16. Wahlperiode

Drucksache **16/3649**

HESSISCHER LANDTAG

15. 02. 2005

Stellungnahme der Landesregierung

betreffend den Zweiunddreißigsten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Drucksache 16/2131

Eingegangen am 15. Februar 2005 · Ausgegeben am 25. Februar 2005

Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Stellungnahme zu:		Seite
1.	Vorwort und Kernpunkten	5
2.	Querschnittsthemen	5
2.1	Telearbeit	5
2.2	Neues Online-Seminar "Datenschutz und Datensicherheit"	5
3.	Europa	5
3.1	Allgemeines	5
3.2	Entwicklung des Schengener Informationssystems	5
3.2.1	Kurzfristig zu realisierende Änderungen	6
3.2.2	Änderungsvorschläge für ein Informationssystem der nächsten Generation (SIS II)	6
3.3	Gemeinsame Überprüfung der Ausschreibungen zu Drittausländern	6
3.4	Überprüfung europäischer Informationssysteme	6
3.5	Kontrolle des zentralen Teils des Schengener Informationssystems (CSIS)	6
4.	Justiz	7
4.1	Postzensur in Justizvollzugsanstalten	7
5.	Polizei und Strafverfolgungsbehörden	7
5.1	Fortsetzung der Rasterfahndung als Reaktion auf den 11. September 2001	7
5.1.1	Richterliche Entscheidung zur Zulässigkeit der Rasterfahndung	7
5.1.2	Reichweite der Auskunftsersuchen betroffener Studenten gegenüber den Hochschulen auf Grundlage des Hessischen Datenschutzgesetzes	7
5.1.3	Durchführung des automatisierten Datenabgleichs	7
5.1.4	Weitere Ermittlungen im Anschluss an den automatisierten Abgleich	7
5.2	Neue Herausforderungen an die Verwendung der DNA-Analyse im Strafverfahren	8
5.3	Fehlende Grundlagen für Massenscreenings	10
5.4	Diskrete Ladung zur Vorsprache bei der Polizei	11
5.5	Anfertigung von Fotografien bei Demonstrationen	11
5.6	Gefährderansprache durch die Polizei	11
5.7	Gelöscht und doch nicht gelöscht	11
5.8	Prüfung der Luftverkehrsbehörde beim Polizeipräsidium Frankfurt am Main	11
6.	Ausländerbehörden Prüfung der Ausländerbehörde des Landkreises Marburg	12
6.1	Einholung von Auskünften beim Landesamt für Verfassungsschutz und Landeskriminalamt im Rahmen von Aufenthaltsgenehmigungen	12
6.2	Datensicherheit im Gebäude des Landratsamtes	12
7.	Finanzen	13
7.1	Aufrechnungen von Forderungen eines Steuerpflichtigen gegenüber Behörden mit Ansprüchen aus dem Steuerschuldverhältnis	13
7.2	Elektronische Signatur im Finanzbereich	13

8.	Kommunen	13
8.1	Internetportal Gewerbemeldungen	13
8.2	Tonbandaufzeichnungen von öffentlichen Sitzungen	13
8.3	Datenübermittlungen an Parteien aus dem Einwohnermelderegister	13
8.4	Datenübermittlungen zwischen Ordnungsamt und Steueramt wegen Haltens gefährlicher Hunde	14
9.	Baurecht	14
9.1	Planfeststellungsverfahren zum Bau der A-380-Wartungshalle - Behandlung der Einwenderdaten	14
9.2	Beteiligung privater Dritter an der Bauleitplanung	14
9.3	Beteiligung des Denkmalbeirats im Baugenehmigungsverfahren	14
10.	Forschung	14
10.1	Aufbau eines Forschungszentrums der Statistischen Landesämter	14
10.1.1	Ausgestaltung und Ziel des Forschungsdatenzentrums	14
10.1.2	Datenschutzkonzept	14
10.2	Datenschutzrechtliche Anforderungen an den Aufbau von medizinischen Forschungszentren	15
11.	Hochschulen Videoeinsatz an Hochschulen	15
12.	Schulverwaltung, Schulen, Bildungseinrichtungen	15
12.1	Datenerhebung im Rahmen der Einschulung	15
12.2	Akteneinsicht in Abiturprüfungsunterlagen bei Schulen	15
12.3	Datenschutz in Volkshochschulen	15
13.	Bibliotheken Ergebnisse der Prüfung einer öffentlichen Bibliothek	15
14.	Gesundheitswesen	16
14.1	Datenschutzrechtliche Aspekte der Reform der gesetzlichen Krankenversicherung	16
14.2	Datenschutzkonzept für das Neugeborenen-Screening in Hessen	16
14.3	Prüfung des Klinikums Offenbach	16
14.4	Prüfung der Vertrauensstelle des Hessischen Krebsregisters	16
14.5	Automatisierung im öffentlichen Gesundheitsdienst	16
15.	Sozialwesen	16
15.1	Existenzgrundlagengesetz	16
15.2	Sozialdatenschutz und Untersuchungsgrundsatz	17
15.3	Opferschutz und Jugendgerichtshilfe	17
16.	Personalwesen	17
16.1	Personalaktenregistratur im Schulbereich	17
16.2	Vereitelung von Akteneinsichtsrechten durch Vernichtung von Unterlagen	17
17.	Recht der Presse, Medien- und Teledienste	17
17.1	Neuordnung der Rundfunkfinanzierung	17
17.2	Erwerb von Adressen durch die Gebühreneinzugszentrale	18
17.3	Online-Bestellung von Newslettern	18

18.	Entwicklungen und Empfehlungen im Bereich der Technik	18
18.1	TCPA	18
18.2	SPAM – die neue Gefahr für die Integrität des Internets	18
18.3	Automatische Software-Updates	18
18.4	Sicherheitsprobleme beim Einsatz von USB-Geräten	18
18.5	Elektronische Authentisierung mit Schlüsseln	18
18.6	Orientierungshilfe Kryptografie - Technische Grundlagen	19
18.7	Die Nutzung digitaler Funktelegramme im Rettungsdienst	19
19.	Bilanz	19
19.1	Übertragung der Zuständigkeit für Untersuchungen zur Dienstfähigkeit von Beamtinnen und Beamten in der hessischen Landesverwaltung auf die Versorgungsämter (31. Tätigkeitsbericht, Nr. 19.2)	19
19.2	Anonymität im Internet (29. Tätigkeitsbericht, Nr. 11.4; 30. Tätigkeitsbericht, Nr. 6.2)	19
19.3	Prüfung von Datensicherheitsmaßnahmen mit Hilfe eines Portscanners (30. Tätigkeitsbericht, Nr. 14.5)	20

Zum Vorwort

Die Landesregierung dankt dem Hessischen Datenschutzbeauftragten und seinen Mitarbeiterinnen und Mitarbeitern ausdrücklich für die geleistete Arbeit, die - auch soweit es sich um die datenschutzrechtliche Beratung der Verwaltung handelt - letztlich allen Bürgerinnen und Bürgern in Hessen zugute kommt.

Zu 1. Kernpunkte des 32. Tätigkeitsberichts

In diesem Abschnitt des Tätigkeitsberichts fasst der Hessische Datenschutzbeauftragte dessen wesentlichen Inhalt zusammen, ohne darüber hinaus weitere Aspekte anzusprechen. Eine gesonderte Stellungnahme der Landesregierung hierzu erübrigt sich daher.

Zu 2. Querschnittsthemen
Zu 2.1 Telearbeit

Die Darstellung des Hessischen Datenschutzbeauftragten ist zutreffend.
Die technischen und IT-organisatorischen Vorgaben (Mindeststandards) für die Einrichtung und für den Betrieb von Telearbeitsplätzen in der Landesverwaltung wurden von einer interministeriellen Arbeitsgruppe unter maßgeblicher Beteiligung des Hessischen Datenschutzbeauftragten erarbeitet und mit dem Hauptpersonalrat beim Ministerium des Innern und für Sport abgestimmt. Die Mindeststandards sind geeignet, notwendige technische Regelungen und Sicherheitsanforderungen zu erläutern und als Handreichungen die Umsetzung zu unterstützen; sie verstehen sich als Ergänzung zu der Anschlussvereinbarung zur Einführung von alternierender Telearbeit in der Landesverwaltung vom 20. Juni 2003 (StAnz. 2003, S. 2748).
Die Absicht des Hessischen Datenschutzbeauftragten, ausgewählte Telearbeitsplätze einer entsprechenden Überprüfung zu unterziehen, wird begrüßt.

Durch das Ministerium der Finanzen wird noch geprüft, in welchen Arbeitsbereichen des Ressorts, in dem zum Großteil äußerst sensible Daten bearbeitet werden, beispielsweise in der Hessischen Bezügestelle oder der Steuerverwaltung, Telearbeit überhaupt möglich sein soll. Über die im Pilotversuch bereits eingerichteten Telearbeitsplätze hinaus sind daher zunächst keine weiteren alternierenden Telearbeitsplätze eingerichtet worden.

Zu 2.2 Neues Online-Seminar "Datenschutz und Datensicherheit"

Die Landesregierung begrüßt das Engagement des Hessischen Datenschutzbeauftragten bei der Entwicklung eines Angebots zur Schulung und Fortbildung im Datenschutz für Beschäftigte in der Landesverwaltung und bei anderen öffentlichen Stellen in Hessen.

