18. Wahlperiode

Drucksache **18/2941**

HESSISCHER LANDTAG

28. 09. 2010

Stellungnahme
der Landesregierung
betreffend den Achtunddreißigsten Tätigkeitsbericht
des Hessischen Datenschutzbeauftragten
Drucksache 18/2027

Eingegangen am 28. September 2010 · Ausgegeben am 28. Oktober 2010
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Stellungnahme zu:

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

1. Einführung

1.1 Allgemeines

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zur Konzeption des informationellen Selbstbestimmungsrechts im Wesentlichen zu, wie den Stellungnahmen zu den nachfolgenden Ziffern des Tätigkeitsberichts im Einzelnen zu entnehmen ist. Die Landesregierung enthält sich jedoch einer Bewertung einzelner Beiträge der in der Literatur geführten Diskussion über das informationelle Selbstbestimmungsrecht.

Zu 1.2 Persönlichkeitsrecht

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

1.3 Datenschutz

Zu 1.3.1 Datenschutzrecht

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.3.2 Datenschutzgrundsätze

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.3.3 Einfachgesetzliche Ausgestaltung des Datenschutzes

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Unter Berücksichtigung der Erfahrungen der Vergangenheit erscheinen jedoch Zweifel angebracht, ob die nach Ansicht des Hessischen Datenschutzbeauftragten dringend gebotene Modernisierung des Datenschutzrechts "aus einem Guss" in absehbarer Zeit realisiert werden kann. Eine politische Diskussion mit derselben Zielsetzung wurde bereits vor rund zehn Jahren geführt. Im September 2001 legte zum Beispiel das Bundesministerium des Innern der Öffentlichkeit ein Gutachten mit dem Titel "Modernisierung des Datenschutzrechts" vor. Die Gutachter, A. Roßnagel, A. Pfitzmann und H. Garstka, forderten u.a., das Datenschutzrecht müsse verständlicher und Datenschutz sowohl für die datenverarbeitenden Stellen als auch für die Betroffenen attraktiver werden. Eingang in die nachfolgende Gesetzgebung zum Bundesdatenschutzgesetz hat das Gutachten nicht gefunden. Dabei bestand weniger Uneinigkeit über das Ziel einer Modernisierung des Datenschutzrechts, als den richtigen Weg, dieses zu erreichen.

Zu 1.3.3.1 Abwehrkomponente

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.3.3.2 Schutzkomponente

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.3.3.3 Datenzugangsschutz

In Bezug auf die Ausführungen zum Datenzugangsschutz wird auf die Stellungnahme der Landesregierung zu Ziffer 1 des 35. Tätigkeitsberichts des Hessischen Datenschutzbeauftragten (Drs. 16/7645) verwiesen. Im Übrigen hat der Hessische Landtag am 23. März 2010 sowohl den Gesetzentwurf der Fraktionen der SPD und BÜNDNIS 90/DIE GRÜNEN für ein Hessisches Gesetz über das Recht auf Informationsfreiheit in Hessen (Drs. 18/1895) als auch den Gesetzentwurf der Fraktion DIE LINKE für ein Hessisches Gesetz über die Freiheit des Informationszugangs (Drs. 18/1225) abgelehnt.

1.4 Rechtsentwicklung

Zu 1.4.1 Überblick

Über den Vollzug des Bundesdatenschutzgesetzes in Hessen berichtet die Landesregierung im Dreiundzwanzigsten Bericht über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, der zugleich mit dieser Stellungnahme dem Hessischen Landtag vorgelegt wurde.

Zu 1.4.2 Rechtsprechung

Die zitierte Entscheidung des OVG Hamburg (Urteil vom 04. Juni 2009 - 4 Bf 213/07-) gibt keinen Anlass zur Änderung von § 23 HSOG. Nach den Feststellungen des Gerichts hat die Polizei die Öffentlichkeitsfahndung selbst nicht zur Abwehr einer konkreten Gefahr vorgenommen, sondern nur zur Gefahrerforschung. Die Hamburger Polizei hat die Maßnahme offenbar auch lediglich auf § 21 Satz 1 Nr. 2 HmbPolDVG (Nachteile für das Gemeinwohl bzw. schwer wiegende Beeinträchtigungen von gewichtigen Rechtspositionen einzelner; vgl. juris Absatz-Nr. 13) gestützt. Das Gericht hat daher § 21 Satz 1 Nr. 1 HmbPolDVG (zur Erfüllung polizeilicher Aufgaben) von vornherein nicht als einschlägig angesehen und ohne jede Begründung verneint (vgl. juris Absatz-Nr. 40). Ganz abgesehen von dem zugrunde liegenden ungewöhnlichen Sachverhalt, kann das Urteil daher nicht als Maßstab für eine dringende Änderung des § 23 HSOG dienen. Gleichwohl ist die weitere Rechtsentwicklung zu beobachten und im Rahmen der nächsten Novellierung zu prüfen, ob auch insoweit Änderungsbedarf besteht.

1.5 Daseinsvorsorge

Zu 1.5.1 Gemeinsamer Ausgangspunkt

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 1.5.2 Landesregierung

Der Hessische Datenschutzbeauftragte gibt die Auffassung der Landesregierung zutreffend wieder.

Zu 1.5.3 Hessischer Datenschutzbeauftragter

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass dem Bundesgesetzgeber die Kompetenz fehlt, für den Landesbereich den Begriff der öffentlichen Stelle zu definieren. Gleichwohl kann der darauf aufbauenden Argumentation des Hessischen Datenschutzbeauftragten nicht gefolgt werden, dass daraus eine Berechtigung zur weiten Auslegung des Begriffs der öffentlichen Stelle nach § 3 Abs. 1 HDSG abzuleiten ist. Wie unter Ziffer 1.5.2 des Tätigkeitsberichts zutreffend wiedergegeben, hat der Bundesgesetzgeber nämlich seine unstreitig bestehende Kompetenz zur Definition der nicht öffentlichen Stelle im Bundesdatenschutzgesetz (BDSG) ausgeschöpft. Ein Unternehmen, das nach der Definition des § 2 Abs. 4 BDSG eine nicht öffentliche Stelle ist, darf nicht durch eine Regelung im Landesrecht oder dessen Auslegung zu einer öffentlichen Stelle im Sinne des Landesrechts umdefiniert werden. Sich überschneidende Definitionen könnten im Einzelfall dazu führen, dass ein

Unternehmen nach dem BDSG als nicht öffentliche Stelle und nach dem HDSG als öffentliche Stelle gilt. Das würde in der Praxis sowohl für die betroffenen Unternehmen als auch für die Aufsichtsbehörden zu erheblicher Rechtsunsicherheit führen. Der Landesgesetzgeber hat deshalb bewusst auf eine eigene Definition des Begriffs der "öffentlichen Stelle" verzichtet.

Die Antwort auf die Frage nach der zutreffenden Auslegung des Begriffs der "öffentlichen Stelle des Landes" kann an dieser Stelle letztlich offen bleiben, da der Hessische Datenschutzbeauftragte unter der folgenden Textziffer einen beiden Auffassungen gerecht werdenden Vorschlag für die Praxis unterbreitet.

Zu 1.5.4 Anwendungsbereiche

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die von ihm genannten Bereiche nicht vollständig der Daseinsvorsorge zugeschlagen werden dürfen, sondern die Kontrollzuständigkeit für ein Unternehmen im Einzelfall der Abklärung zwischen dem Hessischen Datenschutzbeauftragten und dem Regierungspräsidium Darmstadt bedarf.

2. Europa

Zu 2.1 Vertrag von Lissabon

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

2.2 Gemeinsame Kontrollinstanz für das Schengener Informationssystem

Zu 2.2.1 Schengener Informationssystem der zweiten Generation (SIS II)

Es ist zutreffend, dass im Projekt "SIS II" infolge technischer Probleme erhebliche Verzögerungen eingetreten sind. Der Rat für Justiz und Inneres hatte daher im Juni bzw. November 2009 Beschlüsse gefasst, in denen die Durchführung von sogenannten "Meilenstein-Tests" festgelegt und diesbezügliche Performance-Kriterien definiert wurden. Diese Beschlusslage umfasst auch die Absicht, dass bei einem Scheitern der Tests die Entwicklung von SIS II eingestellt werden und stattdessen eine Aufrüstung des bestehenden Systems SIS 1 plus erfolgen soll.

Ein erster Test wurde Ende Januar 2010 durchgeführt und verlief nicht erfolgreich. Dieser gescheiterte erste Test des SIS II wurde im März 2010 wiederholt. Die Testergebnisse wurden in der Sitzung des Rates für Justiz und Inneres am 23. April 2010 kontrovers erörtert. Bei Enthaltung der Delegationen Deutschlands und Österreichs wurde schließlich eine Ratsschlussfolgerung verabschiedet, dass der erste Test erfolgreich durchlaufen wurde. Der vorgeschriebene zweite Test ist für den Sommer 2010 geplant. Zur Sitzung des Rates für Justiz und Inneres am 03./04. Juni 2010 ist die Kommission - gemäß der Ratsschlussfolgerung vom 23. April 2010 - aufgefordert, eine belastbare Zeit- und Finanzplanung für das Projekt SIS II vorzulegen.

Der Beschluss des Europäischen Rates 2008/839/JI vom 24. Oktober 2008 über die Migration vom SIS 1 plus zum SIS II verliert seine Gültigkeit am 30. Juni 2010. Da dieser Termin infolge der vorgenannten technischen Probleme nicht mehr zu halten ist und zudem eine rechtliche Grundlage für eine mögliche Alternativlösung (Aufrüstung des SIS 1 plus) geschaffen werden muss, hat die Kommission bereits am 29. Januar 2010 einen Vorschlag für eine Verordnung zur Änderung des Beschlusses 2008/839/JI vorgelegt.

Die Darstellung des Hessischen Datenschutzbeauftragten, wonach die Rechtsgrundlagen für den Betrieb des SIS II (VO 2007/533/JI) auf jeden Fall - auch bei Ausweichen auf eine Alternativlösung - Anwendung finden sollen, deckt sich mit dem Kenntnisstand der Landesregierung. Demzufolge ist es auch zutreffend, dass die Kontrolle des künftigen SIS nicht mehr von der Gemeinsamen Kontrollinstanz, sondern durch den Europäischen Datenschutzbeauftragten und die nationalen Kontrollinstanzen wahrgenommen werden soll (Art. 62 der VO 2007/533/JI).

Zu 2.2.2 Gemeinsame Überprüfung der Ausschreibungen zur vorläufigen Ingewahrsamnahme

und 2.2.3 Gemeinsame Überprüfung der Ausschreibungen zur Wohnsitz- und Aufenthaltsermittlung

Unter diesen Ziffern berichtet der Hessische Datenschutzbeauftragte in seiner Funktion als Ländervertreter in der europäischen Kontrollinstanz für das Schengener Informationssystem. Aus den Ausführungen geht nicht hervor, auf welche Mitgliedstaaten die Kritik der Kontrollinstanz zielt. Nach dem Erfahrungsbericht des Bundesministeriums des Innern vom 21. Oktober 2009 zum Schengener Durchführungsübereinkommen sind seitens der Gemeinsamen Kontrollinstanz für Deutschland keine besonderen Beanstandungen zu Art. 97 und Art. 98 SDÜ erhoben worden.

Der Vorwurf der Gemeinsamen Kontrollinstanz, dass nicht in allen Schengen-Staaten Verfahrensvorschriften für die Ausschreibung erlassen wurden, betrifft Deutschland nicht. Mit der Polizeidienstvorschrift PDV 384.1 existiert für die deutsche Polizei eine detaillierte Verfahrensvorschrift für Ausschreibungen im Schengener Informationssystem; die dort unter Anlage 4 vorgegebenen Ausschreibungszeiträume und Löschfristen stehen im Einklang mit dem Schengener Durchführungsübereinkommen.

Zu 2.2.4 Leitfaden zum Auskunftsrecht in allen Schengen-Staaten

Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend. Die Internetseite der Gemeinsamen Kontrollinstanz ist unter http://www.schengen-jsa.dataprotection.org/ erreichbar (bis zum Redaktionsschluss allerdings nur in englischer Sprache).

2.3 Gemeinsame Kontrollinstanz für EUROPOL

Zu 2.3.1 Neue Rechtsgrundlagen für EUROPOL

Der Hessische Datenschutzbeauftragte berichtet zutreffend, dass der Beschluss des Rates (2009/371/JI) zur Errichtung des Europäischen Polizeiamts (EUROPOL) mit Wirkung zum 1. Januar 2010 in Kraft getreten ist. EUROPOL hat nun den Status einer EU-Agentur. In Deutschland wurde diese Rechtsänderung bereits mit Gesetz vom 31. Juli 2009 (BGBl. I S. 2504) mit Wirkung zum 5. August 2009 umgesetzt.

