



16. Wahlperiode

Drucksache **16/7645**

# HESSISCHER LANDTAG

22. 08. 2007

## **Stellungnahme**

### **der Landesregierung**

**betreffend den Fünfunddreißigsten Tätigkeitsbericht  
des Hessischen Datenschutzbeauftragten**

**Drucksache 16/6929**

## Inhaltsverzeichnis

### Stellungnahme zu:

1. Einführung
2. Datenschutz bei Public Private Partnerships
3. Europa
4. Bund
  - 4.1 Antiterrordatei
  - 4.2 Folgerungen aus der Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung
  - 4.3 Datenschutz nach der Fußball-WM
    - 4.3.1 Das Akkreditierungsverfahren
    - 4.3.2 Prüfung im Frankfurter Stadion
    - 4.3.3 Personalisierte Tickets
    - 4.3.4 Zukünftige Akkreditierungsverfahren
  - 4.4 Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren am Beispiel ElsterOnline-Portal 5
5. Land
  - 5.2 Justiz
    - 5.1.1 Löschung von Daten der Polizei nach der Ablehnung der Eröffnung des Hauptverfahrens beim Amtsgericht
    - 5.1.2 Ist die Übermittlung von Daten über eine Lebenspartnerschaft an die Kirche bei einem Kirchenaustritt zulässig?
  - 5.2 Polizei und Strafverfolgung
    - 5.2.1 Prüfung der Datei "Gewalttäter Sport"
    - 5.2.2 Auskunft über eigene Daten zur Weitergabe an private Sicherheitsdienste 9
    - 5.2.3 Regelanfrage bei der Polizei vor ausländerrechtlichen Entscheidungen
  - 5.3 Verfassungsschutz
    - 5.3.1 Entwurf für ein Sicherheitsüberprüfungsgesetz
  - 5.4 Verkehrswesen
    - 5.4.1 Missbräuchliche Nutzung von Daten der örtlichen Fahrzeugregister durch Bedienstete einer Ordnungsbehörde?
  - 5.5 Schulen und Schulverwaltung
  - 5.6 Forschung
    - 5.6.1 Aufbau des Deutschen Hämophilieregisters
    - 5.6.2 Generisches Datenschutzkonzept für Biomateriealbanken
    - 5.6.3 Datenschutz bei der Arzneimittelprüfung
  - 5.7 Gesundheitswesen

- 5.7.1 Einführung des flächendeckenden Mammographie-Screening
- 5.7.2 Verwendung von Pflegedokumentationen bei der Durchführung von Qualitätsprüfungen in Pflegeeinrichtungen
- 5.7.3 Kopflausbefall von Kindern - ein Fall für das Gesundheitsamt
- 5.7.4 Übermittlung von Versichertendaten durch die AOK Hessen an Versand-Apotheken
- 5.8 Sozialwesen
  - 5.8.1 Kindeswohl und Datenschutz
  - 5.8.2 Auskunftsanspruch von Unfallversicherungsträgern gegenüber Ärzten
  - 5.8.3 Übermittlung von Sozialdaten zu Zwecken der Durchführung eines Disziplinarverfahrens
- 5.9 Personalwesen
- 5.10 Finanzwesen
  - 5.10.1 Kontendatenabrufersuchen nach §§ 93 Abs. 7 und 8, 93b AO
- 6. Kommunen
- 7. Sonstige Selbstverwaltungskörperschaften
  - 7.1 Hochschulen
  - 7.2 Sparkassen
    - 7.2.1 Sparkasse zeichnet rechtswidrig Telefongespräche auf
- 8. Entwicklungen und Empfehlungen im Bereich der Technik und Organisation
  - 8.1 Zentrale DV in der Landesverwaltung
    - 8.1.1 Ausgangslage
    - 8.1.2 Wichtige Entscheidungen
    - 8.1.3 Prüfungen
      - 8.1.3.1 Zentrale E-Mail
      - 8.1.3.2 Prüfung in Hünfeld<sup>23</sup>
    - 8.1.4 Sachstand zur Verschlüsselung
    - 8.1.5 Sachstand Terminalserver
  - 8.2 Einsatz zentraler Spam-Filter in der Landesverwaltung
  - 8.3 Dokumentenmanagement in der öffentlichen Verwaltung
    - 8.3.1 Dokumentenmanagement in der Hessischen Landesverwaltung
    - 8.3.2 Orientierungshilfe Datenschutz bei Dokumentenmanagementsystemen
- 9. Bilanz

- 9.1 **Videoüberwachung an der Konstablerwache in Frankfurt (34. Tätigkeitsbericht, Ziff. 5.3.1)**
- 9.2 **Sachstand der korrekten Umsetzung der Löschung von auszusondernden Datenspeicherungen der Polizei (34. Tätigkeitsbericht, Ziff. 5.3.2)**
- 9.3 **Liegenschaftsdatenabruf (34. Tätigkeitsbericht, Ziff. 6.2)**
- 9.4 **Hartz IV - Vorlage von Kontoauszügen - (34. Tätigkeitsbericht, Ziff. 5.9.1)**
- 9.5 **Schuleingangsuntersuchung durch die Gesundheitsämter - (34. Tätigkeitsbericht, Ziff. 5.8.5)**

Die Stellungnahme der Landesregierung gibt den Sachstand im April/Mai 2007 wieder.

### **Zu 1. Einführung**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zur Entwicklung des Datenschutzrechts in der Vergangenheit (Ziff. 1.2) zu.

Sie teilt jedoch nicht die Auffassung des Hessischen Datenschutzbeauftragten, dass Hessen bei der Entwicklung der informatorischen Zivilgesellschaft zurückzufallen droht (Ziff. 1.1). Soweit hiermit gemeint ist, dass in acht Bundesländern und im Bund, nicht aber in Hessen ein Informationsfreiheitsgesetz existiert, ist zu erwidern, dass allein der Hinweis auf die Rechtssetzung des Bundes und der anderen Bundesländer nicht ausreicht, um ein Informationsfreiheitsgesetz auch in Hessen zu schaffen. Wegen der verfassungsrechtlich geschützten Grundsätze der Sparsamkeit und Wirtschaftlichkeit der Verwaltung bedarf es vielmehr des Nachweises der Erforderlichkeit eines solchen Gesetzes, um den mit dem Informationszugangrecht verbundenen Verwaltungsaufwand zu rechtfertigen. Dieser Nachweis ist aber noch nicht erbracht worden.

Zu den weiteren Ausführungen des Hessischen Datenschutzbeauftragten zum Informationsfreiheitsgesetz unter dem Thema "Datenzugangsschutz" (Ziff. 1.3) ist zu bemerken, dass keine verfassungsrechtliche Verpflichtung besteht, den Zugang zu amtlichen Informationen ohne Nachweis eines Interesses des Einzelnen zu eröffnen. Die zu dem Gesetzentwurf der Fraktion BÜNDNIS 90 /DIE GRÜNEN für ein Gesetz zur Regelung des Zugangs zu Informationen (Informationsfreiheitsgesetz) - Drs. 16/5913 - und zu dem Antrag der Fraktion der SPD betreffend eines Informationsfreiheitsgesetzes - Drs. 16/5839 - im Landtag durchgeführte mündliche Anhörung hat dies nochmals klargestellt. Auch nach Bundes- und Europarecht besteht keine Verpflichtung. Der Landtag hat mit Beschluss vom 31. Mai 2007 den Gesetzentwurf und den Antrag der SPD abgelehnt. Auf die im Rahmen der zweiten Lesung des Gesetzentwurfs angeführten Argumente gegen ein solches Gesetz wird Bezug genommen. Die Landesregierung hatte dem Landtag empfohlen, den Gesetzentwurf abzulehnen, weil nach ihrer Auffassung keine Veranlassung besteht, für Hessen ein Informationsfreiheitsgesetz zu schaffen. Die Gründe für ihre Auffassung hat Herr Staatsminister Grüttner in seiner Rede vor dem Plenum am 31. Mai 2007 im Einzelnen dargelegt, auf die hier verwiesen wird (vgl. Plenarprotokoll 16/135 vom 31. Mai 2007 zu TOP 75 und 77).

### **Zu 2. Datenschutz bei Public Private Partnerships**

Die Landesregierung hat die Ausführungen des Hessischen Datenschutzbeauftragten zur Abgrenzung des öffentlichen vom privaten Datenschutzrecht bei Public Private Partnerships mit Interesse zur Kenntnis genommen. Die Landesregierung ist jedoch an das geltende Recht - hier das Bundesdatenschutzgesetz - gebunden, nach dessen § 2 für die Abgrenzung, ob ein privatrechtliches Unternehmen als nicht öffentliche oder öffentliche Stelle gilt, noch weitere Kriterien zu berücksichtigen sind, als nur die betriebliche Tätigkeit im Bereich der Daseinsvorsorge. Zur Vermeidung von Wiederholungen sei an dieser Stelle auf die Ausführungen der Landesregierung in ihrer Stellungnahme zum 34. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten zu Ziff. 2.1.2.3 (Drs. 16/5851) verwiesen. Die Frage, welche Datenschutzvorschriften Anwendung finden, kann deshalb nur im jeweiligen Einzelfall und nach Prüfung aller gesetzlichen Voraussetzungen beantwortet werden.

### **Zu 3. Europa**

Hinsichtlich der Tätigkeit des Hessischen Datenschutzbeauftragten für europäische Gremien liegen der Landesregierung keine eigenen Erkenntnisse vor. Soweit der Hessische Datenschutzbeauftragte über das Ergebnis seiner Überprüfung von Ausschreibungen zur verdeckten Registrierung nach Art. 99 SDÜ bei hessischen Polizeipräsidien berichtet (Nr. 3.1.2), stellt die Landesregierung fest, dass der polizeiliche Umgang mit den personenbezogenen Daten in jeder Hinsicht den Anforderungen des Datenschutzrechts gerecht geworden ist.

## **4. Bund**

### **Zu 4.1 Antiterrordatei**

Das Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz - ATDG) lässt die Vorschriften über den Informationsaustausch zwischen den beteiligten Behörden grundsätzlich unberührt. Es zielt nicht darauf ab, bisher auf der Grundlage der bereichsspezifischen Datenschutzvorschriften zulässige Übermittlungen zu unterbinden. Die Gesetzesbegründung bringt deswegen nur eine Selbstverständlichkeit zum Ausdruck, wenn sie die Möglichkeit anspricht, auch personenbezogene Daten zu übermitteln, die in dem Katalog der Antiterrordatei nicht aufgeführt sind. Die Befürchtung des Hessischen Datenschutzbeauftragten, das Antiterrordateigesetz selbst solle über den Datenkatalog des § 3 hinaus die Übermittlung unbenannter Erkenntnisse gestatten (Ziff. 4.1.3), ist daher unbegründet.

