeinen Anspruch auf Auskunftserteilung hinausgeht. § 62 PStG geht als spezielle bereichsspezifische Norm dem allgemeinen Auskunftsanspruch nach § 18 Abs. 3 HDSG vor. Die Subsidiarität gegenüber dem besonderen Datenschutzrecht folgt aus § 3 Abs. 3 HDSG. Danach gehen, soweit besondere Rechtsvorschriften über den Datenschutz bei der Verarbeitung personenbezogener Daten vorhanden sind, diese den Vorschriften des HDSG vor.

Während der Auskunftsanspruch nach § 18 Abs. 3 HDSG gebührenfrei ist, trifft § 62 PStG keine Gebührenregelung. Die Gebührenerhebung für die Erteilung von Personenstandsurkunden und Auskunftsansprüchen ist Ländersache und richtet sich nach §§ 1, 2 HVwKostG i.V.m. § 1 Verwaltungskostenordnung für den Geschäftsbereich des Ministeriums des Innern und für Sport (VwKostO-MdIS) i.V.m. Nrn. 651, 654 des Verwaltungskostenverzeichnisses. Nach Nr. 651 ff. werden für die Ausstellung von Personenstandsurkunden Gebühren zwischen 5 und 10 Euro erhoben, für die Auskunft aus einem oder Einsicht in einen Registereintrag oder Auskunft aus den oder Einsicht in die Sammelakten werden Gebühren nach Zeitaufwand erhoben. Insofern besteht im Hinblick auf die Gebührenerhebung ein Konflikt zwischen § 18 Abs. 3 HDSG und den Gebührenregelungen in Nrn. 651, 654 des Verwaltungskostenverzeichnisses. Dieser Konflikt ist dahin gehend aufzulösen, dass Auskünfte nach § 62 Abs. 2 i.V.m. § 62 Abs. 1 PStG in Bezug auf eigene Daten aufgrund der Regelung in § 18 Abs. 3 HDSG gebührenfrei erteilt werden müssen. Entsprechendes hat für den Anspruch auf Einsicht in eigene Daten zu gelten.

Für die Fälle der Erteilung von Personenstandurkunden nach § 62 Abs. 1 PStG sowie die Auskunfts- und Einsichtsrechte anderer Personen nach § 62 Abs. 2 i.V.m. § 62 Abs. 1 PStG bleibt es bei der nach §§ 1, 2 HVwKostG i.V.m. § 1 VwKostO-MdIS i.V.m. Nrn. 651, 654 des Verwaltungskostenverzeichnisses normierten Gebührenpflicht.

Um dem Rechtsgedanken des § 18 Abs. 3 HDSG zu entsprechen, soll Nr. 654 des Kostenverzeichnisses zur VwKostO-MdIS daher insoweit angepasst werden, als eine Gebühr zukünftig bei einer auf § 62 PStG gestützten Auskunft zu eigenen Daten oder Einsichtnahme in eigene Daten nicht mehr erhoben wird.

Zu 4.1.5.6 Auskünfte an Immobilienmakler über Grundstückseigentümer
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.5.7 Überprüfung schon länger bestehender Anlagen zur Videoüberwachung
Die Ausführungen des Hessischen Datenschutzbeauftragten hat das Landespolizeipräsidium aufgegriffen, um einen Erlass an die Regierungspräsidien zu verfassen, in dem im Zusammenhang mit der Videoüberwachung durch Gefahrenabwehrbehörden nach § 14 Abs. 4 HSOG auch die Hinweise des Hessischen Datenschutzbeauftragen auf Seite 131 des 43. Tätigkeitsberichts aufgriffen wurden.