Zu 2.3.2 Kontrolle des Internets

EUROPOL hat die Initiative "Check the Web" bereits im Jahre 2009 in eine Analysedatei überführt. Deutschland hat mit dem Teil-Projekt "Erforschung extremistischer islamistischer Internetseiten - Analyse und Präventivmaßnahmen" auf europäischer Ebene die Federführung hinsichtlich der Verhinderung der Verbreitung terroristischer Inhalte im Internet übernommen.

Mit Stand 31. Dezember 2009 sind bei EUROPOL insgesamt bereits 20 Analysedateien (Analysis Work Files) für verschiedene Kriminalitätsbereiche eingerichtet, auf die nach hiesigen Erkenntnissen auch Drittstaaten zugreifen. Voraussetzung für die Nutzung der Analysedateien durch Drittstaaten ist dabei, dass diese ein operatives Kooperationsabkommen mit Europol abgeschlossen haben.

Zu 2.3.3 Austausch von Informationen mit Drittstaaten

Der Landesregierung liegen keine Erkenntnisse darüber vor, dass EUROPOL Informationen aus Drittstaaten entgegennimmt, ohne dass hierfür rechtsverbindliche Vereinbarungen getroffen wurden.

Zu 2.3.4 Kontrolle von EUROPOL

Über das Ergebnis der Kontrolle von EUROPOL durch die Gemeinsame Kontrollinstanz liegen der Landesregierung keine Informationen vor.

Zu 2.4 Koordinierungsgruppe für die Kontrolle von EURODAC

Der Hessische Datenschutzbeauftragte berichtet unter dieser Ziffer in seiner Funktion als Mitglied der Gemeinsamen Kontrollinstanz für EURODAC. Er bezieht sich dabei auf die EU-weite Situation und lässt offen, bei welchen Mitgliedstaaten konkret die Verfahrensweisen im Zusammenhang mit EURODAC zu beanstanden sind. Gleichwohl wurden die Feststellungen des Hessischen Datenschutzbeauftragten durch das Ministerium des Innern und für Sport dem zuständigen Bundesministerium des Innern sowie dem Bundesamt für Migration und Flüchtlinge mitgeteilt. Landesrechtliche Zuständigkeiten bestehen insoweit nicht.

3. Bund

Zu 3.1 Bürgerportalgesetz

Die Landesregierung teilt im Wesentlichen die Bedenken des Hessischen Datenschutzbeauftragten gegenüber dem 2009 vorgelegten Gesetzentwurf der Bundesregierung und hat diese Position im Bundesrat mit Nachdruck vertreten. Sollte das Gesetzgebungsverfahren wieder aufgenommen werden und ein neuer Gesetzentwurf die im vorhergehenden Verfahren geäußerten Bedenken und Anforderungen nicht berücksichtigen, wird die Landesregierung über den Bundesrat auf eine Neufassung hinwirken, die die hessische Position - und damit auch Forderungen des Datenschutzbeauftragten - berücksichtigt.

Zu 3.2 Der Auskunftsanspruch Betroffener darf auch in Besteuerungsverfahren nicht verkürzt werden

Das Schreiben des Bundesministeriums der Finanzen (BMF) vom 17. Dezember 2008 - IV A 3 - S0030/08/10001 - richtet sich an die obersten Finanzbehörden der Länder und die ihnen nachgeordneten Landesfinanzbehörden, nicht an Bundesbehörden bzw. Bundesfinanzbehörden. Der Beschluss des Ersten Senats des Bundesverfassungsgerichts (BVerfG) vom 10. März 2008 - 1 BvR 2388/03 -, in dem die Anwendbarkeit von § 19 BDSG im Besteuerungsverfahren bestätigt wurde, betraf nur das Bundeszentralamt für Steuern und damit eine Bundesbehörde. Eine Aussage zu Auskunftsansprüchen gegenüber Landesfinanzbehörden hat das BVerfG - mangels Entscheidungserheblichkeit - nicht getroffen. Für Landes(finanz)behörden gelten aber weder das Bundesdatenschutzgesetz (BDSG) noch das Informationsfreiheitsgesetz des Bundes (IFG).

Durch das BMF-Schreiben sollen bis zur Einführung entsprechender bundesgesetzlicher Regelungen in der Abgabenordnung (AO), die - wie vom Hessischen Datenschutzbeauftragten zutreffend festgestellt - derzeit erarbeitet werden, Mindeststandards für die Auskunftserteilung im Besteuerungsverfahren geschaffen werden, die dem Beschluss des Ersten Senats des BVerfG vom 10. März 2008 Rechnung tragen und weitgehend an § 19 BDSG orientiert sind. Das BMF-Schreiben stellt die Auskunftserteilung nicht in das Ermessen der Finanzbehörde, es enthält lediglich nähere Regelungen zu Art und Umfang der Auskunftserteilung und zu möglichen Ausnahmetatbeständen. Damit wird eine gleichmäßige Rechtsanwendung gewährleistet.

Bei der Ausgestaltung des BMF-Schreibens haben sich die obersten Finanzbehörden des Bundes und der Länder insbesondere von folgenden Aspekten leiten lassen, die auch der vorgenannten Entscheidung des BVerfG zugrunde liegen und dem Bundesbeauftragten für den Datenschutz mitgeteilt wurden:

- Das Grundrecht auf informationelle Selbstbestimmung schützt das Interesse des Einzelnen, von staatlichen informationsbezogenen Maßnahmen zu erfahren, die ihn in seinen Grundrechten betreffen. Nur wenn der Einzelne, der möglicherweise von einem Eingriff in das Recht auf informationelle Selbstbestimmung betroffen ist, eine Möglichkeit hat, von diesem Eingriff zu erfahren, kann er die für die freie Entfaltung seiner Persönlichkeit wichtige Orientierung und Erwartungssicherheit erlangen.
- Eine Informationsmöglichkeit für den von einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung Betroffenen ist Voraussetzung dafür, dass er die Rechtswidrigkeit der Informationsgewinnung oder etwaige Rechte auf Löschung oder Berichtigung geltend machen kann. Insoweit ist der Anspruch auf die Kenntniserlangung ein Erfordernis effektiven Grundrechtsschutzes im Bereich sowohl des behördlichen als auch des gerichtlichen Verfahrens.
- Soweit die Grundrechte die Möglichkeit des Einzelnen schützen, von einer ihn betreffenden informationsbezogenen Maßnahme des Staates Kenntnis zu erlangen, gibt das Grundgesetz allerdings nicht vor, wie dies im Einzelnen gesetzlich auszugestalten ist. Der Gesetzgeber hat unter Beachtung der Grundrechte der Betroffenen eine hinreichende Kenntnischance zu gewährleisten. Das Grundrecht auf informationelle Selbstbestimmung gewährt allerdings keinen Anspruch auf eine bestimmte Art der Informationserlangung.
- Der Einzelne hat Kenntnis der ihn konkret betreffenden Informationen, über die der Staat verfügt, wenn er an der Datenerhebung oder Datenverarbeitung beteiligt wird. So liegt es, wenn Daten offen erhoben werden oder dem Betroffenen eine rechtlich gesicherte Möglichkeit zur Stellungnahme eingeräumt wird. Dies ist im Besteuerungsverfahren der Regelfall.
- Auch können Kenntnisrechte auf Initiative des Betroffenen vorgesehen werden, wie sie etwa durch Ansprüche auf Auskunft oder Akteneinsicht vermittelt werden. Für Bundesfinanzbehörden ergibt sich dies unmittelbar aus § 19 BDSG. Für Landesfinanzbehörden gelten insoweit weder das BDSG noch das landesrechtliche Datenschutzgesetz.
- Bei heimlichen Datenerhebungen kann eine aktive Benachrichtigung des Betroffenen grundrechtlich geboten sein, wenn es sich um einen Grundrechtseingriff von erheblichem Gewicht handelt und andere Kenntnismöglichkeiten den Interessen des Betroffenen nicht hinreichend Rechnung tragen.
- Bei der Ausgestaltung des Zugangs zu Informationen ist zu berücksichtigen, welche Bedeutung ihm für den Grundrechtsschutz des Betroffenen zukommt. Hierfür sind insbesondere Art und Eingriffsintensität der jeweiligen informationsbezogenen Maßnahme von Bedeutung, über die oder über deren Ergebnisse der Betroffene informiert werden will.
- Ist eine staatliche Stelle zu informationsbezogenen Eingriffen berechtigt, deren Vornahme oder Umfang der Betroffene nicht sicher abschätzen kann, da er in den Informationsverarbeitungsprozess nicht oder nicht stets einbezogen wird, und besteht zudem keine Pflicht dieser Stelle zur aktiven Benachrichtigung des Betroffenen, kommt einem Informationsrecht auf eigene Initiative zentrale Bedeutung für den Grundrechtsschutz zu. Dies gilt insbesondere, wenn Daten gesammelt werden, die entweder von vornherein ohne Mitwirkung des Betroffenen erhoben worden sind oder deren Speicherungszweck von dem Erhebungszweck gelöst wurde. Dementsprechend sind für den Betroffenen bei der Datenerhebung Zweck und Umfang einer späteren Speicherung und ihrer möglichen Verknüpfung mit weiteren Datensammlungen nicht absehbar.
- Für ein behördliches Ermessen bei der Entscheidung über die Auskunftserteilung ist in derartigen Fällen verfassungsrechtlich kein Raum. Soweit gegenläufige Geheimhaltungsinteressen des Staates oder Dritter der Information entgegenstehen können, ist es Aufgabe des Gesetzgebers, geeignete Ausschlusstatbestände zu schaffen, die den einander gegenüberstehenden Interessen Rechnung tragen.
- Da Einschränkungen des Informationsrechts bei der Sammlung von Daten, die entweder von vornherein ohne Mitwirkung des Betroffenen erhoben worden sind oder deren Speicherungszweck von dem Erhebungszweck gelöst wurde, den Schutz vor unbegrenzter staatlicher Datenerhebung und Datenverarbeitung zumindest erheblich erschweren können, sind sie nur zulässig, wenn sie gegenläufigen Interessen von größerem Gewicht dienen. § 19 BDSG trägt diesen Anforderungen nach Überzeugung des BVerfG in hinreichender Weise Rechnung.
- Grundsätzlich kann die Sicherung der ordnungsgemäßen Aufgabenerfüllung staatlicher Stellen eine Einschränkung des Auskunftsrechts - wie in § 19 Abs. 4 Nr. 1 BDSG geschehen - rechtfertigen. Ob im Einzelfall eine Auskunftserteilung ausgeschlossen werden darf oder nicht, richtet sich insbesondere nach der Bedeutung des Auskunftsrechts für die Grundrechte des Betroffenen, nach dem Gewicht der jeweiligen behördlichen Aufgabe und nach den Auswirkungen einer Auskunft auf die Aufgabenerfüllung. Die in § 19 Abs. 4 BDSG am Ende enthaltene Abwägungsklausel stellt sicher, dass eine Auskunft nur dann unterbleiben darf, wenn das Interesse an der ordnungsgemäßen Aufgabenerfüllung dem Informationsinteresse des Betroffenen vorgeht.
- Das mit der Geheimhaltung von Daten, die zur Vermeidung von Steuerverkürzungen und Steuerumgehungen gespeichert oder verknüpft wurden, verfolgte Ziel der gleichmäßigen Festsetzung und Erhebung von Steuern hat

verfassungsrechtliches Gewicht. Das Informationsinteresse des Betroffenen wiegt dagegen auch nach Auffassung des BVerfG vergleichsweise geringer.