Der Vorteil der Antiterrordatei besteht im Wesentlichen darin, dass auf der Grundlage von Treffermeldungen gezielt und standardisiert Auskunftersuchen an diejenigen Behörden gestellt werden können, die über einschlägige Erkenntnisse zu einer bestimmten Person verfügen. Nur im Eilfall darf die anfragende Behörde sich die erweiterten Daten selbst freischalten. Die durch Abfrage der Antiterrordatei gewonnenen Erkenntnisse unterliegen besonderen Verwertungsbeschränkungen (§ 6 ATDG). Demgegenüber richtet sich die Übermittlung von Erkenntnissen aufgrund eines in der Folge einer Abfrage gestellten Auskunftersuchens nach den jeweiligen bereichsspezifischen Übermittlungsvorschriften (§ 7 ATDG).

### **Zu 4.2 Folgerungen aus der Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung**

Der 1. Senat des Bundesverfassungsgerichts hat, wie der Hessische Datenschutzbeauftragte zutreffend berichtet, am 4. April 2006 eine Entscheidung zur Rasterfahndung nach dem Polizeigesetz von Nordrhein-Westfalen getroffen. Im Ergebnis bedeutet dieser Beschluss, dass die im Jahre 2002 bundesweit durchgeführte und von zahlreichen obergerichtlichen Entscheidungen bestätigte Rasterfahndung nach islamistischen Schläfern als verfassungswidrig angesehen werden muss. § 26 HSOG, der im selben Jahr mit dem Ziel geändert worden war, eine verlässliche Rechtsgrundlage für die Durchführung dieser Rasterfahndung in Hessen zu schaffen, wird daher erneut zu überprüfen sein. Dabei wird die Rasterfahndung auf Fälle zu beschränken sein, in denen bereits eine Gefahr im polizeirechtlichen Sinne besteht. Insofern besteht Einvernehmen mit dem Hessischen Datenschutzbeauftragten.

Anders als der Hessische Datenschutzbeauftragte hat die Landesregierung den von der FDP-Fraktion im Landtag eingebrachten Gesetzentwurf jedoch nicht als geeignete Grundlage für eine Neufassung des § 26 HSOG angesehen. Insbesondere gilt es, eine Vermischung des Gefahrenbegriffs mit tatsächlichen Anhaltspunkten zu vermeiden, wie dies in der Sachverständigenanhörung auch von einem der Sachverständigen gefordert worden ist.

Zur Zeit ist eine Bund-Länder Arbeitsgruppe mit der Problematik befasst. Wenn deren Ergebnis vorliegt, wird die Landesregierung einen Regelungsvorschlag unterbreiten. Anlass zu besonderer Eile besteht nicht, weil die Vorschrift verfassungskonform interpretiert werden kann. Dass die Bestimmung nur noch einengend im Sinne der Rechtsprechung des Bundesverfassungsgerichts angewendet werden wird, ist sichergestellt, da Rasterfahndungen nach dem Polizeirecht von Gesetzes wegen ohne Ausnahme der Zustimmung des Landespolizeipräsidiums bedürfen (§ 26 Abs. 4 Satz 1 HSOG).

## **4.3 Datenschutz nach der Fußball-WM**

### **Zu 4.3.1 Das Akkreditierungsverfahren**

Hinsichtlich des Akkreditierungsverfahrens für die Fußball-Weltmeisterschaft bestätigt der Hessische Datenschutzbeauftragte der hessischen Polizei erfreulicherweise einen sensiblen Umgang mit den personenbezogenen Daten. Allerdings kritisiert er die Polizei, weil sie die Daten ursprünglich noch bis zu einem Jahr nach Ende der Veranstaltung speichern

wollte. Dabei ist jedoch zu berücksichtigen, dass die Speicherung nicht polizeilichen Zwecken dienen sollte, sondern allein auf der Überlegung beruhte, dass betroffene Personen noch nach längerer Zeit Einsprüche gegen ablehnende Voten einlegen könnten. In diesen Fällen hätte anhand der gespeicherten Daten nachvollziehbar dargelegt werden können, warum die Ablehnung erfolgt ist. Auch mit "approved" beantwortete Datensätze hätten durchaus von Bedeutung sein können. Die Entscheidung über die Akkreditierung ist nämlich nicht durch die Polizei, sondern durch das Organisationskomitee der Fifa-WM getroffen worden. Deswegen hätte es in Streitfällen u.U. notwendig werden können, zu belegen, dass die Polizei keine Einwände erhoben hatte.

Entsprechendes gilt für die Speicherdauer der Daten aus dem "Confed-Cup". Es besteht im Übrigen mit dem Hessischen Datenschutzbeauftragten Einigkeit darin, dass diese Daten nicht für die Bearbeitung des Akkreditierungsverfahrens zur WM 2006 herangezogen werden durften. Ein solcher Schritt war bei der Konzeption des Verfahrens zwar angedacht gewesen. Er ist dann aber nicht weiter verfolgt worden, nachdem der Hessische Datenschutzbeauftragte im Rahmen der frühzeitigen Konsultation Bedenken geäußert hatte.

#### **Zu 4.3.2 Prüfung im Frankfurter Stadion**

Die Landesregierung nimmt mit Befriedigung zur Kenntnis, dass der Hessische Datenschutzbeauftragte bei seiner Prüfung keinen Anlass zu Beanstandungen hatte. Auch das Regierungspräsidium Darmstadt hat bei seiner Prüfung im Frankfurter Stadion keinen Verstoß gegen das Bundesdatenschutzgesetz festgestellt (siehe Zwanzigsten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Ziff. 11.1).

#### **Zu 4.3.3 Personalisierte Tickets**

Die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Vertrieb der personalisierten Eintrittskarten wurde vom Regierungspräsidium Darmstadt eingehend geprüft. Einen Verstoß gegen das Bundesdatenschutzgesetz hat die Aufsichtsbehörde nicht festgestellt (siehe Zwanzigsten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden, Ziff. 11.1).

#### **Zu 4.3.4 Zukünftige Akkreditierungsverfahren**

Der Hessische Datenschutzbeauftragte kritisiert die Entscheidung des Bundeskriminalamts, die "t-spoc"-Infrastruktur (t-spoc = technical single point of contact) auch künftig für weitere Akkreditierungsverfahren im Zusammenhang mit Großveranstaltungen vorrätig zu halten. Die Landesregierung kann dieser Kritik nicht folgen. Sie hält die Entscheidung vielmehr für sachgerecht, weil Akkreditierungsverfahren bei Großveranstaltungen sinnvoll sein können. Bundesweit wurde insoweit abgestimmt, dass Veranstaltungen im Zusammenhang mit der EU-Präsidentschaft Deutschlands und vor allem der G8-Gipfel in Heiligendamm im Juni 2007 als derart herausragende Veranstaltungen anzusehen sind.

#### **Zu 4.4 Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren am Beispiel ElsterOnline-Portal**

Die Unterschiede zwischen Authentisierung und Signatur und deren unterschiedliche rechtliche Wirkungen sind bei der Änderung des § 87a Abs. 6 AO - nach Anhörung der beteiligten Datenschutzbeauftragten - berücksichtigt worden. Die Regelungen des § 87a Abs. 6 (Authentifizierungsverfahren) sind bis zum Jahr 2011 befristet; danach ist zu überprüfen, ob ein Wechsel zur qualifizierten elektronischen Signatur möglich ist. Beide Verfahren beruhen aber auf den gleichen technischen Grundlagen. Die Bewertung des Hessischen Datenschutzbeauftragten hinsichtlich der Sicherheit des Authentisierungsverfahrens wird daher von der Landesregierung nicht geteilt.

## 5. Land

### 5.1 Justiz

#### Zu 5.1.1 Löschung von Daten der Polizei nach der Ablehnung der Eröffnung des Hauptverfahrens beim Amtsgericht

Der Generalstaatsanwalt und die zuständige Staatsanwaltschaft bei dem Landgericht Wiesbaden haben dem Ministerium der Justiz zu dem im Tätigkeitsbericht geschilderten Fall einen Bericht erstattet. Demnach ist der Gang des Verfahrens im Tätigkeitsbericht zutreffend wiedergegeben. Durch ein auf die besondere Gestaltung des Einzelfalls zurückzuführendes bedauerliches Versehen ist die im Zuge der Ermittlungen mit der Sache befasste Polizeibehörde durch die Staatsanwaltschaft nicht über den Verfahrensausgang unterrichtet worden.

Nachdem seitens der Staatsanwaltschaft die Entscheidung getroffen worden war, den Nichteröffnungsbeschluss des Amtsgerichts nicht anzufechten, da sein Inhalt letztlich überzeugte, traf der zuständige Staatsanwalt eine Verfügung bezüglich des asservierten Revolvers und leitete die Akten zur Schlussdurchsicht der zuständigen Rechtspflegerin zu. Hierbei ist bedauerlicherweise die Notwendigkeit einer Unterrichtung der Polizeibehörde nach § 482 Abs. 2 StPO, im Tätigkeitsbericht wird irrtümlich § 484 StPO genannt, von allen Beteiligten übersehen worden.

Wie der Leitende Oberstaatsanwalt in Wiesbaden und der Generalstaatsanwalt in ihrem Bericht zutreffend anmerken, wird dies sicher auch darauf zurückzuführen sein, dass derartige Fallkonstellationen - die Nichteröffnung des Hauptverfahrens - in der Praxis eher selten vorkommen und die auch dann bestehende Notwendigkeit einer Unterrichtung der Polizeibehörde - im Gegensatz zu den Fällen der Verfahrenseinstellung oder des Verfahrensausschlusses durch Urteil - übersehen werden kann.

Der Leitende Oberstaatsanwalt in Wiesbaden hat den Fall zum Anlass genommen, die in seiner Behörde tätigen Dezernentinnen und Dezernenten nochmals ausdrücklich auf die sich aus § 482 Abs. 2 StPO ergebende Unterrichtungspflicht hinzuweisen.