Im Hinblick auf die im Tätigkeitsbericht erwähnten Kommunen, die dem Hessischen Datenschutzbeauftragten auf seine Anfrage zur Mitteilung des Ergebnisses der im zweijährigen Turnus vorzunehmenden Überprüfung der Voraussetzungen in § 14 Abs. 4 Satz 3 i.V.m. Abs. 3 Satz 3 HSOG im Berichtszeitraum noch nicht geantwortet hatten, wurde vom Innenministerium eine Beantwortung veranlasst, nachdem der HDSB die betreffenden Gemeinden benannt hatte; die Beantwortung ist mittlerweile von allen Gemeinden erfolgt.

Zu 4.1.5.8 Einführung von per Funk auslesbaren Wasserzählern
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

4.1.6 Personalwesen

Zu 4.1.6.1 Einsichtsrechte Dritter in die Personalakte
Nach § 90 Abs. 1 HBG ist es ohne Einwilligung der Beamtin oder des Beamten zulässig, die Personalakte für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorzulegen. Das Gleiche gilt für Behörden desselben Geschäftsbereichs, soweit die Vorlage zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist, sowie für Behörden eines anderen

Geschäftsbereichs desselben Dienstherrn, soweit diese an einer Personalentscheidung mitzuwirken haben. Ärztinnen und Ärzten, die im Auftrag der personalverwaltenden Behörde ein medizinisches Gutachten erstellen, darf die Personalakte ebenfalls ohne Einwilligung vorgelegt werden. Für Auskünfte aus der Personalakte gelten § 90 Abs. 1 Satz 1 bis 3 HBG entsprechend. Soweit eine Auskunft ausreicht, ist von einer Vorlage abzusehen. Nach § 90 Abs. 2 HBG dürfen Auskünfte an Dritte nur mit Einwilligung der Beamtin oder des Beamten erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz rechtlicher Interessen von Dritten die Auskunftserteilung erfordert. Inhalt und Empfängerin oder Empfänger der Auskunft sind der Beamtin oder dem Beamten schriftlich mitzuteilen. Diese Vorschriften kommen bei den Tarifbeschäftigten entsprechend zur Anwendung.

Im Übrigen wird der Auffassung des Hessischen Datenschutzbeauftragten zugestimmt, dass durch eindeutige Vorgaben geklärt werden sollte, welche Personen in der Verwaltung Zugang zu Personalakten erhalten und welche Personen im Zweifel über die Gewährung von Akteneinsicht oder -auskunft entscheiden und nach welchen Kriterien dies geschieht.

4.1.7 Ausländerbehörden

Zu 4.1.7.1 Akteneinsicht in Visumakten bei der Ausländerbehörde
Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass Visumantragstellern auch gegenüber der Ausländerbehörde ein Akteneinsichtsrecht zusteht. Auf die bereits im Tätigkeitsbericht zitierte Nr. 6.4.6 der Allgemeinen Verwaltungsvorschrift zum Aufenthaltsgesetz (AVwV-AufenthG) vom 27. Juli 2009 wird verwiesen.

Zu 4.1.7.2 Datenerhebung von Ausländerbehörden bei Jobcentern
Nach § 87 Abs. 1 des Aufenthaltsgesetzes (AufenthG) haben öffentliche Stellen ihnen bekannt gewordene Umstände den in § 86 Satz 1 AufenthG genannten Stellen bzw. den Ausländerbehörden auf Ersuchen mitzuteilen, soweit dies für deren Aufgabenerfüllung notwendig ist. Zu diesen öffentlichen Stellen gehören nach Nr. 87.1.1.1 AVwV-AufenthG u.a. die Bundesagentur für Arbeit, die Träger der Sozialhilfe und die Träger der Grundsicherung für Arbeitssuchende (Jobcenter). Nach Nr. 87.1.3.1 AVwV-AufenthG hat die Ausländerbehörde in ihrem Ersuchen anzugeben:

- die Personalien, die zur Identifizierung des Betroffenen erforderlich sind,
- Aktenzeichen der ersuchten Stelle, soweit bekannt,
- welche Daten sie benötigt,
- für welche Aufgabenerfüllung sie die Daten benötigt, wobei in eindeutigen Fällen die Angabe der Rechtsvorschrift ausreicht, und
- aus welchen Gründen die Daten ohne Mitwirkung des Betroffenen erhoben werden.

