15. Wahlperiode

Drucksache **15/1101**

HESSISCHER LANDTAG

28. 03. 2000

Achtundzwanzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt am 31. Dezember 1999
nach § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 28. März 2000 · Ausgegeben am 30. März 2000

Druck: Wiesbadener Graphische Betriebe GmbH, 65199 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 ·65022 Wiesbaden

Achtundzwanzigster Tätigkeitsbericht

des

Hessischen Datenschutzbeauftragten
Professor Dr. Friedrich von Zezschwitz

vorgelegt zum 31. Dezember 1999
gemäß § 30 des Hessischen Datenschutzgesetzes
vom 7. Januar 1999

Inhaltsverzeichnis

Kernpunkte des 28. Tätigkeitsberichts

1. Hessen hat mit der Neufassung des Datenschutzgesetzes die EG-Datenschutzrichtlinie fristgerecht umgesetzt, sodass während des gesamten Berichtszeitraumes nach neuem Recht verfahren werden konnte (Ziff. 2.1).

2. Als Hilfestellung für die Anwendung des novellierten Hessischen Datenschutzgesetzes hat das Hessische Ministerium des Innern und für Sport Einführungshinweise und Formulare für das von den datenverarbeitenden Stellen zu führende Verfahrensverzeichnis veröffentlicht. Ich habe für die Durchführung der neu eingeführten Vorabkontrolle eine „Checkliste“ und weitere schriftliche Hinweise erstellt und zum Einsichtsrecht in personenbezogene Daten durch den behördlichen Datenschutzbeauftragten, dessen Aufgaben und Befugnisse neu geregelt wurden, eine eingehende Stellungnahme erarbeitet. Außerdem ist ein Vertragsmuster für die Auftragsvergabe von EDV-Arbeiten entwickelt worden (Ziff. 3 und Ziff. 25.2). Die genannten Unterlagen sind auch über das Internet abrufbar (www.datenschutz.hessen.de).

3. Mit der Novelle des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung sollen die Kontroll- und Überwachungsbefugnisse der Polizeibehörden erheblich ausgeweitet werden. Nicht alle beabsichtigten Maßnahmen sind aus der Sicht des Datenschutzes verfassungsrechtlich unbedenklich (Ziff. 5.1).

4. Die hessische Praxis, bei DNA-Analysen zum Zwecke zukünftiger Strafverfolgung von der Einholung der richterlichen Anordnung abzusehen, wenn der Betroffene in das Verfahren eingewilligt hat, steht mit den gesetzlichen Vorgaben nicht im Einklang (Ziff. 5.2).

5. Bei der Überprüfung einer polizeilichen Datenspeicherung habe ich festgestellt, dass Polizeibehörden die Mitteilung der Staatsanwaltschaft über einen Freispruch lediglich zur Akte nahmen, statt die Datenspeicherung zu löschen und die Akte zu vernichten. Mit der Behörde wurde abgesprochen, dass sie die Löschung und Vernichtung künftig durch organisatorische Maßnahmen sicherstellt. Da die Regelung des § 20 Abs. 4 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung mehrdeutig ist, wird

eine generelle Richtlinie erarbeitet werden müssen (Ziff. 5.3).

6. Der Einsatz der elektronischen Fußfessel im Rahmen von richterlichen Weisungen gemäß § 56c Strafgesetzbuch ist grundsätzlich nicht ausgeschlossen. Solange keine bundesrechtliche Regelung verabschiedet ist, kann der Einsatz nur mit Einwilligung des Verurteilten erfolgen. Einzelheiten der im Rahmen der Überwachung vorgesehenen Verarbeitung personenbezogener Daten sind noch klärungsbedürftig (Ziff. 6).

7. Eine verdeckte Videoüberwachung des Personals eines Krankenhauses ist nicht zulässig, hingegen die Abschirmung gentechnischer Anlagen, wenn dort Lebensgefahr droht. (Ziff. 8.4 und Ziff. 8.5).