Zu der seitens des Hessischen Datenschutzbeauftragten angeregten Weiterentwicklung von MESTA hat der Generalstaatsanwalt mitgeteilt, es werde derzeit an einer Optimierung von MESTA gearbeitet. Parallel hierzu habe er die Leiterinnen und Leiter der hessischen Staatsanwaltschaften und den Leiter der Amtsanwaltschaft Frankfurt am Main mit Rundschreiben vom 22. Juni 2007 und einem diesem beigefügten Merkblatt der Gemeinsamen IT-Stelle der Hessischen Justiz (GIT) Hinweise zur Optimierung der Arbeitsweise im Bereich der MESTA-Ergebnismitteilung erteilt. Der Generalstaatsanwalt geht davon aus, dass hierdurch Vorfälle wie der im Tätigkeitsbericht erwähnte künftig vermieden werden können.

Zu der seitens des Hessischen Datenschutzbeauftragten angeregten Weiterentwicklung von MESTA hat der Generalstaatsanwalt mitgeteilt, er werde diese Möglichkeit mit der Gemeinsamen IT-Stelle der Hessischen Justiz erörtern.

Der Hessische Datenschutzbeauftragte befasst sich in seinem Tätigkeitsbericht über den geprüften Einzelfall hinaus allgemein mit der Frage, wie sichergestellt werden kann, dass die Polizei zuverlässig vom Ausgang eines Strafverfahrens Kenntnis erlangt. Er fordert diesbezüglich eine elektronische Weiterverarbeitung der von der Justiz übermittelten Daten bei der Polizei. Die Landesregierung hat, wie in ihrer Stellungnahme zum 34. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (Drs. 16/5891) zu Ziff. 5.3.4.2 angekündigt, die notwendigen Schritte unternommen, um ein geeignetes Verfahren einzurichten.

Unmittelbar nach Einführung der elektronischen Vorgangsbearbeitungssoftware ComVor bei der hessischen Polizei im Jahr 2002 wurde die MESTA-Schnittstelle zum elektronischen Datenaustausch zwischen Polizei und Justiz in Betrieb genommen. In einem ersten Schritt wurden Vorgangsdaten aus ComVor an MESTA geliefert und MESTA-Verfahrensausgänge als RPT-Dateien, die nach Dienststellen aufgeteilt waren, über die HZD elektronisch an die hessische Polizei zurückgeliefert. Diese Verfahrensausgänge wurden dann in Form von Excel-Tabellen den Dienststellen über ein Dateiverzeichnis (Share) zur weiteren Bearbeitung zur Verfügung gestellt. Aus jedem Excel-Eintrag (ein Datensatz pro Zeile) konnte über ein bereitgestelltes Tool ein Ausdruck erzeugt werden, der zur jeweiligen Kriminalakte der Person



bzw. des Beschuldigten hinzugefügt werden konnte. Außerdem wurde manuell durch den Sachbearbeiter - abhängig vom jeweiligen Verfahrensausgang - die neu berechnete Speicherfrist in POLAS gesetzt bzw. der entsprechende Datensatz gelöscht.

Das beschriebene "Excel-Verfahren" wurde bis einschließlich Juli 2005 praktiziert. Seither kommt ein EMail-Verfahren zum Einsatz. Die von MESTA an ComVor gelieferten Verfahrensausgänge werden dabei anhand der Behördenkennziffer automatisiert an ein eigens dafür eingerichtetes MESTA-Postfach der jeweiligen Polizeidienststelle versandt und können dort abgearbeitet werden. Verfahrensausgänge, die z. B. auf Grund zwischenzeitlicher organisatorischer Änderungen nicht zugestellt werden können, werden an ein Auffangpostfach beim PTLV gesandt und von dort an die zuständige Dienststelle weitergeleitet. Somit ist gewährleistet, dass alle Verfahrensausgänge bei der zuständigen Dienststelle des jeweiligen Präsidiums ankommen.

Im Rahmen der Einführung der ComVor-Version 6.5, die nach derzeitiger Planung für Oktober 2007 vorgesehen ist, soll der Datenaustausch auf das neue XJustiz-Verfahren umgestellt werden. Dies bedeutet, es findet ein Wechsel von der bisherigen Übertragung von Festlängendateien auf ein XML-Format statt.

In diesem Zusammenhang soll auch eine weitere Automatisierung und Optimierung der Anlieferung in der Weise erfolgen, dass die relevanten MESTA-Daten zusätzlich in POLAS eingespeist werden, dem zentralen Nachweissystem für die hessischen Kriminalakten. Hierfür ist die Realisierung einer entsprechenden Schnittstelle in POLAS erforderlich. Da POLAS der zentrale Bestandteil von INPOL-Land ist, sind hierzu Abstimmungen mit bis zu 14 Teilnehmern aus Bund und Ländern erforderlich. Die notwendigen Vorabstimmungen haben bereits stattgefunden und erste Planungen sind aufgesetzt. Dabei wird im Einzelnen noch fachlich festzulegen sein, wie die automatisierte bzw. halbautomatisierte (d.h. mit einer vorgeschalteten Qualitätssicherung) Übertragung von MESTA nach POLAS und die anschließende Verarbeitung konkret erfolgen soll.

Mit der Erstellung des erforderlichen Fachkonzepts wird sich die Fachgruppe POLAS der Kooperation Baden-Württemberg/Brandenburg/Hamburg/Hessen im Rahmen des IPCC (INPOL-Land POLAS Competence Center) befassen. Die momentane Planung sieht vor, dass das Fachkonzept sowie eine detaillierte Umsetzungs- und Testplanung noch im Jahr 2007 vorliegen wird. Vorbehaltlich der konkreten Bewertung dieses Konzepts ist nach der momentanen Einschätzung eine Produktivsetzung dieser weiteren Optimierung für Anfang des Jahres 2008 realistisch.

#### **Zu 5.1.2 Ist die Übermittlung von Daten über eine Lebenspartnerschaft an die Kirche bei einem Kirchenaustritt zulässig?**

Die Landesregierung teilt die Auffassung des Hessischen Datenschutzbeauftragten, dass eine Datenübermittlung an die Kirchengemeinde über eine bestehende eingetragene Lebenspartnerschaft bei einem Kirchenaustritt nicht erforderlich und damit unzulässig ist.

Wer in Hessen aus einer Religionsgemeinschaft öffentlichen Rechts mit bürgerlichrechtlicher Wirkung austreten will, hat den Austritt bei dem für seinen Wohnsitz zuständigen Amtsgericht zu erklären (vgl. Hessisches Gesetz, die bürgerliche Wirkung des Austritts aus einer Kirche oder Religionsgemeinschaft betreffend vom 10.09.1878, zuletzt geändert durch Gesetz vom 31.05.1974, GVBl. I S. 281). Damit endet die steuerrechtliche Mitgliedschaft mit Ablauf des Kalendermonats, der auf die Erklärung des Kirchenaustritts beim Amtsgericht folgt (§ 5 Abs. 2 Hessisches Kirchensteuergesetz). Die Austrittsbescheinigung ist dem Finanzamt vorzulegen. Für steuerliche Zwecke bedarf es keiner Angabe über die Eheschließung und den Ehepartner in der Austrittsbescheinigung. Diese Daten liegen dem Finanzamt ohnehin aufgrund der Erklärung der bzw. des Steuerpflichtigen vor. Im Übrigen hat eine eingetragene Lebenspartnerschaft derzeit für die Einkommensbesteuerung keine tarifliche Auswirkung.

Die im Tätigkeitsbericht geschilderte Problematik ist durch das zuständige Oberlandesgericht Frankfurt am Main zutreffend gelöst worden. Der Präsident des Oberlandesgerichts hat die hessischen Amtsgerichte durch Rundverfügung angewiesen, von der Aufnahme von Daten über eine eingetragene Lebenspartnerschaft in die Kirchenaustrittserklärung abzusehen.

## **5.2 Polizei und Strafverfolgung**

### **Zu 5.2.1 Prüfung der Datei "Gewalttäter Sport"**

Die Landesregierung nimmt mit Befriedigung zur Kenntnis, dass der Hessische Datenschutzbeauftragte bei seiner stichprobenartigen Kontrolle des hessischen Datenbestands der Verbunddatei "Gewalttäter Sport" keine Fälle rechtswidriger Datenverarbeitung festgestellt hat.

### **Zu 5.2.2 Auskunft über eigene Daten zur Weitergabe an private Sicherheitsdienste**

Der vom Hessischen Datenschutzbeauftragten geschilderte Sachverhalt, das LKA habe einem Betroffenen auf telefonische Nachfrage mitgeteilt, Anträge auf Selbstauskunft zur Vorlage bei einem Bewachungsunternehmen würden nicht schriftlich beantwortet, kann nicht mehr nachvollzogen werden. Bei telefonischen Anfragen Betroffener weist das LKA stets darauf hin, dass die Vorschrift über die Auskunft nach § 29 Abs. 1 HSOG nur geschaffen wurde, um eine Transparenz behördlicher Datenverarbeitung und -nutzung für den Bürger herzustellen, dass aber selbstverständlich der schriftliche Antrag beantwortet wird.

Sofern erkennbar ist, dass es sich um einen Auskunftsantrag zur Vorlage bei einem Arbeitgeber handelt, erteilt das LKA den Bescheid mit dem Zusatz:

"Es wird darauf hingewiesen, dass diese Auskunft nur für Sie selbst bestimmt ist und es Ihr Recht ist, dass grundsätzlich nur Sie selbst über die Weitergabe der Daten an Dritte bestimmen (§ 29 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung - HSOG)."

Der Bescheid wird im Übrigen stets an den Betroffenen und nicht an den Arbeitgeber gesandt.

Dass Auskunftsanträge gestellt werden, die erkennbar nicht der Selbstauskunft dienen, sondern auf Betreiben eines potentiellen Arbeitgebers zurückgehen, ist seit dem Jahr 1993 bekannt. Damals hat der Landesbeauftragte für den Datenschutz Rheinland-Pfalz auf die Problematik hingewiesen (vgl. dessen 14. Tätigkeitsbericht vom 12. November 1993 - Landtag Rheinland-Pfalz Drs. 12/3858, S. 30). In der Folge haben die behördlichen Datenschutzbeauftragten des Bundeskriminalamts und der Landeskriminalämter das Thema auf einer Sitzung im Januar 1994 beraten, ohne zu einer einheitlichen Bewertung zu gelangen.

Größere Ausmaße hat dieses Phänomen erst in letzter Zeit angenommen. Inzwischen ist in mehr als 90% der Anträge auf Selbstauskunft eindeutig erkennbar, dass es sich um fremdbestimmte Auskunftsverlangen handelt. Sofern dies nicht schon aus dem Text selbst hervorgeht, ergibt sich dies aus folgenden Anhaltspunkten:

- dasselbe äußere Erscheinungsbild (Vordrucke) bzw. gleicher Wortlaut der Auskunftsbegehren,
- Anträge kommen per Sammelpost, in Einzelfällen mit Anschreiben des Arbeitgebers,
- der Brief wurde mit der Frankiermaschine der Firma freigestempelt.

