



17. Wahlperiode

Drucksache **17/662**

# HESSISCHER LANDTAG

16. 09. 2008

## **Stellungnahme der Landesregierung**

**betreffend den Sechsendreißigsten Tätigkeitsbericht  
des Hessischen Datenschutzbeauftragten**

**Drucksache 16/8377**

## **Inhaltsverzeichnis**

### **Seite**

#### **Stellungnahme zu:**

- 1. Einführung**
- 1.1 Allgemeines**
- 1.2 Datenschutz**
- 1.3 Rechtsentwicklung**
- 2. Hessischer Datenschutzbeauftragter**
- 2.1 Daseinsvorsorge**
- 2.1.1 Flughafen Frankfurt**
- 2.1.2 Flughafen Frankfurt-Hahn**
- 2.2 Public Private Partnerships**
- 3. Europa**
- 3.1 Gemeinsame Kontrollinstanz für das Schengener Informationssystem**
- 3.1.1 Neue Rechtsgrundlagen für das Schengener Informationssystem**
- 3.1.2 Gemeinsame Überprüfung von Ausschreibungen zur verdeckten Registrierung**
- 3.1.3 Überprüfung von Ausschreibungen von Drittausländern zur Einreiseverweigerung**
- 3.2 Gemeinsame Kontrollinstanz für EUROPOL**
- 4. Bund**
- 4.1 Online-Durchsuchungen**
- 4.2 Novellierung der Strafprozessordnung**
- 4.2.1 Überwachung der Telekommunikation**
- 4.2.2 Schutz von Berufsgeheimnisträgern**
- 4.2.3 Vorratsdatenspeicherung**
- 4.3 Reform des Personenstandsrechts - technische Umsetzung der automatisierten Registerführung**
- 5. Land**
- 5.1 Querschnitt**
- 5.1.1 Probleme in der Anwendung der Vorschriften des Hessischen Datenschutzgesetzes**
- 5.1.2 Bereitstellung von Daten im Internet**
- 5.1.3 Entwicklungen im Bereich der Videoüberwachung**
- 5.2 Justiz**
- 5.2.1 Bestimmung des Anzeigerstatters als Sachverständiger im Ermittlungsverfahren**

- 5.2.1.1 Einbeziehung der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen in staatsanwaltliche Ermittlungen
- 5.2.1.2 Verdacht des Abrechnungsbetruges durch Pflegedienste
- 5.2.2 Die teilprivatisierte Justizvollzugsanstalt Hünfeld
- 5.3 Verfassungsschutz
  - 5.3.1 Novellierung des Verfassungsschutzgesetzes
    - 5.3.1.1 Einsatz des IMSI-Catchers
    - 5.3.1.2 Einsatz akustischer und optischer Überwachungsmittel in der Wohnung
    - 5.3.1.3 Schutz der Berufsheimnisträger
    - 5.3.1.4 Verwertungsverbot für zu löschende Daten in Sachakten
    - 5.3.1.5 Verfassungsschutzberichte im Internet
  - 5.3.2 Sicherheitsüberprüfungsgesetz
  - 5.3.3 Prüfung des Dezernats "Bekämpfung der organisierten Kriminalität" beim Landesamt für Verfassungsschutz
    - 5.3.3.1 Ansatz der Prüfung
    - 5.3.3.2 Keine vollständige Aktenvorlage
    - 5.3.3.3 Tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten der organisierten Kriminalität
  - 5.3.4 Auskunft über eigene Daten beim Landesamt für Verfassungsschutz
- 5.4 Ausländerrecht
  - 5.4.1 Prüfung von Ausländerbehörden
  - 5.4.2 Elektronische Bearbeitung im Aufenthalts- und Einbürgerungsverfahren
    - 5.4.2.1 E-Aufenthalt
    - 5.4.2.2 E-Einbürgerung
- 5.5 Verkehrswesen
  - 5.5.1 Verfahrensprotokolle beim Kraftfahrt-Bundesamt helfen wirksamen Datenschutz herzustellen
  - 5.5.2 Keine Auskünfte aus den örtlichen Fahrzeugregistern an die Gebühreneinzugszentrale zur Ermittlung der Gebührenpflicht für Autoradios
- 5.6 Schulen und Schulverwaltung
  - 5.6.1 LUSD - Zentrale Lehrer- und Schülerdatenbank
    - 5.6.1.4 Ergebnisse weiterer Prüfungen
      - 5.6.1.4.1 Umsetzung durch die Schulträger
      - 5.6.1.4.2 Unberechtigte Zugriffe auf die Daten der LUSD
      - 5.6.1.4.3 Internet-Nutzung

- 5.6.2 **Änderung der Meldedatenübermittlungsverordnung zur Überwachung der Schulanmeldungen**
- 5.6.3 **Verfahren zum Nachteilsausgleich für schwerbehinderte Lehrkräfte gemäß der Pflichtstundenverordnung**
- 5.6.4 **Datenschutzfragen bei der Erstellung und Behandlung von Schülerfotos**
- 5.7 **Umwelt und Geologie**
- 5.7.1 **Veröffentlichung von Standort-, Funktions- und Eigenschaftskarten**
- 5.8 **Gesundheitswesen**
- 5.8.1 **Hessisches Gesetz über den öffentlichen Gesundheitsdienst**
- 5.8.1.1 **Klarstellung der Unterscheidung zwischen Aufgabenzuweisungen und Befugnissen zur Verarbeitung personenbezogener Daten**
- 5.8.1.2 **Regelung zur Kinder- und Jugendgesundheit (§ 10)**
- 5.8.1.3 **Regelung zum Datenschutz (§ 18)**
- 5.8.1.3.1 **Verfahren bei der Erstellung von Gutachten (Abs. 1)**
- 5.8.1.3.2 **Pauschale Befugnis zur Erhebung der Meldedaten aller Neugeborenen (Abs. 2)**
- 5.8.1.3.3 **Gewährleistung der Geheimhaltungspflichten und der Zweckbindung der personenbezogenen Daten in den Gesundheitsbehörden**
- 5.8.1.3.4 **Vorgaben zur Dauer der Datenspeicherung**
- 5.8.1.3.5 **Verweis auf das Hessische Datenschutzgesetz (Abs. 4)**
- 5.8.2 **Kindergesundheitsschutz-Gesetz**
- 5.8.3 **Forschungsprojekt CIMECS zur einrichtungsübergreifenden elektronischen Fallakte**
- 5.8.4 **Prüfung der Datenverarbeitung ausgewählter Gesundheitsämter**
- 5.8.5 **Prüfung beim MDK Sachsen-Anhalt**
- 5.8.6 **Prüfung beim Klinikum Fulda**
- 5.8.7 **Unzulässiges Einwilligungsfomular der AOK Hessen**
- 5.8.8 **Bilder von Neugeborenen auf der Homepage von Krankenhäusern**
- 5.9 **Sozialwesen**
- 5.9.1 **Feststellung der Pflegebedürftigkeit bei Anträgen auf Sozialhilfe**
- 5.9.2 **Hartz IV - Datenerhebung bei Dritten**
- 5.9.3 **Übermittlung von Sozialdaten durch das Jugendamt an das Familiengericht**
- 5.9.4 **Datenschutzbeauftragter bei Trägern der freien Kinder- und Jugendhilfe**
- 5.10 **Personalwesen**

- 5.10.1 Personalakteneinsicht durch Innenrevision
- 5.10.3 Personaldatenverarbeitung mit SAP R/3 HR
  - 5.10.3.1 Download-Berechtigungen
  - 5.10.3.2 Löschung von Daten im SAP R/3 HR-System
  - 5.10.3.3 Konzept "Zentraler Zugriff"
  - 5.10.3.4 Personalkostenhochrechnung
  - 5.10.3.5 Business-Warehouse-HR (HEPISneu)
- 6. Kommunen
  - 6.1 Ergebnisse der Prüfung von Kommunen
  - 6.2 Speicherung von Wahlhelferdaten
  - 6.3 Vereinsförderung durch Kommunen
  - 6.4 Hepatitiswarnung im Einwohnermeldeamt
  - 6.5 Chipkarte als Eintrittskarte und elektronische Geldbörse
  - 6.6 Zur Nachweispflicht von ledigen Studierenden bei der Begründung eines Nebenwohnsitzes am Studienort
- 7. Sonstige Selbstverwaltungskörperschaften
  - 7.1 Hochschulen
    - 7.1.1 Umfang der Nachweise zu § 6 Abs. 5 Nr. 2 Studienbeitragsgesetz
  - 7.2 Rundfunk
    - 7.2.1 Rechtswidrige Suche nach Schwarzhörern und -sehern
  - 7.3 Handwerksinnung
    - 7.3.1 Handwerksinnung gibt rechtswidrig Einstellungstests von Ausbildungsplatzbewerbern weiter
- 8. Entwicklungen und Empfehlungen im Bereich der Technik
  - 8.1 Einsatz von Signaturen für Verwaltungszwecke
  - 8.2 Datenschutz beim Umgang mit Speichermedien
  - 8.3 Fehler- und Unfalldatenspeicher
- 9. Bilanz
  - 9.1 Datenschutz im Verfahren der Verleihung staatlicher Auszeichnungen und Ehrungen (31. Tätigkeitsbericht, Ziff. 3.3)
  - 9.2 Einsatz zentraler Spam-Filter der Landesverwaltung (35. Tätigkeitsbericht, Ziff. 8.2)

Die Stellungnahme der Landesregierung gibt den Sachstand im April/Mai 2008 wieder.

## **1. Einführung**

### **1.1 Allgemeines**

Die Landesregierung teilt die Auffassung des Hessischen Datenschutzbeauftragten über das Bestehen einer hohen Datenschutzkultur, insbesondere hier in Hessen. Auch die Feststellung, dass den Belange des Datenschutzes allein durch die Abwehr von staatlichen Eingriffen in die informationelle Selbstbestimmung nicht hinreichend Rechnung getragen wird, verdient Zustimmung. Nach Auffassung der Landesregierung stehen die dazu erforderlichen rechtlichen und organisatorischen Mittel bereit.

Soweit es den Datenschutz im öffentlichen Bereich betrifft, hat der Landesgesetzgeber die potentiellen Gefahren der automatisierten Datenverarbeitung bereits bei der Formulierung der Aufgaben des Hessischen Datenschutzbeauftragten berücksichtigt. In § 24 Hessisches Datenschutzgesetz (HDSG) ist nicht nur vorgesehen, dass der Hessische Datenschutzbeauftragte die Einhaltung der geltenden Datenschutzvorschriften durch die öffentlichen Stellen überwacht, sondern dass er auch die Auswirkungen der automatisierten Datenverarbeitung auf die Gewaltenteilung zwischen den Verfassungsorganen des Landes zu beobachten hat. Dabei ist er nach § 24 Abs. 2 Satz 3 HDSG nicht nur berechtigt, sondern sogar verpflichtet, Maßnahmen anzuregen, die ihm geeignet erscheinen, nachteilige Auswirkungen zu verhindern.

Im nicht öffentlichen Bereich wird der Staat selbst aktiv tätig, um die Gefahren, die dem informationellen Selbstbestimmungsrecht durch die Verarbeitung personenbezogener Daten drohen, abzuwehren. Mittels der Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich sorgt er für den ordnungsgemäßen Vollzug des Bundesdatenschutzgesetzes, wo Bürgerinnen und Bürgern unzulässige Eingriffe in die informationelle Selbstbestimmung durch andere Private drohen. Wie effektiv dieser Schutz erfolgt, ist u. a. den in jedem Jahr vorgelegten Berichten der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden zu entnehmen.

### **Zu 1.2 Datenschutz**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zur "Abwehrkomponente" (1.2.1) des Datenschutzes zu. Die Ausführungen zur "Schutzkomponente" (1.2.2) entziehen sich aufgrund ihrer eher allgemeinen Formulierung einer abschließenden Bewertung durch die Landesregierung. Der angesprochene Schutz betrifft den Datenschutz im nicht öffentlichen Bereich. Dort bildet das Bundesdatenschutzgesetz (BDSG) die rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch private Dritte. Die Einhaltung des Gesetzes wird durch die Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich überwacht, in Hessen durch das Regierungspräsidium Darmstadt (vgl. den zusammen mit dieser Stellungnahme vorgelegten 21. Bericht der Landesregierung über der Tätigkeit der Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich). Jeder Betroffene hat das Recht, sich an diese Aufsichtsbehörden zu wenden. Die Aufsichtsbehörde wird dann zum Schutz der Rechte des Betroffenen tätig. Den Ausführungen des Hessischen Datenschutzbeauftragten ist nicht zu entnehmen, ob er einen darüber hinaus gehenden Schutzbedarf sieht.

Hinsichtlich der Ausführungen des Hessischen Datenschutzbeauftragten zum "Datenzugangsschutz" wird auf die Erwiderung der Landesregierung zu seiner Forderung eines Informationsfreiheitsgesetzes in der Stellungnahme zum 35. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Drucks. 16/7645, zu Ziffer 1) verwiesen.

### **Zu 1.3 Rechtentwicklung**

Der Hessische Datenschutzbeauftragte referiert die Entwicklung der Rechtslage anhand aktueller Gesetzgebung und Rechtsprechung zutreffend. Insofern bleibt aus Sicht der Landesregierung anzumerken, dass die Fragen der Online-Durchsuchung sowie der Erfassung von Kfz-Kennzeichen mittlerwei-

le durch das Bundesverfassungsgericht entschieden wurden. Beide Urteile (Urt. vom 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07 – zur Online-Durchsuchung und vom 11. März 2008 – 1 BvR 2074/05 und 1 BvR 1254/07 – zu Kennzeichenlesern) erkennen die Zulässigkeit der Maßnahmen grundsätzlich an.

Den IMSI-Catcher als "ersten Schritt in die schrankenlose Telefonüberwachung" zu bezeichnen, erscheint nach Auffassung der Landesregierung jedoch nicht sachgerecht. Das Bundesverfassungsgericht hat in seinem Beschluss vom 22. August 2006 (Az. 2 BvR 345/03) entschieden, dass die Ermittlung von Mobilfunkdaten durch einen IMSI-Catcher nicht gegen Grundrechte verstößt und insbesondere nicht an Art. 10 Abs. 1 GG zu messen ist. Es fehlt bereits an einem Eingriff in den Schutz der Telekommunikationsfreiheit. Eine entsprechende Datenerhebung "steht nicht im Zusammenhang mit einem Kommunikationsvorgang und betrifft auch keinen Kommunikationsinhalt im Sinne des Art. 10 Abs. 1 GG" (a.a.O. Rdn. 55). Denn beim Einsatz des IMSI-Catchers "kommunizieren" ausschließlich technische Geräte miteinander; es fehlt an einem menschlich veranlassten Informationsaustausch (a.a.O. Rdn. 57).

## **2. Hessischer Datenschutzbeauftragter**

### **2.1 Daseinsvorsorge**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu, soweit die Leistung im Bereich der Daseinsvorsorge durch eine öffentliche Stelle im Sinne des § 3 Abs. 1 Hessisches Datenschutzgesetz (HDSG) bzw. des § 2 Abs. 3 BDSG erbracht wird. Nach § 2 Abs. 3 BDSG gilt ein Unternehmen, an dem keine öffentlichen Körperschaften beteiligt sind, jedoch auch dann nicht als öffentliche Stelle, wenn es im Bereich der Daseinsvorsorge tätig ist. Es unterliegt als solches der Kontrolle durch die zuständige Datenschutzaufsichtsbehörde nach § 38 BDSG. Das ist in Hessen das Regierungspräsidium Darmstadt.