8. Im Kreis Odenwald und in Wiesbaden können Kraftfahrzeughändler die Zulassung von Neuwagen sowie Kraftfahrzeugum- und -abmeldungen per Internet erledigen. Die Überprüfung ergab, dass die datenschutzrechtlichen Vorgaben bei der Ausgestaltung des Verfahrens ausreichend berücksichtigt wurden (Ziff. 9.4).

9. Die elektronische Post (E-Mail) hat gegenüber Briefen und Telefax Vorteile. Diesen Vorteilen stehen aber auch datenschutzrechtliche Risiken gegenüber, die Gegenmaßnahmen erfordern (Ziff. 10.1).

10. Das Angebotsspektrum von EDV-Dienstleistungen hat sich in den letzten Jahren um die Fernadministration und Fernwartung erweitert. Dadurch ergeben sich Risiken, die durch eine planvolle, kontrollierte Vorgehensweise begrenzt werden müssen (Ziff. 10.2).

11. Die im Auftrag des Bundesministeriums des Innern angefertigte Machbarkeitsstudie zu Einsatz einer Smart-Card im Asylverfahren liegt den Innenministerien und Senatoren der Länder vor. Von einer Realisierung des Einsatzes der Smart-Card in dem von der Studie vorgesehenen Umfang ist abzuraten (Ziff. 11.1).

12. Die Vermutung einer mangelhaften Meldemoral vor allem unter Studierenden und die daraus resultierenden Nachteile beim Finanzausgleich rechtfertigen keinen flächendeckenden Abgleich örtlicher Klingelschilder mit den Eintragungen im Melderegister. Diese Maßnahme ist weder melderechtlich vorgesehen noch

datenschutzrechtlich zulässig (Ziff. 12).

13. Meine Umfrage hat ergeben, dass Videoüberwachung in hessischen Städten und Gemeinden derzeit nur in einer begrenzten Zahl von Fällen - ca. 500 - stattfindet. Fehlende bereichsspezifische Eingriffsermächtigungen bei Bildaufzeichnungen erweisen sich als rechtsstaatliches Defizit (Ziff. 13.1 und Ziff. 13.3).

14. Stadtverordnete, die in ihrer Eigenschaft als „normale Bürger“ in Kontakt zu ihrer Stadtverwaltung treten, haben Anspruch darauf, datenschutzrechtlich genauso behandelt zu werden wie alle anderen Bürgerinnen und Bürger. Gegen diesen Grundsatz haben im vergangenen Jahr eine Bürgermeisterin und ein Bürgermeister in zwei hessischen Städten verstoßen (Ziff. 13.4).

1. Vorwort

Das Berichtsjahr war für die Dienststelle und mich vor allem durch umfangreiche Beratungstätigkeiten, die laufende Kontrolltätigkeit, aber auch durch datenschutzrechtlich bedeutsame Gesetzesvorhaben geprägt, die zu umfangreichen Stellungnahmen geführt haben:

- die Vorbereitung des Änderungsgesetzes zum Bundesdatenschutzgesetz, mit dem die Europäische Datenschutzrichtlinie endlich umgesetzt werden soll,

- die beabsichtigte Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung, die die polizeiliche Videoüberwachung und die Schleierfahndung zu ihren wichtigsten Elementen zählt und damit neue Herausforderungen für den Datenschutz bringen wird,

- die beabsichtigte Änderung des Sozialgesetzbuches Teil V, die eine grundlegende Veränderung der datenschutzrechtlichen Belange der Versicherten zum Gegenstand hatte,

- das 8. Wiesbadener Forum Datenschutz, das sich mit den Grenzen der Videoüberwachung im öffentlichen Raum und den aus dieser neuen Technik hervorgehenden Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung befasst hat,

- den ersten Initiativen für ein Hessisches Akteneinsichtsgesetz.