In zahlreichen Telefonaten bestätigten die Antragsteller, dass die Auskunft vom zukünftigen Arbeitgeber gefordert wurde und ein Arbeitsvertrag erst dann abgeschlossen werde, wenn der "Persilschein" des LKA vorliege.

Zum Verständnis der im Tätigkeitsbericht angeführten Praxis eines privaten Sicherheitsunternehmens ist anzumerken, dass nach § 34a Abs. 1 Satz 4 Gewerbeordnung (GewO) ein Bewachungsgewerbetreibender mit der Durchführung von Bewachungsaufgaben nur solche Personen beschäftigen darf, die u.a. hierfür die erforderliche Zuverlässigkeit besitzen. Hierzu hat der Gesetzgeber in § 34a Abs. 3 GewO zur Überprüfung der Zuverlässigkeit des Bewachungspersonals die Einholung von Auskünften aus dem Bundeszentralregister einschließlich Übermittlung des Ergebnisses dieser Überprüfung an den Gewerbetreibenden normiert. Darüber hinaus enthält § 9 Abs. 2 Bewachungsverordnung (BewachV) Regelbeispiele, bei deren Vorliegen die erforderliche Zuverlässigkeit nicht gegeben ist. Die in diesem Bereich tätigen Unternehmen halten allerdings häufig die in dem zuvor genannten Register vorhandenen Daten nicht für ausreichend, um die Frage der Zuverlässigkeit abschließend entscheiden zu können. Das Sicherheitsunternehmen hat aber ein Interesse daran, schon vor der obligatorischen Meldung einer

Wachperson an die zuständige Behörde (vgl. § 9 Abs. 3 Satz 1 BewachV) und damit vor Abschluss eines Arbeitsvertrages zu klären, ob die Person tatsächlich zuverlässig ist. Zu diesem Zweck lassen sich die Unternehmen die Selbstauskunft vorlegen.

Auf eine kürzlich vom LKA durchgeführte Bund-Länder-Umfrage zur Verfahrensweise in Fällen der fremdbestimmten Selbstauskunft haben die Bundesländer Baden-Württemberg, Bayern, Berlin, Hamburg, Niedersachsen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt und Schleswig-Holstein sowie das Bundeskriminalamt geantwortet. Danach wird nach wie vor unterschiedlich reagiert.

In einigen Ländern wird die Auskunft erteilt, teilweise erfolgt allerdings eine ausführliche Erläuterung der Rechtslage unter Hinweis auf die Regelungen des Bundeszentralregisters. Zum Teil wird ein drittbestimmter Antrag auf Selbstauskunft nicht bearbeitet bzw. unter Hinweis auf die Rechtslage die mündliche Auskunftserteilung angeboten.

Wie der Hessische Datenschutzbeauftragte zutreffend mitteilt, hat das LKA ebenfalls erwogen, bei erkennbar fremdbestimmten Auskunftsanträgen nur eine mündliche Auskunft zu erteilen. Dieser Verfahrensweise konnte jedoch das Landespolizeipräsidium nicht zustimmen.

§ 29 HSOG schreibt nicht vor, auf welche Art und Weise die Auskunft zu erteilen ist. Dies liegt folglich im pflichtgemäßen Ermessen der Behörde. Im Normalfall wäre es allerdings fehlerhaft, mündlich Auskunft zu erteilen, weil davon auszugehen ist, dass der Betroffene - jedenfalls wenn Daten über ihn gespeichert sind - die Auskunft ggf. zur Prüfung weiterer rechtlicher Schritte benötigt. Nr. 29.1.1 der Verwaltungsvorschrift zum HSOG (VVHSOG) vom 3. Januar 2005 (StAnz. S. 218) sieht deshalb grundsätzlich die schriftliche Auskunftserteilung vor. Wenn die Polizei - wie in den erörterten Fällen - aus den Umständen erkennen kann, dass die mündliche Auskunftserteilung aus der Sicht des Betroffenen sinnlos ist, wäre diese Form der Auskunftserteilung erst Recht ermessensfehlerhaft.

Die mündliche Auskunftserteilung löst deswegen das Problem nicht, sondern setzt die Wertung voraus, dass die Umstände an sich eine Verweigerung der Auskunft erzwingen. Das Motiv des Betroffenen für die Beantragung der Auskunft hat keine Verankerung im Gesetzeswortlaut gefunden. Insbesondere muss die betroffene Person gegenüber der Polizei nicht darlegen, aus welchen Gründen sie die Auskunft begehrt. Die Polizei hat demzufolge nicht zu prüfen, ob jemand die Auskunft beantragt, um sich Klarheit über die polizeilichen Erkenntnisse zu seiner Person zu verschaffen, um einen Löschungsantrag vorzubereiten oder um sie seinem zukünftigen Arbeitgeber vorzulegen. Die Gründe, weswegen ein Auskunftsantrag abgelehnt werden kann, sind ausdrücklich und abschließend in § 29 Abs. 2 und 3 HSOG niedergelegt. Keiner dieser Gründe liegt hier vor. Die Polizei hat daher auch dann eine schriftliche Selbstauskunft zu erteilen, wenn der Betroffene sie seinem zukünftigen Arbeitgeber vorlegen will.

Allerdings konterkariert dieses Verfahren auch die Zielsetzung des Bundeszentralregistergesetzes. Im Ergebnis besteht daher Einvernehmen mit dem Hessischen Datenschutzbeauftragten, dass es unbefriedigend ist, wenn das Auskunftsverfahren in der beschriebenen Form von Dritten instrumentalisiert wird. Eine klarstellende gesetzliche Regelung erscheint schwierig. Dabei wäre auch zu bedenken, dass auf europäischer Ebene gerade ein Rahmenbeschluss zum Datenschutz bei der Polizei beraten wird, der das Auskunftsrecht der betroffenen Person ebenso wenig einschränken soll, wie die derzeitige hessische Regelung. Es liegt letztlich in der Verantwortung des Betroffenen, ob er die Selbstauskunft einem Sicherheitsunternehmen oder anderen Dritten zur Verfügung stellt.

### **Zu 5.2.3 Regelanfrage bei der Polizei vor ausländerrechtlichen Entscheidungen**

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass eine Befugnis der Ausländerbehörden zur generellen Anfrage bei Polizeibehörden vor der Erteilung von Aufenthaltstiteln nicht besteht. Dies hat das Ministerium des Innern und für Sport einer Ausländerbehörde auf Bitte des Hessischen Datenschutzbeauftragten ausdrücklich mitgeteilt.

### **5.3 Verfassungsschutz**

#### **Zu 5.3.1 Entwurf für ein Sicherheitsüberprüfungsgesetz**

Der Entwurf des Hessischen Sicherheitsüberprüfungsgesetzes ist zwischenzeitlich mit dem Hessischen Datenschutzbeauftragten abgestimmt worden. In einem Punkt ist den Anregungen des Hessischen Datenschutzbeauftragten nicht gefolgt worden. Dieser hat sich dagegen ausgesprochen, dass bei Sicherheitsüberprüfungen nach § 7 Sicherheitsüberprüfungsgesetz neben den Anfragen an die Landeskriminalämter und das Bundeskriminalamt auch Anfragen an die örtlichen Polizeidienststellen der innegehabten Wohnorte der zu überprüfenden Person gerichtet werden, da die Anfrage an das Landeskriminalamt zur Erlangung der notwendigen Erkenntnisse ausreichend sei. Die Anfrage an die örtlichen Polizeidienststellen wurde jedoch zunächst für sinnvoll erachtet.

Nach erneuter Prüfung beabsichtigt das Ministerium des Innern und für Sport dem Kabinett nunmehr im zweiten Kabinettdurchgang vorzuschlagen, entsprechend der Anregung des Hessischen Datenschutzbeauftragten bei Sicherheitsüberprüfungen nach § 7 Sicherheitsüberprüfungsgesetz auf die Anfragen bei den örtlichen Polizeidienststellen zu verzichten.

### **5.4 Verkehrswesen**

#### **Zu 5.4.1 Missbräuchliche Nutzung von Daten der örtlichen Fahrzeugregister durch Bedienstete einer Ordnungsbehörde?**

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass durch automatisierte Protokollierung ein unzulässiger Zugriff auf Daten von Kfz-Haltern aufgedeckt und durch organisatorische Maßnahmen auch die Ordnungsmäßigkeit des Zwecks der Abfrage sowie der Datenempfänger sichergestellt werden kann.

### **Zu 5.5 Schulen und Schulverwaltung**

Die Landesregierung schließt sich den Ausführungen des Hessischen Datenschutzbeauftragten an.

Eine weitere Sensibilisierung der Mitarbeiterinnen und Mitarbeiter in Schulen und Schulverwaltung hinsichtlich datenschutzrelevanter Probleme wird sicher auch durch die Information über die in der Vorbereitung befindlichen Regelungen über die Verarbeitung personenbezogener Daten in Schulen erreicht.

### **5.6 Forschung**

#### **Zu 5.6.1 Aufbau des Deutschen Hämophilieregisters**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

In dem Register sollen Daten von Patienten mit Hämophilie A, B und Willebrand-Syndrom erfasst werden. Das Sozialministerium war in den Abstimmungsprozess im Rahmen des Aufbaus des Datenschutzkonzepts nicht eingebunden.

#### **Zu 5.6.2 Generisches Datenschutzkonzept für Biomaterialbanken**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Biomaterialbanken dienen der molekulargenetischen Erforschung von komplexen Erkrankungen. Sie enthalten Biomaterialien wie z.B. Zellen, Gewebe und Blut, die aufgrund ihrer Zweckbestimmung (DNA-Analyse) keine Arzneimittel sind. Das Sozialministerium war in den Abstimmungsprozess im Rahmen des Aufbaus des Datenschutzkonzepts nicht eingebunden.

### **Zu 5.6.3     Datenschutz bei der Arzneimittelprüfung**

Die Landesregierung stimmt der vom Hessischen Datenschutzbeauftragten beabsichtigten weiteren Vorgehensweise ausdrücklich zu.

## **5.7           Gesundheitswesen**

### **Zu 5.7.1     Einführung des flächendeckenden Mammographie-Screenings**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zum Mammographie-Screening in Hessen zu.