Ein Ersuchen nach § 87 Abs. 1 AufenthG ist zulässig, wenn die Daten gemäß § 4 Abs. 2 Satz 2 Bundesdatenschutzgesetz oder den einschlägigen Datenschutzbestimmungen der Länder ohne Mitwirkung des Betroffenen erhoben werden dürfen (vgl. Nr. 87.1.0 AVwVAufenthG).

Nach § 12 Abs. 1 HDSG sind personenbezogene Daten grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. Bei öffentlichen Stellen dürfen Daten im Einzelfall ohne Kenntnis des Betroffenen nach § 12 Abs. 2 Nr. 2 HDSG u.a. erhoben werden, wenn die Bearbeitung eines vom Betroffenen gestellten Antrags ohne Kenntnis der Daten nicht möglich ist oder Angaben des Betroffenen überprüft werden müssen.

Insbesondere wenn die Ausländerbehörde über den Antrag auf Erteilung oder Verlängerung eines Aufenthaltstitels zu befinden hat und die eigenständige Sicherung des Lebensunterhalts als allgemeine Erteilungsvoraussetzung i.S.d. § 5 Abs. 1 Nr. 1 AufenthG bei der Entscheidung zu berücksichtigen ist, ist ein Ersuchen der Ausländerbehörde an das Jobcenter nach § 87 Abs. 1 AufenthG gemäß § 12 Abs. 2 Nr. 2 HDSG statthaft. Im Übrigen wird dem Hessischen Datenschutzbeauftragten zugestimmt, dass reine Arbeitserleichterungen oder eine pauschale Überprüfung der Angaben des Betroffenen die Erhebung der Daten beim Jobcenter nicht rechtfertigen.

Zum Zeitpunkt der Vorlage des 43. Tätigkeitsberichts waren noch die mittlerweile novellierten Ausweisungsvorschriften der §§ 53 bis 56 AufenthG in der bis zum 31.12.2015 gültigen Fassung des Aufenthaltsgesetzes anzuwenden. Nach § 55 Abs. 2 AufenthG (alt) konnte ein Ausländer ausgewiesen werden, wenn er für sich, seine Familienangehörigen oder für sonstige Haushaltsangehörige Sozialhilfe in Anspruch nimmt. Nach § 87 Abs. 2 S. 1 Nr. 3 AufenthG haben öffentliche Stellen unverzüglich und ohne vorheriges Ersuchen die zuständige Ausländerbehörde zu unterrichten, wenn sie im Zusammenhang mit der Erfüllung ihrer Aufgaben Kenntnis von einem sonstigen Ausweisungsgrund - hier dem Sozialhilfebezug - erlangen.

Der Ausweisungsgrund ist durch den Begriff des Ausweisungsinteresses mit der Neufassung des Ausweisungsrechts zum 1. Januar 2016 abgelöst worden. Der neue § 54 AufenthG definiert, in welchen Fallgestaltungen ein Ausweisungsinteresse mit welchem Gewicht vorliegt. Der Bezug von Sozialhilfe begründet kein Ausweisungsinteresse, sodass eine Übermittlungspflicht des Jobcenters oder anderer Sozialbehörden ohne Ersuchen der Ausländerbehörde nach § 87 Abs. 2 AufenthG seit 1. Januar 2016 nicht mehr besteht.