#### **2.1.1 Flughafen Frankfurt**

Die vom Hessischen Datenschutzbeauftragten nochmals angesprochene Frage der Aufsicht über die Fraport AG (vgl. 33. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drucks. 16/3746, Ziff. 2.2 und die Stellungnahme der Landesregierung zu Ziff. 2.2 des 33. Tätigkeitsberichts des Hessischen Datenschutzbeauftragten, Drucks. 16/4751) ist bereits vor geraumer Zeit geklärt worden. Der Minister des Innern und für Sport hat im Jahr 2006 entschieden, wegen der negativen Folgen für die Rechtssicherheit auf die Fortführung der Diskussion über die Zuständigkeit zu verzichten und Einvernehmen mit dem Hessischen Datenschutzbeauftragten darüber erzielt, dass die Datenschutzaufsicht über die Fraport AG bei dessen Behörde liegt, soweit das Unternehmen im Bereich der Daseinsvorsorge tätig ist.

Die Landesregierung geht davon aus, dass das erzielte Einvernehmen auch auf Seiten des Hessischen Datenschutzbeauftragten unverändert fortbesteht.

#### **2.1.2 Flughafen Frankfurt-Hahn**

Welche Aufsichtsbehörde in Rheinland-Pfalz für den in Hahn gelegenen Flughafen zuständig ist, entzieht sich der Regelungskompetenz der Landesregierung.

### **2.2 Public Private Partnerships**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zur "Beleihung" (Ziffer 2.2.1) und zur "Verwaltungshilfe" (Ziffer 2.2.2) zu. Im Übrigen sind nach geltendem Recht für die Bestimmung des anzuwendenden Datenschutzgesetzes und der zuständigen Aufsichtsbehörde sowohl die Wahrnehmung einer Aufgabe im Bereich der öffentlichen Verwaltung als auch die Beteiligung einer öffentlichen Körperschaft am ausführenden Unternehmen maßgeblich. Zur Vermeidung von Wiederholungen wird auf die Ausführungen zu Ziffer 2.1 (siehe oben) sowie zu Ziffer 2 in der Stellungnahme der Landesregierung zum 35. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Drucks. 16/7645) verwiesen.

### **3. Europa**

#### **3.1 Gemeinsame Kontrollinstanz für das Schengener Informationssystem**

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

##### **Zu 3.1.1 Neue Rechtsgrundlagen für das Schengener Informationssystem**

Nach Kenntnis der Landesregierung wird die Realisierung des SIS II nach derzeitigem EU-Planungsstand nunmehr bis spätestens September 2009 angestrebt.

##### **Zu 3.1.2 Gemeinsame Überprüfung von Ausschreibungen zur verdeckten Registrierung**

Seit dem 26. März 2008 steht im INPOL-Verbund die Funktionalität der in Amtshilfe für die Nachrichtendienste zu erfassenden Fahndungen nach Art. 99 Abs. 3 SDÜ zur Verfügung. Ein direkter Zugriff der Nachrichtendienste auf INPOL/SIS ist damit nicht verbunden, lediglich der lesende Zugriff auf die eigenen Ausschreibungen. Die BKA-Fachdienststelle SIRENE erhält die Ausschreibungsersuchen auf konventionellem Weg und stellt die Daten für die ausschreibende Behörde in INPOL-Bund sowie bei entsprechender Kennzeichnung im Schengener Informationssystem ein. Wird eine so ausgeschriebene Person oder Sache angetroffen, erfolgt die Mitteilung direkt an den Nachrichtendienst und nicht an das BKA.

##### **Zu 3.1.3 Überprüfung von Ausschreibungen von Drittausländern zur Einreiseverweigerung**

Die Landesregierung nimmt die Ausführungen des Hessischen Datenschutzbeauftragten zur Kenntnis.

#### **Zu 3.2 Gemeinsame Kontrollinstanz für EUROPOL**

Die Ausführungen des Hessischen Datenschutzbeauftragten zu den neuen Rechtsgrundlagen für EUROPOL (Ziffer 3.2.1) erstrecken sich auch auf den Beschlussentwurf zur Ersetzung des EUROPOL-Übereinkommens, der u.a. eine Ausweitung des EUROPOL-Mandatsbereichs beinhaltet. Insbesondere durch die Formulierung EUROPOL sei künftig "...zuständig für schwere Kriminalität allgemein..." könnte jedoch der irriige Eindruck entstehen, dass EUROPOL mit einer weitreichenden Zuständigkeit ausgestattet werden soll. Dies ist jedoch nicht der Fall. Faktisch soll zwar die Beschränkung des Mandatsbereichs auf Straftaten der organisierten Kriminalität und des Terrorismus aufgehoben werden, zugleich wird aber mit der Bedingung, dass zwei oder mehr Mitgliedstaaten in einer bestimmten Weise von den genannten schweren Straftaten betroffen sein müssen (Art. 4), ein qualitativ bedeutendes und besonders von deutscher Seite nachdrücklich gefordertes Merkmal festgeschrieben.

### **4. Bund**

#### **Zu 4.1 Online-Durchsuchungen**

Die vom Hessischen Datenschutzbeauftragten beschriebene rechtspolitische Diskussion über die Online-Durchsuchung von Computern ist durch das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 (1 BvR 370/07 und 1 BvR 595/07) zum nordrhein-westfälischen Verfassungsschutzgesetz in ein neues Stadium gelangt. Das Bundesverfassungsgericht hat in dieser Entscheidung - wengleich bezogen auf den präventiven Bereich und nicht auf das Gebiet der Strafverfolgung - Maßstäbe aufgezeigt, unter denen aus seiner Sicht die heimliche Online-Durchsuchung von Computern, auch im Lichte des allgemeinen Persönlichkeitsrechts in der - neu entwickelten - besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zulässig ist. Das neu



entwickelte Grundrecht kann mithin - wie andere Grundrechte auch - durch Gesetz eingeschränkt werden.

Aufgabe des Gesetzgebers wird es nun sein, rasch zu prüfen, wie die aufgezeigten verfassungsgerichtlichen Maßstäbe bei der Schaffung einer gesetzlichen Regelung der Online-Durchsuchung als Ermittlungsmaßnahme umzusetzen sind. Die Schaffung einer solchen Regelung in der Strafprozessordnung ist erforderlich, um insbesondere in den Bereichen des Terrorismus und der organisierten Kriminalität, wo eine immer stärkere Nutzung der modernen Informationstechnologie für kriminelle Zwecke zu verzeichnen ist, eine wirksame Kriminalitätsbekämpfung betreiben zu können. Hierauf hat die Praxis - allen voran die Generalbundesanwältin und der Präsident des Bundeskriminalamts - mit Nachdruck hingewiesen. Aufgrund dessen haben Hessen und Thüringen schon am 9. März 2007 im Bundesrat einen Entschließungsantrag (BR-Drucks. 144/07) eingebracht, mit dem die Bundesregierung aufgefordert wird, die erforderliche Befugnisnorm in der Strafprozessordnung zu schaffen.

Dass eine Online-Durchsuchung, wie der nunmehr vorliegenden Entscheidung des Bundesverfassungsgerichts zu entnehmen sein dürfte, auch zu Strafverfolgungszwecken, nur unter engen rechtlichen Voraussetzungen (z.B. Verdacht einer schweren Straftat, Anordnung der Maßnahme durch den Richter, Schutz des Kernbereichs privater Lebensgestaltung) in Betracht kommt, entspricht der von der Landesregierung stets vertretenen Auffassung. Da bei der Online-Durchsuchung weit in den persönlichen Lebensbereich eingegriffen wird, bedarf es seitens des Gesetzgebers einer sorgfältigen Prüfung und Abwägung anhand der strafprozessualen und verfassungsrechtlichen Grundsätze. Im Kern geht es darum, eine rechtsstaatlich einwandfreie Lösung im Spannungsfeld zwischen der notwendigen Sicherheit der Bevölkerung einerseits und den Freiheits- und Persönlichkeitsrechten des von der Ermittlungsmaßnahme Betroffenen andererseits zu finden. Hier wird der Gesetzgeber das Strafverfolgungsinteresse und den Schutz des Persönlichkeitsrechts in einen angemessenen Ausgleich zu bringen haben.

Die anzustrebende Schaffung einer den aufgezeigten Maßstäben entsprechenden Rechtsgrundlage für die heimliche Online-Durchsuchung von Computern dürfte - anders als im Tätigkeitsbericht angenommen - auch keine nachteiligen Auswirkungen auf Projekte des E-Governments - etwa in Gestalt eines Verlusts des Vertrauens der Bürger in die Möglichkeit einer durch Installation bestimmter Schutzmechanismen sicheren Kommunikation mittels Internet - haben. Den Bürgerinnen und Bürgern wird die sachliche Notwendigkeit, bei Ermittlungen wegen schwerer, insbesondere terroristischer Straftaten unter engen rechtlichen Voraussetzungen und mit richterlicher Billigung die installierten Sicherheitsmaßnahmen des Computers technisch zu überwinden, einleuchten.

Ob und inwieweit nach der Grundsatzentscheidung des Bundesverfassungsgerichts eine entsprechende Ermächtigungsgrundlage für den Verfassungsschutz, insbesondere zur Aufklärung von Bedrohungslagen und zur Gefahrenprävention, geschaffen wird, bleibt der weiteren rechtlichen Prüfung und parlamentarischen Beratung vorbehalten.

#### **Zu 4.2      Novellierung der Strafprozessordnung**

Soweit der Hessische Datenschutzbeauftragte inhaltliche Kritik an einigen Punkten des am 1. Januar 2008 in Kraft getretenen Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG übt und zu dem Ergebnis gelangt, der Gesetzgeber habe die Gelegenheit ungenutzt gelassen, eine ausgewogene Abwägung zwischen dem Recht auf informationelle Selbstbestimmung und der Gewährleistung einer effektiven Strafverfolgung vorzunehmen, betreffen diese Ausführungen vorrangig den Verantwortungsbereich des Bundes. Ungeachtet dessen sollte nicht außer Acht gelassen werden, dass es sich um ein sehr umfangreiches und komplexes Gesetzesvorhaben handelte, dessen Entwurf auf jahrelangen, durch die Einholung rechtswissenschaftlicher und rechtstatsächlicher Gutachten unterstützten Vorüberlegungen - beginnend in der 14. Legislaturperiode des Deutschen Bundestags - beruht. Dabei war der Gesetzgeber ersichtlich von dem intensiven Bemühen getragen, ein harmonisches Gesamtsystem der strafprozessualen heimlichen Ermittlungsmethoden zu schaffen.

#### **Zu 4.2.1 Überwachung der Telekommunikation**

Wenn der Hessische Datenschutzbeauftragte hinsichtlich der Neufassung der Vorschriften über die Telekommunikationsüberwachung den Umfang des in § 100a Abs. 2 StPO enthaltenen Straftatenkatalogs anspricht und diesen als sehr groß einschätzt, ist darauf hinzuweisen, dass die einzelnen Katalogtaten im Gesetzgebungsverfahren sorgfältig auf ihre sachliche Notwendigkeit für eine effektive Strafverfolgung geprüft wurden. Dabei wurde darauf geachtet, dass es sich jeweils um schwere Straftaten handelt. Weiter begrenzt wird die Zulässigkeit der Ermittlungsmaßnahme, worauf im Tätigkeitsbericht zu Recht hingewiesen wird, durch die gesetzliche Einschränkung, dass die Tat auch im Einzelfall schwer wiegen muss.

Soweit der Umfang der im Gesetz vorgesehenen jährlichen Berichtspflicht der Länder über die angeordneten Maßnahmen nach § 100a StPO als nicht ausreichend erachtet wird, um hierdurch eine verfahrensrechtliche Schutzvorkehrung und eine Grundlage für sinnvolle Evaluationsprojekte zu schaffen, kann dem nicht zugestimmt werden. Zu bedenken ist, dass bei der Telekommunikationsüberwachung bisher eine Berichtspflicht im Gesetz - anders als bei der akustischen Wohnraumüberwachung - nicht vorgesehen war. Dennoch wurde bereits seit 1996 jährlich von den Staatsanwaltschaften und auf dieser Grundlage von den Ländern an den Bund berichtet über die Anzahl der Verfahren, in denen eine Anordnung nach den §§ 100a, 100b StPO getroffen worden ist, über die Anzahl der hiervon Betroffenen sowie die Zuordnung zu den Katalogdelikten des § 100a StPO. Diese Erhebung beruhte auf bundeseinheitlichen Vorgaben, die der Strafrechtsausschuss der Justizministerkonferenz im Jahre 1995 erarbeitet hat.

Über den bisherigen Berichtsumfang hinaus wird die Berichtspflicht durch die neue gesetzliche Regelung deutlich erweitert. Die Berichtspflicht erstreckt sich nun auf die Angaben, ob es sich um eine Erst- oder Verlängerungsanordnung handelt und ob sich die Maßnahme auf Festnetz, Mobilfunk oder Internet-Telekommunikation bezieht. Eine noch weitergehende Ausdehnung der Berichtspflicht dahingehend, dass zusätzlich mitzuteilen ist, ob die Maßnahme Ergebnisse erbracht hat, die für das Verfahren von Bedeutung sind, ist im Gesetzgebungsverfahren eingehend erörtert, letztlich aber verworfen worden. Maßgeblich war hierfür in erster Linie, dass durch Angaben zum Erfolg der Maßnahme in dem Maße, in dem qualitative Einzelbetrachtungen an die Stelle quantitativer Stricherfassungen treten, die Methodik der formalisierten Erfassung in Frage gestellt wird. In diesem Zusammenhang hatte der Gesetzgeber die anerkanntermaßen bundesweit sehr hohe Arbeitsbelastung der Staatsanwaltschaften und die nicht unbeträchtliche Zahl der jährlichen Maßnahmen nach § 100a StPO zu bedenken. Allein in Hessen sind im Jahre 2006 596 Telekommunikationsüberwachungsmaßnahmen mit 1389 Betroffenen durchgeführt worden; die Zahlen für 2007 liegen bei Redaktionsschluss für diese Stellungnahme noch nicht vor. Ein Evaluationsbedarf, der diesen erheblichen zusätzlichen Aufwand erforderlich machen würde, besteht aus der Sicht des Gesetzgebers nicht, zumal auch der Umstand, dass eine Telekommunikationsüberwachungsmaßnahme letztlich kein für das Verfahren relevantes Ergebnis erbracht hat, keinen verlässlichen Rückschluss auf ihre Notwendigkeit zum Zeitpunkt der Anordnung zuließe.

Die vom Gesetzgeber für den nachträglichen Rechtsschutz des Betroffenen bestimmte Frist von zwei Wochen ab dem Zeitpunkt der Benachrichtigung erscheint ausreichend bemessen.

#### **Zu 4.2.2 Schutz von Berufsgeheimnisträgern**

Die Landesregierung nimmt die Ausführungen des Hessischen Datenschutzbeauftragten zur Kenntnis.