Die Einführung des flächendeckenden Mammographie-Screenings in Hessen betrifft sowohl den gesundheitspolitischen Aspekt als auch den Röntgenstrahlenschutz. Alle Abstimmungen verliefen in engem Kontakt mit dem Hessischen Datenschutzbeauftragten, wobei seine Einwände und Anregungen berücksichtigt werden konnten.

### **Zu 5.7.2     Verwendung von Pflegedokumentationen bei der Durchführung von Qualitätsprüfungen in Pflegeeinrichtungen**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

### **Zu 5.7.3     Kopflausbefall von Kindern - ein Fall für das Gesundheitsamt**

Kopflausbefall (Pedikulose) ist gemäß Infektionsschutzgesetz (IfSG) keine meldepflichtige Erkrankung. Gleichwohl schreibt das IfSG, wie im 35. Tätigkeitsbericht wörtlich zitiert, bei Verlausung in einer Gemeinschaftseinrichtung der Leitung dieser Einrichtung verpflichtend vor, das zuständige Gesundheitsamt unverzüglich zu benachrichtigen und krankheits- und personenbezogene Angaben zu machen.

Zunächst ergibt sich bei Befall von Kopfläusen für die Kinder ein Besuchsverbot und für die Mitarbeiterinnen und Mitarbeiter ein Tätigkeitsverbot nach § 34 IfSG. Darüber hinaus gibt der Gesetzgeber den Gesundheitsämtern die rechtliche Handhabe, die Entwesung der mit Läusen und Nissen verunreinigten Räumlichkeiten und Gegenstände nach § 18 in Verbindung mit § 17 IfSG anzuordnen.

Aufgrund der namentlichen Meldungen können die Gesundheitsämter außerdem dazu beitragen, den Kopflausbefall bei den Betroffenen einzudämmen, indem sie beratend und unterstützend tätig werden. Kernpunkt dieser Maßnahmen ist die fachliche und organisatorische Unterstützung der Leitungen von Schulen bzw. Kinder- und Jugend-Gemeinschaftseinrichtungen bei der Beseitigung des Kopflausbefalls. Die Gesundheitsämter stellen sowohl für die Einrichtungen als auch für die Betroffenen geeignete Informationsmaterialien bereit. Ziel ist die rasche, korrekte und komplette Untersuchung der gesamten betroffenen Personengruppe.

Die Untersuchung und Beseitigung von Läusen und Nissen ist zunächst eine Aufgabe der Eltern. Die Gesundheitsämter selbst dürfen nur subsidiär tätig werden. Bei wiederholtem Befall mit Kopfläusen suchen die Gesundheitsämter ggf. die Einrichtungen auf und kontrollieren im Einzelfall, ob die betroffenen Kinder läusefrei sind bzw. was als Ursache für den wiederholten Befall eines Kindes auszumachen ist. Nur anhand der gemeldeten Daten ist es möglich, diese Maßnahmen einzuleiten, um die Wiedererkrankungsrate der Kinder an Kopfläusen soweit wie möglich zu minimieren. Die Erhebung der Daten dient grundsätzlich der Vorbeugung der Ausbreitung von Infektionskrankheiten.

Die Speicherdauer der Daten ist weder im FSG noch im HDSG konkret geregelt, da von Fall zu Fall eine höchst unterschiedliche Dauer der Aufbewahrung notwendig sein kann, insbesondere um die Ursache für den wiederholten Befall zu klären. Die Gesundheitsämter sind aber nach § 19 Abs. 3 HDSG verpflichtet, regelmäßig zu prüfen, ob die Erforderlichkeit der Datenspeicherung noch besteht.

Dem Sozialministerium ist die vom Hessischen Datenschutzbeauftragten angesprochene Problematik der unbestimmten Speicherdauer bekannt. Es

wird angestrebt, in Abstimmung mit dem Hessischen Datenschutzbeauftragten eine Regelung zu finden, die sowohl die Interessen der Betroffenen berücksichtigt, als auch die zur Vorbeugung der Ausbreitung notwendigen Daten sicherstellt.

#### **5.7.4 Übermittlung von Versichertendaten durch die AOK Hessen an Versand-Apotheken**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

### **5.8 Sozialwesen**

#### **Zu 5.8.1 Kindeswohl und Datenschutz**

In dem beschriebenen Fall stellt der Hessische Datenschutzbeauftragte fest, dass das Kindeswohl nach § 8a SGB VIII Vorrang vor dem Recht der Eltern des Kindes auf informationelle Selbstbestimmung hat.

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass der spezielle kinder- und jugendhilferechtliche Datenschutz eine die Förderung des Kindeswohls unterstützende Funktion hat. Der Vorrang des Kindeswohls ist selbst dann gegeben, wenn eine Beeinträchtigung des Elternrechts, wie die im Tätigkeitsbericht beschriebene, vorliegt.

#### **Zu 5.8.2 Auskunftsanspruch von Unfallversicherungsträgern gegenüber Ärzten**

Die im Tätigkeitsbericht betonte Pflicht zur Auskunftserteilung kann rechtlich zutreffend von einer Pflicht zur Herausgabe einer Urkunde, des Krankenhausärztlichen Entlassungsberichts, unterschieden werden. Dies ist jedoch von der datenschutzrechtlich im engeren Sinne relevanten Frage zu unterscheiden, in welchem Umfang Auskünfte nach § 203 S. 1 SGG VII verlangt werden können. Nach herrschender Meinung (vgl. hierzu und im Folgenden z.B. Hauck/Noftz, SGB VII, Kommentar, Loseblatt, § 203 Rn 7 ff.) wird durch diese Vorschrift im Rahmen des Erforderlichen eine umfassende Verpflichtung zur Auskunft über medizinische Daten normiert. Ausdrücklich genannt sind die Behandlung, der Zustand sowie die Erkrankungen und frühere Erkrankungen des Versicherten, darüber hinaus aber Daten, die für die medizinische Beurteilung relevant sind bzw. relevant sein können. Nach Abs. 1 S. 1 und 2 dieser Vorschrift ist die Auskunftspflicht allerdings insoweit begrenzt, als nur Angaben verlangt werden können, die "für die Heilbehandlung und die Erbringung sonstiger Leistungen erforderlich" sind. Dabei ist zu berücksichtigen, dass mit den Auskunftsverlangen der Unfallversicherungsträger meist die Grundlagen für medizinische Gutachten vorbereitet werden, durch die erst schwierige Zusammenhänge geklärt werden sollen.

Datenschutzrechtlich kann die Übersendung oder die Anforderung eines krankenhausesärztlichen Entlassungsberichts somit nur dann beanstandet werden, wenn und soweit damit diese Grenzen der Auskunftspflicht überschritten werden.

Die weiteren rechtlichen Ausführungen des Tätigkeitsberichts können aufgrund der unklaren tatsächlichen Verhältnisse, die Anlass für die Prüfung des Hessischen Datenschutzbeauftragten waren, nicht abschließend beurteilt werden. Sollte tatsächlich ein Unfallversicherungsträger einen begünstigenden Verwaltungsakt allein deshalb abgelehnt haben, weil der behandelnde Krankenhausarzt die Übersendung des Entlassungsberichts ablehnt, so wäre dies sicherlich rechtswidrig, vor allem deshalb, weil insoweit dem Versicherten das Verhalten eines Dritten in unzulässiger Weise zugerechnet würde. In der Praxis finden sich demgegenüber nicht selten Entscheidungen, mit denen eine positive Entscheidung in der Sache unter Hinweis auf die dem Versicherten obliegende materielle Beweislast für die Leistungsvoraussetzungen versagt wird, wenn dieser seine Mitwirkungspflichten bei der Sachaufklärung verletzt, z.B. indem er zumutbare medizinische Untersuchungen nicht zulässt und/oder der Verwertung entscheidungsrelevanter medizinischer Unterlagen nicht zustimmt und hierdurch die Sachaufklärung unmöglich oder ganz erheblich erschwert wird.

### **Zu 5.8.3 Übermittlung von Sozialdaten zu Zwecken der Durchführung eines Disziplinarverfahrens**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

### **Zu 5.9 Personalwesen**

Die Begleitung der Einführung der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung durch den Hessischen Datenschutzbeauftragten war während der gesamten Projektlaufzeit immer durch eine vertrauensvolle, offene und intensive Zusammenarbeit geprägt.

Die Landesregierung hofft auch in Zukunft bei Anpassungen und Veränderungen des Landesreferenzmodells HR, z. B. bei einem Release-Wechsel, auf eine Fortsetzung dieser guten und konstruktiven Zusammenarbeit und Beratung durch den Hessischen Datenschutzbeauftragten.

Die Landesregierung bedauert daher, wenn es durch unterschiedliche Wahrnehmungen über Absprachen oder Zusagen zum Einsatz des "Merkmals Z" zu Irritationen gekommen ist.

Bei den Dienststellen der HR Einführungsstaffel 06/2006 wurde das "Merkmal Z" bereits im Umsetzungsprozess, das heißt, zum frühestmöglichen Zeitpunkt implementiert. Der Hessische Datenschutzbeauftragte war über Umfang, Zeitpunkt und Ausprägung des "Merkmals Z" in dieser Staffel durch Besuche vor Ort bei dem Ministerium für Wissenschaft und Kunst und dem HCC unterrichtet, sodass das Ministerium für Wissenschaft und Kunst und das Ministerium des Innern und für Sport eine weitere Unterrichtung nicht für erforderlich angesehen haben.

Das Ministerium der Finanzen hat den Hessischen Datenschutzbeauftragten über die pilotweise Einführung des "Merkmals Z" bei zwei Finanzämtern mit E-Mail vom 17. Juli 2006 informiert.

Die übrigen Ressorts haben keine Personaldatensätze mit dem "Merkmal Z" versehen. In einigen Bereichen konnte die Problematik des Entscheidungsvorbehalts des Ministeriums für bestimmte Personalfälle, z. B. Dienststellenleiter, aufgrund der nur geringen Fallzahlen statt über das "Merkmal Z" durch organisatorische Maßnahmen gelöst werden, in dem die Systempflege für diese Personalfälle vor Ort erfolgt.

Diese Ressorts gingen davon aus, dass eine Unterrichtung des Hessischen Datenschutzbeauftragten nur bei Verwendung des "Merkmals Z" gewünscht sei.

Im Ministerium der Justiz erfolgt die Berechtigungssteuerung über einen gesonderten Mitarbeiterkreis.

Die bei Teilen der Ressorts ursprünglich bestehenden Bedenken bezüglich der technischen Umsetzung des "Merkmals Z" haben sich nicht bestätigt. Die Beschränkungen aufgrund des "Merkmals Z" bei Berichten und Auswertungen werden derzeit zum Teil durch entsprechende Nacharbeiten außerhalb des Systems ausgeglichen.