4.1.8 Schulen, Schulverwaltung, Hochschulen, Archive

Zu 4.1.8.1 Bereitstellung von Daten aus der Lehrer- und Schülerdatenbank für die Kirchen in Hessen

Der Bericht des Hessischen Datenschutzbeauftragten beinhaltet korrekt den im Jahr 2014 abgestimmten und gültigen Sachverhalt für die Bereitstellung von Daten aus der Lehrer- und Schülerdatenbank für die Kirchen in Hessen. Folgeprüfungen und weiterführende Überlegungen haben im Jahr 2015 zu einem optimierten Verfahrensansatz geführt, der zunächst im Kultusministerium und mit der HZD abgestimmt und den Kirchenvertretungen anschließend vorgestellt wurde. Gegenwärtig konkretisieren und aktualisieren die Kirchen ihre Überlegungen dazu, welche personenbezogenen Daten sie unter Berücksichtigung der im Bericht des Hessischen Datenschutzbeauftragten aufgestellten Vorgaben für die Wahrnehmung ihrer Aufgaben im Einzelnen benötigen. Sobald eine konkretisierte und aktualisierte Anforderung seitens der Kirchen vorliegt, können eine entsprechende Abstimmung mit dem Hessischen Kultusministerium und eine abschließende Prüfung, Bewertung, und Genehmigung durch den Hessischen Datenschutzbeauftragten erfolgen.

Nach Genehmigung durch den Hessischen Datenschutzbeauftragten würden sich dann im Wesentlichen folgende Änderungen bzw. Ergänzungen ergeben:

Künftig wird ein Online-Zugriff der Kirchen mit reduziertem Datensatz möglich sein.

Die abgestimmten Kirchenberichte zu Unterrichts- und Personaldaten existieren in dem Informations- und Kommunikationssystem LUSDIK seit ca. zwei Jahren. Die Implementierung der Vorgaben des Hessischen Datenschutzbeauftragten ist abgeschlossen. Nicht personalisierte Unterrichtsdaten für beide Konfessionen sind einsehbar, genehmigte personalisierte Daten nur für die jeweilige Konfession abrufbar. Sie stehen seit August 2015 zur Verfügung, die Freischaltung der Kirchenberichte kann unmittelbar nach der Entscheidung zur Umsetzung der technischen Anbindung der Kirchenvertretungen erfolgen.

Es ist geplant, die Kirchenvertretungen mittels DSL-Router über das gesicherte Hessische Schulverwaltungsnetz (HSVN) an das IT-Anwendungssystem LUSDIK anzubinden, sodass sie online und verschlüsselt auf die jeweils für sie genehmigten und freigeschalteten Kirchenberichte zugreifen können.

Zu 4.1.8.2 Nutzung von sozialen Netzwerken durch Lehrkräfte in hessischen Schulen

Das Hessische Kultusministerium hat gemeinsam mit dem Landesbeauftragten für Jugendmedienschutz eine Handreichung zum Umgang mit sozialen Netzwerken für Lehrkräfte erarbeitet. Die Erarbeitung erfolgte in enger Abstimmung mit dem Hessischen Datenschutzbeauftragten.

Die Handreichung gibt Lehrkräften rechtliche Hinweise zur privaten Kommunikation über soziale Netzwerke sowie Handlungsempfehlungen für einen klar reglementierten Einsatz in der schulischen Kommunikation. Im Gegensatz zu einem generellen Verbot der Nutzung von sozialen Netzwerken im schulischen Kontext, das aus fachlicher Sicht als kontraproduktiv bezogen auf die gesellschaftliche Verbreitung der Netzwerke als Kommunikationsinstrument ist, soll die Handreichung den Lehrkräften Orientierung geben und eine begrenzte Nutzung ermöglichen, nicht zuletzt um Schülerinnen und Schüler in ihrer Lebenswirklichkeit abzuholen und mit ihnen im Rahmen der Medienbildung den sicheren Umgang mit sozialen Netzwerken einzuüben. Dieser pädagogischen Perspektive hat sich der Hessische Datenschutzbeauftragte angeschlossen.