Zu 3. Europa
Zu 3.1 Allgemeines

Die Landesregierung kann hierzu keine Stellungnahme abgeben, da ihr keine weitergehenden Informationen über die Tätigkeiten der Gemeinsamen Kontrollinstanz vorliegen.

Zu 3.2 Entwicklungen des Schengener Informationssystems

Zu den Ausführungen des Hessischen Datenschutzbeauftragten ist anzumerken, dass unter griechischer Ratspräsidentschaft am 25. April 2003 seitens des Rates festgestellt wurde, dass das SIS ein "Treffer/kein Treffer"-System bleiben soll. Allerdings soll das neue SIS zumindest in technischer Hinsicht so entwickelt werden, dass z.B. eine Aufnahme neuer Kategorien von Ausschreibungen möglich ist. Gleichermaßen sollen die technischen Voraussetzungen geschaffen werden, die eine Speicherung, Übertragung und den eventuellen Abruf biometrischer Daten, insbesondere von Lichtbildern und Fingerabdrücken, ermöglichen. Inwieweit das SIS II sich von einem reinen Informationssystem zu einem Ermittlungssystem entwickeln könnte, ist derzeit noch nicht absehbar. Der Feststellung im Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, dass das SIS II weit über die ursprüngliche Zielsetzung hinausgehe, kann daher in dieser Form nicht zugestimmt werden.
Die vom Hessischen Datenschutzbeauftragten erhobene Frage, inwieweit redundante Funktionen im Hinblick auf schon bestehende Informationssys-

teme geschaffen werden, wird auch in den zuständigen Arbeitsgremien des Rats noch diskutiert.
Im Übrigen wird den Ausführungen des Hessischen Datenschutzbeauftragten zugestimmt.

Zu 3.2.1 Kurzfristig zu realisierende Änderungen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu, soweit sich aus dem Nachfolgenden nichts anderes ergibt.

Zu "Rechtsgrundlage für SIRENE"

Die Landesregierung entnimmt dem Tätigkeitsbericht, dass die Gemeinsame Kontrollinstanz die Rechtsgrundlage für SIRENE gebilligt hat. Die vom Hessischen Datenschutzbeauftragten geäußerte Kritik kann dann allerdings nicht nachvollzogen werden. Bei einer Überführung personenbezogener Angaben aus den SIRENE-Unterlagen in nationale Dateien unterliegen diese selbstverständlich den Löschungsfristen des nationalen Rechts und nicht mehr jenen des SIS oder Schengener Durchführungsübereinkommens.

Zu "Zugriff der Geheimdienste"

Eine Stellungnahme erübrigt sich, da die Bundesrepublik Deutschland an dem Zugriff der Nachrichtendienste auf das SIS nicht beteiligt ist.

Zu 3.2.2 Änderungsvorschläge für ein Informationssystem der nächsten Generation (SIS II)

Zu "Übernahme der Daten aus dem Europäischen Haftbefehl"

Der Haltung der Gemeinsamen Kontrollinstanz bezüglich der Speicherung der im Europäischen Haftbefehl enthaltenen Daten ist aus Sicht der Landesregierung zu widersprechen. Sämtliche darin enthaltene Daten sind für die jeweilige Verfahrensbearbeitung durch die Strafverfolgungsbehörden von Relevanz. Diese nicht im SIS zu speichern, würde aufwendige Nachfragen und Nachbearbeitung im SIRENE-Büro zur Folge haben. In diesem Sinne wird auch weiterhin für eine Speicherung der im Europäischen Haftbefehl enthaltenen Daten im SIS II votiert.

Zu "Aufnahme von Lichtbildern, Fingerabdrücken und anderen biometrischen Daten"

Der Hessische Datenschutzbeauftragte erhebt die Frage nach der Praktikabilität bei Fingerabdrücken, ob diese für den Beamten vor Ort eine Hilfe darstellen.
Aus Sicht der Landesregierung ist dies zu bejahen. Bereits zum Kontrollzeitpunkt ist es mit Blick auf weitere zu veranlassende polizeiliche Maßnahmen von großem Wert, Kenntnis über vorhandene Fingerabdrücke zu erhalten. Durch das Vorhalten dieser im SIS kann darüber hinaus sehr schnell eine Personenidentifizierung erfolgen, ohne dass weitergehende zeitintensive Informationswege beschritten werden müssen. Bezüglich der Aufnahme von Lichtbildern und Fingerabdrücken im SIS II besteht auf EU-Ebene bereits Einvernehmen.

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

Zu 3.3 Gemeinsame Überprüfung der Ausschreibungen zu Drittausländern

Eine Stellungnahme der Landesregierung zu der beabsichtigten Maßnahme der Gemeinsamen Kontrollinstanz erübrigt sich.

Zu 3.4 Überprüfung europäischer Informationssysteme

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 3.5 Kontrolle des zentralen Teils des Schengener Informationssystems (CSIS)

Der Prüfbericht der Gemeinsamen Kontrollinstanz ist der Landesregierung nicht bekannt, eine Bewertung kann daher nicht erfolgen.

Zu 4. Justiz
Zu 4.1 Postzensur in Justizvollzugsanstalten

Die Landesregierung, der der Vorfall nicht bekannt geworden war, teilt die Rechtsauffassung des Hessischen Datenschutzbeauftragten zu § 29 Abs. 2 Satz 3 StVollzG ohne Einschränkung. Es wird davon ausgegangen, dass es sich um einen bedauerlichen Einzelfall gehandelt hat. Nach der Entschuldigung der nicht genannten Anstaltsleitung besteht kein Handlungsbedarf mehr.

Zu 5 Polizei und Strafverfolgungsbehörden
Zu 5.1 Fortsetzung der Rasterfahndung als Reaktion auf den 11. September 2001
Zu 5.1.1 Richterliche Entscheidung zur Zulässigkeit der Rasterfahndung

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 5.1.2 Reichweite der Auskunftsersuchen betroffener Studenten gegenüber den Hochschulen auf Grundlage des Hessischen Datenschutzgesetzes

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 5.1.3 Durchführung des automatisierten Datenabgleichs

Der Hessische Datenschutzbeauftragte führt aus, dass "ein weiterer Abgleich bei dem Bundeskriminalamt (BKA) mit den dort erhobenen Daten anderer Stellen" erfolgt sei. Der beim BKA erfolgte Datenabgleich wurde anhand der so genannten "Abgleichdateien" durchgeführt. Diese Daten waren zum überwiegenden Teil durch die Bundesländer erhoben und dem BKA zum länderübergreifenden Abgleich übermittelt worden. In Hessen betraf dies die Inhaber von Gefahrgutscheinen, Besucher des AKW Biblis, Inhaber von privaten Pilotenlizenzen, nach § 29d Luftverkehrsgesetz sicherheitsüberprüfte Flughafenbeschäftigte sowie nach Atomgesetz sicherheitsüberprüfte Personen. Das BKA selbst hatte ebenfalls Abgleichdaten erhoben (z.B. Berufspilotenlizenzen des Luftfahrtbundesamtes) und diese ergänzend zum Abgleich hinzugefügt.

Der Hessische Datenschutzbeauftragte führt weiter aus, dass die beim behördlichen Datenschutzbeauftragten des Landeskriminalamtes unter Verschluss gelagerten Originaldatenträger und Sicherungskopien erst gelöscht wurden, nachdem er die Aufbewahrung kritisiert hatte. Die Datenträger wurden beim behördlichen Datenschutzbeauftragten unter Verschluss gelagert, weil die Aufbewahrung lediglich Verfahrenssicherungszwecken diente. Die Vernichtung der Datenträger erfolgte im Einvernehmen mit dem Hessischen Datenschutzbeauftragten.

Zu 5.1.4 Weitere Ermittlungen im Anschluss an den automatisierten Abgleich

Der Hessische Datenschutzbeauftragte berichtet, dass sich die ermittelnden Polizeibehörden bei ihren Anfragen zum Teil auf § 26 HSOG statt auf § 13 HSOG gestützt hatten. Diese in Einzelfällen festgestellte Vorgehensweise wurde vom Landeskriminalamt zum Anlass genommen, die Polizeibehörden im Juni 2003 schriftlich darauf hinzuweisen, dass die Maßnahmen im Anschluss an die Rasterfahndung auf der Grundlage des § 13 Abs. 1 Nr. 3 HSOG vorgenommen werden. Danach gestaltete sich die Datenerhebung grundsätzlich relativ problemlos, zumal die ersuchten Stellen entsprechende Informationen bei der Datenerhebung erhielten.

Die Einschätzung des Hessischen Datenschutzbeauftragten, dass "diese Aktion" - hiermit dürfte die Beendigung der weiteren Ermittlungen in den so genannten Prüffällen gemeint sein - in Kürze abgeschlossen sein wird, beruht nicht auf polizeilichen Informationen. Von ursprünglich 289 Prüffällen waren bei Redaktionsschluss dieser Stellungnahme noch 18 Vorgänge in der Bearbeitung. Eine Einschätzung zum weiteren zeitlichen Bedarf kann nicht gegeben werden.