Unter anderem auch vor diesem Hintergrund hat der Kabinettsausschuss "Verwaltungsreform und Verwaltungsinformatik" am 10. Oktober 2006 beschlossen, dass eine Arbeitsgruppe bestehend aus Vertretern des Finanz-, Innen- und Kultusministeriums sowie des Justizministeriums und der Staatskanzlei u. a. prüfen soll, ob und ggf. welche Rechtsänderungen möglich und sachgerecht wären, um hier zu Verbesserungen zu kommen. Diese Prüfung ist noch nicht abgeschlossen. Das Ergebnis der Prüfung wird mit dem Hessischen Datenschutzbeauftragten eingehend erörtert werden.

Bislang war ein versehentliches Ansteuern "fremder" Drucker, z. B. in anderen Behörden, systemseitig nicht ausgeschlossen. Die Feststellungen des Hessischen Datenschutzbeauftragten sind insoweit zutreffend. Zwischenzeitlich konnte in Zusammenarbeit mit dem Hessischen Datenschutzbeauftragten eine Lösung entwickelt werden. An deren Umsetzung wird gegenwärtig gearbeitet.

Im Rahmen des Release-Wechsels bei SAP HR werden u.a. auch Änderungen des Verfahrens bei der Personalkostenhochrechnung geprüft und die Beratung durch den Hessischen Datenschutzbeauftragten begrüßt.

## **5.10 Finanzwesen**

### **Zu 5.10.1 Kontendatenabrufersuchen nach §§ 93 Abs. 7 und 8, 93b AO**

Nach Auffassung des Hessischen Datenschutzbeauftragten haben sich insbesondere Mängel bei der Dokumentation der Kontenabrufe sowie bei der Information der Betroffenen ergeben. Der Arbeitskreis Steuerverwaltung der Datenschutzbeauftragten des Bundes und der Länder hat dazu ein Muster- und Maßnahmen-Formular entwickelt.

Der Einsatz dieses Formulars wurde von der Arbeitsgruppe AO grundsätzlich begrüßt. Die Arbeitsgruppe AO hat den Vordruck dann in der Sitzung AGAO II/2006 inhaltlich und redaktionell überarbeitet. Dieser Vordruck wird derzeit von der Oberfinanzdirektion Frankfurt am Main noch automatisch aufbereitet. Mit einem Einsatz in den hessischen Finanzämtern ist in Kürze zu rechnen.

Im Übrigen ist Folgendes zu bemerken:

Die Anmerkungen des Hessischen Datenschutzbeauftragten zur Erforderlichkeit des Kontenabrufs und zur Dokumentation der Entscheidung lassen die Ansicht erkennen, ein Kontenabruf im Vollstreckungsverfahren dürfe nur als letzte Maßnahme durchgeführt werden.

Diese Ansicht kann weder aus dem Gesetz noch aus dem Anwendungserlass zur AO (AEAO) oder aus anderen Verwaltungsanweisungen abgeleitet werden.

Die Finanzbehörden sind nach den Vorschriften der Abgabenordnung verpflichtet, festgesetzte Steueransprüche erforderlichenfalls zwangsweise durchzusetzen. Zur Vorbereitung der Vollstreckung können die Finanzbehörden die Vermögens- und Einkommensverhältnisse des Vollstreckungsschuldners ermitteln (§ 249 Abs. 2 Satz 1 AO). Nach der Ermittlung der Vermögens- und Einkommensverhältnisse des Vollstreckungsschuldners sollen die Maßnahmen ergriffen werden, von denen unter Berücksichtigung der Belange des Vollstreckungsschuldners am schnellsten und sichersten ein Erfolg zu erwarten ist (Abschnitt 23 Abs. 2 VollstrA). Diese Voraussetzungen werden am besten durch die Pfändung von Kontoguthaben oder Depotwerten erfüllt. Da Vollstreckungsschuldner solche Vollstreckungsmöglichkeiten in der Regel dem Gläubiger nicht freiwillig offenbaren, sondern im Gegenteil versuchen, diese Werte der Vollstreckung zu entziehen, ist ein Kontenabruf im Vollstreckungsverfahren grundsätzlich immer geeignet. Es kann auch nicht auf andere Ermittlungsmöglichkeiten zur Aufdeckung von verborgenem Vermögen, wie beispielsweise das Verfahren zur Abgabe der eidesstattlichen Versicherung, verwiesen werden. Zum einen können hier Vermögenswerte trotz Strafandrohung verschwiegen werden, zum anderen ist die eidesstattliche Versicherung für den Vollstreckungsschuldner wegen der Eintragung in das Schuldnerverzeichnis wesentlich einschneidender als der Kontenabruf. An der Erforderlichkeit des Kontenabrufs kann es allenfalls dann fehlen, wenn die Vollstreckung nach den bekannten Vermögens- und Einkommensverhältnissen des Vollstreckungsschuldners aussichtslos erscheint und eine Vermögensverschleierung unwahrscheinlich ist oder die Höhe der Forderung den mit dem Kontenabruf verbundenen Verwaltungsaufwand nicht rechtfertigen kann (vgl. AEAO, § 93 Tz. 2.3 2. Abs.).

Der Hessische Datenschutzbeauftragte bemängelt ferner, in den meisten Fällen sei keine Dokumentation darüber vorhanden, ob der Steuerpflichtige gehört wurde. Es handelt sich hier sicherlich nicht um eine fehlende Dokumentation, sondern tatsächlich um eine fehlende Anhörung. Wenn 85 % der Kontenabrufe im Vollstreckungsbereich stattfinden, ist dies allerdings nicht verwunderlich. § 93 Abs. 7 AO setzt zwar grundsätzlich ein vorheriges Auskunftsverlangen an den Steuerpflichtigen voraus. Im Vollstreckungsverfahren verbietet es sich jedoch, zunächst ein Auskunftersuchen zur Ermittlung einer Bankverbindung an den Vollstreckungsschuldner zu richten. Er könnte diese Gelegenheit u.U. nutzen, das Konto "abzuräumen".

Abschließend bezweifelt der Hessische Datenschutzbeauftragte allgemein den Erfolg der Maßnahme "Kontenabruf". Es habe nur sehr wenige erfolgreiche Fälle gegeben. In einem Einzelfall seien Mehrsteuern in Höhe von 22.000 € festgesetzt worden. Im Vollstreckungsverfahren seien einmal 9.300 € aufgrund der Pfändung in eine neu bekannt gewordene Bankverbindung erhoben worden. Entscheidend ist, wie man "erfolgreich" im Zusammen-



hang mit dem Kontenabruf definiert. Nach Ansicht der Landesregierung ist das Verfahren auch dann erfolgreich, wenn dadurch festgestellt werden kann, dass die Steuerpflichtigen ihren Erklärungspflichten ordnungsgemäß nachgekommen sind oder wenn im Vollstreckungsverfahren durch den Kontenabruf ermittelt wurde, dass der Vollstreckungsschuldner vermögenslos ist und der Fall - natürlich auch aufgrund weiterer Ermittlungen - durch Niederschlagung beendet werden kann.

## **Zu 6. Kommunen**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

## **7. Sonstige Selbstverwaltungskörperschaften**

### **Zu 7.1 Hochschulen**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

### **7.2 Sparkassen**

#### **Zu 7.2.1 Sparkasse zeichnete rechtswidrig Telefongespräche auf**

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die Sparkasse Telefonanrufe von Kunden ohne wirksame Einwilligung der Betroffenen im Sinn des Datenschutzrechts aufgezeichnet hat.

Eine Strafbarkeit von Verantwortlichen der Sparkasse nach § 201 Abs. 1 Nr. 1 StGB dürfte nach dem mitgeteilten Sachverhalt jedoch nicht gegeben sein, weil das Aufzeichnen der Telefongespräche nicht "unbefugt" im Sinne der Strafvorschrift, sondern mit einem den Tatbestand der Norm ausschließenden Einverständnis der Anrufer erfolgt ist. Ein solches Einverständnis liegt hier deshalb vor, weil die Anrufer durch die automatisierte Ansage, mit welcher ausdrücklich auf die Gesprächsaufzeichnung hingewiesen wurde, Kenntnis von dem Umstand der Aufzeichnung hatten und durch das Weiterführen des Telefonats konkludent in die Aufzeichnung einwilligten.

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

### **8.1 Zentrale DV in der Landesverwaltung**

#### **Zu 8.1.1 Ausgangslage**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

#### **Zu 8.1.2 Wichtige Entscheidungen**

Gemäß der Leitlinie der Hessen-PKI werden die Zertifikate für die fortgeschrittene elektronische Signatur auf Smartcards herausgegeben. Die Zertifikate für fortgeschrittene und qualifizierte elektronische Signaturen werden durch getrennte PINs geschützt.

In § 2 Nr. 2c Signatur-Gesetz (SigG) wird verlangt, dass fortgeschrittene elektronische Signaturen "...mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann...", für qualifizierte elektronische Signaturen verlangt § 2 Nr. 3b SigG zusätzlich, dass sie "mit einer sicheren Signaturerstellungseinheit erzeugt werden ...".

In der Hessen-PKI werden auch die fortgeschrittenen Signaturen mit einer sicheren Signaturerstellungseinheit (SmartCard NetKey E4) erzeugt und so ein deutlich höheres Sicherheitsniveau erzielt, als es das Signaturgesetz für fortgeschrittene elektronische Signaturen verlangt.

Die Anregung des Hessischen Datenschutzbeauftragten zur dauerhaften Speicherung verschlüsselt eingegangener Dokumente ist berechtigt. Sie wird in der technischen Spezifikation berücksichtigt und die Anwender im Sinne dieser Anregung geschult. Darüber hinaus werden die Organisationsverant-

wortlichen der Dienststellen gezielt auf die Problematik hingewiesen. Dem Bedarf für eine verschlüsselte, dauerhafte Speicherung wird mit der dafür eingerichteten Arbeitsgruppe "Gruppenverschlüsselung", unter Beteiligung des Hessischen Datenschutzbeauftragten, begegnet (siehe unten zu 8.1.4).

Die Beratung durch den Hessischen Datenschutzbeauftragten bei der Behandlung des Verfahrens "eBeihilfe" im Rahmen des AD-Projekts hat dazu geführt, dass für dieses Verfahren mit hochsensiblen Daten eine getrennte AD-Domäne eingerichtet wurde.