Im Unterschied zum hessischen Gesetzgeber, der die Dreijahresfrist für die Umsetzung der Europäischen Richtlinie vorbildlich eingehalten hat, war der Bund bislang nicht imstande, sein Datenschutzrecht an die neuen Anforderungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten anzupassen. Die Neuregelung wird vor allem für die Kontrollen nicht-öffentlicher Stellen beträchtliche Auswirkung haben. Offen ist deswegen nach wie vor die Frage, ob die Ausweitung der datenschutzrechtlichen Aufgaben und die europäischen Rechtsgarantien für die Unabhängigkeit der Überwachungsstellen nicht eine Neuorganisation der hessischen Datenschutzverwaltung erzwingen werden. Es ist zu hoffen, dass die überparteiliche und sachliche Zusammenarbeit des Parlaments und der Landesregierung in Sachen Datenschutz auch diese Frage einer sachgerechten Lösung zuführen wird.

Die in den vorausgehenden Tätigkeitsberichten angesprochene Frage der Verselbständigung und möglichen Zusammenlegung der zur Zeit noch bei den Regierungspräsidien angesiedelten Datenschutzkontrollstellen sollte nach Abschluss der Bundesgesetzgebung einer baldigen gesetzlichen Regelung zugeführt werden. Die Auslegung der Richtlinie, wonach die Datenschutzkontrollstellen für alle Bereiche funktional und institutionell unabhängig anzusiedeln sind, hat in allen Fraktionen des Hessischen Landtags Anhänger gefunden, da die Eingliederung in die weisungsfreie Behörde des Datenschutzbeauftragten verfassungsrechtliche Bedenken vermeiden kann. Es ist zu hoffen, dass die Beschlüsse des 62. Deutschen Juristentages, die eine dahingehende Umstrukturierung empfehlen, die Entschließungen des Hessischen Landtages fördern werden. Der Deutsche Juristentag hatte gefordert, dass das materielle Datenschutzrecht für den öffentlichen und den privaten Bereich anzugleichen ist und dass die Kontrolle für die privatwirtschaftliche Datenverarbeitung „verselbstständigt und weisungsfrei“ zu institutionalisieren ist. Dass bei der Angliederung an meine Behörde ein „ministerialfreier“ Raum entsteht, ist insofern unproblematisch, als eine starke Rückkopplung zum Landtag und die kurze Wahlperiode des Datenschutzbeauftragten einen Ausgleich bieten. Ich trete deswegen nach wie vor dafür ein, dass das Land Hessen im Rahmen seiner föderativ-verfassungsrechtlichen Möglichkeiten der in einigen Bundesländern bereits vollzogenen Neuordnung folgen möge.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat ihre Bemühungen um gemeinsame Standards zum Schutz des Rechtes der Bürgerinnen und Bürger auf informationelle Selbstbestimmung fortgesetzt. Der ständige Austausch mit allen an dieser Aufgabe arbeitenden Stellen hat zu intensiven Sachdiskussionen und Klärungen streitiger Rechtsfragen geführt, deren Ergebnisse unter Ziff. 24 zu diesem Bericht abgedruckt sind, soweit sie in förmliche Entschließungen eingeflossen sind. Der bei diesen Anlässen geführte konstruktive Gedanken-, Erfahrungs- und Meinungsaustausch hat die zunehmenden Vernetzungen informationeller Einzelvorgänge deutlich bewusst gemacht. Einzelfragen des Datenschutzes werden in verschiedenen Arbeitskreisen kontinuierlich erörtert und – soweit möglich – bundesweit koordiniert.