Zu 5.2 Neue Herausforderungen an die Verwendung der DNA-Analyse im Strafverfahren

Bei dem Einsatz des genetischen Fingerabdrucks zum Zwecke der Identitätsfeststellung handelt es sich um ein hoch effizientes und sehr zuverlässiges Ermittlungsinstrument, das in Strafverfahren zunehmend als Standardmaßnahme eingesetzt wird. Angesichts der mit der Maßnahme erzielten Erfolge bei der Aufklärung von Straftaten sieht die Landesregierung ein rechtspolitisches Bedürfnis, den Anwendungsbereich zu erweitern. Dieses Bedürfnis ergibt sich insbesondere aus

- den Chancen einer Verbesserung und Beschleunigung der Aufklärung von Straftaten,
- einer denkbaren Minderung des Ermittlungsaufwands im Einzelfall und damit der Freisetzung von Ressourcen für andere Strafverfahren sowie
- der mit einer Effektivierung der Strafverfolgung verbundenen Steigerung des Schutzes der Bevölkerung vor Straftätern.

Das Ministerium der Justiz hat sich im Rahmen dieser Diskussion an der auch im Tätigkeitsbericht angesprochenen Arbeitsgruppe des Strafrechtsausschusses der Konferenz der Justizministerinnen und -minister beteiligt, die ihren Bericht im Juni 2004 vorgelegt hat. Die 75. Konferenz der Justizministerinnen und Justizminister vom 17. bis 18. Juni 2004 in Bremerhaven hat hierzu unter TOP 11.1 folgenden Beschluss gefasst:

"Weitere Anwendungsmöglichkeiten der DNA-Analyse im Strafverfahren
1. Die Justizministerinnen und Justizminister nehmen den Bericht des Strafrechtsausschusses mit den Kernaussagen zu den biologischen und verfassungsrechtlichen Grundlagen und zu weiteren Anwendungsmöglichkeiten der DNA-Analyse im Strafverfahren zur Kenntnis.
2. Die Justizministerinnen und Justizminister sehen sich durch den Bericht in ihrer Auffassung bestätigt, dass die DNA-Analyse ein hoch wirksames Mittel zur Aufklärung von Straftaten ist. Die gegenwärtigen gesetzlichen Regelungen für DNA-Analysen zum Zweck der Identifizierung in künftigen Strafverfahren schöpfen den verfassungsrechtlichen Rahmen aber nicht voll aus und belassen dem Gesetzgeber Spielräume für eine Ausweitung des Anwendungsbereichs, insbesondere durch
a) Schaffung einer ausdrücklichen gesetzlichen Grundlage für Massen-Gentests,
b) Überarbeitung der Vorschriften über die Löschung gespeicherter Daten,
c) Streichung des Richtervorbehalts bei der Untersuchung anonymer Spuren,
d) Verzicht auf einen Anlasstatenkatalog unter Beibehaltung der qualifizierten Negativprognose,
e) Verzicht auf den Richtervorbehalt bei dokumentierter Freiwilligkeit.
3. Die Justizministerinnen und Justizminister sind darüber hinaus der Auffassung, dass zu prüfen sei, ob und gegebenenfalls in welchen verfassungsrechtlichen Grenzen die DNA-Analyse zum Zwecke der Identifizierung in künftigen Strafverfahren entsprechend erkennungsdienstlichen Maßnahmen genutzt werden könne.
4. Die Justizministerinnen und Justizminister sprechen sich dafür aus, den Verzicht auf einen Anlasstatenkatalog im Rahmen der im Bundesrat anhängigen Gesetzgebungsverfahren einzubringen.
Sie beauftragen darüber hinaus den Strafrechtsausschuss, die weiteren unter Ziffer 2 und 3 angesprochenen Punkte zu prüfen und der Justizministerkonferenz hierzu Vorschläge vorzulegen."

Klarzustellen ist, dass die Identitätsprüfung mittels DNA-Mustern überhaupt nicht auf eine Offenlegung und Nutzung von Erbinformationen aus dem genetischen Code, sondern ausschließlich auf den Abgleich von Mustern und dabei die Feststellung von Übereinstimmung oder Abweichung zielt. Die Strafprozessordnung enthält ein klares Verbot, die DNA-Analyse zu anderen Zwecken als den der Feststellung von Abstammung und Identität des Spurenlegers einzusetzen. Die einzige Ausnahme, die eine qualitative Exploration zulässt, ist die Feststellung des Geschlechts, wie sich aus dem Wortlaut des § 81e Abs. 1 StPO ergibt:

"An dem durch Maßnahmen nach § 81a Abs. 1 erlangten Material dürfen auch molekulargenetische Untersuchungen durchgeführt werden, soweit sie zur Feststellung der Abstammung oder der Tatsache, ob aufgefundenes Spurenmaterial von dem Beschuldigten oder dem Verletzten stammt, erforderlich sind; hierbei darf auch das Geschlecht der Person bestimmt werden. Unter-

suchungen nach Satz 1 sind auch zulässig für entsprechende Feststellungen an dem durch Maßnahmen nach § 81c erlangten Material. Feststellungen über andere als die in Satz 1 bezeichneten Tatsachen dürfen nicht erfolgen; hierauf gerichtete Untersuchungen sind unzulässig."

Die Landesregierung hat gemeinsam mit dem Freistaat Bayern im Bundesrat den Entwurf eines Gesetzes zur Verbesserung der Regelungen zur DNA-Analyse (BR-Drucks. 465/03) vorgelegt, der den Anwendungsbereich der DNA-Analyse zu Zwecken künftiger Strafverfahren im Bereich der Anlasstat erweitern sowie den Richtervorbehalt für die molekulargenetische Untersuchung von anonymen Spuren entfallen lassen soll. Es handelt sich hierbei um das unter Nr. 4 des oben zitierten Beschlusses der Konferenz der Justizministerinnen und -minister genannte Gesetzgebungsverfahren. Hinsichtlich anonymer Tatspuren ist anzumerken, dass ein Personenbezug erst durch den Abgleich mit einem weiteren Muster einer bekannten Person hergestellt wird. Dessen Erhebung aber beruht nach geltendem Recht bereits auf einer richterlichen Anordnung.

Die von der Konferenz der Justizministerinnen und -minister beauftragte Arbeitsgruppe hat sich auch mit der Frage einer Gewinnung von persönlichkeitsrelevanten Informationen aus dem DNA-ldentitätsmuster nach neueren Erkenntnissen der Forschung beschäftigt (Nr. 5.2.2 im Tätigkeitsbericht). Nach dem derzeitigen Stand von Wissenschaft und Technik ist davon auszugehen, dass die zum Zwecke der Identitätsfeststellung gewonnenen DNA-Muster über die Geschlechtszuordnung hinaus keine kriminalistisch verwertbaren Aussagen über persönliche Eigenschaften des Betroffenen zulassen.

Der Hessische Datenschutzbeauftragte verweist in seinen Ausführungen, in denen er sich mit den indirekten Aussagen der Short-Tandem-Repeats (STR) über genetische Merkmale befasst, auf eine immer wieder zitierte Publikation aus dem Jahr 1995 (Meloni et al.), die scheinbar einen Zusammenhang zwischen einer seltenen Variante des STR-Systems TH01 und einer Disposition für Schizophrenie belegt. Er betrachtet dies zwar noch nicht als absoluten wissenschaftlichen Beweis, hält die Ergebnisse der Untersuchung aber auch noch nicht für widerlegt.

Tatsächlich muss diese Meinung zwischenzeitlich als veraltet eingestuft werden. Mit Ausnahme des Geschlechts ist es nicht möglich, aus den für den genetischen Fingerabdruck erhobenen Daten Rückschlüsse über persönlichkeitsrelevante oder äußerlich sichtbare Merkmale zu ziehen. Sämtliche hierzu bislang in den einschlägigen Publikationen vermuteten Kopplungen zwischen einem speziellen DNA-Muster und einer Disposition für eine bestimmte Krankheit haben sich als wissenschaftlich nicht haltbar erwiesen.

Beispielhaft soll hier auf die vom Hessischen Datenschutzbeauftragten angesprochene Kopplung eines seltenen DNA-Musters im Datenbanksystem TH01 mit der Schizophrenie eingegangen werden. Obwohl diese vermeintliche Kopplung immer wieder als Argument gegen eine Ausweitung der strafprozessualen DNA-Maßnahmen angeführt wird, muss sie inzwischen eindeutig als widerlegt angesehen werden (Burgert et al. 1998, Johnsson et al. 1998). Es gilt heute vielmehr als gesichert, dass Schizophrenie immer aus einem komplexen Zusammenspiel multipler Umwelt- und genetischer Faktoren entsteht. Über die genetischen Faktoren weiß man bis dato, dass nicht weniger als 26 verschiedene DNA-Bereiche auf insgesamt 17 verschiedenen Chromosomen an der Ausprägung der Krankheit beteiligt sind (Prasad et al. 2002).