#### **Zu 4.2.3 Vorratsdatenspeicherung**

Über die Verfassungsmäßigkeit der im Gesetz nunmehr vorgesehenen Vorratsspeicherung von Telekommunikationsverkehrsdaten wird das Bundesverfassungsgericht aufgrund der dort anhängigen Verfassungsbeschwerden zu entscheiden haben. Der am 11. März 2008 (1 BvR 256/08) ergangenen Entscheidung dieses Gerichts im Eilverfahren lässt sich jedoch bereits entnehmen, dass im Grundsatz keine durchgreifenden verfassungsrechtlichen Bedenken gegen die gesetzliche Regelung bestehen. Im Übrigen beruht diese

Entscheidung nicht auf einer Prognose des Verfahrensausgangs, sondern auf einer Folgenabwägung (a.a.O. Abs.-Nr. 139). Die einstweilige Anordnung gilt auch nicht in Bezug auf die Erfüllung präventivpolizeilicher und nachrichtendienstlicher Aufgaben nach § 113b Satz 1 Nr. 2 und 3 TKG (a.a.O. Abs.-Nr. 185), was jedoch damit zusammenhängt, dass es in nächster Zeit noch keine diesbezüglichen Vorschriften geben wird, die die §§ 113a, 113b TKG ausdrücklich in Bezug nehmen (vgl. § 113b Satz 1 TKG sowie a.a.O. Abs.-Nr. 12).

Mit der im Gesetz vorgesehenen Speicherdauer von sechs Monaten hat sich der Gesetzgeber für die in der EU-Richtlinie vorgesehene Mindestfrist entschieden. Aus der Sicht der Ermittlungsbehörden wäre eine Speicherdauer von 12 Monaten vorzugswürdig gewesen. Die hessischen Staatsanwaltschaften, die zu dem Entwurf des EU-Rahmenbeschlusses zur Einführung von Mindestspeicherfristen für Telekommunikationsverbindungsdaten vom 28. April 2004 beteiligt worden sind, haben sich aus Gründen der effektiven Strafverfolgung einhellig für eine Mindestspeicherfrist von zwölf Monaten ausgesprochen.

#### **Zu 4.3 Reform des Personenstandsrechts - technische Umsetzung der automatisierten Registerführung**

Der Hessische Datenschutzbeauftragte hat das Ministerium des Innern und für Sport bei der Vorbereitung der Personenstandsnovelle von Anfang an beratend begleitet. Das gilt sowohl für das Gesetzgebungsverfahren auf Bundesebene, das mit dem am 1. Januar 2009 in Kraft tretenden Gesetz zur Reform des Personenstandsrechts vom 19. Februar 2007 (BGBl. I S. 122) seinen Abschluss gefunden hat, als auch für die Erarbeitung der untergesetzlichen Ausführungsbestimmungen auf Bundesebene sowie die landesinterne Umsetzung. Da das Ministerium in Arbeitsgruppen zur Vorbereitung des Personenstandsgesetzes, der Personenstandsverordnung und zur Entwicklung eines von der ekom21 zu betreibenden Registerverfahrens vertreten war bzw. noch ist, konnten aus Hessen bereits in einer frühen Phase wichtige Hinweise aus der Perspektive des Datenschutzes in die Regelwerke und IT-Konzepte eingebracht werden.

Gleichwohl waren nicht alle Positionen des Hessischen Datenschutzbeauftragten mehrheitsfähig. Die qualifizierte elektronische Signatur, die der Hessische Datenschutzbeauftragte für den Abschluss einer elektronischen Personenstandsbeurkundung durch Standesbeamte fordert, ist auf Wunsch des Bundesrates aus dem Gesetzentwurf der Bundesregierung gestrichen worden. Dabei hat sich der Gesetzgeber allerdings die Begründung des Bundesrates nicht zu Eigen gemacht, sondern vielmehr die Regelung der Anforderungen an das elektronische Verfahren dem Verordnungsgeber überlassen. In den Vorarbeiten für den Entwurf einer Personenstandsverordnung des Bundes nach § 73 PStG-2009 ist erneut eine qualifizierte elektronische Signatur vorgesehen, um den besonderen Anforderungen an die auf Dauer zu gewährleistende Integrität und Authentizität von Personenstandsbeurkundungen gerecht zu werden. Diese Position befindet sich noch in der fachlichen Diskussion: Der Lenkungsausschuss des priorisierten Deutschland-Online-Vorhabens Personenstandswesen hat im Hinblick auf den Aufwand für Nachsignierungen und den Vergleich mit einfacheren Verfahren - beispielsweise im Grundbuchbereich - eine Prüfung der Erforderlichkeit dieser Vorgabe in Auftrag gegeben. Deren Ergebnis bleibt abzuwarten, bevor der Punkt abschließend bewertet werden kann.

Für die Sicherungsregister hat der Bundesgesetzgeber eine weitere Speicherung der Personenstandsbeurkundung ebenfalls in elektronischen Registern geregelt (§ 4 Abs. 1 PStG-2009). Er hat sich damit - nicht zuletzt aus Aufwandsgesichtspunkten - entgegen einem Vorentwurf der Bund-Länder-Arbeitsgruppe gegen alternative Medien wie Papier oder Mikrofilm entschieden und dies mit guten Erfahrungen in anderen Verwaltungsbereichen begründet. Mit einer Revision dieser gesetzgeberischen Entscheidung noch vor dem Inkrafttreten der Novelle dürfte nicht zu rechnen sein.

Noch nicht abschließend entschieden ist das technische Datenmodell für das Personenstandsregister; es ist im Rahmen der Personenstandsverordnung des Bundes festzulegen. Nach dem derzeitigen Entwurfsstand ist - übereinstimmend mit der Forderung des Hessischen Datenschutzbeauftragten - eine Kombination von Bild- und strukturierter Datei vorgesehen, bei der die

XML-Datei signiert werden soll. Aufgrund des Zusammenhangs mit dem Prüfungsauftrag hinsichtlich der qualifizierten elektronischen Signatur ist auch hier die Entscheidungsfindung noch nicht abgeschlossen.

Die Ankündigung des Hessischen Datenschutzbeauftragten, die Personenstands-Novelle in ihrer Entstehungsphase weiterhin konstruktiv begleiten zu wollen, wird von der Landesregierung begrüßt; die frühzeitige intensive Zusammenarbeit trägt maßgeblich zu einem Ergebnis bei, das von allen Beteiligten getragen und zügig umgesetzt werden kann.

## **5. Land**

### **5.1 Querschnitt**

#### **Zu 5.1.1 Probleme in der Anwendung der Vorschriften des Hessischen Datenschutzgesetzes**

Der Hessische Datenschutzbeauftragte beschreibt die mit der Einführung ressort- oder landesweit einheitlicher DV-Verfahren oft verbundenen datenschutzrechtlichen Fragen zutreffend. Seine Vorschläge zur Änderung des Hessischen Datenschutzgesetzes wird die Landesregierung im Rahmen der nächsten Änderung des Gesetzes in ihre Erwägungen einziehen.

Das Angebot des Hessischen Datenschutzbeauftragten, an der Überarbeitung der Vorschriften mitzuwirken, wird von der Landesregierung ausdrücklich begrüßt.

#### **Zu 5.1.2 Bereitstellung von Daten im Internet**

Die Ausführungen des Hessischen Datenschutzbeauftragten zur unbeabsichtigten Veröffentlichung von Informationen im Internet durch die Polizei sind zutreffend. Die Verfahrensweise der Einstellung von Informationen in das Internet wurde nach diesem Vorfall geändert, um vergleichbare Vorkommnisse in der Zukunft zu vermeiden. Will ein Web-Redakteur eine Datei in den Internet-Auftritt der Polizei einstellen, bekommt er nunmehr einen deutlichen optischen Warnhinweis, der für eine weitere Bearbeitung bestätigt oder verneint werden muss. Zusätzlich werden alle Namen von Dateien, die für die Einstellung in das Internet vorgesehen sind, andersfarbig dargestellt.

Darüber hinaus wurde sichergestellt, dass bei künftigen Problemfällen die Verantwortlichen von Google Deutschland persönlich angesprochen werden können.

Die Aufnahme der vertretungsberechtigten Personen einer Stiftung in das Stiftungsregister dient dem Zweck, dem interessierten Bürger nicht nur das vertretungsberechtigte Organ einer Stiftung sondern auch die insoweit handelnden Personen mitzuteilen, z.B. die gemeinschaftliche Vertretung zweier Vorstandsmitglieder. Jegliche vertraglichen Beziehungen, aber auch Mahnbescheide und Klagen bedürfen der Kenntnis der verfassungsgemäß richtigen Vertretung der Stiftung. Diesbezügliche Anfragen an die Registerbehörde sowie die Ausstellung von Vertretungsbescheinigungen erübrigen sich dadurch.

#### **Zu 5.1.3 Entwicklungen im Bereich der Videoüberwachung**

Die Ausführungen des Hessischen Datenschutzbeauftragten zur Videoüberwachungsanlage an der Konstabler Wache in Frankfurt am Main sind zutreffend. Die Kameras wurden im Dezember 2007 auf Kosten des Polizeipräsidiums Frankfurt am Main ausgetauscht. Derzeit befindet sich das Polizeipräsidium in Verhandlungen mit der Stadt Frankfurt am Main mit dem Ziel der Übernahme der Anlage durch die Stadt.

Im Übrigen war die Landesregierung in den im Tätigkeitsbericht geschilderten Beispielfällen für die Installation von Anlagen zur Videoüberwachung nicht beteiligt.

## **5.2 Justiz**

#### **Zu 5.2.1 Bestimmung des Anzeigerstatters als Sachverständiger im Ermittlungsverfahren**

Der Hessische Datenschutzbeauftragte geht zutreffend davon aus, dass den Ermittlungsbehörden in einigen speziellen Bereichen nur eine geringe Zahl

von geeigneten Sachverständigen oder sachverständigen Zeugen zur Verfügung steht, deren Sachverstand für eine effektive Strafverfolgung in diesen Bereichen aber dringend benötigt wird. Die hessischen Staatsanwaltschaften sind sich bewusst, dass trotz dieses Umstandes stets das Gebot der Unparteilichkeit zu beachten ist.

#### **Zu 5.2.1.1 Einbeziehung der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen in staatsanwaltschaftliche Ermittlungen**

Die Frage der Einbeziehung der Mitarbeiter der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) in die staatsanwaltschaftlichen Ermittlungen ist im Rahmen der Sitzung des Strafrechtsausschusses der Justizministerkonferenz im Juni 2007 erörtert worden. Zur Vorbereitung dieser Behandlung der Thematik im Strafrechtsausschuss hat das Ministerium der Justiz den Generalstaatsanwalt bei dem Oberlandesgericht beteiligt.

Die im Tätigkeitsbericht dargelegte Einschätzung, wonach der GVU nur die verdächtigen Datenträger, nicht jedoch ganze Rechner oder Festplatten, die möglicherweise personenbezogene Daten des Beschuldigten oder Dritter beinhalten, ausgehändigt werden dürfen, entspricht der Auffassung, die vom Ministerium der Justiz in Übereinstimmung mit dem Generalstaatsanwalt im Strafrechtsausschuss vertreten wurde und die dort auf Zustimmung gestoßen ist.

In einem Punkt besteht indes keine Übereinstimmung mit den Ausführungen des Hessischen Datenschutzbeauftragten im Tätigkeitsbericht. In Übereinstimmung mit dem Diskussionsstand im Strafrechtsausschuss der Justizministerkonferenz wird gegen eine Übermittlung des Namens des Beschuldigten an die GVU rechtlich nichts einzuwenden sein. Dies folgt schon aus dem Umstand, dass Mitarbeiter der GVU - im Rahmen des stets zu beachtenden Gebots der Unparteilichkeit - zu Durchsuchungen hinzugezogen werden dürfen, mit der Möglichkeit des Bekanntwerdens des Namens des Beschuldigten, soweit deren Sachkunde vor Ort zur Identifizierung und Einordnung offensichtlich raubkopierter Daten erforderlich ist. Eine Mitteilung der Personalien des Beschuldigten an die GVU dürfte aber auch ansonsten unbedenklich sein, wenn sie zum Zwecke der Entscheidung über die Stellung eines Strafantrags namens des von der GVU vertretenen Geschädigten erfolgt.

#### **Zu 5.2.1.2 Verdacht des Abrechnungsbetruges durch Pflegedienste**

Mit den Ausführungen des Hessischen Datenschutzbeauftragten besteht im Wesentlichen Übereinstimmung. Die Frage der Einbeziehung von Mitarbeitern der anzeigeerstattenden Krankenkasse als sachverständige Zeugen in die Ermittlungen, insbesondere bei der Sichtung und Auswahl der zu beschlagnehmenden Unterlagen vor Ort, hat der Hessische Datenschutzbeauftragte im April 2006 an das Ministerium der Justiz herangetragen und um eine grundsätzliche Klärung gebeten. In seiner daraufhin eingeholten Stellungnahme hat der Generalstaatsanwalt bei dem Oberlandesgericht darauf hingewiesen, dass es sich nur um sehr wenige Fälle handelt, in denen seitens der Staatsanwaltschaften verfahren wurde, wie vom Hessischen Datenschutzbeauftragten beschrieben.

Der Generalstaatsanwalt hat darüber hinaus in seinem Bericht ausführlich dargelegt, aus welchen Gründen die Auswertung sichergestellter Unterlagen durch Mitarbeiter der Krankenkasse rechtlich zulässig ist, und in diesem Zusammenhang hervorgehoben, dass die zweifellos nicht unproblematische "Doppelrolle" von Mitarbeitern der Krankenkasse in der Literatur weitgehend akzeptiert wird. Gleichwohl hat der Generalstaatsanwalt die Ausführungen des Hessischen Datenschutzbeauftragten zum Anlass genommen, nach Alternativen zu suchen und eine Erörterung der Problematik im Rahmen der Arbeitstagung der Leiterinnen und Leiter der hessischen Staatsanwaltschaften im Dezember 2006 vorzunehmen. Mit Rundverfügung vom Januar 2007 hat der Generalstaatsanwalt die Staatsanwaltschaften schließlich auf zwei Unternehmen hingewiesen, die in der Lage seien, die Aufgaben eines Sachverständigen bei den Ermittlungsverfahren wegen des Verdachts des ärztlichen Abrechnungsbetrugs zu erfüllen.

In Übereinstimmung mit dem Hessischen Datenschutzbeauftragten ist davon auszugehen, dass die Staatsanwaltschaften diesen Hinweis bei der Auswahl von Sachverständigen bzw. sachverständigen Zeugen aufgreifen werden.

### **Zu 5.2.2 Die teilprivatisierte Justizvollzugsanstalt Hünfeld**

Der Hessische Datenschutzbeauftragte macht in seinem Bericht deutlich, dass sich die Befürchtungen, die er im Vorfeld der Inbetriebnahme der JVA Hünfeld geäußert hatte, nicht bewahrheitet haben. Die gesetzlichen Grundlagen und Richtlinien zum Datenschutz werden in vollem Umfang berücksichtigt und umgesetzt. Den Ausführungen des hessischen Datenschutzbeauftragten ist nichts hinzuzufügen.

## **5.3 Verfassungsschutz**

### **5.3.1 Novellierung des Verfassungsschutzgesetzes**

#### **Zu 5.3.1.1 Einsatz des IMSI-Catchers**

Nach Auffassung der Landesregierung stellt die Befugnis zum Einsatz eines IMSI-Catchers im Zusammenspiel mit anderen Maßnahmen der Erkenntnisgewinnung ein grundsätzlich wertvolles Instrument für eine effektive und effiziente Bekämpfung vor allem des islamistischen Terrorismus dar.