- Eine Auskunftserteilung über derart "sensible" Daten würde es dem Betroffenen ermöglichen, sein Erklärungsverhalten auf den Kenntnisstand der Finanzbehörden einzustellen. Dies würde zu einer weitgehenden Wertlosigkeit der Daten nach einer Auskunftserteilung und damit zu einer Erschwerung oder Unmöglichkeit der Aufgabenerfüllung der Behörde führen.
- Die Daten werden dem Betroffenen ohnehin bei Durchführung des Besteuerungsverfahrens, z.B. durch eine Anhörung nach § 91 AO oder in der Begründung eines belastenden Verwaltungsakts (vgl. § 121 AO) offenbart, soweit sie für die Festsetzung und Erhebung von Steuern erheblich sind.
- Aus dem Unterlassen einer Auskunft können den Betroffenen keine irreparablen Nachteile entstehen. Der gegen die Datenerhebung und -sammlung zu gewährleistende Rechtsschutz wird nicht faktisch ausgeschlossen, sondern auf einen späteren Zeitpunkt im staatlichen Informationsverarbeitungsprozess verlagert, zu dem die Belange des Betroffenen noch hinreichend gewahrt werden können. Der Betroffene hat nämlich die Möglichkeit, die Zulässigkeit der Datenerhebung und -speicherung und die Richtigkeit der jeweils betroffenen Informationen umfassend zur Überprüfung zu stellen, sobald diese mit für ihn nachteiligen Folgen genutzt werden, also im Rahmen eines konkreten Besteuerungs- oder Steuerstrafverfahrens.
- Mit einer Auskunftsverweigerung wird zwar das grundrechtlich geschützte Interesse des Beschwerdeführers beeinträchtigt, Gewissheit über die ihn betreffenden Informationen zu erlangen. Ein vollständiger Überblick über die gesammelten Daten bleibt dem Betroffenen grundsätzlich versagt. Dies ist jedoch angesichts des hohen Gewichts der Ziele der Datenerhebung und -sammlung verfassungsrechtlich hinnehmbar.

Zu 3.3 Abfrage von Steuerkonten über das Internet im Verfahren ELSTER (Elektronische Steuererklärung)

Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geforderte Verfahrensumstellung bei der Berechtigungsprüfung vom qualifizierten Zertifikat zum sogenannten Authentifizierungszertifikat einer Signaturkarte wurde bereits vor mehreren Jahren vorgenommen.

Im ELSTER Online Portal sind die derzeit unterstützten Signaturkarten für Authentifizierung gelistet. Vom Verfahren werden nur solche Signaturkarten akzeptiert und unterstützt, die eine sogenannte ELSTER-Policy erfüllen. In diesem Regelwerk werden die Anforderungen an die Signatur-Erzeugungskomponente, die von der Signaturerzeugungskomponente herausgegebenen Zertifikate und die Arbeitsweise des Herausgebers der Signaturerzeugungskomponente für den Ausgabeprozess geregelt. Der dort beschriebene Mindeststandard wurde in Anlehnung an das Signaturgesetz festgelegt und wird bei der Integration einer Signaturkarte durch einen Dritten verifiziert.

Die bislang dort festgelegte minimale Schlüsselstärke für das verwendete RSA-Verfahren beträgt 1024 Bit Schlüssellänge und entspricht der bis Ende 2007 gültigen Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik und der Bundesnetzagentur. Teilweise werden aber bereits heute Signaturkarten mit stärkeren Schlüssellängen (2048 Bit) genutzt, welche vom Verfahren ELSTER in Anlehnung an die Empfehlungen des BSI und der Bundesnetzagentur empfohlen werden.

Ab 2011 wird die Schlüssellänge im Verfahren ELSTER auf die in der aktuell gültigen Übersicht über geeignete Algorithmen empfohlene Länge von 2048 Bit (Mindestlänge 1976 Bit) für RSA Verfahren angehoben (vgl. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung der Bundesnetzagentur vom 6. Januar 2010, veröffentlicht im Bundesanzeiger Nr. 19 vom 4. Februar 2010, Seite 426).

Ab diesem Zeitpunkt werden vom Verfahren ELSTER keine Signaturkarten mehr unterstützt, die eine geringere Schlüsselstärke anbieten.

Insofern ist die im Tätigkeitsbericht getroffene Aussage, dass mit der Korrektur des Verfahrens zwar die richtige Version benutzt werde, aber das Sicherheitsniveau abgesenkt worden sei, nur teilweise korrekt. Das Sicherheitsniveau wurde gleichbleibend unterstützt und wird nunmehr auf die aktuelle Empfehlung angehoben.

4. Land

4.1 Querschnitt

Zu 4.1.1 Verdeckte Bildaufnahmen während der Räumung des Camps von Flughafenausbaugegnern im Kelsterbacher Wald

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.2 Einsatz von Videotechnik zu Planungszwecken

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.1.3 Einsatz von Videotechnik zur Verkehrsüberwachung

Es ist zutreffend, dass das Ministerium des Innern und für Sport die betroffenen Behörden über die Entscheidung des Bundesverfassungsgerichts vom 11. August 2009 unterrichtet hat; dazu ergingen am 9. September 2009 Erlasse an die Polizeibehörden und an die Regierungspräsidien.

Ergänzend ist anzumerken, dass mit der Bedienung von Geschwindigkeits- und Abstandsmesssystemen grundsätzlich nur Bedienstete der Polizei und Ordnungsbehörden beauftragt werden, die an der Polizeiakademie Hessen (ehem. Hessischen Polizeischule) entsprechend unterwiesen wurden (vgl. Erlass "Verkehrsüberwachung durch örtliche Ordnungsbehörden und Polizeibehörden" vom 6. Januar 2006, StAnz. 5/2006 S. 286, geändert durch Erlass vom 9. Juli 2008, StAnz. 31/2008 S. 1958). Bei der Ausbildung zum Einsatz der relevanten Verkehrsüberwachungssysteme wird ebenfalls darauf hingewiesen, dass verdachtslose Bildaufzeichnungen mangels gesetzlicher Ermächtigungsgrundlage unzulässig sind.

4.2 Justiz, Strafvollzug und Polizei

Zu 4.2.1 Novellierung des HSOG

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend.

Zu 4.2.1.1 Vertrauensschutz für Berufsgeheimnisträger

Der Hessische Datenschutzbeauftragte kritisiert die unterschiedliche Behandlung der Berufsgeheimnisträger als nicht nachvollziehbar. Hierzu ist anzumerken, dass der Gesetzentwurf aus der Mitte des Landtags die in der Koalitionsvereinbarung zu diesem Punkt getroffene Absprache umsetzt (vgl. Nr. 8 des Abschnitts "Innen und Recht). Der Kreis der Berufsgeheimnisträger nach § 53 StPO ist in seiner jetzigen Zusammensetzung nicht durch höherrangiges Recht vorgegeben. Erst recht gibt es keine Verpflichtung, im Polizeirecht denselben Kreis von Berufsgeheimnisträgern zu schützen wie im Strafprozessrecht. Die Freistellung bestimmter Berufsgruppen von Zeugnis- bzw. Auskunftspflichten muss deswegen auch keineswegs zwischen den verschiedenen, völlig eigenständigen Berufsgruppen gerechtfertigt werden, sondern nur im Hinblick auf die wahrzunehmende öffentliche Aufgabe.

Nach dem dreistufigen Konzept der Vorschrift können alle Berufsgeheimnisträger nach § 53 StPO die Aussage verweigern, es sei denn es besteht eine Gefahr für Leib, Leben oder Freiheit einer Person. Die Ausnahme betrifft also nur höchstrangige Individualrechtsgüter. Da Nichtstörer nach § 12 Abs. 2 Satz 1 HSOG lediglich unter den Voraussetzungen des § 9 HSOG in Anspruch genommen werden dürfen, muss die Gefahr in diesen Fällen zudem nicht nur konkret, sondern schon gegenwärtig sein (§ 9 Abs. 1 Nr. 1 HSOG). Wohnraumüberwachung sowie Telekommunikationsüberwachung erfordern stets, dass die Maßnahme zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist (§ 15 Abs. 4, § 15a Abs. 1, § 15b Abs. 1 HSOG), gehen also nochmals über diese ohnehin schon hohen Anforderungen hinaus.

Wenn ein Berufsgeheimnisträger danach in Anspruch genommen werden darf, ist naturgemäß dem Verhältnismäßigkeitsgrundsatz (§ 4 HSOG) besondere Beachtung zu schenken. Soweit Ärzte und Psychologische Psychotherapeuten betroffen sind, wird dabei auch zu berücksichtigen sein, dass deren Berufsordnungen durchaus eine Durchbrechung der Schweigepflicht zum Schutz eines höherwertigen Rechtsguts zulassen (vgl. § 9 Abs. 2 Satz 1 der Berufsordnung für die Ärztinnen und Ärzte in Hessen vom 2. September 1998, zuletzt geändert am 1. Dezember 2008, sowie § 11 Abs. 2 Satz 1 der Berufsordnung der Landeskammer für Psychologische Psychotherapeutinnen und -therapeuten und Kinder- und Jugendlichenpsychotherapeutinnen und -therapeuten Hessen vom 25. April 2009). Soweit andererseits ausnahmsweise der Kernbereich privater Lebensgestaltung betroffen ist (vgl. BVerfG, Urt. vom 03.03.2004, 1 BvR 2378/98 und 1 BvR 1084/99, Absatz-Nr. 148), gelten ohnehin die diesbezüglichen Schutzvorschriften (§ 15 Abs. 4 Satz 4 und 5 HSOG, ggf. in Verbindung mit § 15a Abs. 1 Satz 2 bzw. § 15b Abs. 5 HSOG).

Zu 4.2.1.2 Videoüberwachung

Die Verwaltungsvorschrift zum HSOG ist zwischenzeitlich unter Berücksichtigung von Vorschlägen des Hessischen Datenschutzbeauftragten an die neue Rechtslage angepasst und im Staatsanzeiger veröffentlicht worden (Erlass des Ministeriums des Innern und für Sport vom 1. Februar 2010, StAnz. 7/2010 S. 322). Das Hessische Landeskriminalamt ist mit der entsprechenden Anpassung der Handlungsempfehlung beauftragt worden.

Zu 4.2.1.3 Kernbereichsschutz bei der Wohnraumüberwachung

§ 15 Abs. 4 Satz 4 HSOG erklärt die Wohnraumüberwachung für unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme bestehen, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Der Hessische Datenschutzbeauftragte meint zu Unrecht, dass eine solche Konstellation praktisch niemals vorliege. Ihm ist allerdings zuzugeben, dass Satz 4 nur ausnahmsweise zur Anwendung kommen wird. Ein Anwendungsfall wäre z.B., dass eine Gesprächsvereinbarung zu einem Kernbereichsthema mitgehört wird und nichts darauf hindeutet, dass das abgehörte Gespräch konspirativen Charakter trägt. Umgekehrt wäre aber die Wohnraumüberwachung kaum je möglich, wenn die Maßnahme schon dann ausgeschlossen wäre, wenn tatsäch-

liche Anhaltspunkte dafür vorliegen, dass irgendwann während eines Gesprächs in geringem Umfang Kernbereichsdaten anfallen.

Die Kritik des Hessischen Datenschutzbeauftragten ist gemessen an den Maßstäben des Urteils des Bundesverfassungsgerichts vom 3. März 2004 zur akustischen Wohnraumüberwachung im Strafverfahren (1 BvR 2378/98 und 1 BvR 1084/99) verständlich. Das Bundesverfassungsgericht hat allerdings seither seine Kernbereichsrechtsprechung modifiziert und in seinem Urteil zur Online-Durchsuchung vom 27. Februar 2008 (1 BvR 370/07 und 1 BvR 595/07) ein zweistufiges Schutzkonzept vorgestellt. Die gesetzliche Regelung hat demnach nur noch darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten möglichst unterbleibt. Gleichwohl erhobene kernbereichsrelevante Daten dürfen nicht verwertet werden und sind unverzüglich zu löschen. In der Sache ist damit der vormals apodiktisch formulierte Kernbereichsschutz auf ein Optimierungsgebot reduziert, dessen zentrales Element die Sichtung des erhobenen Materials ist (Volkmann, DVBl 2008, 590, 593).

Zu 4.2.1.4 Telekommunikationsüberwachung an informationstechnischen Systemen (Quellen-TKÜ)

Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend. Ergänzend ist anzumerken, dass das Hessische Landeskriminalamt den Auftrag erhalten hat, in Abstimmung mit dem Hessischen Datenschutzbeauftragten konkretisierende Verwaltungsvorschriften zur Quellen-TKÜ zu erlassen.

Zu 4.2.1.5 Rasterfahndung

Wie der Hessische Datenschutzbeauftragte zutreffend darlegt, ist die Rasterfahndung nach der Neufassung des § 26 HSOG keine Vorfeldmaßnahme mehr. Sie knüpft vielmehr wie das klassische Polizeirecht an das Vorliegen einer konkreten Gefahr an. Damit wäre es unvereinbar gewesen, Formulierungen in die Vorschrift aufzunehmen, die Vorfeldmaßnahmen rechtliche Konturen verleihen sollen. Die Subsidiaritätsklausel wurde gestrichen, um die durch die Neufassung erzwungene größere Schadensnähe wenigstens partiell auszugleichen.