In diesem Zusammenhang sei angemerkt, dass es Mitte der 90er-Jahre eine vergleichbare Diskussion über die mögliche Kopplung bestimmter Merkmalsvarianten des Datenbanksystems VWA mit einem Onkogen (Krebsgen) gab. Auch in diesem Fall konnte ein Zusammenhang nie bewiesen werden. Es bleibt somit festzustellen, dass es derzeit keinen einzigen wissenschaftlich belegten Fall einer entsprechenden Korrelation zwischen einem forensisch relevanten DNA-System und einem "Krankheitsgen" gibt.

Weiter skizziert der Hessische Datenschutzbeauftragte eine im Zusammenhang mit den seltenen "numerischen Chromosomenaberrationen" bestehende theoretische Möglichkeit, im Rahmen der Erstellung der genetischen Fingerabdrücke gesundheitsrelevante Zusatzerkenntnisse festzustellen. Unter numerischen Chromosomenaberrationen versteht man das Auftreten von mehr

oder weniger als zwei der in der Regel paarig angelegten Chromosomen. Die klinisch wichtigsten - weil häufigsten - autosomalen Aberrationen sind die Trisomien der Chromosomen 13, 18 und 21. Forensisch relevant dürfte im Wesentlichen die Trisomie 21 (Down-Syndrom) sein.

Beim Down-Syndrom tritt das Chromosom 21 dreifach auf. Theoretisch könnte somit die Untersuchung des Datenbanksystems D21S11 - welches auf dem Chromosom 21 liegt - Hinweise auf diese seltene Erbkrankheit liefern. Eine sichere, statistisch relevante Diagnose, dass der Spurenverursacher tatsächlich an dieser auch äußerlich sichtbaren Krankheit leidet, kann jedoch in keinem Fall getroffen werden. Zum Beispiel können derartige Abweichungen auch durch einen simplen somatischen Mosaizismus erklärt werden, der zu keiner Krankheit führt. Unter somatischem Mosaizismus versteht man dabei eine Mutation, die in der frühen Embryonalentwicklung auftritt und nur ein bestimmtes Gewebe betrifft, das dann ein abweichendes Merkmal besitzen kann. Eine sichere Diagnose setzt also immer eine zytologische Untersuchung voraus, die über die Möglichkeiten eines kriminaltechnischen Labors weit hinausgeht.

Als weiteres Beispiel nennt der Hessische Datenschutzbeauftragte numerische Aberrationen der Geschlechtschromosomen, wie z.B. das Klinefelter- oder Turner-Syndrom. Aber auch hier gilt, dass eine sichere Diagnose nur zytogenetisch getroffen werden kann.

Bei der im Tätigkeitsbericht erwähnten ethnischen Zuordnung handelt es sich nicht um codierte Erbinformationen, sondern vielmehr um die Auswertung einer statistischen Verteilung bestimmter Konstellationen in den DNA-Identitätsmustern. Die insoweit zu gewinnenden eher vagen Wahrscheinlichkeitsaussagen sind für Ermittlungs- oder Fahndungszwecke ebenso wenig verwertbar wie die unter dem Begriff der "Koppelung" in der Wissenschaft diskutierten Möglichkeiten einer mittelbaren Deutung nicht codierender Abschnitte.

Nicht ausgeschlossen werden kann freilich, dass mit dem Fortschritt von Wissenschaft und Technik zu irgendeinem künftigen Zeitpunkt weitergehende qualitative Aussagen zu persönlichen Eigenschaften des Betroffenen auch auf der Grundlage der DNA-Identitätsmuster möglich sein werden. Stand der Kriminaltechnik ist dies nicht und es erscheint nicht sinnvoll, die gesetzlichen Voraussetzungen für den Einsatz des genetischen Fingerabdrucks an spekulativen Vorhersagen zur Entwicklung der Wissenschaft auszurichten.

Zu 5.3 Fehlende Grundlagen für Massenscreenings

So genannte Massenscreenings auf freiwilliger Basis sind nicht auf die Durchführung von DNA-Analysen beschränkt. Gegenstand sind Aufforderungen an die Bevölkerung bzw. an - etwa lokal, nach Geschlecht und Alter - qualifizierte Bevölkerungsanteile, sich freiwillig der Abnahme von daktyloskopischen Fingerabdrücken oder aber von Speichelproben mit dem Ziel der molekulargenetischen Untersuchung zur Aufklärung einer Straftat zu unterziehen. Entsprechende Maßnahmen sind - dies gebietet schon der Aufwand für Vorbereitung und Durchführung - ultima ratio bei Verfahren etwa wegen schwerer Gewaltverbrechen, wenn auf andere Weise eine weitere Tataufklärung aussichtslos erscheint.

Dem Tätigkeitsbericht ist zuzustimmen, dass die Bitte um Mitwirkung an Personen gerichtet wird, die selbst nicht in einem Anfangsverdacht im Sinne des § 152 Abs. 2 StPO stehen. Typischerweise werden solche Untersuchungen in einem Umfang durchgeführt, bei dem schon aufgrund der Anzahl der befragten Personen nicht von Beschuldigten gesprochen werden kann.

Der Tätigkeitsbericht qualifiziert die hier beschriebenen Ermittlungsmaßnahmen als Grundrechtseingriff und folgert daraus den Vorbehalt einer gesetzlichen Eingriffsnorm. Dabei wird unterstellt, dass es sich bei der Zustimmung der Betroffenen nicht um ein freiwillig erteiltes Einverständnis, sondern angesichts der Gesamtumstände tatsächlich um eine staatlich erzwungene Duldung bzw. Mitwirkung handelt. Diese Bewertung stellt auf ein Verständnis von Eingriff und Freiwilligkeit ab, das an die Praxis der Strafverfolgung unrealistische Anforderungen stellt. Als Beispiel mag angeführt werden, dass auch der freiwillige Einlass von Ermittlungsbeamten unter dem Eindruck einer sonst drohenden Anordnung der Hausdurchsuchung jenseits einer völlig freien Willensentscheidung liegt. Gleichwohl bestehen kaum

Zweifel daran, dass im Falle einer solchen Zustimmung die Wohnung auch ohne richterliche Durchsuchungsanordnung betreten werden darf. Gleiches gilt für die freiwillige Herausgabe von Beweismitteln, wenn diese nur zur Abwendung der gerichtlichen Beschlagnahme erfolgt.

Nicht anders zu beurteilen sind die im Tätigkeitsbericht angesprochenen Reihenuntersuchungen. Allein ein gewisser sozialer Druck qualifiziert die Bitte der Strafverfolgungsbehörden um Mitwirkung nicht zur staatlichen Zwangsmaßnahme mit Eingriffscharakter. Auch der Umstand, dass die Verweigerung der Zustimmung im Einzelfall geeignet sein mag, einen Verdacht auf den Betroffenen zu fokussieren, kann nicht als Verstoß gegen das Selbstbegünstigungsprinzip oder als unzulässige Abpressung informationeller Freiräume angesehen werden. Der Betroffene hat es in der Hand, seine Zustimmung zu geben oder zu verweigern. Es handelt sich nicht um eine Zwangsmaßnahme und daher auch nicht um einen dem Gesetzesvorbehalt unterfallenden Grundrechtseingriff, sondern vielmehr gerade um die Ausübung der informationellen Selbstbestimmung des Betroffenen. Da es um eine freiwillige Mitwirkung im Strafverfahren geht, gilt insoweit auch nicht die Beschränkung durch den Begriff des Anfangsverdachts.

Freilich dürfte die Zulässigkeit einer langfristigen, über die sich aus dem Anlassfall ergebende Erforderlichkeit hinausreichenden Speicherung oder Nutzung der gewonnenen Daten zweifelhaft sein. Hierauf erstreckt sich auch die Zustimmung der Betroffenen nicht. Aber eine solche den konkreten Zweck überschreitende Verwendung der DNA-Muster oder Fingerabdrücke steht bisher auch nicht in Rede. Insbesondere werden die im Rahmen entsprechender Reihenuntersuchungen gewonnenen DNA-Identifizierungsmuster nicht in die DNA-Datei des Bundeskriminalamts eingestellt.

Zu 5.4 Diskrete Ladung zur Vorsprache bei der Polizei

Die Landesregierung teilt die Einschätzung des Hessischen Datenschutzbeauftragten zur Vorgehensweise bei der Übermittlung einer Vorladung zwecks Abgabe einer Speichelprobe bei der Polizei uneingeschränkt.
Die Polizeipräsidien und das Landeskriminalamt wurden daher per Erlass aufgefordert, eine entsprechende Verfahrensweise zu gewährleisten.

Zu 5.5 Anfertigen von Fotografien bei Demonstrationen

Die vom Hessischen Datenschutzbeauftragten durchgeführten Überprüfungen haben belegt, dass die Polizei rechtmäßig gehandelt hat. Die Landesregierung teilt die Auffassung des Hessischen Datenschutzbeauftragten, dass im Anwendungsbereich des Versammlungsgesetzes dessen Vorschriften über Bild- und Tonaufzeichnungen (§ 12a und § 19a) § 14 Abs. 2 HSOG vorgehen.

Zu 5.6 Gefährderansprache durch die Polizei

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 5.7 Gelöscht und doch nicht gelöscht

Der Sachverhalt ist vom Hessischen Datenschutzbeauftragten korrekt dargestellt. Es handelt sich um einen bedauerlichen Einzelfall, bei dem ein Polizeipräsidium das Landeskriminalamt entgegen den bestehenden Verwaltungsvorschriften (Nr. 17.4 KPS-Richtlinien) nicht über die vorgenommene Löschung in Kenntnis gesetzt hatte.