### **8.1.3 Prüfungen**

#### **Zu 8.1.3.1 Zentrale E-Mail**

Der Forderung des Hessischen Datenschutzbeauftragten hinsichtlich einer erweiterten Protokollierung und der Schaffung einer IT-Revisionsstelle in der HZD wurde umgehend Rechnung getragen. Diese Revisionsstelle hat ihre Arbeit aufgenommen.

#### **Zu 8.1.3.2 Prüfung in Hünfeld**

Die Darstellung des Hessischen Datenschutzbeauftragten, dass das Administrationsteam weder ausschließlich die Systeme der Justiz betreut, noch dass die Systeme der Justiz nur am Standort Hünfeld betrieben werden, ist zutreffend. Diese Organisation der Administration erfolgte im Rahmen des Beschlusses des Kabinettsausschusses "Verwaltungsreform und Verwaltungsinformatik" vom 9. Dezember 2004. Der Beschluss müsste dem Hessischen Datenschutzbeauftragten bekannt sein, weil er ihm nachrichtlich zugestellt wurde.

Das Administrationskonzept unterliegt laufend der Abstimmung mit dem Hessischen Datenschutzbeauftragten. Nicht zuletzt in der Klausur zwischen dem CIO und dem Hessischen Datenschutzbeauftragten am 26. Juni 2006 bestand die Möglichkeit, strittige Fragen grundsätzlicher Natur anzusprechen. Dieses Thema wurde auf der Klausur nicht vom Hessischen Datenschutzbeauftragten problematisiert. Gleichwohl unternimmt die HZD in vertrauensvoller Zusammenarbeit mit dem Ministerium der Justiz und dem Hessischen Datenschutzbeauftragten auf Arbeitsebene erhebliche Anstrengungen, die Kritikpunkte abzarbeiten und hat im vorliegenden Fall sehr zeitnah Erweiterungen in der Protokollierung der Zugriffe auf E-Mail und AD der Justiz durch die Mitarbeiter der HZD umgesetzt.

#### **Zu 8.1.4 Sachstand zur Verschlüsselung**

Die Ausführungen des Hessischen Datenschutzbeauftragten geben den Sachstand korrekt wieder. Die Landesregierung verfolgt in enger Abstimmung mit dem Hessischen Datenschutzbeauftragten das Ziel, eine Lösung bereitzustellen, die es erlaubt, Dokumente mit hohem Schutzbedarf verschlüsselt im Dokumenten-Managementsystem zu speichern.

#### **Zu 8.1.5 Sachstand Terminalserver**

Im Rahmen des Projekts "DMS" besteht zurzeit innerhalb der Teilprojekte "eAkte" und "Archivierung" sowie im Projekt "HCN" eine intensive Zusammenarbeit mit dem Hessischen Datenschutzbeauftragten.

Da das im Tätigkeitsbericht angesprochene Produkt "GERVA" zwischenzeitlich vom Markt genommen wurde, gibt es derzeit kein explizit für den Einsatz im Terminalserverumfeld zertifiziertes und nach dem SigG bestätigtes Produkt. Daher wird weiter nach einer Lösung gesucht, die den Anforderungen des SigG genügt.

Der Hessische Datenschutzbeauftragte führt im Tätigkeitsbericht weiter aus, die Einbindung der elektronischen Signatur in Fachverfahren werde nach dem Ende der Ausschreibung für eine Signatursoftware weiterbehandelt. Inzwischen wurde dem Hessischen Datenschutzbeauftragten das Ergebnis der Ausschreibung mitgeteilt und es werden erste Tests zur Integration in Fachverfahren durchgeführt. Nach Abschluss dieser grundlegenden Tests werden die weiteren Schritte mit dem Hessischen Datenschutzbeauftragten abgestimmt.

## **Zu 8.2 Einsatz zentraler Spam-Filter in der Landesverwaltung**

Die ausführlichen Anmerkungen des Hessischen Datenschutzbeauftragten zur privaten Nutzung des E-Mail-Dienstes sind für die Landesregierung sehr hilfreich.

Die sehr streitige Rechtslage und die strafrechtlichen Probleme im Hinblick auf den Einsatz von Spam-Filtern bei zugelassener privater E-Mail-Nutzung wird vom Hessischen Datenschutzbeauftragten zutreffend wieder gegeben. In Betracht kommt durch den Einsatz des Spam-Filters eine Strafbarkeit nach § 206 Abs. 2 Nr. 2 und § 303a StGB.

Bei § 206 StGB ist bereits fraglich, ob die Dienststelle, die den Beschäftigten die private E-Mail-Nutzung gestattet, zum Anbieter eines Telekommunikationsdienstes wird, der diese Tätigkeit geschäftsmäßig ausübt, wobei eine Gewinnerzielungsabsicht nicht gefordert ist. Dies wird zum Teil für Behörden auch dann bestritten, wenn sie Telekommunikationsleistungen für Dritte erbringen. Streitig ist darüber hinaus, unter welchen Voraussetzungen Sendungen "anvertraut" sind. Nach herrschender Meinung in der Literatur sind nur körperliche Gegenstände geschützt, so dass der E-Mail-Verkehr insoweit vom Schutzbereich ausgenommen wäre. Schließlich muss auch die Tatbestandsvoraussetzung "unbefugt" erfüllt sein, die bei einem - zum Beispiel im Rahmen einer Dienstvereinbarung über E-Mail-Nutzung - erteilten Einverständnis aber entfällt.

Bei einer möglichen Strafbarkeit nach § 303a StGB stellt sich die Frage, wie im Übrigen auch für § 206 Abs. 2 Nr. 2 StGB, ob eine E-Mail unterdrückt werden kann, wenn sich die E-Mail noch nicht vollständig in der Mail-Box des Empfängers befindet, was durch den Einsatz der Spam-Filter der Fall wäre. In der Literatur wird dies verneint. Darüber hinaus stellt sich auch hier die Frage der Rechtswidrigkeit, die bei Vorliegen eines Einverständnisses entfällt.

Zu beiden Vorschriften liegt für die dargestellte Problematik noch keine Rechtsprechung vor, so dass eine endgültige rechtliche Bewertung nicht abgegeben werden kann. Die juristische Diskussion zum Thema private E-Mail-Nutzung und Spam-Filter wird weiter aufmerksam beobachtet. Bei der Erarbeitung der eigenen Position werden auch die Erfahrungen der anderen Bundesländer und des Bundes im Rahmen des KoopADV Berücksichtigung finden.

Die Landesregierung sieht derzeit keinen Handlungsbedarf, da gemäß der E-Mail-Richtlinie (Stand vom 4. Mai 2005, Anlage 6 zu § 12a GGO) elektronische Post grundsätzlich nur für dienstliche Zwecke genutzt werden darf.

Das Ministerium des Innern und für Sport hat die HZD inzwischen angewiesen, die Daten der Greylisting-Datenbank ausschließlich zur Abwehr von Spam-E-Mails zu verwenden. Eine Auswertung zur Verhaltens- oder Leistungskontrolle erfolgt nicht. Auch werden keine Kommunikationsprofile einzelner Personen erstellt.

Die vom Hessischen Datenschutzbeauftragten vorgeschlagene Aufteilung der Daten eines Kommunikationsvorgangs auf verschiedene Datenbanken oder die Speicherung in Form von Hash-Werten wird von der am Markt verfügbaren und für die E-Mail-Umgebung geeigneten Greylisting-Software nicht unterstützt. Die Reduzierung der zu speichernden Daten durch "Whitelisting" wurde bereits im fachlichen Konzept berücksichtigt. Darüber hinaus wird geprüft, ob das Whitelisting teilweise automatisiert und so der Umfang zu speichernder Daten - im Sinne der Datensparsamkeit - weiter reduziert werden kann.

## **8.3 Dokumentenmanagement in der öffentlichen Verwaltung**

### **Zu 8.3.1 Dokumentenmanagement in der Hessischen Landesverwaltung**

Im Rahmen der Projektarbeit zur Einführung eines DMS in der Landesverwaltung ist auf die frühzeitige Einbeziehung des Hessischen Datenschutzbeauftragten großen Wert gelegt worden, um datenschutzrechtliche Fragestellungen von Anfang an in die Betrachtung mit einzubeziehen.

Die Zusammenarbeit beschränkt sich nicht nur auf die intensive Beratung der Themen in der Arbeitsgruppe "Datenschutz", sondern erstreckt sich auch auf begleitende Felder, z. B. die Einbindung der Signatur in das DMS,

die elektronische Aktenführung, die Erarbeitung eines Aktenführungserlasses, die Aussonderung und Archivierung elektronischer Akten. Der Hessische Datenschutzbeauftragte wird weiterhin zu den Sitzungen der Projektgruppe "DMS" eingeladen werden, in der die Staatskanzlei und alle Ressorts vertreten sind.

In der AG "Datenschutz" wurden die im Rahmen der Einführung von IT-Verfahren nach dem HDSG erforderlichen Dokumente (Vorabkontrolle nach § 7 Abs. 6 HDSG; Verfahrensverzeichnis nach § 6 HDSG) als Muster erarbeitet. Sie wurden den Dienststellen, die DMS einführen, zur Verfügung gestellt. Auf dieser Grundlage führen die Dienststellen die Untersuchungen nach § 7 Abs. 6 HDSG durch, zeichnen das Ergebnis und dessen Begründung auf und leiten es dem behördlichen Datenschutzbeauftragten zur Prüfung zu.

Wie in Ziffer 8.3.1 des Tätigkeitsberichts ausgeführt, haben bereits einbezogene Dienststellen eigene Vorabkontrollen erstellt und mit ihren behördlichen Datenschutzbeauftragten abgestimmt. Im Rahmen der Umstellung der Registraturen und der Einrichtung von Scan-Stellen erfolgte dies in der Staatskanzlei und allen Ministerien unter Zugrundelegung der zentral erarbeiteten Muster. Auch das Präsidium für Technik, Logistik und Verwaltung, das ebenfalls den Muster-Registratur-Client (MRC) einführte, hat eine Vorabkontrolle nach diesem Muster angefertigt.

Für die Einführung des Bearbeiter-Clients, des Muster-DMS-Clients (MDC), wurde die gleiche Vorgehensweise gewählt. Der MDC wird derzeit bereits in nahezu allen Ministerien, der Staatskanzlei, der HZD, dem Hauptstaatsarchiv Wiesbaden und dem Amt für Lehrerbildung, Frankfurt (AfL) eingesetzt. Vorabkontrollen hat neben den vom Hessischen Datenschutzbeauftragten erwähnten Ministerien inzwischen auch die HZD erstellt und mit ihrem behördlichen Datenschutzbeauftragten abgestimmt.