Zu 4.2.2 SoPart - Automationsunterstützung für Soziale Dienste in der Justiz

Der Hessische Datenschutzbeauftragte hat den Einsatz des Verfahrens SoPart bei der Bewährungshilfe überprüft. Bereits im Zuge seiner Prüfung im Jahr 2009 hat er mit den beteiligten Stellen gesprochen und den von ihm festgestellten Nachbesserungsbedarf mitgeteilt. Dies führte zu entsprechenden Änderungen im Verfahren bei der schriftlichen Dokumentation des Anlegens neuer Benutzer.

Gegenstand der Erörterung des Datenschutzbeauftragten mit der Justizverwaltung ist noch die Suchfunktion (zu 4.2.2.5), mit der die Benutzer in der Bewährungshilfe hessenweit in der gemeinsamen Datenbank nach gespeicherten Personen suchen und auf die Stammdaten zugreifen können. Die Diskussion, ob diese Suchfunktion erforderlich ist oder durch eine Funktion ersetzt werden könnte, die bei der Erfassung von Namen und Geburtsdaten automatisch auf eine frühere Erfassung dieses Probanden hinweist, ist noch nicht abgeschlossen. Die Gemeinsame IT-Stelle der Hessischen Justiz (GIT) hat darauf hingewiesen, dass die Suchfunktion der Vermeidung der Mehrfachanlage von Probanden dient. Sie gibt Hinweise auf die Dienststelle und den zuständigen Bewährungshelfer. Es wird noch weiter zu prüfen sein, wieweit die Suchfunktion, insbesondere auch beim Austausch von Daten mit den Sozialdiensten des Justizvollzugs, unverzichtbar ist. An einer datenschutzrechtlich befriedigenden Lösung wird derzeit gearbeitet. Mit dem nächsten Update der Fachanwendung im Oktober dieses Jahres sollten die noch bestehenden Probleme ausgeräumt werden können.

Zu 4.2.3 Neue Formen der Zusammenarbeit zum Umgang mit "Gewalt-Kids"

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Es ist unabdingbar, dass der Sozialdatenschutz bezüglich der Entwicklung von neuen Konzepten, Maßnahmen und Projekten rund um die Jugendkriminalität den entsprechenden Stellenwert erfährt.

Zu 4.2.3.1 Haus des Jugendrechts

Für das Projekt Haus des Jugendrechts wurde in einer ressortübergreifenden Arbeitsgruppe unter der Federführung des Ministeriums der Justiz, für Integration und Europa die Struktur einer solchen Einrichtung erarbeitet. Das Projekt wurde von Anfang an vom Hessischen Datenschutzbeauftragten begleitet. Die dort entwickelten Konzepte wurden daher jeweils zur Beurteilung dem Hessischen Datenschutzbeauftragten vorgelegt. Er wird auch die Umsetzung unmittelbar begleiten.

Zu 4.2.3.2 Vorschlag einer Fallkonferenz als Ergebnis der Arbeit eines kommunalen Präventionsrates

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Um die Zusammenarbeit von Institutionen und Behörden in Hessen einheitlich zu regeln, hat unter Federführung des Landespolizeipräsidiums eine ressortübergreifende Arbeitsgruppe "Zusammenarbeit bei der Prävention und Bekämpfung von Jugendkriminalität" ihre Arbeit aufgenommen. "Fallkonferenzen" sind dabei eines von mehreren Instrumenten der Zusammenarbeit der beteiligten Behörden und Institutionen, die die Arbeitsgruppe thematisieren wird. Neben dem Ministerium für Arbeit, Familie und Gesundheit, dem Kultusministerium und dem Ministerium

der Justiz, für Integration und Europa ist auch der Hessische Datenschutzbeauftragte ständiges Mitglied der Arbeitsgruppe, um allen datenschutzrechtlichen Aspekten von Anfang an Rechnung tragen zu können.

4.3 Verfassungsschutz

Zu 4.3.1 Neues Datenverarbeitungssystem HARIS beim Hessischen Landesamt für Verfassungsschutz

Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend.

Zu 4.3.2 Verwaltungsvorschriften des Hessischen Landesamtes für Verfassungsschutz

Die Ausführungen des Hessischen Datenschutzbeauftragten sind zutreffend. Die im Tätigkeitsbericht genannten Verwaltungsvorschriften wurden inzwischen in Kraft gesetzt.

4.4 Verkehrswesen

Zu 4.4.1 Anlassunabhängige personenbeziehbare Kontrollen der Prüfer von Kfz durch staatliche Aufsichtsbehörden

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Das Ministerium für Wirtschaft, Verkehr und Landesentwicklung hat den Bericht des Hessischen Datenschutzbeauftragten zum Anlass genommen, das Regierungspräsidium Darmstadt anzuweisen, bei der Überprüfung der anderen in Hessen anerkannten Überwachungsorganisationen entsprechend zu verfahren.

4.5 Schulen und Schulverwaltung

Zu 4.5.1 Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.5.2 Digitale Schwarze Bretter in Schulen und Veröffentlichungen auf der Schul-Homepage

Die Landesregierung begrüßt es, dass der Hessische Datenschutzbeauftragte die Schulen bei der Nutzung von digitalen Schwarzen Brettern unterstützt, indem er den Umgang mit personenbezogenen Daten erläutert. Der Hinweis, wie restriktiv mit Daten umzugehen ist, ohne zum Beispiel beim Vertretungsplan oder bei Schulpräsentationen den Zweck zu verfehlen, hilft den Schulen sehr. Hilfreich wäre lediglich eine etwas deutlichere Klarstellung zu den beiden unterschiedlichen technischen Konzepten mit jeweils unterschiedlichen Handlungskonsequenzen, je nach dem ob digitale Schwarze Bretter als reine Inhouse-Lösung oder als internetbasierte Systeme mit externem Hosting eingesetzt werden.

Zu 4.5.3 Neue Schulbroschüre

Die Landesregierung begrüßt die Herausgabe der Broschüre durch den Hessischen Datenschutzbeauftragten. Es handelt sich hierbei um eine für Schulen und Eltern hilfreiche Zusammenstellung datenschutzrechtlicher Informationen sowie aller relevanten Rechtsgrundlagen.

4.6 Gesundheitswesen

4.6.1 Probleme bei der Umsetzung des Kindergesundheitsschutzgesetzes

Zu 4.6.1.1 Einleitung

und 4.6.1.2 Probleme mit fehlerhaften Erinnerungs- und Mahnschreiben an die Eltern

Seit Januar 2008, dem Beginn der Umsetzung des Hessischen Kindergesundheitsschutzgesetzes, sind in einigen Fällen Eltern bereits verstorbener Kinder vom Hessischen Kindervorsorgezentrum (HKVZ), eventuell später auch vom Jugendamt angeschrieben worden. Das ist höchst bedauerlich und die vom Hessischen Datenschutzbeauftragten angesprochenen Probleme deshalb auch von allen Beteiligten mit großem Engagement bearbeitet worden.

Im Rahmen der vom Hessischen Datenschutzbeauftragten beschriebenen Fehleranalyse stellte sich heraus, dass eine große Zahl von Übermittlungsfehlern zu den vom Hessischen Datenschutzbeauftragten beschriebenen Problemen beigetragen hat. Die Verfahrensabläufe mussten optimiert werden, indem die Datensätze einen Zeitstempel erhalten und die Meldebehörden ihre Daten nicht nur, wie rechtlich vorgesehen, wöchentlich, sondern täglich an das HKVZ übermitteln. Die tägliche Datenübermittlung wird inzwischen praktiziert, der Zeitstempel im Datensatz wird in Kürze in der Meldedaten-Übermittlungsverordnung verankert sein.

Als weitere Optimierungsmaßnahme wurden in dem an die Meldebehörden und Standesämter gerichteten Erlass vom 2. Februar 2009 (die im Tätigkeitsbericht genannten Daten "2. März 2009" und "2. Januar 2010" sind nicht

korrekt) deren diesbezügliche Aufgaben dargelegt und darum gebeten, eine regelmäßige und zeitnahe Datenübermittlung der Sterbefälle an das HKVZ sicherzustellen. Die Meldebehörden haben danach sämtliche Änderungen täglich an das HKVZ zu übermitteln.

Darüber hinaus wurde im Vorfeld der Umstellung auf ein Einladungsverfahren (s.u.) ein neues Software-Modul entwickelt und installiert, welches bei Eingang der Meldedaten im HKVZ diese auf Vollständigkeit und Plausibilität prüft. Mit Hilfe dieses neuen Software-Moduls (QS-Modul) ist es bereits jetzt gelungen, eine Vielzahl falscher Meldedaten, insbesondere sog. Dubletten (Kinder, die sich mehrfach in den Datenbeständen der HKVZ befanden) heraus zu filtern.

Auch die nachträgliche Übermittlung von Meldedaten bereits als verstorben gemeldeter Kinder ohne Sterbedatum wird durch das Modul erkannt und kann dann durch die Leitung der HKVZ geklärt werden. Es ist zu erwarten, dass damit auch die Anschreiben an Eltern verstorbener Kinder reduziert werden können. Darüber hinaus können durch dieses Modul und in Verbindung mit neuen Funktionen zur Bereinigung und Vermeidung von doppelten Datensätzen Doppelinformationen an Eltern und Jugendämter weitgehend vermieden werden.

Derzeit werden die Sorgeberechtigten der Kinder, wenn - je nach anstehender Untersuchung kurz vor bzw. bei Erreichen des Endes der Untersuchungsfrist noch keine Untersuchungsbestätigung vorliegt -, in einem ersten Erinnerungsschreiben auf die Verbindlichkeit der Untersuchung hingewiesen. Es ist geplant, auf ein Einladungssystem zu wechseln; es ist zu erwarten, dass damit die Akzeptanz bei Eltern und Ärzten verbessert wird. Dazu sollen die Sorgeberechtigten aller Kinder, für die eine Vorsorgeuntersuchung ansteht, vor dem Beginn des Vorsorgetoleranz-Intervalls angeschrieben und zur anstehenden Untersuchung eingeladen werden. Sofern eine Einladung an die betreffenden Eltern versendet worden ist, sollen nur noch eine Mahnung und danach die Information des Jugendamtes erfolgen.

Durch die Umstellung des bisherigen Erinnerungs- und Mahnverfahrens auf ein Einladungssystem, die Einladung erfolgt ca. zwei Wochen vor dem Beginn des Untersuchungszeitraums für das jeweilige Kind, wird den Eltern aufgrund der frühen Information die Planung des Untersuchungstermins bei einem Kinderarzt erleichtert. Damit wird auch erreicht, dass den Eltern Informationen über die bisher noch nicht flächendeckend bekannte U7a-Untersuchung vorliegen. Außerdem ist es für die Eltern verständlicher und erscheint weniger "fordernd", wenn sie vor dem Beginn des Untersuchungszeitraums eine Einladung erhalten, als wenn sie, obwohl sie vielleicht schon eine ärztliche Untersuchung geplant oder gar haben durchführen lassen, ein "Erinnerungsschreiben" erhalten.

Bisher mussten Ärzte die ihnen zur Verfügung gestellten Formulare mit den Daten des Kindes und dem Untersuchungsdatum bedrucken, die durchgeführte Untersuchung ankreuzen sowie Stempel und Unterschrift aufbringen. Durch das Einladungsverfahren, bei dem die Eltern das Anschreiben einschließlich eines Bescheinigungsabschnitts, auf dem die Daten des Kindes bereits aufgedruckt sind, zur Untersuchung mitbringen sollen, entfällt für den Arzt das Bedrucken des Formulars.

Auch die Nachbestellung von Bescheinigungsformularen entfällt weitgehend. Ärzte, die in benachbarten Bundesländern praktizieren, können den Bescheinigungsabschnitt ausfüllen und müssen nicht zuvor bei dem HKVZ registriert werden, um Formulare zu bestellen. Insofern ist auch für die Ärzte das neue Verfahren einfacher zu handhaben.

Seit Januar 2010 werden alle Schreiben des HKVZ mit einer Korrespondenznummer versehen. Durch die Einführung einer Korrespondenznummer auf den Schreiben an die Eltern wird es diesen erleichtert, bei Anrufen oder in sonstiger Korrespondenz ohne Nennung von Kindesdaten mit dem HKVZ in Kontakt zu treten. Dies betrifft insbesondere Eltern ohne ausreichende deutsche Sprachkenntnisse. Gleichzeitig wird durch die reine Angabe der Korrespondenznummer eine weitgehend anonymisierte telefonische Kommunikation ermöglicht und zumindest sichergestellt, dass sich der Anrufer im Besitz des betreffenden Schreibens befindet. Hierfür wurde ein Software-Modul etabliert, welches eine anonymisierte Auskunftsübersicht bietet. Dadurch kann auch verhindert werden, dass dem Anrufenden seitens des HKVZ versehentlich Personendaten genannt werden.