Das LfV Hessen hat aufgrund der neuen Rechtslage (§ 5 Abs. 2 Gesetz über das Landesamt für Verfassungsschutz/LfVG) bisher in einem Fall im Bereich der Bekämpfung des islamistischen Terrorismus einen IMSI-Catcher eingesetzt. Dabei konnten Informationen gewonnen werden, die ihrerseits für die Durchführung einer Beschränkungsmaßnahme nach dem G10-Gesetz von Bedeutung gewesen sind.

#### **Zu 5.3.1.2 Einsatz akustischer und optischer Überwachungsmittel in der Wohnung**

Mit der Norm des § 5a LfVG wurde die Befugnis zur akustischen Wohnraumüberwachung an die Vorgaben des Bundesverfassungsgerichts angepasst. Diese Vorgaben werden vom LfV Hessen bereits seit der Verfassungsgerichtsentscheidung eingehalten, wie es Art. 20 Abs. 3 GG gebietet. Selbst in seinem Urteil zur sog. "Online-Durchsuchung" geht das Bundesverfassungsgericht davon aus, dass es Fälle geben kann, in denen es praktisch unvermeidbar ist, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann. Daher müsse "für hinreichenden Schutz in der Auswertungsphase gesorgt" werden.

Mit dem neuen § 5a Abs. 4 Satz 2 LfVG hat der Gesetzgeber einen Vorschlag des Hessischen Datenschutzbeauftragten aufgegriffen. In der Begründung zum Gesetzentwurf wird dazu folgendes ausgeführt:

"Zur Erleichterung der praktischen Umsetzung der genannten Grundsätze im Einzelnen, insbesondere geeigneter Maßnahmen im Hinblick auf einen wirksamen Kernbereichsschutz sowie eine effektive Durchführung von Wohnraumüberwachungsmaßnahmen, kann die zuständige Behörde in einer konkretisierenden Dienstanweisung entsprechende Handlungsempfehlungen geben."

Aufgrund dessen werden derzeit Regelungen im Rahmen von Dienstvorschriften gegenüber dem Erlass einer normenkonkretisierenden Verwaltungsvorschrift favorisiert. In der gegenwärtig stattfindenden Überarbeitung der Dienstvorschriften des LfV Hessen werden die Vorgaben zum Schutz des Kernbereichs privater Lebensgestaltung daher auch in den jeweiligen Dienstvorschriften entsprechend schriftlich konkretisiert und eingearbeitet. Hierüber wird zu gegebener Zeit eine Abstimmung mit dem Hessischen Datenschutzbeauftragten erfolgen.

#### **Zu 5.3.1.3 Schutz der Berufsheimnisträger**

Der Schutz der Berufsheimnisträger ist im erforderlichen Umfang gewährleistet. Insoweit wird auf die Ausführungen auf den Seiten 10 bis 12 der Begründung zum Gesetzentwurf der Landesregierung für ein Gesetz zur Änderung des Gesetzes über das Landesamt für Verfassungsschutz und des Hessischen Ausführungsgesetzes zum Gesetz zu Artikel 10 Grundgesetz vom 22. Februar 2007 (Drs. 16/6936) verwiesen.

#### **Zu 5.3.1.4 Verwertungsverbot für zu löschende Daten in Sachakten**

Zum Umgang mit personenbezogenen Daten in Sachakten gibt es in den Verfassungsschutzbehörden von Bund und Ländern unterschiedliche Regelungen

hinsichtlich der Löschung bzw. Vernichtung. Die Vorschrift in § 6 Abs. 5 Satz 3 LfVG zum Umgang mit personenbezogenen Daten in Sachakten entspricht der EntschlieÙung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24./25. Oktober 2002. Dort heißt es:

"Die Konferenz fordert, dass in Sachakten personenbezogene Angaben, die nicht mehr erforderlich sind, auch in Ländern ohne gesetzliches Lösungsgebot zumindest zu sperren sind."

#### **Zu 5.3.1.5 Verfassungsschutzberichte im Internet**

Die Einstellung von Verfassungsschutzberichten im Internet für fünf Jahre entspricht nach Auffassung der Landesregierung dem Grundsatz der Verhältnismäßigkeit. Die Publikation personenbezogener Daten im Internet stellt aufgrund ihrer Recherchierbarkeit einen Eingriff in das Recht am eigenen Namen sowie das "Recht auf Vergessen" als besondere Ausprägungen des allgemeinen Persönlichkeitsrechts dar. Dieser Eingriff in die Privatsphäre auf der einen und das öffentliche Informationsinteresse auf der anderen Seite müssen daher zu einem schonenden Ausgleich gebracht werden. Dies ist durch die zeitliche Limitierung geschehen.

Das Thema wurde auch bereits auf Bundesebene thematisiert. Der Bundesbeauftragte für Datenschutz und Informationsfreiheit hatte seinerzeit in der Löschung der Berichte nach fünf Jahren eine adäquate Limitierung gesehen, sodass eine entsprechende Regelung in zahlreiche Landesverfassungsschutzgesetze Eingang gefunden hat.

#### **Zu 5.3.2 Sicherheitsüberprüfungsgesetz**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

#### **Zu 5.3.3 Prüfung des Dezernats "Bekämpfung der organisierten Kriminalität" beim Landesamt für Verfassungsschutz**

##### **Zu 5.3.3.1 Ansatz der Prüfung**

Der Hessische Datenschutzbeauftragte gibt die Vorgehensweise und den Ablauf der Prüfung der Datenverarbeitung im Bereich der Beobachtung der organisierten Kriminalität in seinem Tätigkeitsbericht zutreffend wieder.

##### **Zu 5.3.3.2 Keine vollständige Aktenvorlage**

Hinsichtlich der Kritik des Hessischen Datenschutzbeauftragten an einer unvollständigen Aktenvorlage ist anzumerken, dass nicht in "mindestens einem Fall", sondern tatsächlich nur in einem einzigen Fall eine Akte vorgelegt wurde, aus der zuvor einzelne Schriftstücke vorsorglich entnommen wurden. Dies erfolgte aus Gründen des Quellenschutzes mit Blick auf die in § 29 Abs. 2 HDSG zugelassenen Beschränkungen der Auskunftspflicht. Aus pragmatischen Gründen wurde vom LfV Hessen zunächst auf eine förmliche Feststellung des Ministeriums des Innern und für Sport nach § 29 Abs. 2 HDSG verzichtet, zugleich jedoch durch eine ständige Verfügbarkeit der Leitungsebene (Abteilungsleitung, Dezernatsleitung) und der Sachbearbeiter-ebene während der gesamten Prüfungsdauer sichergestellt, dass Lücken in der Erklärbarkeit von Zusammenhängen oder Abfolgen der gesammelten Informationen durch entsprechende Erläuterungen geschlossen werden konnten. Nachdem von Seiten der Behörde des Hessischen Datenschutzbeauftragten ausdrücklich zugesichert wurde, die Vertraulichkeit der Informationen zu Quellen zu respektieren, wurde auf die Einholung einer förmlichen Feststellung durch das Ministerium gänzlich verzichtet und die entnommenen Schriftstücke zur Einsichtnahme zur Verfügung gestellt.

Das LfV Hessen hat sich bereits mit dem Hessischen Datenschutzbeauftragten auf die vorgeschlagene Verfahrensweise verständigt, zukünftig in entsprechenden Fällen Fehlblätter mit Angaben zu den Gründen der Entnahme in die Akte einzuheften.

### **Zu 5.3.3.3 Tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten der organisierten Kriminalität**

Das LfVG und der Arbeitsplan CRIME geben den Beginn der Informationssammlung bei personenbezogenen Daten vor. Danach ist das Speichern von Daten zu einer Person nur zulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass diese Person innerhalb eines für das Beobachtungsobjekt organisierte Kriminalität (OK) relevanten Arbeitsschwerpunkts aktiv ist. Die Prüfung, dass tatsächliche Anhaltspunkte vorliegen, ist mit einer Speicherung in CRIME bzw. NADIS positiv abgeschlossen.

Der gesetzliche Beobachtungsauftrag im Bereich OK setzt allerdings nicht erst dann ein, wenn die Begehung von entsprechenden Straftaten festgestellt wird oder unmittelbar bevorsteht, sondern - ebenso wie in den klassischen Feldern der Verfassungsschutzarbeit - bereits in deren Vorfeld. Das LfV Hessen klärt Sachverhalte und Personenzusammenschlüsse auf, bei denen aufgrund von Verdachtsmomenten davon auszugehen ist, dass sie der organisierten Kriminalität zuzurechnen sind. Hierbei müssen nicht alle Merkmale der OK-Definition zu Beginn der Sachverhaltsaufklärung beweiskräftig gegeben sein. Ziel der Aufklärung des LfV Hessen ist vielmehr, zu erkennen und zu untersuchen, ob die Merkmale der organisierten Kriminalität gegeben sind und ein Personenzusammenschluss im Sinne der OK-Merkmale agiert. Es ist schließlich unzweifelhaft, dass sich das Vorliegen der tatsächlichen Anhaltspunkte als Voraussetzung auch aus der Aktenlage nachvollziehbar ergeben muss. Davon wird der Prüffall nach § 4 Abs. 1 LfVG mit seinen besonderen Rechtsfolgen scharf abgegrenzt, der auch für den Bereich der OK denkbar und zulässig ist.

### **Zu 5.3.4 Auskunft über eigene Daten beim Landesamt für Verfassungsschutz**

Angesichts der positiven Ausführungen des Hessischen Datenschutzbeauftragten über das Auskunftsverhalten des LfV Hessen ist seitens der Landesregierung nur anzumerken, dass von dem Recht auf Auskunft über die zur Person gespeicherten Daten nach § 18 Abs. 1 LfVG in den vergangenen zwei Jahren stärker als zuvor Gebrauch gemacht wurde. Das LfV Hessen hat für diesen Zeitraum zum Teil einen Anstieg an Auskunftersuchen um mehr als das Doppelte verzeichnet.

Trotz des gestiegenen Arbeitsaufwands wird weiterhin versucht, dem Auskunftsinteresse des Einzelnen noch stärker zu entsprechen. So wird in Fällen, in denen die Voraussetzungen einer Auskunftsverweigerung nach § 18 Abs. 2 LfVG vorliegen, trotzdem nach Möglichkeit zumindest der Phänomenbereich der Speicherung bekanntgegeben. Die Annahme eines Ausforschungsversuchs erfolgt unter äußerst restriktiver Anwendung als absolute Ausnahme.

## **5.4 Ausländerrecht**

### **Zu 5.4.1 Prüfung von Ausländerbehörden**

Die Ausländerbehörden des Hochtaunuskreises und der Stadt Fulda bestätigten in ihren anlassbezogenen Berichten gegenüber dem Ministerium des Innern und für Sport, die zur Aufgabenerfüllung entbehrliche Datenerhebung, insbesondere bei erwerbstätigen EU-Bürgern, umgehend eingestellt zu haben.

Die Stadt Fulda berichtete darüber hinaus, dass die Änderung der räumlichen Unterbringung der Ausländerbehörde im Hinblick auf deren im Jahr 2008 geplante Zusammenlegung mit der Ausländerbehörde des Landkreises Fulda bisher ausgesetzt wurde. Es sei ein Umzug der Mitarbeiter der Stadt Fulda in die Gebäude des Landkreises vorgesehen, wenn die Bildung einer gemeinsamen Ausländerbehörde realisiert werde. Auf einen kurzfristigen Umbau der eigenen Räume werde aus diesem Grunde verzichtet. Sofern im Laufe des Jahres 2008 allerdings abzusehen sei, dass die Zusammenlegung der Ausländerbehörden nicht zustande komme, werde die geforderte Änderung der räumlichen Situation alsbald umgesetzt.



## **5.4.2 Elektronische Bearbeitung im Aufenthalts- und Einbürgerungsverfahren**

### **Zu 5.4.2.1 E-Aufenthalt**

Der Hessische Datenschutzbeauftragte beschreibt das mit E-Aufenthalt beabsichtigte Verfahren umfassend in seinem Tätigkeitsbericht.

Zurzeit werden Gespräche, in die der Hessische Datenschutzbeauftragte eingebunden ist, über eine Vereinbarung der beteiligten Dienststellen zur Nutzung einer Schnittstelle geführt. Das zum Datenaustausch eingesetzte Verfahren richtet sich nach Vorschriften des Telekommunikationsgesetzes. Mit der Vereinbarung soll datenschutzrechtlichen Belangen Rechnung getragen werden.

Die Zusammenarbeit mit dem Hessischen Datenschutzbeauftragten gestaltet sich sehr konstruktiv. Mit einem Ergebnis ist in Kürze zu rechnen.

### **Zu 5.4.2.2 E-Einbürgerung**

Der Hessische Datenschutzbeauftragte hat das Ministerium des Innern und für Sport bei der Entwicklung des E-Government-Verfahrens der E-Einbürgerung beratend begleitet. Seit dem 1. Januar 2007 läuft die Anwendung produktiv, sie wird sukzessiv an weitere untere Verwaltungsbehörden ausgerollt. Derzeit arbeiten neben den drei Regierungspräsidien 70 Kommunen, darunter sämtliche kreisfreien Städte sowie die Sonderstatusstädte mit der E-Einbürgerung; sie decken ca. 70 v.H. des Fallaufkommens ab. Bis zum Jahresende werden weitere 70 Gemeinden einbezogen.

## **5.5 Verkehrswesen**

### **Zu 5.5.1 Verfahrensprotokolle beim Kraftfahrt-Bundesamt helfen wirksamen Datenschutz herzustellen**

Die Ausführungen des Hessischen Datenschutzbeauftragten treffen zu. Mit den verantwortlichen Bediensteten wurden Personalgespräche geführt, um sie für Datenschutzfragen zu sensibilisieren.

### **Zu 5.5.2 Keine Auskünfte aus den örtlichen Fahrzeugregistern an die Gebühreneinzugszentrale zur Ermittlung der Gebührenpflicht für Autoradios**

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die GEZ keinen Anspruch auf Auskunft aus den Fahrzeugregistern hat, um säumige Gebührenzahler oder nicht angemeldete Autoradios zu ermitteln.

Aus diesem Anlass erging auch das vom Hessischen Datenschutzbeauftragten erwähnte Rundschreiben an die Kfz-Zulassungsstellen.

Es ist davon auszugehen, dass die Landesrundfunkanstalten das Thema in ihren Arbeitsgruppen erörtern und ggf. im Rahmen der Facharbeitsgruppe der Rundfunkreferenten initiativ werden, damit eine ausreichende Rechtsgrundlage für entsprechende Auskünfte geschaffen werden kann.

## **5.6 Schulen und Schulverwaltung**

### **Zu 5.6.1 LUSD - Zentrale Lehrer- und Schülerdatenbank**

Der Hessische Datenschutzbeauftragte beschreibt die tatsächlichen Gegebenheiten in den Ziffern 5.6.1.3.1 bis 5.6.1.3.3 seines Berichts zutreffend. Jedoch sind ergänzende Anmerkungen erforderlich.