Ferner wurde mit dem Hessischen Datenschutzbeauftragten ein Standard-Berechtigungskonzept erörtert und einvernehmlich erstellt. Zentrale Frage war dabei, welche Daten in eine Recherche einbezogen und welche Treffer dem Recherchierenden angezeigt werden dürfen. Im Ergebnis wurde Einvernehmen darüber erzielt, dass sich Recherchen über den gesamten Datenbestand inklusive der Metadaten erstrecken können, als Treffer aber nur die Datensätze angezeigt werden dürfen, für die Recherchierende mindestens über ein Leserecht verfügen.

Auch dieses Standardwerk sowie eine Anleitung zur Erstellung eines dienststellenbezogenen Berechtigungskonzepts stehen nunmehr den Dienststellen als Muster zur Verfügung.

Nach der erfolgreichen Ausschreibung der Signatur-Software wird mittlerweile deren Einbindung in das DMS projektseitig evaluiert. Die rechtlichen Rahmenbedingungen der elektronischen Signatur wurden in mehreren Gesprächen zwischen dem Projekt "DMS" und dem Hessischen Datenschutzbeauftragten abgestimmt.

### **Zu 8.3.2 Orientierungshilfe Datenschutz bei Dokumentenmanagementsystemen**

Die Orientierungshilfe "Datenschutz bei Dokumentenmanagementsystemen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder enthält eine umfassende Beschreibung datenschutzrechtlicher Aspekte und schlägt zahlreiche Maßnahmen vor. Die Landesregierung begrüßt diese Orientierungshilfe und nutzt sie im Rahmen der Einführung des DMS in der Landesverwaltung.

Zahlreiche Anregungen und Hinweise der Orientierungshilfe wurden aufgenommen und umgesetzt. Einige der vorgeschlagenen Maßnahmen können aus heutiger Sicht aus technischen oder wirtschaftlichen Gründen nicht umgesetzt werden. Andere vorgeschlagene Maßnahmen werden bei der Erstellung der noch ausstehenden Feinkonzepte geprüft.

## **9. Bilanz**

### **Zu 9.1 Videoüberwachung an der Konstablerwache in Frankfurt (34. Tätigkeitsbericht, Ziff. 5.3.1)**

Hinsichtlich der Videoüberwachung im Bereich der Konstablerwache steht das Polizeipräsidium Frankfurt am Main im ständigen Kontakt zum Hessi-

schen Datenschutzbeauftragten. Wie dieser zutreffend bemerkt, ist die Situation derzeit nicht völlig zufriedenstellend gelöst.

Entsprechend der Absprache mit dem Hessischen Datenschutzbeauftragten im Vorfeld der Fifa-WM 2006 hat das Polizeipräsidium Frankfurt am Main alle erforderlichen Hinweisschilder auf dem videoüberwachten Raum angebracht. Ebenso wurde das Verzeichnis auf die miterfassten Straßenzüge erweitert und die Dienstanweisung für die Videoüberwachungsanlagen Konstablerwache und Hauptbahnhof erneuert.

Darüber hinaus sollten neue Kameras beschafft werden, bei denen die Einsicht in Privatbereiche unterbunden werden kann. Bis zur Umsetzung wurde der Situation durch eine entsprechende Regelung in der Dienstanweisung Rechnung getragen.

Hinsichtlich des anstehenden Austausches der Kameras 1 und 3 durch DOME-Kameras hat das Polizeipräsidium Frankfurt am Main der Stadt Frankfurt am Main im Mai 2006 vorgeschlagen, dass diese die Videoüberwachungsanlage Konstablerwache übergeben bekommt und – im Gegenzug – für den weiteren Betrieb und anstehende Investitionen die Kosten übernimmt.

Im Oktober 2006 hat das Polizeipräsidium Frankfurt am Main das Landespolizeipräsidium gebeten, zu prüfen, ob hinsichtlich der durch den beabsichtigten Kameraaustausch bedingten Kosten von ca. 20.000,- € bis 40.000,- € eine Lösungsmöglichkeit bestehe. Dazu wurde das Angebot einer Fachfirma eingeholt, wonach für den Austausch der Kameras 1 und 3 sowie für die Programmierung der Privatschutzzonen in der Software der neuen Kameras Kosten in Höhe von knapp 30.000 € anfallen.

Nachdem bis zum Jahresende 2006 keine Antwort der Stadt vorlag, hat schließlich das Innenministerium im Januar 2007 die Stadt Frankfurt am Main gebeten, sich zu dem Vorschlag des Polizeipräsidiums zu äußern. Die Antwort der Stadt steht noch aus.

Im weiteren Verfahren wird das Polizeipräsidium auch prüfen, ob für den videoüberwachten Bereich noch die gesetzlichen Voraussetzungen des § 14 HSOG gegeben sind.

#### **Zu 9.2 Sachstand der korrekten Umsetzung der Löschung von aussondernden Datenspeicherungen der Polizei (34. Tätigkeitsbericht, Ziff. 5.3.2)**

Die Feststellungen des Hessischen Datenschutzbeauftragten zu den Fehlern beim Aussonderungsprüfverfahren wurden zum Anlass genommen, die Problemstellung von Grund auf detailliert zu analysieren. Es fanden hierzu mehrere – zum Teil länderübergreifende - Workshops und Abstimmungen statt. Durch die Komplexität des Systems war die Thematik aufgrund des hohen Abstimmungsaufwands mit dem Bundeskriminalamt, der Entwicklung POLAS bzw. INPOL-Land und innerhalb der Kooperation der Länder sowohl fachlich als auch zeitlich sehr aufwändig.

Zu überarbeiten waren nicht nur die Aussonderungsprüfung für die U-Gruppe (Nachweis über eine kriminalpolizeiliche Unterlage, insbesondere Kriminalakte), sondern auch die Aussonderung der Daten verstorbener Personen sowie die Überwachung der E-Gruppen (Erkennungsdienst). Hier kam es bei den regelmäßigen Löschläufen immer wieder zu Fehlern durch das Einspielen von veralteten oder fehlerhaften Scripten.

Die Betriebsabläufe sind nunmehr optimiert. Aufgrund der Erfahrungen der Vergangenheit wurde dabei Wert auf eine gesicherte und ordnungsgemäße Umsetzung sowie entsprechende Tests und Abnahmen gelegt. Mit der aktuellen Umsetzung sind alle im Bericht des Hessischen Datenschutzbeauftragten ehemals gerügten Sachverhalte einer Lösung zugeführt worden. Ein gesonderter ausführlicher Abschlussbericht wird dem Hessischen Datenschutzbeauftragten zugeleitet werden.

Die Einführung der automatisierten Bereinigungsfunktion ist nach dem folgenden Zeitplan durchgeführt worden:

- ab 08.01.2007 Beginn interner Tests durch die Fachgruppe POLAS
- ab 15.01.2007 Beginn der Tests mit dem HLKA und externer Mitarbeiter von den Dienststellen sowie Fehlerverifizierung

- ab 18.01.2007 Fehlerbehebung und Überprüfung durch die Fachgruppe POLAS
- ab 05.02.2007 Abschlusstest mit dem HLKA, Anmeldung CAB-Verfahren
- ab 08.03.2007 Produktivsetzung

Somit ist davon auszugehen, dass die personenbezogenen Daten in POLAS seit dem 8. März 2007 fristgerecht gelöscht werden. Vorübergehend besteht lediglich insoweit eine Ausnahme, als bei der Zuspicherung einer ausländischen Ausschreibung zur Fahndung bis vor etwa einem Jahr in POLAS aus technischen Gründen ebenfalls eine U-Gruppe angelegt wurde. Grundsätzlich verhindert das Vorhandensein einer aktuellen Fahndungsausschreibung, für die eine eigene Frist läuft, die Aussonderungsprüfung nach der U-Gruppe. Bei einer Ausländerfahndung sollte dies jedoch nicht gelten, weil die U-Gruppe nach dem Ende der Fahndung funktionslos wird. Die nunmehr in Angriff genommene manuelle Bereinigung ist sehr zeitaufwändig, weil der zuständige Sachbearbeiter jeden betroffenen Datensatz auf weitere interne Abhängigkeiten hin überprüfen muss. Auf die Programmierung einer automatisierten Lösung wurde verzichtet, da die restlichen Altbestände mit der Produktivsetzung der INPOL-Land-Version 5.0.1 am 30. Juni 2007 ohnehin bereinigt werden.

### **Zu 9.3 Liegenschaftsdatenabruf (34. Tätigkeitsbericht, Ziff. 6.2)**

Die Landesregierung begrüßt die Feststellung des Hessischen Datenschutzbeauftragten, dass die geprüften Stellen inzwischen ihrer Dokumentationsverpflichtung in dem erforderlichen Maße nachkommen. Das Hessische Landesamt für Bodenmanagement und Geoinformation wird die Einhaltung der datenschutzrechtlichen Bestimmungen auch weiterhin durch regelmäßige Stichproben bei den zugelassenen Abrufern überwachen.

### **Zu 9.4 Hartz IV - Vorlage von Kontoauszügen - (34. Tätigkeitsbericht, Ziff. 5.9.1)**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu. Wie bereits in der Stellungnahme zum 34. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten ausgeführt, besteht Übereinstimmung darin, dass das Vorgehen der zuständigen Leistungsträger nach dem SGB II, von den Antragstellern Kontoauszüge der letzten drei bis sechs Monate anzufordern, als bisher auch schon im Sozialhilferecht übliche Standardmaßnahme bei der Entscheidung über die Gewährung von Leistungen nach dem SGB II zulässig ist. Der im Bericht des Hessischen Datenschutzbeauftragten angegebene Beschluss des Landessozialgerichts Sachsen vom 25. April 2006 (Az.: L 3 B 931 O6AS- ER) unterstützt ebenso diese Auffassung. Leider ist es nicht gelungen, im Zuge der Beratungen des Fortentwicklungsgesetzes zum SGB II § 60 Abs. 1 Nr. 1 in diesem Sinne dahingehend zu ändern, dass die Anforderung von Kontoauszügen bereits im Gesetzestext enthalten ist.

### **Zu 9.5 Schuleingangsuntersuchung durch die Gesundheitsämter - (34. Tätigkeitsbericht, Ziff. 5.8.5)**

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Wiesbaden, 20. August 2007

Der Hessische Ministerpräsident:

**Koch**

Der Hessische Minister  
des Innern und für Sport:

**Bouffier**