Die Gründe für fehlerhafte Anschreiben an Eltern sind aufgeklärt. Eine weitere Minimierung der Fehlerquote dürfte durch die vollständige Implementierung der aufgezeigten Maßnahmen zu erwarten sein.

Zu 4.6.1.3 Weiterverarbeitung der Daten im Jugendamt

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.6.2 Ausgestaltung der Zugriffe auf Krankenhausinformationssysteme

Die Landesregierung begrüßt, dass der Hessische Datenschutzbeauftragte die gesetzliche Regelung des Datenschutzes im Krankenhaus in § 12 Hessisches Krankenhausgesetz für ausreichend erachtet, den Schutz von Patientendaten innerhalb eines Krankenhauses sicherzustellen. Die Beschränkung der Verwendung von Patientendaten innerhalb des Krankenhauses zwischen verschiedenen Fachabteilungen ist im Sinne einer strukturierten Behandlungsplanung nicht immer opportun. Angesichts der klaren Rechtsprechung zur Anwendbarkeit von § 203 Strafgesetzbuch (Verletzung von Privatgeheimnissen) zwischen einzelnen Ärzten/Abteilungen ein und desselben Krankenhauses ist dies jedoch nicht zu vermeiden.

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die Krankenhäuser die technischen Möglichkeiten im Rahmen ihrer Krankenhausinformationssysteme schaffen müssen, um die landesgesetzlichen Vorgaben einzuhalten.

Zu 4.6.3 Krankenhausmitarbeiter als Patienten im Krankenhaus

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.
Die Einhaltung der gesetzlichen Regelungen des Schutzes von Patientendaten ist umso mehr erforderlich, wenn es um die Behandlung von eigenen Mitarbeitern des Krankenhauses geht. Dann besteht nämlich die Gefahr, dass medizinische Daten für personalrelevante Entscheidungen herangezogen werden.

Zu 4.6.4 Ausgestaltung der Zugriffsmöglichkeiten auf Patientendaten innerhalb eines Medizinischen Versorgungszentrums

Der Hessische Datenschutzbeauftragte verweist auf das im Bericht abgedruckte, von der Landesärztekammer entwickelte Mehrstufenmodell, das auf die Anzahl der in dem jeweiligen Medizinischen Versorgungszentrum (MVZ) tätigen Ärzte und somit indirekt auf die Größe des MVZ abstellt. Dabei kommt er zu dem Ergebnis, dass die differenzierte und fundierte Stellungnahme der Landesärztekammer einen geeigneten Orientierungsrahmen für MVZ darstellt.

Die dargelegten datenschutzrechtlichen Probleme werden im vorliegenden Tätigkeitsbericht zwar auf MVZ bezogen. Bei solchen handelt es sich allerdings nicht um eine eigene Rechtsform, sondern um eine Versorgungsform im vertragsärztlichen Bereich. Die Trägergesellschaft eines MVZ kann insoweit sowohl eine Gemeinschaftspraxis, als auch eine juristische Person des Privatrechts sein, wenn die in § 95 Abs. 1 SGB V niedergelegten Voraussetzungen erfüllt werden. Bei diesen Berufsausübungsgemeinschaften ist von den beteiligten Ärzten das Berufsrecht, hier die Berufsordnung der Landesärztekammer Hessen zu beachten. Vor diesem berufsrechtlichen Hintergrund steht hier auch die Tätigkeit der Landesärztekammer im Vordergrund der Diskussion. Die rechtlich relevanten Normen sind insbesondere § 9 Abs. 4 sowie § 10 Abs. 4 und 5 der Berufsordnung.

Nach dem Vorschlag der Landesärztekammer ist darauf abzustellen, ob in einem MVZ eine überschaubare Anzahl von Ärzten arbeitet oder ob es sich um ein MVZ mit einer großen Anzahl von insbesondere angestellten Ärzten handelt. Bei einem solch großen MVZ soll im Unterschied zu einem kleinen MVZ datenschutzrechtlich nicht mehr davon ausgegangen werden können, dass die Patienten mit einem Zugriff auf ihre Patientendaten durch alle Ärzte der jeweiligen Fachgruppe einverstanden sind. Hier muss dann eine besondere Einwilligung erfolgen, die näher dargelegt wird.

Die von der Landesärztekammer Hessen aufgestellten Verfahrensgrundsätze stellen ebenfalls einen geeigneten Weg für die Handhabung von Zugriffsmöglichkeiten innerhalb des MVZ dar. Das genaue Procedere muss freilich noch dargelegt werden. Eine analoge Vorgehensweise wäre auch bei der Datenübermittlung zwischen Kliniken und MVZ (siehe Ziffer 8.3 des Tätigkeitsberichts) zu begrüßen.

Zu 4.6.5 Zentrale Datenbank für die Erforschung des chronischen Nierenversagens

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.6.6 Zuweiserportale in Krankenhäusern

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Für die Einwilligung eines Patienten in die Weitergabe seiner medizinischen Daten gibt es kein Schriftformerfordernis. Eine Änderung des Hessischen Krankenhausgesetzes zur Vorgabe einer schriftlichen Einwilligung wird jedoch nicht für nötig befunden. Da zur Absicherung des Krankenhauses aber in aller Regel eine Dokumentation erfolgen soll, wird die Empfehlung des Hessischen Datenschutzbeauftragten zur Einholung einer schriftlichen Einwilligung unterstützt.

Zu 4.6.7 Prüfung der DMP-Datenstelle

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.6.8 Auskunftsanspruch gegenüber dem Gesundheitsamt

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

4.7 Sozialwesen

Zu 4.7.1 Zusammenarbeit von SGB-II-(Hartz-IV-)Behörden mit Gesundheitsämtern

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.7.2 Auskunftsanspruch von Berufsgenossenschaften

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 4.7.3 Datenverarbeitung bei der Anmeldung in Kindertageseinrichtungen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

4.8 Personalwesen

Zu 4.8.1 Heimliche Personalbeurteilung durch externes Unternehmen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu

Zu 4.8.2 Prüfung von Beihilfevorgängen durch die Innenrevision

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu, wie bereits zu dessen Ausführungen im 36. Tätigkeitsbericht (Drs. 16/8377, Ziffer 5.10.1) zum Thema "Personalakteneinsicht durch Innenrevision". Die Darstellung der Auffassung des Hessischen Datenschutzbeauftragten im 36. Tätigkeitsbericht trug zur Rechtssicherheit in der Landesverwaltung, da darin nicht nur auf die Rechtmäßigkeit der Personalakteneinsicht durch die Innenrevision abgestellt wird, sondern auch die Grenzen der Einsichtnahme aufgezeigt werden. Auch dem Hinweis des Hessischen Datenschutzbeauftragten auf die Regelung beim Bund in § 107 Abs. 2 BBG hat die Hessische Landesregierung zugestimmt und die Prüfung der Aufnahme einer solchen klarstellenden Regelung in das Hessische Beamtengesetz im Rahmen der Dienstrechtsreform zugesagt. Daran wird festgehalten. Allerdings lässt der derzeitige Stand der 2. Stufe der Dienstrechtsreform diesbezüglich noch keine konkreteren Aussagen zu.

Zu 4.8.3 Löschung von Daten in SAP R/3 HR

Bei der Einführung der komplexen SAP-Anwendung in einem Flächenland mit einer so differenzierten Personalorganisation und vielfältigen Personalstrukturen hat es die Landesregierung von Anfang an begrüßt, dass der Hessische Datenschutzbeauftragte das Projekt intensiv und konstruktiv begleitet hat. Es war Konsens zwischen der Landesregierung und dem Hessischen Datenschutzbeauftragten, pragmatisch die SAP-HR-Anwendung als Landesreferenzmodell Personalwesen umzusetzen und bei erkannten Schwachstellen, auch bei datenschutzrechtlichen, nachzusteuern.

So auch bei dem Thema Löschen von Daten im Landesreferenzmodell Personalwesen. Bereits in den Stellungnahmen zum 36. und zum 37. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten hat die Landesregierung klargestellt, dass ihre Bemühungen zur Beseitigung der benannten Schwachstellen und die Mitwirkung des Hessischen Datenschutzbeauftragten einhergehen. Der Hessische Datenschutzbeauftragte ist deshalb von Beginn an in das im Herbst 2008 aufgesetzte Projekt "Löschen von Daten" eingebunden. Begrüßt wird auch die Teilnahme des Datenschutzbeauftragten in dem in 2008 gegründeten Arbeitskreis "Löschen von Personaldaten im SAP-System im Rahmen von Fristen und Datenschutzvorschriften" der SAP AG, in dem auch die Landesverwaltung vertreten ist.

Die uneingeschränkte Behauptung des Hessischen Datenschutzbeauftragten, dass das Löschen von Daten im SAP-System nicht vorgesehen sei, trifft in dieser Absolutheit nicht zu. Tatsächlich bestanden im SAP-System immer Möglichkeiten, Daten zu löschen. Dies betrifft das Löschen fehlerhafter Eingaben und das Löschen ganzer Personalfälle. Letzteres war allerdings nur möglich bevor diese Personalfälle produktiv in der Bezügeabrechnung verarbeitet worden sind.

Seit dem Releasewechsel 2007 hat die SAP AG auch auf Anforderung der Landesregierung Programme zum Löschen ganzer Personalfälle und von einzelnen Abwesenheitsdaten entwickelt und dem Land Hessen zu Testzwecken zur Verfügung gestellt.

Löschen von Bewerberdaten
Seit Mai 2008 wurde im Hessischen Competence Center für Neue Verwaltungssteuerung ein eigener Löschreport für die Komponente Personalbeschaffung für den Kultusbereich entwickelt. Am 1. August 2009 fand die Produktivsetzung für das Programm zum Löschen von Bewerberdaten statt, nachdem Ende Juli 2009 eine Freigabe für das Löschprogramm durch das Hessische Kultusministerium erfolgt war. Damit liegen seit diesem Zeitpunkt die technischen Voraussetzungen zum Löschen von Bewerberdaten im Landesreferenzmodell Personalwesen vor. Somit ist diese Schwachstelle aus dem Komplex "Löschen von Personaldaten" im Landesreferenzmodell Personalwesen endgültig behoben.

Löschen von ganzen Personalfällen
Erste Tests, auch Massentests, zum Löschen ganzer Personalfälle wurden in einer Testumgebung im Hessischen Competence Center für Neue Verwaltungssteuerung durchgeführt. Hierbei sind keine Fehler aufgetreten, die Personalnummern waren in den Systemen endgültig gelöscht.

Löschen von Abwesenheitsdaten zu Erkrankung und zum Erholungsurlaub
In dem in 2008 gegründeten Arbeitskreis "Löschen von Personaldaten im SAP-System im Rahmen von Fristen und Datenschutzvorschriften" wurden Anforderungen an ein Programm zum Löschen von Abwesenheitsdaten aufgestellt und von der SAP AG umgesetzt.

Dieses Programm wurde in einer Testumgebung im Hessischen Competence Center für Neue Verwaltungssteuerung 2009 installiert und getestet. Die Tests sind durchweg erfolgreich verlaufen. Es sind keine Fehler beim Löschvorgang aufgetreten. Die technischen Möglichkeiten zum Löschen einzelner Abwesenheitsdaten im Landesreferenzmodell Personalwesen liegen daher grundsätzlich vor.

Das Löschprogramm wurde seit Beginn 2010 noch weiter an die Bedürfnisse des Landes Hessen und der anderen Teilnehmer des Arbeitskreises "Löschen" (Vertreter aus Industrie und öffentlicher Verwaltung) angepasst. Diese Bedürfnisse resultieren nicht zuletzt aus rechtlichen Anforderungen. So muss sichergestellt sein, dass Daten, die noch für andere Zwecke benötigt werden, z.B. Gerichtsverfahren, Berechnen der unständigen Bezüge in Altersteilzeitfällen, aus der Löschung ausgenommen werden. Die SAP AG hat diese Anforderungen in das Löschprogramm implementiert und im Mai 2010 zum weiteren pilotweisen Testen freigegeben.

Gegenwärtig werden darüber hinaus in der hessischen Landesverwaltung noch weitere rechtliche und organisatorische Fragen geklärt. Das Ministerium der Finanzen lässt beim Rechnungsprüfungsamt Kassel und den Spitzenverbänden der Sozialversicherung derzeit prüfen, ob und in welcher Form Krankheitsdaten der Tarifbeschäftigten für steuer- und sozialversicherungsrechtliche Zwecke bereitgehalten werden müssen. Sollte im Ergebnis die Hessische Bezügestelle die Daten in den Infotypen weiter benötigen, müsste das Löschprogramm entsprechend angepasst werden. Der Zugriff der Personalsachbearbeiter auf diese Daten müsste dann ausgeschlossen werden, um dem Datenschutz Rechnung zu tragen.