Zu 5.8 Prüfung der Luftverkehrsbehörde beim Polizeipräsidium Frankfurt am Main

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zur Luftfahrtbehörde beim Polizeipräsidium Frankfurt am Main zu.

In Bezug auf die Datenkommunikation mit dem APIS-System ist darauf hinzuweisen, dass eine elektronische Datenübermittlung lediglich bis zum Landeskriminalamt und nicht direkt in das Bundeszentralregister beim Generalbundesanwalt erfolgt.

Die vom Hessischen Datenschutzbeauftragten beschriebene automatisierte Erstellung der Bescheinigung über die Anerkennung der luftverkehrsrechtlichen Zuverlässigkeit und Übermittlung an die Fraport AG findet nur auf

Anstoß ("Tastendruck") der jeweiligen Sachbearbeiterin bzw. des jeweiligen Sachbearbeiters statt.

Zu 6. Ausländerbehörden
Prüfung der Ausländerbehörde des Landkreises Marburg

Zu 6.1 Einholung von Auskünften beim Landesamt für Verfassungsschutz und Landeskriminalamt im Rahmen von Aufenthaltsgenehmigungen

Durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 wurde auch das Ausländergesetz (AuslG) geändert, um die Sicherheit in der Bundesrepublik Deutschland zu erhöhen. Es wurde ein erweiterter Versagungsgrund (§ 8 Abs. 1 Nr. 5) in das Ausländergesetz eingefügt, wonach die Aufenthaltsgenehmigung auch bei Vorliegen eines Anspruchs nach dem Ausländergesetz zu versagen ist, wenn Tatsachen belegen, dass der Ausländer

- die freiheitliche demokratische Grundordnung oder die Sicherheit der Bundesrepublik Deutschland gefährdet,
- sich bei der Verfolgung politischer Ziele an Gewalttätigkeiten beteiligt,
- öffentlich zu Gewalttätigkeiten aufruft oder mit Gewalttätigkeit droht, und
- wenn Tatsachen belegen, dass er einer Vereinigung angehört, die den internationalen Terrorismus unterstützt.

Zudem werde in § 64a AuslG geregelt, dass die vorhandenen Erkenntnisse bei den Sicherheitsbehörden abgefragt werden können. Dies gilt sowohl für die Auslandsvertretungen als auch für die Ausländerbehörden.

Die Ausländerbehörden haben Abfragen durchzuführen bei befristeten Aufenthaltserlaubnissen nach einem Länderkatalog und vor Verfestigungen (unbefristeter Aufenthaltserlaubnis und Aufenthaltsberechtigung) in jedem Einzelfall. Es ist richtig, dass die Polizeibehörden bereits aufgrund anderer Vorschriften (§ 76 Abs. 4 AuslG) zur Übermittlung bestehender Erkenntnisse verpflichtet sind. Der Hessische Datenschutzbeauftragte stellt insoweit die Frage, ob eine erneute Anfrage überhaupt ein Mehr an Informationen bringen könne.

Die Erfahrungen haben gezeigt, dass trotz gesetzlicher Verpflichtung nicht alle Ermittlungsverfahren den Ausländerbehörden mitgeteilt werden und dass es auch immer wieder zu längeren Fristen bei den Mitteilungen kommt. Im Hinblick auf die mit der Änderung des Ausländergesetzes angestrebte Erhöhung der Sicherheit müssen die Doppelmitteilungen insoweit hingenommen werden, zumal darin kein datenschutzrechtlicher Verstoß erkennbar ist.

Zu 6.2 Datensicherheit im Gebäude des Landratsamtes

Im September 2003 fand eine datenschutzrechtliche Prüfung durch Bedienstete des Hessischen Datenschutzbeauftragten bei der Ausländerbehörde des Landrats des Landkreises Marburg-Biedenkopf statt. Im Zuge der Prüfung wurden gravierende datenschutzrechtliche Mängel bei der Datensicherung im Gebäude der Kreisverwaltung festgestellt, unter anderem dass in den Flurbereichen des 1., 2. und 3. Stockes des Verwaltungsgebäudes nicht verschlossene Stahlschränke, in denen sich zum großen Teil personenbezogene Unterlagen bzw. Akten befanden, aufgestellt waren. In der Abschlussbesprechung der Prüfung wurden diese festgestellten Mängel dem Datenschutzbeauftragten des Kreisausschusses vorgetragen; er wurde aufgefordert, umgehend für die Beseitigung der Mängel Sorge zu tragen.

Der Datenschutzbeauftragte des Kreisausschusses forderte noch am selben Tag die zuständigen Fachbereichs- bzw. Amtsleitungen zur sofortigen Behebung der Mängel auf. Dieser Aufforderung wurde umgehend Folge geleistet; der Datenschutzbeauftragte überzeugte sich persönlich von der Mängelbehebung.

Nach Vorlage des Prüfberichts des Hessischen Datenschutzbeauftragten Anfang November 2003 richtete der Datenschutzbeauftragte des Kreisausschusses ein Rundschreiben an alle Mitarbeiterinnen und Mitarbeiter beim Kreisausschuss des Landkreises Marburg-Biedenkopf, in dem sie nochmals auf die festgestellten Mängel und das zukünftig Verfahren hingewiesen wurden.

Bedingt durch im Jahr 2003 durchzuführende bauliche Maßnahmen in den Büros war es nicht zu vermeiden, dass in einigen Bereichen des Gebäudes der Kreisverwaltung Aktenschränke im Flurbereich aufgestellt werden muss-

ten. Nach Abschluss dieser baulichen Maßnahmen stehen inzwischen separate verschlossene Aktenräume zur Verfügung.

Zu 7. Finanzen

Zu 7.1 Aufrechnungen von Forderungen eines Steuerpflichtigen gegenüber Behörden mit Ansprüchen aus dem Steuerschuldverhältnis

Die Aussage des Hessischen Datenschutzbeauftragten, dass der Erlass des Ministeriums der Finanzen vom 18. Februar 1981 bereits im Rahmen der Erlassbereinigung außer Kraft getreten ist, trifft zu. Die Anwendung der seinerzeitigen Regelung zur regelmäßigen Prüfung der Aufrechnungslage vor Auszahlungen ist nicht mehr vorgesehen.

Im Rahmen des Sollkonzepts "Zahlbarmachung", das für die nach § 71a Landeshaushaltsordnung kaufmännisch buchenden Verwaltungseinheiten (Buchungskreise) und das Hessische Competence Center für neue Verwaltungssteuerung (HCC) verbindlich ist, wird vielmehr grundsätzlich von Anfragen beim zuständigen Finanzamt wegen Steuerrückständen abgesehen.

Liegt ein begründeter Verdacht vor, dass ein Geschäftspartner Steuerrückstände hat, wird von diesem Grundsatz eine Ausnahme gemacht. Dies gilt insbesondere für Insolvenzfälle.

Zu 7.2 Elektronische Signatur im Finanzbereich

Die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausgesprochenen grundsätzlichen Empfehlungen zur Förderung der qualifizierten Signatur im Projekt ELSTER (vgl. Nr. 20.1.6 des Tätigkeitsberichts) werden von der Landesregierung unterstützt.

Die Vorbehalte gegen das Vorgehen der Finanzverwaltung, in einer Übergangszeit von den durch das Signaturgesetz vorgegebenen Anforderungen an eine "qualifizierte elektronische Signatur" abzuweichen, sind aus datenschutzrechtlicher Sicht verständlich. Sie stehen jedoch dem angestrebten zügigen und kostenreduzierten Aufbau der elektronischen Kommunikation zwischen den Steuerpflichtigen und der Finanzverwaltung entgegen, der ohne Einbindung der nicht akkreditierten Signaturkartenherausgeber - insbesondere der Banken und Arbeitgeber - nicht möglich wäre. Nähere Einzelheiten ergeben sich aus der Begründung zur Steuerdaten-Übermittlungsverordnung und wurden unter anderem dem Bundesbeauftragten für Datenschutz im Rahmen der Beteiligung im Gesetzgebungsverfahren bekannt gegeben.

Das Bundesministerium der Finanzen ist mit den am Pilotversuch "Elster-Signatur" beteiligten Herausgebern von Signaturkarten dem Signaturbündnis als Gründungsmitglied beigetreten, um unter anderem die elektronische Signatur im Sinne des § 87a Abs. 6 Abgabenordnung und die qualifizierte Signatur im Sinne des Signaturgesetzes innerhalb der Übergangszeit bis Ende 2005 zusammenzuführen. Die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschriebenen Empfehlungen werden in der Arbeitsgruppe StEDV (ELSTER) erörtert.

Zu 8. Kommunen

Zu 8.1 Internetportal Gewerbemeldungen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 8.2 Tonbandaufzeichnungen von öffentlichen Sitzungen

Mit dem besprochenen Einzelfall war das Hessische Ministerium des Innern und für Sport nicht befasst. Die Rechtsauffassung des Hessischen Datenschutzbeauftragten wird jedoch geteilt.