Der Hessische Datenschutzbeauftragte stellt bei der Würdigung des Sachverhalts insbesondere auf die Verantwortlichkeit der Schulleiterin bzw. des Schulleiters nach § 10 HDSG ab. Das Kultusministerium muss bei seinen Implementierungsstrategien jedoch beachten, dass die Schulleitung im vorliegenden Fall im Auftrag "zweier Herren" arbeitet, nämlich im Auftrag des Landes, soweit das Lehrpersonal betroffen ist, und im Auftrag des Schulträgers, soweit es sich um Verwaltungspersonal oder die sächliche Ausstattung der Schulverwaltung handelt. Diese doppelte Verantwortlichkeit kompliziert die Aufgabenerfüllung gerade im Bereich der IT-Sicherheit, die sich immer als ein Bündel technischer, baulicher

und organisatorischer Maßnahmen darstellt (s. auch unten zu Ziff. 5.6.4.1.1 "Umsetzung durch die Schulträger").

Das Kultusministerium hat im Bereich seiner Zuständigkeit schon im Einführungserlass zur zentralen LUSD vom 23. November 2006 (ABl. 12 / S. 1026) die Schulleitungen und die Lehrkräfte zur Beachtung von IT-Sicherheitsregeln verpflichtet. Ergänzend hierzu wurde eine gemeinsame Arbeitsgruppe mit Vertretern der Schulträger eingerichtet, die sich die Verbesserung der IT-Sicherheit an den Schulen und die Klärung gemeinsamer Standards zur Aufgabe gesetzt hat. Der Hessische Datenschutzbeauftragte war an dieser Arbeitsgruppe beteiligt.

Die Einhaltung der Absprache des Kultusministeriums mit dem Hessischen Datenschutzbeauftragten, eine Muster-Vorabkontrolle und ein allgemeines Verfahrensverzeichnis durch schulspezifische Aufzeichnungen ergänzen zu lassen, wurde von den Schulen offensichtlich unterschiedlich umgesetzt. Dabei bleibt aber offen, ob die Stichproben des Hessischen Datenschutzbeauftragten so repräsentativ sind, dass die Feststellung, "die Vorabkontrolle durch die Schulen wurde, soweit ich ersehen konnte, bisher nicht durchgeführt", gerechtfertigt ist.

Mit Abschluss der Entwicklung der LUSD 2008 wird im Benehmen mit dem Hessischen Datenschutzbeauftragten festgestellt werden, ob eine Ergänzung der bisherigen Unterlagen oder eine Neufassung angestrebt werden soll. Wie auch immer diese Entscheidung ausfällt, es wird Anlass sein, den Schulen noch einmal eine aktualisierte Fassung der Unterlagen zur Verfügung zu stellen und sie auf ihre Pflichten hinzuweisen.

In einem Punkt wird die Schule allerdings entlastet werden. Da auf Initiative des Hessischen Datenschutzbeauftragten die LUSD künftig protokollieren wird, welchen Personen zu welchen Zeiten von den Schulen welche Berechtigungen verliehen worden sind, kann die entsprechende Aufzeichnungspflicht für die Schulen entfallen.

#### **5.6.1.4 Ergebnisse weiterer Prüfungen**

##### **Zu 5.6.1.4.1 Umsetzung durch die Schulträger**

Es liegt nicht im Regelungs- und Verantwortungsbereich der staatlichen Schulverwaltung, dass manche Träger für ihre Schulverwaltungen zentrale Administration vorhalten, die keinen Systemzugang vor Ort erlaubt; die Aspekte "Vernichtung von Festplatten" und "Remote-Zugriff" sind ebenso Angelegenheit der Schulträger.

Die Feststellung, dass die Schulträger nur unzureichend vorbereitet gewesen wären und einer stärkeren Hilfestellung durch das Kultusministerium bedurft hätten, berücksichtigt nicht das komplexe Verhältnis zwischen den Schulträgern und der Landesverwaltung.

Die Implementation eines landesweiten Verfahrens stößt auch im Schulbereich auf die Schwierigkeit, dass äußerst unterschiedliche vorhandene IT-Infrastrukturen, aber auch unterschiedliche Ziel- und Prioritätensetzungen integriert werden müssen. Dieser Schwierigkeit versuchte das Projekt LUSD auf zweierlei Weise gerecht zu werden.

Zum einen durch die Übernahme von Kosten, die eigentlich der Schulträger hätte tragen müssen. Dies war vor allem im Projektbereich Schulnetz der Fall. Mit wenigen Ausnahmen verfügten die 33 hessischen Schulträger über kein eigenes abgesichertes Verwaltungsnetz für ihre Schulen. Wie auch vom Hessischen Datenschutzbeauftragten immer wieder beanstandet, waren Verwaltungsrechner ohne besondere Schutzmaßnahmen an das Internet angebunden und unterhielten Postfächer bei bekannten Internet-Providern, obwohl immer wieder darauf hingewiesen wurde, dass dies nicht statthaft war. Das Land Hessen finanzierte daher in diesen Fällen den Aufbau einer abgesicherten Netzverbindung für die Schulverwaltung bis Ende 2009, mit der Maßgabe, dass die Schulträger bis dahin eigene Lösungen anbieten sollten.

Zum anderen durch Reduktion der Anforderungen an Hard- und Software. Bei der Konzeption der zentralen LUSD war eine Grundentscheidung zu treffen, ob an den Schulen ein "Smart-Client" mit eigener Intelligenz vor-

gehalten werden oder eine WEB-Lösung angestrebt werden sollte. Die Entscheidung für eine WEB-Lösung beruhte auf der Einschätzung, dass diese die geringsten Anforderungen an die Verwaltungsrechner und deren Administration stellte und damit der höchst unterschiedlichen Ausstattungsstruktur der Schulträger am Besten gerecht würde. Damit wurden allerdings auch die Anforderungen an die zentrale Lösung deutlich erhöht.

Für übergreifende Projekte wirkt es sich an dieser Stelle als besonders belastend aus, dass seitens der Schulträger keine gemeinsamen Standards für die Ausstattung der Schulverwaltungen, aber wohl auch für die Ausstattung der Verwaltungen generell - etwa mit Hilfe der Spitzenverbände - entwickelt wurden. Damit fehlte eine solide Planungsbasis für derart übergreifende Projekte, die auch durch eine "Hilfestellung" seitens des Kultusministeriums nicht hätte ersetzt werden können.

#### **Zu 5.6.1.4.2 Unberechtigte Zugriffe auf die Daten der LUSD**

Das aufgetretene Problem ist zutreffend beschrieben. Ergänzend sei darauf hingewiesen, dass die Leiter der betroffenen Schulen korrekterweise sofort die örtliche Schulaufsicht und das Fachreferat im Kultusministerium informierten, sodass innerhalb eines Tages die Fehlersuche und -behebung gestartet werden konnte.

#### **Zu 5.6.1.4.3 Internet-Nutzung**

Auch hier löst das Schulverwaltungsnetz eine vorher bestehende potenziell gefährliche Situation auf. Für die Internet-Zugänge galt das Gleiche, was bereits über Postfächer bei Internet-Providern gesagt wurde. Hier haben der Hessische Datenschutzbeauftragte und das Kultusministerium das gleiche dringende Interesse, restliche bestehende "illegale" Zugänge aufzuspüren und stillzulegen.

#### **Zu 5.6.2 Änderung der Meldedatenübermittlungsverordnung zur Überwachung der Schulanmeldungen**

Der Tätigkeitsbericht befasst sich mit der Entstehung der Verordnung zur Änderung der Meldedaten-Übermittlungsverordnung (MeldDÜVO), die am 6. Februar 2008 erlassen und im Gesetz- und Verordnungsblatt vom 6. März 2008 (GVBl. I S. 28) verkündet worden ist. Die im Übrigen zutreffenden Ausführungen geben dabei im letzten Absatz nicht den letzten Stand der Entwurfsfassung wieder. Durch die Änderungsverordnung hat § 17 Abs. 1 und 2 MeldDÜVO eine neue Fassung erhalten. Danach erfolgen die Datenübermittlungen nunmehr an die jeweils zuständige Grundschule. Der bisherige Datenempfänger, das "Schulverwaltungsverfahren Lehrer- und Schülerdatenbank" (LUSD) wurde herausgenommen. Die Neufassung berücksichtigt das tradierte Verwaltungsverfahren im Bereich der Übermittlung von Meldedaten an Schulen zum Zwecke der Überwachung der Schulpflicht und konkretisiert die Norm ohne Änderung der bestehenden Übermittlungspraxis. Zugleich ermöglicht die offene Formulierung in Bezug auf den eigentlichen Übermittlungsvorgang eine künftige elektronische Übermittlung, um so das Verwaltungshandeln der Meldebehörden zu vereinfachen und über eine zentrale Datenverarbeitung eine Entlastung der übermittelnden Stellen zu erreichen.

#### **Zu 5.6.3 Verfahren zum Nachteilsausgleich für schwerbehinderte Lehrkräfte gemäß der Pflichtstundenverordnung**

Das Kultusministerium wird alle staatlichen Schulämter durch Erlass auffordern, die vom Hessischen Datenschutzbeauftragten vorgeschlagenen Formulierungen zu verwenden.

#### **Zu 5.6.4 Datenschutzfragen bei der Erstellung und Behandlung von Schülerfotos**

Den Schulen ist bekannt, dass die Organisation von Fototerminen sich lediglich auf die Organisation von Termin und Gelegenheit zu beschränken hat und dies die Rechtsbeziehung zwischen Eltern, Schülern und Schule nicht berührt.

Das Kultusministerium prüft zurzeit, ob ein allgemeiner Hinweis an alle Schulen tatsächlich erforderlich ist oder ob es sich bei dem im Bericht ge-

nannten Fall um einen Einzelfall von Unkenntnis der Rechtslage handelt. Gegebenenfalls wird ein entsprechender Hinweis durch Erlass erfolgen.

## **5.7 Umwelt und Geologie**

### **Zu 5.7.1 Veröffentlichung von Standort-, Funktions- und Eigenschaftskarten**

Die Frage, inwieweit die Veröffentlichung von Geodaten datenschutzrechtlichen Voraussetzungen genügt, spielt bei verschiedenen Verwaltungsaufgaben eine Rolle. Daher wurden die Themen "Geodaten im Internet", "Herausgabe von Geodaten aufgrund einer entsprechenden Vereinbarung" und die "Abgabe von Geodaten im Rahmen von Anfragen gegenüber dem Amt für Bodenmanagement" im Ministerium für Umwelt, ländlichen Raum und Verbraucherschutz datenschutzrechtlich geprüft. Bei strenger Beachtung der im 36. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten dargelegten Rechtsauffassung könnten die mit diesen Aufgaben verbundenen Ziele (z.B. Öffentlichkeitsarbeit) nur ganz eingeschränkt erreicht werden. Europäische Vorgaben, wie z.B. die Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (die sog. "INSPIRE-Richtlinie"), sehen dagegen neue und weitreichendere Anforderungen an die Verbreitung von Umwelt- bzw. Geodaten vor. INSPIRE steht für "Infrastructure for Spatial Information in Europe" und aufgrund der Richtlinie müssen die in den Behörden der Mitgliedstaaten vorhandenen, qualitativ hochwertigen Geodaten unter einheitlichen Bedingungen (Europäische Geodateninfrastruktur) Bürgern, Verwaltungen und der Wirtschaft zugänglich gemacht werden. Dadurch soll die Formulierung, Umsetzung und Bewertung europäischer und nationaler Politikfelder unterstützt werden. Seitens der deutschen Geoinformationswirtschaft wird die Richtlinie ausdrücklich begrüßt, schafft sie doch Transparenz und Planungssicherheit und beseitigt Markthemmnisse. Die Umsetzung der INSPIRE-Richtlinie in nationales Recht hat innerhalb einer Frist von zwei Jahren zu erfolgen.

Um das rechtliche Spannungsverhältnis zwischen den weitreichenden europäischen Vorgaben und dem Hessischen Datenschutzgesetz vor dem Hintergrund der Ausführungen im 36. Tätigkeitsberichts des Hessischen Datenschutzbeauftragten zu diskutieren und zu bewerten, plant das Ministerium für Umwelt, ländlichen Raum und Verbraucherschutz alsbald ein Gespräch mit dem Hessischen Datenschutzbeauftragten und dem Ministerium für Wirtschaft, Verkehr und Landesentwicklung zu führen.

## **5.8 Gesundheitswesen**

### **5.8.1 Hessisches Gesetz über den öffentlichen Gesundheitsdienst**

#### **Zu 5.8.1.1 Klarstellung der Unterscheidung zwischen Aufgabenzuweisungen und Befugnissen zur Verarbeitung personenbezogener Daten**

Die Erhebung und Speicherung von personenbezogenen Daten ist derzeit nur vorgesehen im Rahmen der Schuleingangsuntersuchung. Die Erhebung, Verarbeitung und Weiterleitung dieser Daten ist in der Verordnung zur Schulgesundheit festgelegt.

#### **Zu 5.8.1.2 Regelung zur Kinder- und Jugendgesundheit (§ 10)**

Nach Auffassung der Landesregierung ist keine Änderung zur vorherigen Rechtslage eingetreten. Nach der Rechtsverordnung zur Schulgesundheit (Verordnung über die Zulassung und die Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege) können über die Schuleingangsuntersuchung hinaus Untersuchungen vorgenommen werden. Ob und in welchen Fällen dies erfolgt, entscheiden die Landkreise und kreisfreien Städte; je nach regionalen Besonderheiten werden zusätzlich z.B. Untersuchungen von Jugendlichen angeboten. Die Verarbeitung dabei gewonnener Daten richtet sich nach der benannten Verordnung.

### **5.8.1.3 Regelung zum Datenschutz (§ 18)**

#### **Zu 5.8.1.3.1 Verfahren bei der Erstellung von Gutachten (Abs. 1)**

Das Verfahren wird von den Gesundheitsämtern wie beschrieben durchgeführt, die Übermittlung von medizinischen Daten erfolgt also nur, wenn angefragt wurde und das Einverständnis der betroffenen Person vorliegt.

#### **Zu 5.8.1.3.2 Pauschale Befugnis zur Erhebung der Meldedaten aller Neugeborenen (Abs. 2)**

Eine erneute Prüfung durch das Sozialministerium hat ergeben, dass die Vorschrift nach Verabschiedung des Hessischen Gesetzes zur Verbesserung des Gesundheitsschutzes für Kinder vom 14. Dezember 2007 entbehrlich ist. Bei einer Novellierung des Hessischen Gesetzes über den öffentlichen Gesundheitsdienst soll die Vorschrift aufgehoben werden.

#### **Zu 5.8.1.3.3 Gewährleistung der Geheimhaltungspflichten und der Zweckbindung der personenbezogenen Daten in den Gesundheitsbehörden**

Nach Auffassung der Landesregierung ist die Formulierung eindeutig und umfasst auch die Aufbewahrung und Herausgabe von Akten.

#### **Zu 5.8.1.3.4 Vorgaben zur Dauer der Datenspeicherung**

Die Dauer der Aufbewahrung von Daten ist von der Zweckbestimmung abhängig und daher je nach Art der Daten unterschiedlich geregelt. Unklarheiten bestanden im letzten Jahr über die Dauer der Aufbewahrung von Meldungen über Läusebefall. Inzwischen wurde eine Aufbewahrungsfrist von 1 Jahr festgelegt und dies auch dem Hessischen Datenschutzbeauftragten mitgeteilt.