Die Landesregierung erwartet ebenfalls, dass eine zeitnahe Lösung für das Löschen krankheits- und urlaubsbedingter Abwesenheitsdaten in das Landesreferenzmodell Personalwesen implementiert wird. Sie begrüßt, dass der Hessische Datenschutzbeauftragte hierbei konstruktiv und pragmatisch mit der Landesverwaltung zusammenarbeitet.

Nächste Schritte
Das Ergebnis der Überprüfung der noch offenen Fragen wird derzeit in ein Fachkonzept eingearbeitet. Nach Fertigstellung dieses Konzeptes, wird als nächster Schritt das Löschprogramm ggf. zeitlich gestaffelt im Pilotbetrieb durch einzelne Anwender getestet werden. Bei all diesen Schritten wird der Hessische Datenschutzbeauftragte wie bisher eingebunden.

Die Landesregierung wird ferner das Landesreferenzmodell Personalwesen umfassend dahingehend überprüfen, ob weitere im SAP-System nicht mehr erforderliche Daten zu löschen sind, für Auswertungszwecke anonymisiert werden, z.B. lange Zeitreihen, oder nach dem Aktenführungserlass ausgesondert werden müssen.

Im Übrigen hat sich die Landesregierung bereits in ihrer Stellungnahme zum 36. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Drs. 17/662, dort zu Ziffer 5.10.3.2) zu der Problematik geäußert. Das vom Hessischen Datenschutzbeauftragten im 38. Tätigkeitsbericht dargestellte, dem Ganzen zu Grunde liegende rechtliche Erfordernis der Einhaltung der Fristen im SAP R/3 HR-System des Landes aufgrund der einschlägigen Vorschriften zur Löschung von Daten (§ 107f HBG, § 19 Abs. 3 und § 34 Abs. 4 HDSG) wurde dabei zu keiner Zeit in Frage gestellt.

Zu 4.8.4 Download-Berechtigungen und Protokollierungen im SAP R/3 HR-System

Der Hessische Datenschutzbeauftragte führt aus, die Problematik der Downloadberechtigungen werde dadurch verschärft, dass eine Protokollierung des Downloads nicht erfolge und Einstellungen für eine gezielte Protokollierung auf SAP-Ebene für das HR-System bzw. die WTS-/Betriebssystemebene sowohl für den Download als auch das Kopieren von Informationen aus dem HR-System nicht existieren.

Das Ministerium der Finanzen hat bezogen auf die im NVS-Umfeld eingesetzten Zugriffstechnologien in den Projekten "NVS-WTS-Modernisierung" (Start 10/2009) und "Protokollierung Up-/Downloads in den zentralen SAP-Systemen" (Start 03/2010) die technischen Möglichkeiten einer gezielten Protokollierung des Datenzugriffs auf die zentralen SAP Systeme des Landes untersuchen lassen. Auf der Grundlage der bisher vorliegenden Projektergebnisse plant das Ministerium der Finanzen die Umsetzung der folgenden Maßnahmen:

SAP-Standard Protokollierung - SAP Security Audit Log als Ad-Hoc Maßnahme
Diese Ad-Hoc Maßnahme (geplante Umsetzung bis 10/2010) erfolgt mit Mitteln des SAP-Standards. Der Protokolleintrag im SAP Security Log enthält die Merkmale "Benutzer", "Datum", "Uhrzeit", "Instanz" (SAP-System), "Dateiname" (inkl. kompletter Laufwerkspfad), "Dateigröße" und "Transaktionscode". Über den protokollierten Transaktionscode kann ermittelt werden, welche Daten exportiert wurden. Die Lesbarkeit des SAP-Protokolls, der benötigte Speicherplatz für die Protokolle sowie das Antwortzeitverhalten müssen noch geprüft werden.

SAP Berechtigungssteuerung zum Download und Upload inkl. Cut und Paste
Diese Maßnahme soll im Rahmen der Umsetzung des Sollkonzeptes "NVS-WTS-Modernisierung" (Start ab 10/2010) umgesetzt werden. Durch Aktivierung des Berechtigungsobjektes "S_GUI" (verfügbar ab SAP ERP ECC

5.0) mit den Aktivitäten 60 (Importieren) und 61 (Exportieren) kann eine Berechtigungsprüfung im SAP-Standard erfolgen. Eine separate Prüfung bzw. eine Berechtigungsverwaltung auf beispielsweise der WTS-Systemebene ist dann nicht notwendig. Über das Berechtigungsobjekt "S_GUI" kann nicht nur der explizite Download zum Beispiel nach MS-Excel, unterbunden werden, sondern auch das Kopieren von Daten (Cut und Paste) direkt aus dem jeweiligen SAP-System per Tastenkombination. Bevor jedoch diese SAP-Funktionalität genutzt werden kann, sind alle Entwicklungen, wie zum Beispiel die Word-Serienbriefe, die die Funktionalität des Up-/Download nutzen, durch das HCC zu prüfen, programmtechnisch anzupassen und zu testen, um die vorhandene Funktionalität für den Anwender weiterhin sicherzustellen.

Die Protokollierung bzw. Steuerung kann damit für alle zentralen SAP-Systeme, alle derzeit genutzten Zugriffstechnologien wie WTS und lokaler SAP-GUI, zukünftige Zugrifftechnologien wie Portalzugriff und alle Benutzer in der gleichen Weise erfolgen.

Zu 4.8.5 HEPIS-Neu - Einrichtung einer zentralen Stelle für Auswertungen aus SAP R/3 HR

Im Ministerium des Innern und für Sport wurde das Referat "Hessisches Personalinformationssystem neu, Personaldatenbank" eingerichtet. Die Aufgaben des Referates umfassen die Erstellung von landesweiten und ressortübergreifenden anonymisierten Personalinformationen aus den Personalsystemen des Landes Hessen und der Personaldatenbank des Ministeriums des Innern und für Sport. Die Arbeit erfolgt auf der Grundlage des Hessischen Beamtengesetzes und des Hessischen Datenschutzgesetzes.

Die Landesregierung ist an einer weiteren engen und konstruktiven Zusammenarbeit und Beratung durch den Hessischen Datenschutzbeauftragten interessiert. Ein erstes Gespräch auf Arbeitsebene mit Vertretern des Hessischen Datenschutzbeauftragten hat bereits stattgefunden.

5. Kommunen

Zu 5.1 Forderungsmanagement durch Kommunen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zum Forderungsmanagement durch Kommunen zu.

Zu 5.2 Elektronisches Personenstandsregisterverfahren bei der ekom21

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend. Die Landesregierung begrüßt seine konstruktive Begleitung des unter kommunaler Verantwortung erfolgenden Aufbaus elektronischer Personenstandsregister durch die ekom21-KGRZ Hessen. Inzwischen bedienen sich 320 hessische Standesämter des Verfahrens, so dass für Hessen mit einer flächendeckenden Nutzung vor Ablauf der im Personenstandsgesetz eingeräumten Übergangsfrist (31. Dezember 2013) gerechnet werden kann.

Zu 5.3 Öffentliche Hinweispflicht der Meldebehörden über Widerspruchsrechte ihrer Einwohner vor Wahlen

Mit der "Anordnung über die Bundestagswahl 2009" vom 4. Januar 2009 (BGBl. I S. 2) wurde als Wahltag für die Bundestagswahl 2009 der 27. September 2009 festgesetzt. Die Meldebehörden hätten danach den Hinweis auf das Widerspruchsrecht nach § 35 Abs. 5 HMG spätestens am 26. Januar 2009 öffentlich bekannt machen müssen. Das Ministerium des Innern und für Sport hat die Meldebehörden mit Erlass vom 12. Mai 2010 an diese Pflicht erinnert und darauf hingewirkt, dass die Bekanntmachungen zukünftig rechtzeitig erfolgen.

Zu 5.4 Auskunft über eine erteilte erweiterte Melderegisterauskunft

Ein neuer Gesetzentwurf für ein Bundesmeldegesetz liegt den Ländern noch nicht vor. Ob der Bund die Forderung des Hessischen Datenschutzbeauftragten in das Bundesgesetz übernehmen wird, bleibt abzuwarten.

Zu 5.5 Ordnungsgemäße Verwendung der Zuzugstransaktion bei PAMELA

Die Landesregierung begrüßt die Absicht des Hessischen Datenschutzbeauftragten, weiterhin entsprechende Prüfungen der Datenbankprotokolle zu veranlassen und die betroffenen Kommunen direkt zu informieren.

Zu 5.6 Auskunft über Mitglieder eines Naturschutzbeirates

Die Weitergabe personenbezogener Daten über die Mitglieder eines Beirats oder einer anderen öffentlichen Institution muss auf die Informationen beschränkt bleiben, die in direktem Zusammenhang mit dem öffentlichen Amt stehen.

Nachdem die Anfrage einer Bürgerinitiative gegenüber dem Umweltamt einer Stadt als Untere Naturschutzbehörde, welche Personen dem nach § 52 HENatG zu berufenden Naturschutzbeirat angehören, nach Klärung der Rechtslage vom angefragten Umweltamt in entsprechender Art und Weise beantwortet wurde, war durch das Ministerium für Umwelt, Energie, Landwirtschaft und Verbraucherschutz nichts weiter zu veranlassen.

5.7 Datenschutz bei der Feuerwehr

Zu 5.7.1 "Florix-Hessen"

Die Darstellung des Sachverhalts durch den Hessischen Datenschutzbeauftragten in den Ziffern 5.7.1 bis einschließlich 5.7.1.4 ist zutreffend.

Durch den Erlass betreffend "Feuerwehr-Software ‚Florix Hessen', Nutzung der Web-basierten Landeslösung" vom 2. April 2009 hat das Ministerium des Innern und für Sport die Kommunen bzw. Feuerwehren auf die datenschutzrechtlichen Aspekte hingewiesen. Der Erlass enthält jeweils ein Muster

- eines "Verfahrensverzeichnisses nach § 6 HDSG" (Anlage 1 zum Erlass),
- eines Vordrucks "Datenschutzrechtliche Information über die Erfassung von Daten zum Zwecke der öffentlich-rechtlichen Einrichtung Feuerwehr" (Anlage 2 zum Erlass),
- eines Vordrucks "Datenschutzrechtliche Einwilligung zur Nutzung von Daten der öffentlich-rechtlichen Feuerwehr durch die Feuerwehrvereine und deren Verbände" (Anlage 3 zum Erlass),
- eines Vordrucks "Datenschutzrechtliche Regelungen zur Verwendung kommunaler DV-Anwendungen (hier: ZMS-Florix)" (Anlage 4 zum Erlass) und
- Hinweise zu "Datenschutzrechtlichen Regelungen zur Verwendung kommunaler DV-Anwendungen (hier: ZMS-Florix) auf privaten Rechnersystemen" (Anlage 5 zum Erlass).

In dem Erlass vom 2. April 2009 wird insbesondere auf die Trennung der Nutzung der Daten durch die Feuerwehr als öffentliche Einrichtung und der Nutzung durch den Verein als privat-rechtliche Einrichtung nach BGB hingewiesen. Während für die Nutzung durch die Feuerwehr als öffentliche Einrichtung dem Angehörigen ein Vordruck zur "datenschutzrechtlichen Information über die Erfassung von Daten zum Zwecke der öffentlich-rechtlichen Einrichtung Feuerwehr" (Anlage 2 zum Erlass) vorzulegen ist, mit dessen Unterschrift er dokumentiert, dass er über die Speicherung und Verarbeitung seiner personenbezogenen Daten unterrichtet wurde, ist es für die Nutzung durch den Verein zwingend notwendig, dass der Vordruck über die "datenschutzrechtliche Einwilligung zur Nutzung von Daten der öffentlich-rechtlichen Feuerwehr durch die Feuerwehrvereine und deren Verbände" (Anlage 3 zum Erlass) durch den Angehörigen unterschrieben wird, womit er der Speicherung und Verarbeitung seiner Daten durch den Verein zustimmt. Dies gilt analog auch für die Vereinsmitglieder, die nicht gleichzeitig Angehörige der öffentlichen Feuerwehr sind. Wird diese Zustimmung verweigert, darf der Verein auf die Daten dieses Angehörigen nicht zugreifen bzw. die Daten dieses Vereinsmitgliedes nicht speichern. Dies wird durch die administrative Festlegung von Rollen und Rechten durch die Kommune bzw. die Feuerwehr gewährleistet.