Zu 8.3 Datenübermittlung an Parteien aus dem Einwohnermelderegister

Die Landesregierung hält eine Klärung des Problems der Datenübermittlungen an Parteien im Erlasswege für ausreichend. Eine ausdrückliche Regelung im Rahmen der Novellierung des Meldegesetzes ist nicht vorgesehen.

Zu 8.4 Datenübermittlungen zwischen Ordnungsamt und Steueramt wegen Haltens gefährlicher Hunde

Mit dem besprochenen Einzelfall war das Ministerium des Innern und für Sport nicht befasst. Die Rechtsauffassung des Hessischen Datenschutzbeauftragten wird jedoch geteilt.

Zu 9. Baurecht

Zu 9.1 Planfeststellungsverfahren zum Bau der A-380-Wartungshalle - Behandlung der Einwenderdaten

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die Weitergebe der Einwendungen nur anonymisiert erfolgen darf. Das Regierungspräsidium Darmstadt hat dies bereits umgesetzt und die Daten nur in anonymisierter Form an die Fraport AG übermittelt.

Zu 9.2 Beteiligung privater Dritter an der Bauleitplanung

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass es dem im Baugesetzbuch geregelten Verfahren an der nötigen Transparenz mangelt. Das Ministerium für Wirtschaft, Verkehr und Landesentwicklung wird die Empfehlung des Hessischen Datenschutzbeauftragten aufgreifen und die Regierungspräsidien bitten, die für die Bauleitplanung zuständigen Gemeinden auf das vorgeschlagene Verfahren hinzuweisen.

Zu 9.3 Beteiligung des Denkmalbeirats im Baugenehmigungsverfahren

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu, dass die Einbeziehung des Denkmalbeirats rechtlich nicht zu beanstanden war.

Zu 10. Forschung

Zu 10.1 Aufbau eines Forschungszentrums der Statistischen Landesämter

Die Statistischen Landesämter haben die Aufforderung des Gründungsausschusses des Rates für Sozial- und Wirtschaftsdaten aufgegriffen und ein Forschungsdatenzentrum der Statistischen Landesämter gegründet.

Zu 10.1.1 Ausgestaltung und Ziel des Forschungsdatenzentrums

Die Landesregierung stimmt der Darstellung des Hessischen Datenschutzbeauftragten zu. Mit Wirkung vom 1. April 2002 haben die Leiterinnen und Leiter der statistischen Landesämter das Forschungsdatenzentrum der Statistischen Landesämter (FDZ) in Form einer Arbeitsgemeinschaft eingerichtet, mit regionalen Standorten in allen statistischen Landesämtern und einer fachlich zentralisierten Datenhaltung.

Zu 10.1.2 Datenschutzkonzept

Die Landesregierung stimmt der Darstellung des Hessischen Datenschutzbeauftragten weitgehend zu.

Es ist zutreffend, dass die zentrale Vorhaltung der Statistikdaten auf der Grundlage einer Datenverarbeitung im Auftrag erfolgt. Hinsichtlich der von den Datenschutzbeauftragten geforderten Verschlüsselung der zentral vorgehaltenen Daten besteht aber noch Gesprächsbedarf.

Den Ausführungen zu "Faktisch anonymisierten Mikrodaten zur Off-Site-Nutzung" (scientific use files) wird zugestimmt. Aber bei dem Punkt "Faktisch anonymisierte Mikrodaten zur On-Site-Nutzung" ist darauf hinzuweisen, dass der Arbeitsplatz für Gastwissenschaftler abgeschottet eingerichtet und jede Möglichkeit des Zuspielens von Zusatzwissen organisatorisch und technisch unterbunden wird. Das dazugehörige Sicherheitskonzept wird zurzeit erarbeitet.

Die Ausführungen zu "Nicht anonymisierte Mikrodaten für die On-Site-Nutzung im Rahmen von Projekten, die im Auftrag einer Bundes- oder Landesbehörde als Zusatzaufbereitung oder im eigenen Interesse eines statistischen Amtes durchgeführt werden", erwecken den Eindruck, als sei dies eine wesentliche Aufgabe des FDZ. Diese Form der Datennutzung dürfte jedoch die Ausnahme darstellen, deren Realisierung im Einzelfall mit dem Datenschutzbeauftragten abzustimmen wäre.

Zu 10.2 Datenschutzrechtliche Anforderungen an den Aufbau von medizinischen Forschungszentren

Der Hessische Datenschutzbeauftragte hat die datenschutzrechtlichen Anforderungen an den Aufbau von medizinischen Forschungsnetzen exemplarisch an dem "Kompetenznetz Parkinson" überprüft und keine gravierenden Mängel festgestellt.

Auch bei diesem Projekt - wie auch beim "Forschungsnetz" - hat sich die frühzeitige Einschaltung des Hessischen Datenschutzbeauftragten bewährt. Bei solchen besonders datenschutzrechtlich sensiblen Projekten eröffnet eine frühe enge Kooperation mit dem Hessischen Datenschutzbeauftragten die Entwicklung tragfähiger Datenschutzkonzepte, die einfach und problemlos in der Praxis umgesetzt werden können.

Zu 11. Hochschulen
Videoeinsatz an Hochschulen

Der Hessische Datenschutzbeauftragte hat sich rechtsgutachtlich zu den datenschutzrechtlichen Anforderungen einer Videoüberwachung geäußert, die zur Gefahrenabwehr eingesetzt wird. Es wurden in diesem Zusammenhang die notwendigen Rahmenbedingungen aufgezeigt, die eine solche Videoüberwachung zulassen. Damit können jetzt unter anderem auch im Hochschulbereich, wo ein hoher Bedarf an solchen Sicherheitseinrichtungen zur Diebstahlabwehr besteht, besonders gefährdete Räume wirtschaftlich abgesichert werden.

Zu 12. Schulverwaltung, Schulen, Bildungseinrichtungen
Zu 12.1 Datenerhebung im Rahmen der Einschulung

Nach § 83 Abs. 1 Hessisches Schulgesetz dürfen Schulen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zu einer rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrags erforderlich ist.

Die Verordnung über die Verarbeitung personenbezogener Daten in Schulen vom 30. November 1993 (ABl. 1994, S. 114) legt die Daten abschließend fest. Über den in der Verordnung festgelegten Katalog hinausgehende Daten dürfen nur auf freiwilliger Basis erhoben werden. In dem Bericht des Hessischen Datenschutzbeauftragten wird dargelegt, in der Schulwirklichkeit würden mit Formularen für die Einschulung zusätzliche Daten ohne einen deutlichen Hinweis auf die Unterscheidung zwischen Pflichtangaben und freiwillige Angaben erhoben. Aufgrund dieser Feststellung des Hessischen Datenschutzbeauftragten wird das Kultusministerium die Schulen nochmals auf die Rechtslage und das in Abstimmung mit dem Hessischen Datenschutzbeauftragten entwickelte Formular hinweisen.

Zu 12.2 Akteneinsicht in Abiturprüfungsunterlagen bei Schulen

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten hinsichtlich der Frage des Akteneinsichtsrechtes in Unterlagen der Abiturprüfung zu. Da das Recht auf Einsicht in die Abiturarbeiten nicht gesetzlich befristet ist, besteht dieser Rechtsanspruch bis zur Vernichtung der Unterlagen. Das Einsichtsrecht endet folglich nach der gegenwärtigen Rechtslage mit der Vernichtung der Abiturunterlagen nach zehn Jahren.

Aufgrund des Berichts des Hessischen Datenschutzbeauftragten wird das Kultusministerium auf die geltende Rechtslage allgemein hinweisen.

Zu 12.3 Datenschutz in Volkshochschulen

In den Volkshochschulen liegt die Verantwortlichkeit für den Datenschutz bei dem jeweiligen kommunalen Träger (kreisfreie Städte, Landkreise und kreisangehörige Gemeinden). Die Hinweise des Hessischen Datenschutzbeauftragten richten sich an diese Träger der Volkshochschulen. Eine Stellungnahme der Landesregierung erübrigt sich.

Zu 13. Bibliotheken
Ergebnisse der Prüfung einer öffentlichen Bibliothek

Der Hessische Datenschutzbeauftragte hat bei der Prüfung einer großen öffentlichen Bibliothek Mängel festgestellt, deren Darstellung und Beseitigung für andere Bibliotheken exemplarisch sein können.

Zu 14. Gesundheitswesen
Zu 14.1 Datenschutzrechtliche Aspekte der Reform der gesetzlichen Krankenversicherung

Die vom Hessischen Datenschutzbeauftragten angeführten Sachverhalte sind der Landesregierung bekannt. Das GKV-Modernisierungsgesetzes (GMG) ist insoweit noch nicht umgesetzt. Im Rahmen der Änderung des Vergütungssystems ärztlicher Leistungen sollen von den kassenärztlichen Vereinigungen versichertenbezogene Daten an die Krankenkassen übermittelt werden. Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu, dass dabei sicherzustellen ist, dass die Daten ausschließlich zweckgebunden verwendet und keine umfassenden Versichertenprofile erstellt werden.