#### **Zu 5.8.1.3.5 Verweis auf das Hessische Datenschutzgesetz (Abs. 4)**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

### **Zu 5.8.2 Kindergesundheitsschutz-Gesetz**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

### **Zu 5.8.3 Forschungsprojekt CIMECS zur einrichtungsübergreifenden elektronischen Fallakte**

Das Projekt "CIMECS" (ursprünglich "IT-Modellierung einer Plattform zur Steuerung sektorübergreifender Behandlungsprozesse im Rahmen der integrierten Versorgung") wird seit dem Jahr 2005 vom Ministerium für Wirtschaft, Verkehr und Landesentwicklung gefördert. Projektträger ist das Universitätsklinikum Gießen und Marburg.

In dem Förderbescheid vom November 2005 hat sich der Projektträger verpflichtet, alle erforderlichen datenschutzrechtlichen Bestimmungen bei der Entwicklung der Kommunikationsplattform einzuhalten sowie die Kompatibilität des Portals mit der elektronischen Gesundheitskarte zu gewährleisten.

Der Projektträger hat das Projekt dem Hessischen Datenschutzbeauftragten bekannt gemacht. Die im 36. Tätigkeitsbericht aufgeführten offenen Fragen werden zurzeit zwischen dem Hessischen Datenschutzbeauftragten und dem Projektträger mit dem Ziel einer einvernehmlichen Lösung erörtert.

### **Zu 5.8.4 Prüfung der Datenverarbeitung ausgewählter Gesundheitsämter**

Das Regierungspräsidium Darmstadt wird im Auftrag des Sozialministeriums eine Umfrage bei den Gesundheitsämtern durchführen, welche medizinischen Unterlagen dort anfallen und inwieweit deren Aufbewahrungsfristen festgelegt sind. Die Auswertung der Umfrage wird dem Sozialministerium

vorgelegt werden. Das Sozialministerium beabsichtigt, die Aufbewahrungsfristen zusammenzustellen und im Erlasswege zu regeln.

Im Übrigen stimmt die Landesregierung den Ausführungen des Hessischen Datenschutzbeauftragten zu.

#### **Zu 5.8.5 Prüfung beim MDK Sachsen-Anhalt**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

#### **Zu 5.8.6 Prüfung beim Klinikum Fulda**

Die Landesregierung stimmt der Bewertung des Hessischen Datenschutzbeauftragten zu.

#### **Zu 5.8.7 Unzulässiges Einwilligungsfomular der AOK Hessen**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

#### **Zu 5.8.8 Bilder von Neugeborenen auf der Homepage von Krankenhäusern**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

### **5.9 Sozialwesen**

#### **Zu 5.9.1 Feststellung der Pflegebedürftigkeit bei Anträgen auf Sozialhilfe**

Das beschriebene Verfahren betrifft die Ausführung des SGB XII im Rahmen der kommunalen Selbstverwaltung. Über die Verfahrensweise wurde ausweislich des Tätigkeitsberichts sowie eines vom Sozialministerium angeforderten Berichts des Sozialamts der Stadt Frankfurt Übereinstimmung erzielt. Nach Rückmeldung des örtlichen Sozialamts der Stadt Frankfurt wurde das in Rede stehende Einwilligungsfomular mittlerweile überarbeitet und zunächst dem Datenschutzbeauftragten der Stadt Frankfurt am Main zur Würdigung vorgelegt. Eine Rückmeldung von diesem stand bei Redaktionsschluss für diese Stellungnahme noch aus. Die Landesregierung geht nach dem bisherigen Verlauf des Kontakts und der Absprachen zwischen dem Hessischen Datenschutzbeauftragten und der Stadt Frankfurt davon aus, dass die von dem Hessischen Datenschutzbeauftragten im Rahmen seiner Prüfung angesprochene Problematik einvernehmlich bereinigt werden wird.

#### **Zu 5.9.2 Hartz IV - Datenerhebung bei Dritten**

Die Landesregierung stimmt der Auslegung des § 67a SGB X durch den Hessischen Datenschutzbeauftragten in Bezug auf die Erhebung von Daten über den Leistungsempfänger bei einem Dritten, z.B. dem Vermieter, im Zusammenhang mit Erkundigungen zu einem vermuteten Sozialleistungsbruch zu.

#### **Zu 5.9.3 Übermittlung von Sozialdaten durch das Jugendamt an das Familiengericht**

Die Landesregierung war in dieser Angelegenheit der kommunalen Selbstverwaltung nicht beteiligt. Sie stimmt gleichwohl der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die Übermittlung der Sozialdaten durch die Übersendung der Akte des Jugendamts an das Familiengericht nach § 64 Abs. 2 SGB VIII, § 69 Abs. 1 Nr. 2 SGB X zulässig war. Das Gericht ist auf die Übermittlung der Daten angewiesen, da es im familiengerichtlichen Verfahren die für die Entscheidung erforderlichen Tatsachen nach § 12 FGG von Amts wegen zu ermitteln hat.

#### **Zu 5.9.4 Datenschutzbeauftragter bei Trägern der freien Kinder- und Jugendhilfe**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

## **5.10 Personalwesen**

### **Zu 5.10.1 Personalakteneinsicht durch Innenrevision**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Die Darstellung der Auffassung des Hessischen Datenschutzbeauftragten im Tätigkeitsbericht dient der Rechtssicherheit in der Landesverwaltung, da sie nicht nur auf die Rechtmäßigkeit der Personalakteneinsicht durch die Innenrevision abstellt, sondern auch die Grenzen der Einsichtnahme aufgezeigt werden.

Der Hessische Datenschutzbeauftragte weist darüber hinaus zutreffend darauf hin, dass der Bund beabsichtigt, den Zugang der Innenrevision zur Personalakte gesetzlich ausdrücklich klarzustellen (vgl. Entwurf eines Gesetzes zur Neuordnung und Modernisierung des Bundesdienstrechts, Dienstrechtsneuordnungsgesetz - DneuG, Art. 1 Bundesbeamten-gesetz, § 107 Abs. 2 Satz 2, BR Drucks. 720/07, S. 47). Die Aufnahme einer solchen klarstellenden Regelung in das Hessische Beamten-gesetz wird im Rahmen der Dienstrechtsreform geprüft werden.

### **5.10.3 Personaldatenverarbeitung mit SAP R/3 HR**

#### **5.10.3.1 Download-Berechtigungen**

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die Vergabe der Download-Berechtigungen aus den im Tätigkeitsbericht genannten Gründen restriktiv erfolgen muss.

Eine Überprüfung durch die Ressorts hat bislang ergeben, dass eine restriktive Vergabe erfolgt ist. In Einzelfällen hat sie zur Löschung von Download-Berechtigungen geführt. Bei dem Ministerium der Justiz dauert die Überprüfung bei Redaktionsschluss für diese Stellungnahme noch an. Im Rahmen der Überprüfung ist erneut auf § 7 Abs. 2 der Erklärung des Ministeriums des Innern und für Sport zur Einführung von SAP HR hingewiesen worden. Darin heißt es:

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

Anwender, die aufgrund anderer Anwendungen über eine WTS-Up-Download-Berechtigung verfügen, können diese auch in SAP nutzen. Seit dem Release-Wechsel bei SAP HR können die Berechtigungen so angepasst werden, dass der jeweilige Anwender auch bei Vorhandensein einer WTS-Up-Download-Berechtigung nur exportieren oder importieren kann, sofern er explizit in SAP über die technische Berechtigung verfügt. Im Rahmen des Release-Wechsels bei SAP HR wurde im Jahr 2007 versucht, diese WTS-unabhängige Berechtigungsprüfung zu aktivieren. Dieses Vorhaben ist aber zunächst daran gescheitert, dass bei einer Aktivierung die für SAP HR extra entwickelten WORD-Serienbrief-Funktionalitäten nicht mehr nutzbar gewesen wären.

Die Landesregierung beabsichtigt, Lösungsansätze zu erarbeiten, damit eine Realisierung der WTS-unabhängigen Berechtigungsprüfung in SAP HR erfolgen kann, ohne weitere negative Auswirkungen innerhalb des SAP-Systems zu verursachen.

#### **5.10.3.2 Löschung von Daten im SAP R/3 HR-System**

Wie der Hessische Datenschutzbeauftragte zutreffend darstellt, war die Löschung kompletter Personalstammsätze sowie einzelner Infotypen, wie z.B. Krankheits- oder Abwesenheitsdaten, im SAP-Standard zunächst nicht vorgesehen.

Die Anforderungen der hessischen Landesverwaltung wurden im Dezember 2005 an die SAP AG adressiert. Die entsprechenden Funktionalitäten und Standard-Löschreports stehen erst mit dem Release SAP ERP 6.0 zur Verfügung. Dieser Release-Stand ist in Hessen seit Ende Juni 2007 produktiv.

Bei den anschließenden Tests des Standard-Reports zur Löschung von Personalstammsätzen kam es zu Fehlermeldungen. Diese machen weitere Testaktivitäten erforderlich, in die auch direkt der Entwicklungsbereich der SAP AG einbezogen werden wird.

Der von der SAP AG bereitgestellte Beispielreport für das Löschen einzelner Infotypen löscht nur die Daten in den jeweiligen Infotypen. Auf in den Abrechnungsklustern stehende abgeleitete Daten hat der Report keine Auswirkungen. Die dadurch bewirkten Inkonsistenzen in den Datensätzen sind allen Beteiligten bewusst und werden in Kauf genommen.

Das Löschen einzelner Infotypen ist allerdings nur außerhalb einer noch für das Land festzulegenden Rückrechnungstiefe möglich. Hier gibt es derzeit noch unterschiedliche Anforderungen für die Bereiche des aktiven Personals und der Versorgungsempfänger. Dieser Punkt befindet sich derzeit in Klärung; eine Entscheidung zur Rückrechnungstiefe wird kurzfristig angestrebt.

Das vom Kultusministerium gefertigte Konzept zur Löschung von Bewerberdaten in SAP R/3 wurde nach Abstimmung der konkreten Anforderungen sowie Aufnahme von Ergänzungen Ende 2007 in Abstimmung mit dem Hessischen Datenschutzbeauftragten Anfang des Jahres 2008 nochmals überarbeitet und angepasst. Nunmehr wird eine Löschung der Daten direkt im SAP-System erfolgen, ohne den ursprünglich vorgesehenen Zwischenschritt, die Daten zur Prüfung und ggf. Korrektur mit einem Report zunächst im Excel-Format abzulegen und anschließend zum endgültigen Löschen in die Selektionsmaske hochzuladen. Nach Durchführung der erforderlichen Programmier- und Testarbeiten ist die Produktivsetzung dieser Alternativlösung für Mai bzw. spätestens Juni 2008 vorgesehen.

Die vom Hessischen Datenschutzbeauftragten auch zukünftig vorgesehene zeitnahe und konkrete Überprüfung der Löschkonzepte wird von der Landesregierung ausdrücklich begrüßt. Die von der Landesregierung angestoßenen Verbesserungen tragen den datenschutzrechtlichen Anforderungen an die Löschung von Daten Rechnung.

### **Zu 5.10.3.3 Konzept "Zentraler Zugriff"**

Das vom Hessischen Datenschutzbeauftragten angesprochene Diskussionspapier enthält Vorschläge einer interministeriellen Arbeitsgruppe zur Änderung der §§ 107 ff HBG.

Kern des Papiers ist, dass den übergeordneten Dienstbehörden auch zur Ausübung von Aufsichts- und Kontrollbefugnissen oder zur Erstellung von Auswertungen im Bereich der Personalverwaltung und Personalwirtschaft in einem automatisierten Personalverwaltungssystem der Zugriff auf Personalaktendaten gestattet wird, soweit dies erforderlich ist. Hierdurch soll den obersten Dienstbehörden auch im Fall der Aufgabendelegation ermöglicht werden, ihrer Gesamtverantwortung nach § 4 HBG nachkommen zu können.

Neben dem Aspekt der Dienst- und Fachaufsicht ergibt sich die Notwendigkeit von Zugriffsrechten auf Personaldaten des nachgeordneten Bereichs auch aus sonstigen originären Aufgabenstellungen der Ministerien, etwa im Bereich der ressortweiten Personalbewirtschaftung und Personaleinsatzplanung (vergleichende Personalausstattung, übergreifende Stellenbesetzungsentscheidungen / Personalrekrutierungen u.a.m.).

Zudem soll klargestellt werden, dass die §§ 107 ff. HBG nicht nur für Personalaktendaten in Papierform, sondern auch in elektronischer Form bzw. in einem automatisierten Personalverwaltungssystem gelten. Im Zuge der Einführung moderner Systeme der Vorgangsbearbeitung im Personalaktenwesen besteht ein Bedürfnis für das Führen sogenannter Hybridakten und die Verwendung automatisierter Personalverwaltungssysteme. Auch bei der "gemischten Aktenführung" verbleibt es begrifflich bei einer Personalakte, weil auf den materiell-rechtlichen Begriff der Personalaktendaten abzustellen ist.



Im Hinblick auf das "Merkmal Z" geht der Hessische Datenschutzbeauftragte von der Annahme aus, mit der Ansiedelung der Zuständigkeit für diesen Personenkreis auf Ministeriumsebene entfielen automatisch die Notwendigkeit des Zugriffs auf diese Personalfälle bei den nachgeordneten Instanzen. Dies ist jedoch nicht der Fall, denn charakteristisch ist hier eine arbeitsteilige Bearbeitung auf allen Verwaltungsebenen mit jeweils spezifischer eigener Aufgabenstellung. Während im Ministerium die Entscheidungen über statusberührende Personalmaßnahmen getroffen werden, liegen die Aufgabenstellungen der Mittelbehörde im Bereich des Beurteilungswesens, der Aus- u. Fortbildung und im Bereich der Berichtsvorlagen zur Vorbereitung bestimmter Personalentscheidungen. Der Ortsinstanz obliegt die Personalaktenführung, sowie das "operative Tagesgeschäft" (Gewährung von Urlaub, Dienstbefreiung, Genehmigung von Nebentätigkeiten usw.). Gerade diese ineinandergreifenden aber auch parallelen Aufgabenstellungen setzen Zugriffsrechte auf allen drei Behördenebenen im Sinne einer effizienten Nutzung des SAP-Systems zwingend voraus. Der Ansatz des Hessischen Datenschutzbeauftragten, schreibende Zugriffsrechte in den Ministerien und lesende Rechte in der Beschäftigungsdienststelle seien hier ausreichend, wird den Erfordernissen mehrstufiger Verwaltungen nicht gerecht.

Unter Federführung des Ministeriums der Finanzen wurde ein konkreter Vorschlag für eine Gesetzesänderung des hessischen Personalaktenrechts unter den beteiligten Ressorts abgestimmt. Mit einer Überarbeitung der §§ 107 ff HBG soll den Bedürfnissen der Verwaltung bei der Nutzung des SAP Systems Rechnung getragen werden.

Das Ministerium der Finanzen hat diesen Vorschlag dem Hessischen Datenschutzbeauftragten vorgestellt und die entsprechende Begründung ausführlich in zwei Besprechungen im Juli und November 2007 dargelegt.