Der Hessische Datenschutzbeauftragte hat nach Erläuterung der Vorteile einer Handreichung gegenüber einem Erlass der Form der Handreichung zugestimmt, da sie eine etablierte Form für konkrete Handlungsempfehlungen für Schulen darstellt. Sie macht darüber hinaus inhaltliche Anpassungen flexibel möglich, was für den dynamischen Bereich der sozialen Netzwerke, der sich in permanenter Weiterentwicklung befindet, von Vorteil ist. Die gewählte Form der Handreichung kommt auch der Forderung von Lehrerverbänden (allen voran der GEW) entgegen, die im Gegensatz zu einem Verbot der sozialen Netzwerke im schulischen Kontext die Forderung nach konkreten Handlungsempfehlungen gestellt hat.

Mit dem Hessischen Datenschutzbeauftragten wurde vereinbart, dass die Handlungsempfehlungen zum Umgang mit sozialen Netzwerken regelmäßig überprüft und bei Bedarf an aktuelle Erfordernisse und mediale Entwicklungen angepasst werden. Vor diesem Hintergrund ist den Darstellungen im Tätigkeitsbericht des Hessischen Datenschutzbeauftragten bezüglich der Nutzung von sozialen Netzwerken durch Lehrkräfte zuzustimmen.

Zu 4.1.8.3 Unzulässige Datenerhebung und Speicherung in einer Schülerakte

Der geschilderte Fall ist der Landesregierung nicht bekannt.

5. 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.

6. Bilanz

Zu 6.1 Prüfung der Hessischen Zentrale für Datenverarbeitung Hünfeld (42. Tätigkeitsbericht, Nr. 3.3.2.2)

Der Hessische Datenschutzbeauftragte bilanziert eine Ergebnisnachverfolgung von durch die HZD zu erledigenden Aufgaben aus einer im Jahre 2013 durchgeführten Überprüfung der HZD als Rechenzentrum der Hessischen Justiz.

- **Kontrolle von Besitzübernahmen durch Systemrevisoren der Justiz**

Die im Tätigkeitsbericht erwähnte Beschreibung wurde als Anleitung am 24. Juni 2013 im Mitarbeiterportal der Justiz veröffentlicht. Sie basiert auf der Angabe spezieller Filter in der Ergebnisansicht der Ereignisprotokollierung, die den Systemrevisoren der Justiz die Besitzübernahme von Konten (zum Beispiel Zugriff auf gesperrte persönliche Verzeichnisse von Richtern) ersichtlich macht.

- **Anzahl (Domänen-)Administratoren**

Das neue Administrationskonzept der HZD für die Domäne der Justiz wurde im Januar 2016 verabschiedet und soll im 2. Halbjahr 2016 entsprechend umgesetzt werden. Das Konzept sieht vor, die Zahl der Domänenadministratoren auf wenige (ca. fünf Personen) zu beschränken.

- **Nachvollziehbarkeit der Tätigkeit von Administratoren auf der E-Mail-Plattform der Justiz**

Die Kontrollsoftware für die Administratoren (Logmanagementsystem) ist in der HZD nach den im Jahr 2014 vom Hessischen Datenschutzbeauftragten gemachten Vorgaben für die E-Mail-Plattform eingerichtet worden. Für eine Umsetzung auf der E-Mail-Plattform der Justiz bedarf es in Abstimmung mit dem Hessischen Datenschutzbeauftragten noch weiterer Anpassungen, um eine datenschutzkonforme Lösung zu realisieren. Hierüber wurde der Justiz ein entsprechender Lösungsvorschlag unterbreitet.

- **Nachvollziehbarkeit der Bearbeitung von Aufträgen**

Der Hessische Datenschutzbeauftragte beschreibt die softwarebasierte Abhandlung von Vorgängen wie beispielsweise Störungen und Änderungen an IT-Systemen zu Dokumentationszwecken (sogenanntes "Ticketsystem"). Die im Bericht erwähnten Anforderungen werden bis zum 31.12.2016 - ungeachtet der mittlerweile erfolgten Überprüfung des geplanten neuen Ticketsystems - im bisher eingesetzten Ticketsystem der HZD umgesetzt.

Wiesbaden, 2. Dezember 2016

Der Hessische Ministerpräsident
Bouffier

Der Hessische Minister des Innern und für Sport
Beuth