Zu 14.2 Datenschutzkonzept für das Neugeborenen-Screening in Hessen

Der Hessische Datenschutzbeauftragte stellt den Sachverhalt zutreffend dar. Es wurde ein Grundsatzpapier erarbeitet, das alle in dem Tätigkeitsbericht aufgeworfenen Fragen berücksichtigt. Das Grundsatzpapier befindet sich noch im Stadium der Abstimmung. Die datenschutzgerechte Ausgestaltung des Verfahrens soll in Abstimmung mit dem Hessischen Datenschutzbeauftragten umgesetzt werden.

Zu 14.3 Prüfung des Klinikums Offenbach

Der Sachverhalt war der Landesregierung nicht bekannt, da die Umsetzung der datenschutzrechtlichen Bestimmungen zu den innerorganisatorischen Angelegenheiten eines Krankenhauses gehört. Allerdings unterliegt die grundsätzliche Beachtung der datenschutzrechtlichen Bestimmungen der Rechtsaufsicht nach § 12 Hessisches Krankenhausgesetz. Insoweit wird das Sozialministerium das Klinikum um einen Bericht bitten, ob die aufgrund der Beanstandungen des Hessischen Datenschutzbeauftragten erforderlichen Maßnahmen umgesetzt wurden.

Der Rechtsauffassung des Hessischen Datenschutzbeauftragten wird zugestimmt.
Es ist allerdings darauf hinzuweisen, dass die Tätigkeit im Krankenhaus zunehmend interdisziplinär ausgerichtet wird und die Fachabteilungsstrukturen zugunsten von Zentrenbildungen allmählich aufgelöst werden. Insofern sind auch an Zugriffsrechte auf Patientendaten künftig andere Anforderungen zu stellen, etwa dahin gehend, dass der Zugriff auf Röntgenbilder für diejenigen Ärzte und Abteilungen ermöglicht wird, die an der interdisziplinären Behandlung des Patienten beteiligt sind.

Zu 14.4 Prüfung der Vertrauensstelle des Hessischen Krebsregisters

Ergänzend zu dem vom Hessischen Datenschutzbeauftragten zutreffend dargestellten Sachverhalt ist zu berichten, dass die Personalaufstockung im Zuge des Organisationsaufbaus der Vertrauensstelle nur verzögert erfolgen konnte. Gleichzeitig gingen sehr viele Erstmeldungen ein, sodass es zu Bearbeitungsstaus kam, die eine zeitlich begrenzte Überschreitung der Löschungsfristen nach sich zog. Mit fortschreitender Organisationsentwicklung wird dieser Überhang abgebaut und den gesetzlichen Erfordernissen Genüge getan werden. Das Sozialministerium hat die gegenüber dem Hessischen Datenschutzbeauftragten angekündigten Maßnahmen insoweit umgesetzt, als entsprechende Mittel für die Personalausweitung bereitgestellt wurden.

Der Rechtsauffassung des Hessischen Datenschutzbeauftragten wird zugestimmt. Die Pathologen müssen auf ihre Pflichten hingewiesen und die personenidentifizierenden Datensätze innerhalb der Fristen gelöscht werden.

Zu 14.5 Automatisierung im öffentlichen Gesundheitsdienst

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu. Es handelt sich um hochsensible Daten, die nur Befugten zugänglich sein dürfen. Die Gesundheitsämter sind bemüht, im Rahmen der Automatisierung die erforderlichen datenschutzrechtlichen Voraussetzungen umzusetzen.

Zu 15. Sozialwesen
Zu 15.1 Existenzgrundlagengesetz

Der vom Bundesrat in den Bundestag eingebrachte Gesetzentwurf für ein Existenzgrundlagengesetz hat sich durch die Verabschiedung und das In-

Kraft-Treten des Vierten Gesetzes für moderne Dienstleistungen am Arbeitsmarkt vom 24. Dezember 2003 (BGBl. I S. 2954) und das Gesetz zur Einordnung des Sozialhilferechts in das Sozialgesetzbuch vom 27. Dezember 2003 (BGBl. I S. 3022) erledigt.

Zu 15.2 Sozialdatenschutz und Untersuchungsgrundsatz

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 15.3 Opferschutz und Jugendgerichtshilfe

Die Landesregierung stimmt der Bewertung des Hessischen Datenschutzbeauftragten sowie dem mit dem Jugendamt vereinbarten Verfahren zu.

Zu 16. Personalwesen
Zu 16.1 Personalaktenregistratur im Schulbereich

Der Hessische Datenschutzbeauftragte weist in seinem Bericht darauf hin, dass das neu gebildete und hier zuständige Amt für Lehrerausbildung im Zuge der Umorganisation der Schulaufsicht von den Regierungspräsidien und den Staatlichen Schulämtern seit dem Jahr 2001 eine große Zahl unsortierter Personalakten übernehmen musste. Für die umfangreiche Aufgabe der Personalaktenregistratur wurde speziell eine Arbeitskraft eingestellt.

In der Zwischenzeit wurde die Situation weitestgehend bereinigt. Die rechtlichen Vorschriften über Personalakten werden beachtet und es kann Akteneinsicht genommen werden.
Gleichwohl wird das Kultusministerium die Ausführungen des Hessischen Datenschutzbeauftragten zum Anlass nehmen, um eine aktuelle Überprüfung durchführen zu lassen.

Zu 16.2 Vereitelung von Akteneinsichtsrechten durch Vernichtung von Unterlagen

Der Hessische Datenschutzbeauftragte stellt zutreffend fest, dass das Ministerium des Innern und für Sport nach Unterrichtung über die Angelegenheit bestätigt hat, dass die Aktenvernichtung rechtswidrig gewesen ist und den Landeswohlfahrtsverband aufgefordert hat, solche Rechtsverstöße zukünftig zu unterlassen.

Zu 17. Recht der Presse, Medien- und Teledienste
Zu 17.1 Neuordnung der Rundfunkfinanzierung

Die im Tätigkeitsbericht skizzierten Überlegungen, die Rundfunkgebühr im privaten Bereich künftig haushaltsbezogen zu erheben und im nicht privaten Bereich Daten weiterer Stellen (Kammern, Kraftfahrtbundesamt) heranzuziehen, sind nicht mehr Gegenstand der Beratungen der Länder zur Neustrukturierung der Rundfunkgebühr.

Mit Blick auf die im Tätigkeitsbericht angeführten, bisher praktizierten Datenübermittlungen ist hervorzuheben, dass es im Interesse der gebührenzahlenden Rundfunkteilnehmer liegt, die Zahl der "Schwarzseher" und "Schwarzhörer" möglichst gering zu halten und damit im Ergebnis einer weiteren Erhöhung der Rundfunkgebühr entgegenzuwirken. Der mittlerweile in sämtlichen Ländern durchgeführte so genannte Meldedatenregisterabgleich leistet hierzu einen entscheidenden Beitrag. Die Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten (KEF) hatte aus diesem Grunde entsprechende Meldedatenübermittlungen in sämtlichen Ländern angemahnt. In ihrem jüngst vorgelegten 14. Bericht begrüßt die KEF ausdrücklich, dass der Meldedatenregisterabgleich jetzt in allen Ländern angewendet werde und die Kommunen aktiv zum Vollzug beitrugen.

Die Landesregierung stimmt mit der von der KEF in ihrem 14. Bericht geäußerten Auffassung überein, dass in der effektiven Handhabung des Meldedatenregisterabgleichs ein unerlässliches Mittel zur Durchsetzung der Gebührenpflicht und der Gebührengerechtigkeit zu sehen ist.

Der Hessische Datenschutzbeauftragte geht in seinem Tätigkeitsbericht noch davon aus, dass die vorläufige Freistellung von der Rundfunkgebührenpflicht für Computer, die über das Internet Rundfunkprogramme empfangen können, am 31. Dezember 2004 ende. Dies bedarf der Richtigstellung. Das in § 5a des Rundfunkgebührenstaatsvertrages niedergelegte so genannte

Gebührenmoratorium für "Internet-PCs" wurde durch den Siebten Rundfunkänderungsstaatsvertrag, der am 1. April 2004 in Kraft getreten ist, bis zum 31. Dezember 2006 verlängert.

Zu 17.2 Erwerb von Adressen durch die Gebühreneinzugszentrale

Nach dem gegenwärtigen Stand der Beratungen der Länder zur Reform des Rundfunkgebührenrechts ist geplant, für so genannte Mailing-Aktionen der Rundfunkanstalten einschließlich des damit verbundenen Erwerbs von Adressen eine explizite staatsvertragliche Grundlage zu schaffen. Der Anlass für die in dem Tätigkeitsbericht dargelegten unterschiedlichen rechtlichen Bewertungen des Hessischen Datenschutzbeauftragten und des Hessischen Rundfunks zur Zulässigkeit des Erwerbs von Adressen dürfte damit entfallen.

Maßgeblich für die in Aussicht genommene staatsvertragliche Übereinkunft sind die bereits angeführten Gesichtspunkte der Durchsetzung der Gebührenpflicht und der Gebührengerechtigkeit. Diese Gesichtspunkte kommen überdies bereits in dem in § 4 Abs. 5 des Rundfunkgebührenstaatsvertrages normierten Auskunftsanspruch der Rundfunkanstalten zum Ausdruck, der im Verwaltungszwangsverfahren durchgesetzt werden kann.
Unabhängig hiervon hat sich der Hessische Rundfunk bereit erklärt, gegenüber der GEZ auf eine bürgerfreundlichere Ausgestaltung des Mailing-Verfahrens hinzuwirken.