Die Programmierung zur Erfüllung der aufsichtsrechtlichen Funktionen befindet sich zurzeit noch in der Planungsphase. Dabei wird beachtet, dass die Zugriffsrechte auf den im Tätigkeitsbericht unter Ziffer 5.7.1.3 genannten Personenkreis (Feuerwehrführungskräfte, Jugendfeuerwehrwarte) beschränkt bleibt. Damit wird auch sichergestellt, dass die Aufsichtsbehörden nur auf die Daten zugreifen können, die sie zur Erledigung ihrer Aufgaben benötigen.

Ebenfalls noch in der Planung befindet sich das Workflowsystem zur Lehrgangsorganisation. Hier ist vorgesehen, von jeder Person, die sich zu einem Lehrgang anmeldet, die persönlichen Daten zu erfassen, die für das Anmeldeverfahren benötigt werden. Neben den Adressdaten geht es hier insbesondere um Daten zum Nachweis der zu erfüllenden Lehrgangsvoraussetzungen sowie zur Erstattung der Reisekosten und des Verdienstausfalls. Es sollen keine über das heutige papiergebundene Anmeldeverfahren hinaus gehende Daten erhoben werden. Die für das Anmeldeverfahren benötigten persönlichen Daten sollen für die am Workflow beteiligten Organisationen nur temporär von dem Zeitpunkt der Anmeldung bis zum Lehrgangsende zugänglich sein. Danach soll eine automatische Sperrung des Zugriffs auf diesen Datensatz erfolgen. Etwas anderes soll für den zuständigen Wehrführer gelten, der nach Lehrgangsende die Statusmeldung " Lehrgang bestanden" bzw. "Lehrgang nicht bestanden" abrufen kann.

5.7.1.5 Probleme

Zu 5.7.1.5.1 Freiwilligkeit der Verarbeitung von Vereinsdaten

Der Schutz der persönlichen Daten der Vereinsmitglieder wird durch die administrative Vergabe von Rollen und Rechten gewährleistet, wodurch der Zugriff von Angehörigen der Feuerwehr als öffentliche Einrichtung auf die persönlichen Daten eines Vereinsmitgliedes ausgeschlossen werden kann. Auf persönliche Daten der Vereinsmitglieder sollen die Aufsichtsbehörden grundsätzlich keinen Zugriff haben. Dass einige Feuerwehren und Kommunen die datenschutzrechtlichen Bestimmungen und den Erlass vom 2. April 2009 nicht kannten und beachtet haben, musste auch die zuständige Fachabteilung des Ministeriums des Innern und für Sport aufgrund von Anfragen feststellen.

Der Erlass vom 2. April 2009 ist inzwischen auf der Homepage des Ministeriums des Innern und für Sport und der Hessischen Landesfeuerwehrschule (Infothek) als Download verfügbar und damit für jeden zugänglich. Zusätzlich wird der Erlass obligatorisch im Florix-Grundlehrgang und im Florix-Fortbildungsseminar behandelt, sowie auf Wunsch im Fortbildungsseminar für Leiter einer Feuerwehr erörtert.

Zu 5.7.1.5.2 Nutzung privater PC

Um die Tätigkeit für ehrenamtliche Funktionsträger zu erleichtern, hat das Ministerium des Innern und für Sport der Nutzung von Florix auf privaten (heimischen) PC zugestimmt. Zur Sicherstellung des Datenschutzes sollen künftig in diesem Bereich ausschließlich bootfähige USB-Sticks mit Browser und Zertifikat eingesetzt werden. An der Umsetzung dieser Lösung wird mit dem Hersteller gearbeitet, wobei die technische Realisierung, z.B. wegen vorhandener unterschiedlicher Betriebssysteme, derzeit noch auf Schwierigkeiten stößt.

Als Interimslösung steht ein USB-Stick zur Verfügung, auf dem ein portabler Browser installiert ist. Diese Lösung wurde den Brandschutzdienststellen auf einer Informationsveranstaltung zum Thema "Florix" und den Florix-Ansprechpartnern der Kreise, kreisfreien Städte und Städte mit Sonderstatus auf drei Fortbildungsseminaren an der Hessischen Landesfeuerwehrschule im Herbst 2009 vorgestellt. Die Anwender machen hiervon bislang nur zurückhaltend Gebrauch.

Zu 5.7.2 Verarbeitung von Gesundheitsdaten

Es wurde festgestellt, dass in einem Landkreis medizinische Daten von Teilnehmern an einer Übung in der Atemschutzübungsstrecke dauerhaft gespeichert wurden. Da diese Daten nach Abschluss des Übungsgangs nicht mehr erforderlich sind, ist deren Speicherung unzulässig. Der betreffende Landkreis wurde aufgefordert, diese Praxis einzustellen; die gespeicherten Daten wurden zwischenzeitlich gelöscht.

Von 26 bei öffentlichen Feuerwehren betriebenen Atemschutzübungsstrecken im Lande Hessen verfügen 13 Einrichtungen über eine EDV-gestützte Überwachung (Stand: April 2009). Bei fünf Einrichtungen war eine elektronische Speicherung von Gesundheitsdaten erfolgt. Mit Erlass des Ministeriums des Innern und für Sport vom 8. April 2010 sind die betroffenen Einrichtungen auf die datenschutzrechtliche Unzulässigkeit der Speicherung der medizinischen Daten über das Ende des Übungsgangs hinaus hingewiesen und aufgefordert worden, diese Praxis einzustellen und die betreffenden gespeicherten Daten zu löschen.

6. Sonstige Selbstverwaltungskörperschaften

6.1 Rundfunk

Zu 6.1.1 Ergebnisse der Prüfung der GEZ

Die Ausführungen des Hessischen Datenschutzbeauftragten zur GEZ sind zutreffend.

6.1.1.1 Datenübermittlungen der GEZ an Dritte

Zu 6.1.1.1.1 Auskünfte an Polizei- und Staatsanwaltschaften

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend.

Zu 6.1.1.1.2 Auskunftsersuchen von Finanzämtern, kommunalen Behörden und Sozialleistungsträgern

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend.

Zu 6.1.1.1.3 Datenübermittlungen an die Firma Creditreform

Die datenschutzrechtliche Kontrolle der Firma Creditreform wurde seit ihrer Beauftragung durch die zuständige Aufsichtsbehörde nach § 38 Bundesdatenschutzgesetz sichergestellt. Dem Anliegen des Datenschutzes wird durch die vom Hessischen Rundfunk zugesagte Vertragsanpassung, nach der sich die Firma Creditreform einer zusätzlichen Kontrolle durch den Hessischen Datenschutzbeauftragten unterwerfen wird, Rechnung getragen. Die vertragliche Ausgestaltung wird mit dem Hessischen Datenschutzbeauftragten abgestimmt.
Die Firma Creditreform ist vertraglich verpflichtet, streng nach den vom Hessischen Rundfunk für die Einziehung von rückständigen Rundfunkgebühren, insbesondere für die Zahlungsmodalitäten und den Verlauf des Mahnverfahrens, vorgegebenen Regelungen zu verfahren. Unabhängig hiervon dürfte die Frage des Einflusses des Verwaltungshelfers auf die Gestaltung der Zahlungsmodalitäten und des Mahnverfahrens eher von verwaltungsrechtlicher als von datenschutzrechtlicher Relevanz sein.

Zu 6.1.1.2 Zugriff der Rundfunkgebührenbeauftragten auf Teilnehmerkonten
Es trifft zu, dass beim Hessischen Rundfunk sowohl die Hauptbeauftragten als auch unter bestimmten Voraussetzungen deren Nebenbeauftragte bundesweit auf die Rundfunkteilnehmerkonten zugreifen können. Der Datenzugriff ist nach dem Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) passwortgeschützt. Die Datenübertragung erfolgt verschlüsselt. Jede Recherche wird protokolliert. Eine Zwischenspeicherung der gelesenen Daten auf Festplatten oder nicht temporären Speichern ist nicht möglich.

Die vom Hessischen Rundfunk vorgebrachten Gründe, in Übereinstimmung mit der von den Landesrundfunkanstalten Norddeutscher Rundfunk, Radio Bremen, Südwestrundfunk und Saarländischer Rundfunk geübten Praxis am bundesweiten Datenzugriff festzuhalten, erscheinen vor dem Hintergrund, dass sich Teilnehmerbewegungen nicht nur innerhalb des jeweiligen Sendegebietes, sondern bundesweit abspielen, nachvollziehbar. Auch im gewerblichen

Bereich würde eine Einschränkung der Zugriffsmöglichkeit zu erheblichen Gebührenmindereinnahmen führen, die auch im Interesse der abgabenrechtlich gebotenen Belastungsgleichheit nicht hinnehmbar wären. Gerade bei Unternehmen und Firmen mit bundesweiten Standorten ist eine Prüfung der von ihnen bereits angemeldeten Gerätebestände, ihre Korrektur und Aktualisierung im Wege einer bundesweiten Online-Abfrage unerlässlich. Eine unbürokratische Ermittlung außerhalb eines schriftlichen Abfrageverfahrens liegt auch im Interesse der betroffenen Unternehmen, die oftmals keinen Gesamtüberblick über die an ihren einzelnen Standorten gemeldeten Geräte haben.

Die Länder beraten derzeit über eine Neuordnung der Finanzierung des öffentlich-rechtlichen Rundfunks. Zur Diskussion stehen einerseits das Modell einer fortgeschriebenen geräteabhängigen Rundfunkgebühr und andererseits das Modell eines geräteunabhängigen Rundfunkbeitrags. Die Reformüberlegungen zielen insgesamt auch darauf ab, die datenschutzrechtlich sensible Tätigkeit der Rundfunkgebührenbeauftragten möglichst weitgehend zurückzuführen.

Zu 6.1.1.3 Betriebsstättendatenbank

Die Darstellung der Funktion der Betriebsstättendatenbank (NP-Datenbank) und des Umfangs der in ihr gespeicherten Merkmale ist zutreffend.

Die in der NP-Datenbank gespeicherten und von externen Anbietern bezogenen Daten sind erforderlich, um im Sinne des § 8 Abs. 4 Satz 2 Nr. 1 RGebStV Rückschlüsse auf die Gebührenpflicht ziehen zu können.

Es trifft zwar zu, dass die Datenbestände der Adressenlieferanten selbst nicht öffentlich zugänglich sind. Dies ändert jedoch nichts daran, dass ihre Daten ausschließlich aus allgemein zugänglichen Quellen stammen. Dies wird zwischen den Rundfunkanstalten und dem jeweiligen Adressenhändler durch eine vertragliche Vereinbarung sichergestellt, nach dem letztere nur solche Adressen in ihre Firmenadressen-Datenbank aufnehmen dürfen, die von mindestens zwei unterschiedlichen und voneinander unabhängigen Quellen als "gewerblich" eingestuft sind. Zu diesen Quellen, die schon nach ihrer Publikationsform einem unbegrenzten Personenkreis zugänglich sind, zählen etwa das Handelsregister, der Bundesanzeiger, die Tages- und Fachpresse, Messekataloge, Kongressverzeichnisse, Geschäftsberichte und Firmenprospekte.

Die Länder beabsichtigen, den vom Hessischen Datenschutzbeauftragten geäußerten Bedenken, § 8 Abs. 4 Satz 2 Nr. 2 Rundfunkgebührenstaatsvertrag (RGebStV) sei eine abschließende bereichsspezifische Regelung, die eine mittelbare Datenerhebung der dort nicht ausdrücklich aufgeführten Daten aus allgemein zugänglichen Quellen auf der Grundlage des § 3 Abs. 4 HDSG nicht zulasse, im Rahmen der anstehenden Überarbeitung der staatsvertraglichen Rechtgrundlagen der Rundfunkfinanzierung, deren datenschutzrechtlich relevanten Bestimmungen mit den Datenschutzbeauftragten der Länder abgestimmt werden, durch eine entsprechende Klarstellung der Nachfolgeregelung des § 8 Abs. 4 RGebStV Rechnung zu tragen.

Zu 6.1.1.4 Online An- und Änderungsmeldungen

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend.

7. Entwicklungen und Empfehlungen im Bereich der Technik

Zu 7.1 Datenschutzgerechter Einsatz von Voice over IP in der Landesverwaltung; Projekt HessenVoice

Die Landesregierung begrüßt die positiven Feststellungen des Hessischen Datenschutzbeauftragten zu Voice over IP. Beim Thema Verschlüsselung hat die Landesregierung sich mit dem Hessischen Datenschutzbeauftragten darauf verständigt, bei der künftigen Ausschreibung das Leistungsmerkmal Verschlüsselung abzufragen. Eine Entscheidung, ob die Verschlüsselung zum Einsatz kommt, ist noch nicht getroffen.