Der Hessische Datenschutzbeauftragte räumt im vorletzten Absatz seiner Ausführungen ausdrücklich ein, dass Ministerien im Einzelfall die Möglichkeit haben müssen, im Rahmen ihrer Dienst- und Fachaufsicht auf Daten der Beschäftigten des nachgeordneten Bereichs zugreifen zu können, wie dies in der Vergangenheit auch der Fall war.

Die Landesregierung geht deshalb davon aus, dass ein weiterer und vertiefter Austausch der Begründungen eine einvernehmliche Lösung herbeiführen kann.

#### **5.10.3.4 Personalkostenhochrechnung**

Die Landesregierung stimmt der Feststellung des Hessischen Datenschutzbeauftragten zu, dass es in der Landesverwaltung keine einheitliche Vorgehensweise bei der Personalkostenhochrechnung gibt.

Die Landesregierung hält die Möglichkeit des Zugriffs auf die Einzelabrechnungen des Personals durch das Ministerium, insbesondere das im Bereich des Kultusministeriums angewendete Verfahren, für erforderlich. Die zahlenmäßige Größenordnung des in diesem Ressort beschäftigten Personals stellt besondere Anforderungen an die Personalkostenhochrechnung, um die notwendige verlässliche Haushaltsplanung und -überwachung zu gewährleisten.

Die SAP-Personalkostenhochrechnung (PKPL) ist im Zuge des Einführungs- und Entwicklungsprojekts (ENVS und LRM HR) landesweit eingeführt worden. Für die Lehrkräfteverwaltung wird bereits seit dem Jahr 2004 die PKPL produktiv eingesetzt. Die Nutzung der PKPL ist für die monatliche Personalausgabenmeldung an das Ministerium der Finanzen und die halbjährliche Meldung an den Hessischen Landtag zu einem unerlässlichen Werkzeug geworden. Im Jahr 2004 erzielte das Kultusministerium eine sehr gute Prognose mit der PKPL von nur 0,04 v.H. Abweichung von der März-Prognose und dem IST-Jahresergebnis. Es handelt sich also um ein Instrument, dass auf der Basis einer individuellen Berücksichtigung von Abrechnungsergebnissen einen sehr hohen Genauigkeitsgrad erlangen kann.

Der Haushalt des Kultusressorts beinhaltet den größten Personalausgabenblock des Landes (rd. 2,5 Mrd. €). In keinem anderen Ressort muss bei der Prognose des voraussichtlichen Personalmittelbedarfs mitten im Haushaltsjahr ein Schuljahreswechsel mit einer sehr hohen Fluktuationsrate (ca. 1.500 Neueinstellungen, mehrere tausend neue Vertretungsverträge, mehrere tausend neue Abordnungen) verarbeitet werden. Eine Abweichung von nur 0,5 v.H. hat eine finanzielle Auswirkung von über 12,0 Mio. €. Die vorgelegten

Ergebnisse sind Grundlage für Berichte an den Hessischen Landtag und dienen als Basis für die Veranschlagung von Mehrbedarfen in Nachtragshaushalten. Der Hessische Landtag erwartet - völlig zu Recht - die Meldung eines realistischen Bedarfs. Dies ist nur zu erreichen, wenn die Ergebnisse der Hochrechnungen in SAP, die regelmäßig mit sehr hohem Aufwand erstellt werden, einer umfassenden Qualitätskontrolle unterzogen werden. Um diesen hohen Qualitätsstandard für das Kultusministerium sicherzustellen, sind Plausibilitätsprüfungen ggf. bis auf die Ebene des Einzelfalls notwendig.

Sowohl im Rahmen des Entwicklungsprojekts Landesreferenzmodell SAP/HR PKPL als auch im Kultusministerium wurde den Vertretern des Hessischen Datenschutzbeauftragten an Hand von Beispielen die Notwendigkeit des Einzelzugriffs erläutert, u.a. auch im SAP-System. Dabei äußerten sie durchaus Verständnis dafür, dass der Zugriff in bestimmten Fällen notwendig ist.

Nach Aufforderung durch den Hessischen Datenschutzbeauftragten wurde das Entwicklungsteam daher aufgefordert, das PKPL-Sollkonzept im Hinblick auf die Rolle des Hochrechners wie folgt zu ergänzen:

"Der Ressorthochrechner liefert monatliche Hochrechnungsergebnisse über die Entwicklung der Personalausgaben für den Haushaltsbeauftragten des Ressorts sowie für das Hessische Ministerium der Finanzen. Hochrechnungen werden grundsätzlich dezentral nach Ressortvorgaben erstellt. Im Rahmen der Aggregation der Hochrechnungsdaten muss jedoch eine Nachprüfbarkeit auch für den Einzelfall an zentraler Stelle gewährleistet sein."

Das Sollkonzept wurde mit dieser Ergänzung vom Projektausschuss abgenommen.

Um die jahresbezogene Hochrechnung zu erstellen, müssen Kosten eingeplant werden, die noch nicht durch die Abrechnung und die anschließende Simulation der personenbezogenen Personalausgaben im System erfasst sind. Die Pflege von vakanten Planstellen stellt daher eine wichtige Planungsgröße dar. Zudem muss im Lehrkräftebereich der Vertretungsbedarf prognostiziert werden. Die Planungsgrößen "vakante Planstellen" und "Vertretungsbedarf" stehen in Beziehung zueinander und dürfen nicht isoliert betrachtet werden. Um plausible Hochrechnungsergebnisse zu erhalten, müssen die Planungsgrößen sorgfältig kalkuliert werden.

Von zentraler Stelle ist auch regelmäßig das Systemverhalten zu überprüfen. Das über die Jahre weiterentwickelte Landesreferenzmodell (LRM HR) berücksichtigt viele ressortspezifische Anforderungen, die Auswirkungen auf die Personalkostenhochrechnung haben. Auch Jahre nach der Einführung müssen zum einen durch die hohen Fluktuationszahlen (s.o.) neue Eingabefehler zum anderen immer noch feststellbare Systemfehler behoben werden. Diese laufenden Überprüfungen sind notwendig, weil Systemanpassungen in den anderen Modulen unmittelbare Auswirkungen auf die PKPL haben können.

Aktuelle Systemfehler in der SAP-Hochrechnung werden nach dem Geschäftsprozessmodell der Personalkostenplanung zunächst ressortintern geklärt. Dies entspricht dem Konzept des Projektbüros Marburg. Auftretende Probleme betreffen oft das gesamte Ressort, daher benötigt der Ressorthochrechner die ressortweite Berechtigung.

Der Zugriff auf die Einzelabrechnungsergebnisse ist zudem notwendig, um bestimmte Analysen zur Beurteilung des Hochrechnungsergebnisses durchzuführen:

- Ermittlung von Fallzahlen (z.B. Fälle Mutterschutz, Elternzeit)
- Überprüfung der Datenqualität (Pflege IT 9001)
- Ermittlung der Personalausgaben für Neueinstellungen
- Ermittlung der IST-Ausgaben
- Ermittlung der Ausgaben für einzelne Kostenbestandteile (z.B. Einmalzahlung, Urlaubsgeld, Sonderzuwendung)
- Erstellung von Zeitreihen für die o.g. Tatbestände

Nach Auffassung der Landesregierung ist es erforderlich, hinsichtlich der Datenqualität das bestmögliche Ergebnis zu erreichen. Eine gewisse Fehler-toleranz ohne weiteres zu akzeptieren, weil es sich um eine Hochrechnung handelt, würde deren Aussagegehalt erheblich mindern. Aus Sicht der Landesregierung muss die SAP-Datenbasis korrekt sein, um plausible Hochrechnungen durchführen zu können. Treten z.B. bei Personen mit einer bestimmten Abfolge von Maßnahmen Fehler auf, können diese bei einer

hohen Fallzahl gravierende Auswirkungen auf die Hochrechnungsergebnisse haben.

Für den Lehrerbereich sind zeitnahe Auswertungen erforderlich, die nur personenbezogen und amtsübergreifend erfolgen können. Für Verwendungsnachweise aus EU-Projekten (EIBE, SchuB, RegNets etc.) werden bisher die Personalnummern der betroffenen Lehrkräfte zur Verfügung gestellt. Dies ist die Grundlage, die exakten Kosten auf Landesebene aus HR zu ermitteln. Bei Nichtvorliegen der schulamtsübergreifenden Berechtigung wäre eine Abfrage bei fünfzehn Staatlichen Schulämtern erforderlich. Der Aufwand ist nicht zu vertreten. Dem Ministerium obliegt die Verantwortung für die Richtigkeit der Verwendungsnachweise.

Für die Altersteilzeit muss regelmäßig der exakte Bedarf ermittelt werden, da im Lehrerbereich der jährliche Bedarf veranschlagt wird. Eine pauschale Veranschlagung führte in der Vergangenheit zu Abweichungen von über 20 Mio. €. Eine übergreifende Auswertung ermöglicht eine individuelle monatliche finanzielle Betrachtung der ATZ-Fälle. Nur so können die exakten Einsparbeiträge in der Arbeitsphase und die Belastungen in der Freiphase saldiert werden. Das Ministerium muss bei der Aufstellung des Haushalts die exakten Bedarfe nachweisen. Im Hinblick auf die Größenordnung (50 bis 70 Mio. €) muss das Ministerium in der Lage sein, auch Einzelergebnisse überprüfen zu können, um eine Unter- oder Überveranschlagung zu vermeiden.

Die Verantwortung für die Hochrechnungsergebnisse dem Hessischen Landtag gegenüber liegt eindeutig im Kultusministerium. Im Hinblick auf die Höhe des größten Personalausgabenblocks innerhalb der Landesverwaltung ist eine Notwendigkeit zur zentralen Überprüfung der von den nachgeordneten Bereichen angelegten Planungsgruppen auf Einzeldatenbasis unabdingbar. Für die beschriebenen Auswertungsbedarfe gibt es dienstlich-sachliche Erfordernisse.

Die Landesregierung beabsichtigt, die nach ihrer Auffassung im Rahmen der Personalkostenhochrechnung erforderliche Verarbeitung von Personaldaten auf eine sichere rechtliche Grundlage zu stellen. Der oben zitierte Vorschlag zur Änderung der §§ 107 ff HBG (siehe zu Ziffer 5.10.3.3) würde zugleich den Anforderungen der Personalkostenhochrechnung genügen. Die Landesregierung strebt in der weiteren Erörterung des Vorschlags mit dem Hessischen Datenschutzbeauftragten an, auch insoweit zu einer einvernehmlichen Lösung zu gelangen.

#### **5.10.3.5 Business-Warehouse-HR (HEPISneu)**

Das Vorprojekt Business Warehouse HR/"HEPISneu" hatte entgegen der Darstellung des Hessischen Datenschutzbeauftragten eindeutige inhaltliche Vorgaben. Es wurden Anforderungen und Zielgruppen eines Gesamt-Personal-Berichtswesens (operatives HR-System und Business Warehouse) definiert sowie eine Projekt- und Aufwandsplanung erstellt, auf deren Grundlage ein Realisierungsprojekt "HEPISneu" nach Beschluss des Kabinettsausschusses Verwaltungsreform und Verwaltungsinformatik vom 25. März 2008 im April 2008 gestartet wurde.

Die Bedenken des Hessischen Datenschutzbeauftragten hinsichtlich der Auswertung personenbezogener Daten in einem Business Warehouse wurden vom Steuerungsgremium des Vorprojekts dahingehend berücksichtigt, dass die Entscheidung getroffen wurde, in einem Business Warehouse aggregierte (nicht personenbezogene) Berichte zur Verfügung zu stellen. Personenbezogene Auswertungen sollen nur im operativen HR-System erstellt werden.

Die Landesregierung hofft auf eine weitere offene und konstruktive Zusammenarbeit und Beratung durch den Hessischen Datenschutzbeauftragten.

## **6. Kommunen**

### **Zu 6.1 Ergebnisse der Prüfung von Kommunen**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

### **Zu 6.2 Speicherung von Wahlhelferdaten**

Die Gewinnung von ehrenamtlichen Wahlhelfern für die Besetzung der Wahlvorstände stellt für die dafür zuständigen Gemeinden seit Jahren eine ebenso schwierige wie verantwortungsvolle Aufgabe dar. Die Leitung der Wahlhandlung soll für das Wahlrecht auf allen Ebenen von autonomen, aus dem Kreis der Wahlberechtigten rekrutierten Wahlorganen und damit nicht von der Verwaltung als solcher vorgenommen werden. Dies macht es notwendig, Ehrenamtliche zu finden, die bereit sind, für ein geringes sogenanntes Erfrischungsgeld Dienst an den Wahlsonntagen zu tun. Die Bereitschaft hierzu ist bei regionalen Unterschieden insgesamt eher gering. Gleichzeitig erfordert die Aufgabe eines Mitglieds im Wahlvorstand genaue Kenntnisse des formellen und materiellen Wahlrechts; eine diesbezügliche Vorbildung oder vorhandenes Erfahrungswissen prädestiniert Betroffene für die Funktion des Wahlvorstehers und des Schriftführers.

Als Hilfsmittel für die Gemeinden gibt es im Bundes- und Landeswahlrecht die vom Hessischen Datenschutzbeauftragten referierte Behördenklausel sowie die Befugnis, die Daten von geeigneten Bürgerinnen und Bürgern für die Besetzung von Wahlvorständen bei künftigen Wahlen zu verarbeiten. Mit der Speicherung geht die Verpflichtung einher, die Betroffenen über ihr Recht zu informieren, der in Rede stehenden Datenverarbeitung zu widersprechen.

Das Ministerium des Innern und für Sport hat die Beobachtung des Hessischen Datenschutzbeauftragten hinsichtlich der nur teilweise ordnungsgemäßen Umsetzung der gesetzlichen Vorgaben zum Anlass genommen, den Punkt im Rahmen der Sitzung der AG Wahlen in Hessen am 4. März 2008 zu erörtern und die dort vertretenen Multiplikatoren, darunter der Hessische Städte- und Gemeindebund sowie der Hessische Städtetag, gebeten, entsprechende Hinweise zu verbreiten. Innenministerium und Landeswahlleiter werden darüber hinaus im Vorfeld von allgemeinen Wahlen in diesem Sinne informieren.

### **Zu 6.3 Vereinsförderung durch Kommunen**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

### **Zu 6.4 Hepatitiswarnung im Einwohnermeldeamt**

Der vom Hessischen Datenschutzbeauftragten geschilderte Fall ist auch für die polizeiliche Praxis außergewöhnlich. Zum besseren Verständnis bedarf es noch einer Ergänzung des Sachverhalts.

Der Betroffene wurde wegen Verkehrsunfallflucht gesucht. Nachdem Beamte der zuständigen Polizeistation zunächst die Halterin des Fahrzeugs, seine Lebensgefährtin, aufgesucht hatten, erschienen beide kurze Zeit später auf der Dienststelle. Dem polizeilichen Sachbearbeiter fiel dabei sogleich der labile Gesundheitszustand des Betroffenen auf. Sein Gesicht war verschwitzt und die Augen waren wässrig trüb. Er war an der Hand verletzt und machte einen angespannten Eindruck. Im weiteren Verlauf der Vernehmung bemerkte der Beamte bei dem Betroffenen eine zunehmende Unruhe und mangelnde Konzentration. Auf Befragen verneinte der Betroffene jedoch gesundheitliche Probleme. Den ihm zur Last gelegten Sachverhalt räumte er ein und eine Atemalkoholkontrolle verlief negativ.