Zu 17.3 Online-Bestellung von Newslettern

Die Landesregierung stimmt der Auffassung des Hessischen Datenschutzbeauftragten zu.

Die Voraussetzungen der Nutzung von E-Mail-Adressen für Werbezwecke wurde bereits ausführlich im Sechzehnten Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden (Drucks. 16/1680) unter Nr. 11.2 behandelt.

Zu 18. Entwicklungen und Empfehlungen im Bereich der Technik
Zu 18.1 TCPA

Die Landesregierung hat die Darstellung des Hessischen Datenschutzbeauftragten zur Kenntnis genommen und wird die weitere Entwicklung verfolgen.

Zu 18.2 SPAM – die neue Gefahr für die Integrität des Internets

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Die Nutzung von E-Mail-Adressen für unverlangte Werbung ("SPAM") und deren rechtliche Beurteilung wurde bereits mehrfach in den Tätigkeitsberichten der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden behandelt, zuletzt im Fünfzehnten Tätigkeitsbericht (Drucks. 15/4659) unter Nr. 8.8.
Die vom Hessischen Datenschutzbeauftragten angeführte Vorschrift gegen unverlangte E-Mails ist mit dem Gesetz gegen den unlauteren Wettbewerb (UWG) vom 3. Juli 2004 (BGBl. I S. 1414) am 8. Juli 2004 in Kraft getreten.

Zu 18.3 Automatische Software-Updates

Die Landesregierung beurteilt den Nutzen automatischer Software-Updates durchaus positiv. Ein möglichst gut unterstütztes automatisches Software-Update kann auftretende Sicherheitslücken schnell schließen und dient damit der Systemsicherheit. Die Belange des Datenschutzes müssen natürlich beachtet werden.

Zu 18.4 Sicherheitsprobleme beim Einsatz von USB-Geräten

Die vom Hessischen Datenschutzbeauftragten vorgeschlagene Dienstanweisung zum Betrieb von USB-Geräten soll umgesetzt und in die Regelungen zur IT-Sicherheit übernommen werden.

Zu 18.5 Elektronische Authentisierung mit Schlüsseln

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Im Übrigen ist darauf hinzuweisen, dass in der Landesverwaltung Anfang 2004 das Projekt "Hessen-PKI" gestartet wurde. In der ersten Phase dieses Projekts wurden von der HZD, die hier die Funktion einer Zertifizierungsstelle wahrnimmt, 120 Chipkarten mit einer fortgeschrittenen Signatur an ausgewählte Landesbedienstete ausgegeben. Diese Pilotteilnehmer sammeln Erfahrungen im Umgang mit Signatur und Verschlüsselung. Ziel ist die Ausstattung aller Landesbediensteten mit einer solchen Chipkarte, die bei Bedarf um zusätzliche Funktionen erweitert werden kann.

Zu 18.6 Orientierungshilfe Kryptografie - Technische Grundlagen

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 18.7 Die Nutzung digitaler Funktelegramme im Rettungsdienst

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Zu 19. Bilanz

Zu 19.1 Übertragung der Zuständigkeit für Untersuchungen zur Dienstfähigkeit von Beamtinnen und Beamten in der hessischen Landesverwaltung auf die Versorgungsämter (31. Tätigkeitsbericht, Nr. 19.2)

Der Hessische Datenschutzbeauftragte verkennt bei seiner Forderung nach einer besonderen Rechtsgrundlage für die Datenverarbeitung durch die Versorgungsämter, dass durch § 51 Abs. 1 Satz 4 Hessisches Beamtengesetz (HBG) in Verbindung mit § 18a der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens diese bereits besteht. Wie schon in der Stellungnahme der Landesregierung zum 31. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten zu Nr. 19.2 (LT-Drucks. 16/1679, Seite 28) ausgeführt, hat der Arzt nach § 51 Abs. 1 Satz 4 HBG, wenn er kein Amtsarzt ist, der Behörde sein Gutachten "sowie in entsprechender Anwendung der für Amtsärzte geltenden Rechtsvorschriften auch die Angaben zur Vorgeschichte und den Untersuchungsbefund" mitzuteilen. Die für Amtsärzte geltenden Rechtsvorschriften sind die in § 18a der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens enthaltenen Regelungen. Diese geben dem Arzt des Versorgungsamts - wie einem Amtsarzt - vor, welche Daten zu erheben und an die Behörde, die die Untersuchung veranlasst hat, zu übermitteln sind. Es ist nicht nachvollziehbar, weshalb die Vorschrift des § 18a zwar als Grundlage für die Datenverarbeitung bei den Gesundheitsämtern genügen soll, wie der Hessische Datenschutzbeauftragte zu Recht in seinem Bericht feststellt, nicht aber für die Ärzte der Versorgungsämter, nachdem § 51 Abs. 1 Satz 4 HBG sie ausdrücklich für anwendbar erklärt hat.

Von der Frage der Rechtsgrundlage für die Datenverarbeitung zu trennen ist die nach der Rechtsgrundlage für die Wahrnehmung der Aufgabe der Untersuchung der Dienstfähigkeit. Diese ist hier aber für die Rechtmäßigkeit der Datenverarbeitung ohne Belang, weil den Ärzten bei den Versorgungsämtern durch den Kabinettsbeschluss vom 8. Mai 2001 nicht die Funktion der Amtsärzte bei den Gesundheitsämtern übertragen wurde. Die Entscheidung diente vielmehr dem Zweck, die Landesbehörden anzuhalten, die Dienstfähigkeit von Beamtinnen und Beamten in der Regel durch Ärzte der Versorgungsämter untersuchen zu lassen bzw. gegenüber den Versorgungsämtern, die entsprechenden Untersuchungen durch ihre Ärzte vorzunehmen, wobei diese in Bezug auf ihre Rechtsposition den frei praktizierenden Ärzten gleichgestellt sind. Für eine nur verwaltungsintern wirkende Weisung an die Landesbehörden benötigt die Landesregierung keine Rechtsverordnung.

Zur Klarstellung wird das Sozialministerium die Hinweise auf den Vordrucken entsprechend der vorstehend dargestellten Rechtslage ergänzen.

Zu 19.2 Anonymität im Internet (29. Tätigkeitsbericht, Nr. 11.4; 30. Tätigkeitsbericht, Nr. 6.2)

Ausgangspunkt des im Tätigkeitsbericht wiedergegebenen Konfliktes ist ein Ermittlungsverfahren gegen einen europaweit agierenden Personenkreis wegen des Verdachts der gewerbsmäßigen Herstellung und Verbreitung kinderpornographischer Schriften (Bilddateien). Die Ermittlungen der Staatsanwaltschaft sind nach wie vor nicht abgeschlossen. Mittlerweile hat

die Staatsanwaltschaft die von der landgerichtlichen Beschwerdeentscheidung betroffenen Datensätze gelöscht, sodass dem Anliegen des Hessischen Datenschutzbeauftragten Rechnung getragen worden ist.

Aus Sicht der Landesregierung bleibt klarzustellen, dass es sich bei der Frage der Dokumentation und Verwertung der im Strafverfahren erhobenen Erkenntnisse nicht um eine der Regelung durch den Landesgesetzgeber zugängliche Materie handelt; § 19 HDSG ist insoweit nicht einschlägig. Im Übrigen dürfte die Auffassung der Staatsanwaltschaft, dass die Konsequenzen einer unzulässigen Beweiserhebung im Ermittlungsverfahren - jedenfalls vor dem rechtskräftigen Abschluss des Verfahrens - primär im Bereich des strafprozessualen Beweisrechts zu suchen sind, zutreffen. Vorgaben über die Vernichtung bzw. Löschung von Daten im hier betroffenen Bereich ergeben sich im Übrigen aus § 100h Abs. 1 Satz 3 in Verbindung mit § 100b Abs. 6 StPO.

Zu 19.3 Prüfung von Datensicherheitsmaßnahmen mit Hilfe eines Portscanners (30. Tätigkeitsbericht, Nr. 14.5)

Die Landesregierung stimmt den Ausführungen des Hessischen Datenschutzbeauftragten zu.

Beide vom Hessischen Datenschutzbeauftragten genannten Aspekte sind sehr wichtig. Zum einen die Schließung der vorhandenen Lücken und zum anderen organisatorische Maßnahmen, die verhindern, dass durch Änderungen und Anpassungen neue Lücken entstehen. Die Anzahl der geöffneten Ports muss so klein wie irgend möglich gehalten werden. Daher sollte jede Öffnung gut überlegt und entsprechend dokumentiert werden. Es stehen geeignete Portscanner zur Verfügung, die ohne großen Aufwand die Überprüfung durchführen. Daher sollte eine Überprüfung mindestens quartalsweise erfolgen.

In dem Bericht werden die Server der DMZ als Beispiel genannt. Die Überprüfung muss die Firewall selbst natürlich mit einbeziehen.

Wiesbaden, 14. Februar 2005

Der Hessische Ministerpräsident:
Koch

Der Minister des Innern und für Sport:
Bouffier