Zu 7.2 Einsatz von USB-Sticks

Die vom Hessischen Datenschutzbeauftragten dargestellte Idee der Nutzung eines USB-Speichers zur Bereitstellung einer Arbeitsumgebung ist - auch aus wirtschaftlicher Sicht - sehr interessant und wird von der Landesregierung positiv beurteilt. Es ergibt sich eine Vielfalt von Anwendungsmöglichkeiten, von denen der Hessische Datenschutzbeauftragte einige aufgeführt hat. Die Einschätzung der aufgezeigten Risiken wird von der Landesregierung geteilt.

Inzwischen hat die Landesregierung mehrere Anbieter solcher Produkte angesprochen und zu einer Produktvorstellung eingeladen. Die erste Vorstellung eines solchen Systems hat unter Beteiligung des Hessischen Datenschutzbeauftragten stattgefunden, auch die weiteren Vorstellungen sind unter seiner Beteiligung geplant. In der darauf folgenden Phase wird gemeinsam mit dem Datenschutzbeauftragten die Einsetzbarkeit der Produkte geprüft und über den Einsatz entschieden.

Die vom Hessischen Datenschutzbeauftragten geforderte und im Tätigkeitsbericht unter Ziffer 7.2.1.3 "Erstellen sonderpädagogischer Gutachten am Privat-PC" dargestellte Lösung geht deutlich über die Forderung anderer Aufsichtsbehörden, zum Beispiel des Datenschutzbeauftragten des Landes Schleswig-Holstein, hinaus und ist aus Sicht der Schulen und der Lehrkräfte nicht praktikabel. Es gab hierzu einen eingehenden Meinungsaustausch zwischen dem Hessischen Datenschutzbeauftragten und dem Kultusministerium, bei dem jedoch keine Einigung erzielt werden konnte. Im Erlass des Kultusministeriums wurde deshalb keine eigene Regelung getroffen, sondern auf die Forderung des Hessischen Datenschutzbeauftragten verwiesen.

Zur Darstellung in Ziffer 7.2.1.4 "Feuerwehr" wird auf die Stellungnahme zu Ziffer 5.7.1.5.2 verwiesen.

Zu 7.2.2 Der USB-Stick als Speichermedium

Die beschriebene direkte Kommunikation zwischen der Landesärztekammer Hessen und dem Hessischen Datenschutzbeauftragten hinsichtlich des Einsatzes von USB-Sticks wird von der Landesregierung begrüßt. Den Ausführungen des Hessischen Datenschutzbeauftragten wird zugestimmt.

Zu 7.3 Public-Key-Infrastrukturen (PKI) für Bürger - technische Anforderungen an die Standards

Die Ausführungen des Hessischen Datenschutzbeauftragten zu den Anforderungen an die Weiterentwicklung der Common-PKI Spezifikation sind überzeugend. Der "Standard" Common-PKI (als Nachfolger der Interoperabilitätsspezifikation ISIS-MTT) wird jedoch von einer nicht-kommerziellen Initiative der Vereine T7 und Teletrust definiert und veröffentlicht. Über den Verein T7 sind die Trustcenter und Zertifikatsdiensteanbieter vertreten, über den Verein Teletrust wesentliche Hersteller von IT-Sicherheitslösungen und Produkten aus dem Bereich der elektronischen Signatur sowie wissenschaftliche Einrichtungen.

Die Forderungen des Hessischen Datenschutzbeauftragten wurden in diesem Gremium anerkannt, aber nur als Empfehlung in den Standard Common-PKI 2.0 übernommen. Hier kommt der starke Einfluss der Hersteller zum Tragen, die die fachliche Logik der Argumentation des Hessischen Datenschutzbeauftragten zwar anerkennen, deren Umsetzung aber nicht für marktfähig halten. Die Hersteller von Signaturanwendungssoftware streben, nicht zuletzt aufgrund des bislang geringen Markterfolges der PKI-Lösungen, derzeit vorrangig eine bessere Marktdurchdringung über preiswertere und einfacher zu bedienende Signatur-Lösungen an.

Die öffentliche Verwaltung und damit auch die Landesregierung hat außer der Mitarbeit in Verbänden (vertreten durch BSI, BMI, BMWT) und ihrer Rolle als Auftraggeber keinen Einfluss auf derartige Initiativen der Wirtschaft.

Zu 7.4 Aktionsplan der EU-Kommission für elektronische Signaturen

Der Aktionsplan der EU definiert mit der fortgeschrittenen, auf einem qualifizierten Zertifikat beruhenden, elektronischen Signatur ein zusätzliches Signaturniveau. Da es nicht an eine sichere Signaturerstellungseinheit (Smart-Card, Kryptographie-Chip) gebunden ist, bleibt dieses neue Signaturniveau hinter den Anforderungen der qualifizierten elektronischen Signatur nach deutschem Recht zurück.

Die EU-Kommission reagiert damit auf die schwache Akzeptanz der bisherigen Signaturlösungen und wirbt für die Anerkennung des neuen Signatur-Niveaus in grenzüberschreitenden Transaktionen. Sie überlässt aber letztendlich weiterhin den Mitgliedsländern die Entscheidung, welches Signaturniveau für welche Anwendungszwecke gefordert wird. Aus diesem Grund besteht kein akuter Handlungsbedarf.

Die Bundesrepublik Deutschland ist in allen relevanten EU-Projekten (PEPPOL, STORK) aus dem Bereich der elektronischen Signaturen und der elektrischen Identifikation direkt, durch einzelne Bundesländer oder über verbundene Firmen vertreten. Die einzelnen Aktivitäten werden vom BMI und vom BMWT koordiniert.

Die nationale Diskussion findet sowohl im akademischen Umfeld, in der Wirtschaft als auch in der öffentlichen Verwaltung statt. Aufgrund der relativ geringen Nutzerzahlen entzieht sie sich jedoch weitgehend der öffentlichen Wahrnehmung und bleibt einem relativ kleinen Kreis von Spezialisten vorbehalten. Die Diskussion wird einerseits von den Interessen der Hersteller und andererseits von dem übergreifenden Ziel der Kommission, Handelshemmnisse abzubauen, geprägt.

Zu 7.5 Zertifizierungen

Die Landesregierung teilt die Auffassung des Hessischen Datenschutzbeauftragten, dass die genannten Standards ISO 27001 und Common Criteria auf sehr unterschiedliche Objekte zielen. Die internationale Norm ISO 27001 bezieht sich auf die Gestaltung von IT-Sicherheit in Organisationen, während der Standard Common Criteria Sicherheitseigenschaften von Produkten und Systemen der Informationstechnik festlegt. Als Beispiele seien genannt, dass sich die Informationssicherheitsleitlinie für die Landesverwaltung auch an der ISO 27001 orientiert und ein Hersteller für Geräte mit Telefon- und E-Mail-Funktionalität mit der Common Criteria-Zertifizierung für bestimmte seiner Produkte wirbt.

Zu 7.5.3 Beispiel ELSTER

Der Hessische Datenschutzbeauftragte hat seine Feststellung zur Mechanismenstärke des eingesetzten Verfahrens mit "maximal niedrig" nicht hinsichtlich der Punkte konkretisiert, aufgrund deren diese Einordnung getroffen wurde. Insofern ist dazu eine Stellungnahme nicht möglich.

Der Hessische Datenschutzbeauftragte zitiert eine Argumentation der Steuerverwaltung, wonach die ELSTER-Anwendungen - einschließlich RA-Dienst -, Systeme, Räume und Sicherheitsmanagement-Prozesse für ihre Clearingstellen nach ISO 27001 auf der Basis der Grundschutzkataloge zertifiziert seien und erklärtermaßen auch dem hohen bis sehr hohen Schutzbedarf genügten, um diese im Anschluss als "in mehrfacher Hinsicht irreführend" zu bewerten.

Die Ausführungen des Hessischen Datenschutzbeauftragten sind grundsätzlich zutreffend. Im Internet ist unter der Adresse https://www.elster.de/iso27001_nw.php eine für den Steuerbürger und Datenübermittler verständliche Erläuterung zur Zertifizierung nach ISO 27001 einsehbar. Dort wird u. a. darauf hingewiesen, dass die Leistungen von ELSTER in einer nach ISO 27001 auf Basis der IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik zertifizierten eigenen IT-Infrastruktur erbracht werden und mit der Zertifizierung dokumentiert werden soll, dass für diese zur Verfügung gestellten Dienste, der IT-Grundschutz nach ISO 27001 vollständig implementiert wurde und die Auseinandersetzung mit IT-Sicherheitsthemen ein essentieller Bestandteil der Ziele der Finanzverwaltung ist. Mit dieser Erläuterung wählte die Finanzverwaltung eine für den "üblichen Nutzer" der ELSTER-Verfahren verständliche Formulierung des äußerst komplexen Themas Zertifizierung. Die vom Hessischen Datenschutzbeauftragten bemängelte "Unschärfe" in der Formulierung dient also nicht der Irreführung, sondern der Verständlichkeit für den Endanwender. Vor diesem Hintergrund betrachtet, ist die Einschätzung "als in mehrfacher Hinsicht irreführend" für eine mit der Materie vertraute Person allerdings nachvollziehbar.

Bezüglich der vom Hessischen Datenschutzbeauftragten ausgeführten Anforderungen an die Algorithmen und Parameter nach dem Algorithmenkatalog gemäß der Signaturverordnung wird auf die Stellungnahme zu Ziffer 3.3 verwiesen.

Abschließend ist darauf hinzuweisen, dass mit Schreiben des Bayerischen Staatsministeriums der Finanzen vom 13. Januar 2010 Unterlagen zur Evaluierung des "anderen sicheren Verfahrens" nach § 87a Abs. 6 AO an das Bundesministerium der Finanzen übersandt wurden. Das BMF beabsichtigt diesbezüglich, den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu informieren.

Den übersandten Unterlagen liegt ein Gutachten der secunet SwissIT AG vom 11. November 2009 bei, worin bestätigt wird, dass die Sicherheitsdokumentation in Anlehnung an den Standard "Common Criteria" (CC) formal korrekt durchgeführt wurde und dass die Spezifikation der IT-Sicherheitsarchitektur der ELSTER-Software als "auf dem Niveau einer CC-Sicherheitsvorgabe befindlich" bezeichnet werden kann. Damit wird zwar der Forderung des Hessischen Datenschutzbeauftragten nach einer Zertifizierung des Verfahrens ELSTER nach CC noch nicht Rechnung getragen, zeigt aber, dass die Finanzverwaltung einer Auseinandersetzung mit IT-Sicherheitsthemen wesentliche Bedeutung beimisst.

Zu 7.6 Orientierungshilfen des Arbeitskreises Technik

Die Landesregierung befürwortet die Aktualisierung und Klarstellungen der Orientierungshilfe zum Thema "Protokollierung". Die Ausführungen in der Orientierungshilfe "Biometrische Authentisierung - Möglichkeiten und Grenzen" werden begrüßt.

Die Landesregierung begrüßt weiter die Orientierungshilfe "Datenschutz und Datensicherheit in Projekten: Projekt und Produktivbetrieb". Es ist vorgesehen, einen Hinweis darauf in das geplante Projektmanagementhandbuch zu übernehmen.

8. Bilanz

Zu 8.1 Neuregelung der Aufbewahrungsfristen in den Gesundheitsämtern (36. Tätigkeitsbericht, Ziff. 5.8.4.3)

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Nachdem der Hessische Datenschutzbeauftragte in seinem 36. Tätigkeitsbericht (Drs. 16/8377) fehlende Aufbewahrungsbestimmungen festgestellt und beanstandet hatte, wurden von den Gesundheitsämtern in einer Arbeitsgruppe unter Beteiligung des Hessischen Datenschutzbeauftragten konkrete Speicherfristen für personenbezogene medizinische Unterlagen festgelegt. Das Ministerium für Arbeit, Familie und Gesundheit war bisher über das Ergebnis dieser Arbeitsgruppe nicht informiert und wird nun unter Einbeziehung dieser Ergebnisse die Speicherfristen in einem Erlass allgemeinverbindlich für den öffentlichen Gesundheitsdienst regeln.

Zu 8.2 Optische Archivierung: Abschluss der Auftragsdatenverarbeitung durch den MDK Sachsen-Anhalt (36. Tätigkeitsbericht, Ziff. 5.8.5)

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 8.3 Prüfung der Datenübermittlungen zwischen Kliniken und MVZ (37. Tätigkeitsbericht, Ziff. 4.7.4)

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Wiesbaden, 27. September 2010

Der Hessische Ministerpräsident:
Bouffier

Der Hessische Minister des Innern und für Sport:
Rhein