Nachdem die Vernehmung bis zu diesem Zeitpunkt schleppend verlaufen war, änderte sich die Situation schlagartig, als der Beamte den Beschuldigten, der im Polizeisystem als BTM-Konsument gekennzeichnet war, nach einem möglichen Drogenkonsum befragte. Der Beschuldigte gab seine bisherige defensive Haltung auf. Er wurde erregt und lebendig. Während er sich über den Schreibtisch in Richtung auf den Sachbearbeiter beugte, bestätigte er, vor Antritt der Fahrt, Heroin geschnupft zu haben. Dabei fuhr er mit seiner verletzten rechten Hand über den Schreibtisch. Dies hinterließ dort eine ca. 30 cm lange Blutspur. Anschließend nahm er ein Papiertaschentuch, das er zuvor dazu benutzt hatte, um Augenausfluss aufzunehmen, der nach seiner Angabe von einer Entzündung stammte, um die Sekrete großflächig auf dem Schreibtisch zu verteilen. Dabei verkündete er, an Hepatitis C erkrankt zu sein.

Hepatitis C ist eine infektiöse Leberkrankheit, die vor allem durch Blutkontakt übertragen wird. Die Übertragung über andere Körperflüssigkeiten ist zwar nicht sehr wahrscheinlich, lässt sich jedoch nicht ausschließen. Es handelt sich um eine schwere Erkrankung, die chronisch werden kann. Leberzirrhose und Leberkrebs können folgen. Einen Impfstoff gibt es bislang nicht.

Auch im weiteren Verlauf der Vernehmung benetzte der Betroffene den Schreibtisch noch mehrfach mit seinem Blut. Ein durchgeführter Drogentest bestätigte seine Angaben zum Heroin-Konsum. Gegenüber dem die Blutprobe durchführenden Arzt wiederholte er den Hinweis auf seine Hepatitis C-Erkrankung.

Obwohl es nicht gelang, Details zu klären, geht das zuständige Polizeipräsidium davon aus, dass in der Folge die Wohnortgemeinde des Betroffenen unter Außerachtlassung der Protokollierungspflicht über die Erkrankung unterrichtet worden ist. Konkrete Hinweise darauf, dass der Betroffene ein städtisches Amt aufsuchen wird, bestanden dabei nicht.

Nach Auffassung des Hessischen Datenschutzbeauftragten war die Datenübermittlung an die Stadt rechtswidrig. Dem wäre für den Normalfall einer erkannten Hepatitis C-Erkrankung, bei der der Betroffene verantwortungsbewusst mit seiner Erkrankung umgeht, ohne weiteres zu folgen. Im vorliegenden Fall, der durch eine Kombination der Erkrankung mit einer durch Drogenkonsum zusammenhängenden psychischen Auffälligkeit gekennzeichnet ist, liegen die Dinge indes anders. Der Hessische Datenschutzbeauftragte lehnt diese Auffassung unter Hinweis auf die Aktenlage des Strafverfahrens ab.

Die Warnung an die Heimatgemeinde des Betroffenen, deren Ämter aus den verschiedensten Anlässen von Zeit zu Zeit aufgesucht werden müssen, war nicht an eine bestimmte Verwaltungsaufgabe geknüpft, sondern diene allgemein dazu, Gefahren von den Mitarbeitern der Stadt abzuwenden. Angesichts der zahlreichen Aufgaben der Stadt als Gefahrenabwehrbehörde, z. B. gerade auch im Pass- und Personalausweiswesen (vgl. § 1 Nr. 1 HSOG-DVO), erübrigt sich ein Rückgriff auf § 22 Abs. 2 Satz 1 Nr. 2 HSOG. Rechtsgrundlage ist bereits § 22 Abs. 1 Satz 3 HSOG, wonach zwischen den Gefahrenabwehrbehörden, anderen für die Gefahrenabwehr zuständigen Behörden oder öffentlichen Stellen und den Polizeibehörden personenbezogene Daten übermittelt werden können, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgabe der empfangenden Stelle erforderlich erscheint. Liegen diese Voraussetzungen vor, besteht eine Übermittlungspflicht nach § 1 Abs. 6 Satz 2 HSOG.

Von der Zulässigkeit der Übermittlung ist die Frage zu unterscheiden, wie der Empfänger die Daten verwenden darf. § 22 Abs. 1 Satz 3 HSOG erlaubt, wie dargelegt, die Übermittlung personenbezogener Daten bereits dann, wenn dies aus der Sicht der übermittelnden Stelle erforderlich erscheint. Der Empfänger ist dann, wenn er die ihm übermittelten Daten nicht rechtmäßig verarbeiten kann, verpflichtet, sie zu löschen.

Die Beantwortung der Frage, ob die Stadt die Daten speichern durfte, ist deshalb differenzierter zu beantworten.

Dem Hessischen Datenschutzbeauftragten ist darin zuzustimmen, dass eine Speicherung nach den Vorschriften des Melderechts bzw. des Pass- oder Personalausweisrechts unzulässig war. Das von der Stadt eingesetzte DV-Verfahren für das Einwohnerwesen PAMELA (Plattformunabhängiges Melde-, Lohnsteuer- und Ausweiswesen) ist jedoch keine rechtliche Größe, sondern ein technisches Verfahren, das – wie der Name schon sagt – mehrere Rechtsbereiche zusammenfasst. Rechtlich wäre es deshalb auch möglich, das Freitextfeld des Einwohnerdatensatzes mit einer eigenen Zweckbestimmung zu versehen, z. B. dem der Eigensicherung. Rechtsgrundlage für die Speicherung wäre dann § 20 Abs. 1 HSOG. Eine derartige Zweckbestimmung müsste allerdings auch formell über ein Verzeichnissverzeichnis nach § 28 HSOG abgesichert werden.

#### **Zu 6.5 Chipkarte als Eintrittskarte und elektronische Geldbörse**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

## **Zu 6.6 Zur Nachweispflicht von ledigen Studierenden bei der Begründung eines Nebenwohnsitzes am Studienort**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

## **7. Sonstige Selbstverwaltungskörperschaften**

### **7.1 Hochschulen**

#### **Zu 7.1.1 Umfang der Nachweise zu § 6 Abs. 5 Nr. 2 Studienbeitragsgesetz**

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die drei genannten Verfahrensarten datenschutzrechtlich konforme Möglichkeiten darstellen, den Nachweis über die Pflege eines Angehörigen im Sinne des § 6 Abs. 5 Nr. 2 Hessisches Studienbeitragsgesetz zu führen.

### **7.2 Rundfunk**

#### **Zu 7.2.1 Rechtswidrige Suche nach Schwarzhörern und -sehern**

Der Hessische Rundfunk hat die erforderlichen Maßnahmen getroffen. Aus Sicht der Landesregierung ist nichts Weiteres zu veranlassen.

### **7.3 Handwerksinnung**

#### **Zu 7.3.1 Handwerksinnung gibt rechtswidrig Einstellungstests von Ausbildungsplatzbewerbern weiter**

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass Handwerksinnungen und Ausbildungsbetriebe die Ergebnisse von Ausbildungstests nur mit schriftlicher Einwilligung des Ausbildungsplatzbewerbers an andere Betriebe weitergeben dürfen.

Die vom Hessischen Datenschutzbeauftragten beanstandete Vorgehensweise war der Landesregierung nicht bekannt, da die Aufsicht über die Innungen den Handwerkskammern obliegt. Die zuständige Handwerkskammer hat in ihrer Eigenschaft als Aufsichtsbehörde im Sinne der Rechtsauffassung des Hessischen Datenschutzbeauftragten bei der betroffenen Innung interveniert, sodass letztlich eine datenschutzkonforme Handhabung herbeigeführt werden konnte.

Dies aufgreifend, wird das Ministerium für Wirtschaft, Verkehr und Landesentwicklung vorsorglich allen hessischen Handwerkskammern die Ausführungen des Hessischen Datenschutzbeauftragten zu dieser Thematik mit der Bitte zur Kenntnis geben, die Innungen entsprechend zu unterrichten.

## **8. Entwicklungen und Empfehlungen im Bereich der Technik**

### **8.1 Einsatz von Signaturen für Verwaltungszwecke**

Die Landesregierung teilt die Auffassung des Hessischen Datenschutzbeauftragten, dass fortgeschrittene elektronische Signaturen keinesfalls qualifizierte elektronische Signaturen ersetzen können. Alle elektronischen Dokumente für die gesetzlich die Schriftform vorgeschrieben ist, müssen ausschließlich qualifiziert elektronisch signiert werden.

Es ist allerdings in jedem Einzelfall kritisch zu prüfen, ob die derzeit im papiergebundenen Prozess geforderten Unterschriften aufgrund rechtlicher Vorgaben tatsächlich erforderlich sind. Vor der Betrachtung des jeweiligen Beweiswerts von Signaturen innerhalb eines Verwaltungsprozesses muss deshalb zunächst das Erfordernis einer Signatur untersucht werden.

Die fortgeschrittene elektronische Signatur hat neben der qualifizierten elektronischen Signatur auch im Kontext des Verwaltungshandelns ihre Berechtigung. Sie ist, wie im Tätigkeitsbericht richtig wiedergegeben, trotz der Probleme im Zusammenhang mit der Prüfung nach dem Schalenmodell, geeignet, die Authentizität und Integrität von Dokumenten und E-Mails zum Zeitpunkt des Eingangs nachzuweisen. Selbst wenn bei einer späteren Prü-

fung die Gültigkeit der Signatur zum Prüfzeitpunkt nicht mehr gegeben ist, hat der Empfänger zumindest den Nachweis der Integrität.

Dem Vorschlag des Hessischen Datenschutzbeauftragten, in der Verwaltung flächendeckend statt fortgeschrittener elektronischer Signaturen nur qualifizierte elektronische Signaturen mit Anbieterakkreditierung zu verwenden, kann nicht entsprochen werden. Er würde zwar alle im Tätigkeitsbericht aufgeworfenen Fragestellungen stark vereinfachen, aber er wird weder den zuvor genannten Aspekten unterschiedlicher Verwendungszwecke noch dem Ziel eines wirtschaftlichen Verwaltungshandelns gerecht.

Die Frage der Beweiswerterhaltung bei der Langzeitaufbewahrung elektronisch signierter Dokumente wird im Rahmen des Archivierungskonzepts, unter Beteiligung des Hessischen Datenschutzbeauftragten, untersucht. Dabei werden die Ergebnisse des ArchiSig-Projekts berücksichtigt.

Der Empfehlung des Hessischen Datenschutzbeauftragten vor dem Einsatz von elektronischen Signaturen ausführlich über die Unterschiede der Signaturniveaus zu informieren, wird in unterschiedlicher Form nachgekommen. Zum Einen wird im Rahmen des für die Anwender verbindlich vorgeschriebenen E-Learning-Angebots auf diese Thematik eingegangen. Zum Anderen wird in dem projektbegleitenden "PKI-Handbuch" der Unterschied dargestellt und erläutert.

Die Landesregierung begrüßt, dass der Hessische Datenschutzbeauftragte die Diskussion über den Einsatz und die Weiterentwicklung der elektronischen Signatur auf allen Ebenen aktiv unterstützt. Insbesondere die von ihm angesprochene Klärung der Fragen zu den grundlegenden etablierten Standards und den Vorgaben der Verwaltungs-PKI mit der Bundesnetzagentur und dem Bundesamt für die Sicherheit in der Informationstechnologie (BSI) wird aufmerksam verfolgt.

## **8.2 Datenschutz beim Umgang mit Speichermedien**

Die Landesregierung bewertet die Ausführungen des Hessischen Datenschutzbeauftragten als wertvolle Hinweise zum Datenschutz. Sie wird in den entsprechenden Gremien auf die Gefahren - hohes Verlustrisiko, Risiko des Einschleppens von Schadsoftware, Risiko des Ausspähens von Inhalten bei Nutzung an fremden Rechnern - im Umgang mit den USB-Sticks hinweisen. Bei zukünftigen Ausschreibungen von Digitalkopierern wird die Funktionalität "Löschen der Kopiererfestplatte" berücksichtigt werden. Die Dienststellen werden aufgefordert, vertragliche Regelungen zur Datenlöschung für Leasingrückläufer zu finden.

Die hessische Sicherheitsleitlinie vom 7. Dezember 2004 fordert die Anwendung des IT-Grundschriftbuchs (heute: Grundschriftkatalogs) des BSI zur Abdeckung eines normalen Schutzbedarf in der hessischen Landesverwaltung. Die fachgerechte Entsorgung von Altgeräten einschließlich der sicheren Löschung von Festplatten ist eine der geforderten Maßnahmen. Zur Unterstützung wird die Landesregierung die HZD bitten, die Dienststellen bei der fachgerechten Entsorgung von Altgeräten durch Beratung und Vermittlung zertifizierter Entsorgungsunternehmen zu unterstützen und den Dienststellen die Nutzung dieser Leistung bei der Entsorgung empfehlen. Darüber hinaus werden die Dienststellen des Landes über die IT-Sicherheitsgremien aufgefordert, die Festplatten von Altgeräten und andere digitale Speichermedien, wie sie z. B. in Digitalkameras und PDAs sowie Druck- oder Kopiergeräten Verwendung finden, vor der Weitergabe an andere Stellen mit dem Hinweis auf die vom Hessischen Datenschutzbeauftragten erwähnten Löschroutinen sicher zu löschen.

## **8.3 Fehler- und Unfalldatenspeicher**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Ergänzend ist zu berichten, dass die Aufsichtsbehörden des Düsseldorfer Kreises bei ihrer Sitzung im April 2008 in Wiesbaden vereinbart haben, die den deutschen Markt beliefernden Automobilhersteller und -importeure nach den in ihren Fahrzeugen verwendeten Datenerfassungssystemen zu befragen. Auf der Grundlage der Umfrageergebnisse werden die Aufsichtsbehörden die weitere datenschutzrechtliche Bewertung der einzelnen Systeme vornehmen.

**9. Bilanz****Zu 9.1 Datenschutz im Verfahren der Verleihung staatlicher Auszeichnungen und Ehrungen (31. Tätigkeitsbericht, Ziff. 3.3)**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

**Zu 9.2 Einsatz zentraler Spam-Filter der Landesverwaltung (35. Tätigkeitsbericht, Ziff. 8.2)**

Die Landesregierung begrüßt, dass der Hessische Datenschutzbeauftragte das pilotweise Aufsetzen zentraler Spam-Filter in der Landesverwaltung positiv würdigt.

Der Hessische Datenschutzbeauftragte weist darauf hin, dass die seit dem Jahr 2006 konzipierten und mit ihm abgestimmten Anti-Spam-Maßnahmen an dem zentralen Internet-Mail-Relay-Gateway des Landes erfolgreich umgesetzt und damit mehrere Spam-Wellen mit Spitzenlasten bis zu 10.000 Mails pro Minute abgewehrt wurden. Die Landesregierung nimmt mit Befriedigung zur Kenntnis, dass die Anti-Spam-Struktur diesen Angriffen Stand gehalten hat, der produktive Mail-Verkehr ohne Unterbrechung und Leistungsverlust weiterlief und die internen, geschützten Systeme von den Spam-Angriffen nicht erreicht worden sind.

Wiesbaden, 15. September 2008

Der Hessische Ministerpräsident:

**Koch**

Der Hessische Minister  
des Innern und für Sport:  
**Bouffier**