Die nach der Neuwahl in den Mittelpunkt des politischen Interesses gerückte Videoüberwachung des öffentlichen Raumes hat ein besonders sensibles Gebiet der informationellen Selbstbestimmung berührt. Die im Zusammenhang damit entstandenen

politischen Kontroversen haben uns veranlasst, die Videoüberwachung zum Gegenstand des 8. Wiesbadener Forum Datenschutz zu machen. Das seit 1992 jährlich vom Präsidenten des Hessischen Landtags und vom Hessischen Datenschutzbeauftragten veranstaltete Forum hat seit jeher zum Ziel, besondere Problemzonen des Grundrechts auf informationelle Selbstbestimmung aufzugreifen. Die Videoüberwachung erzeugt ein hohes Spannungsverhältnis zur verfassungsrechtlichen Garantie der Privatsphäre. Das rechtspolitische Interesse einer Erhöhung der Sicherheit im öffentlichen Raum führt zu umfangreicher Erhebung, Verarbeitung und Verwertung personenbezogener Daten. Der staatliche Gefahrenabwehrauftrag muss mit den Grundsätzen des Datenschutzrechts in Einklang gebracht werden, sodass ein unzumutbarer Verlust an Selbstbestimmung vermieden wird. Auf dem Forum diskutierten Verfassungsrechtsjuristen, leitende Polizeibeamte, Kriminologen und Datenschutzexperten, ob das Grundrecht und der Sicherheitsgewinn in eine praktische Konkordanz gebracht werden können. Der Tagungsband unter dem Titel „Videoüberwachung und Datenschutz“ soll wiederum im Nomos-Verlag erscheinen. Er wird den Wortlaut der Referate und Diskussionen wiedergeben.

Die im nachstehenden Datenschutzbericht von meinen Mitarbeiterinnen und Mitarbeitern verfassten Beiträge geben nicht nur wieder, wo die Schwerpunkte der Tätigkeit gelegen haben. Die Auswahl erfolgte auch mit dem Ziel, kritisch zu wertende Anlässe für datenschutzrechtliche Beanstandungen aufzuzeigen. Ich hoffe, dass die Art der Darstellung deutlich macht, dass alle Mitarbeiterinnen und Mitarbeiter wie auch ich bemüht sind, uns nicht als Gegner der hessischen Staats- und Kommunalverwaltung, sondern als Gesprächspartner zu verstehen. Beratender Tätigkeit haben wir den Vorrang vor objektiv prüfender und kritisierender Kontrolle gegeben. Immer wieder zeigt sich für beide Seiten, dass erst die genauere Analyse zu einer zutreffenden Beurteilung des Gefahrenpotentials führt. Beispielhaft mögen die elektronische Fußfessel (Modellversuch Frankfurt am Main, Ziff. 6), die Erhebung über die höchst unterschiedlich motivierten Videoeinrichtungen der hessischen Gemeinden (Ziff. 13.1), die Smart-Card für Asylsuchende (Ziff. 11.1), die Gesundheitsreform mit ihren anfänglich deutlichen Schritten zum „gläsernen Patienten“ (Ziff. 8.1) genannt werden.

Die überwiegende Zahl der im Bericht erörterten Themen besitzt einen hessischen Anlass. Zuweilen reichen die aufgeworfenen Fragen allerdings deutlich über Hessen hinaus. Das gilt insbesondere für die nach wie vor ungelösten Probleme der Justizverwaltungen im Hinblick

auf Datenerhebung und Datenübermittlung, denn die hier erforderlichen Rechtsgrundlagen für datenschutzerhebliche Vorgänge bei den Gerichten und Staatsanwaltschaften sind noch immer nicht verabschiedet. In den Fragen DNA-Analysen auf „freiwilliger“ Basis hat trotz der engen Ermächtigungsschranken der § 81a ff. StPO keine befriedigende Lösung mit dem Justizministerium gefunden werden können. Zu den aus meiner Sicht noch nicht befriedigend gelösten Problemen gehören der in einer hessischen Gemeinde stattfindende Abgleich von Melderegisterdaten anhand der Anschriften von Wohnungsinhabern auf den Briefkästen (Ziff. 12.1), die Zwangsanzeige des Kontostandes bei Geldausgabeautomaten, ein Verfahren , das die überwiegende Zahl der hessischen Sparkassen anwendet (Ziff. 15.1), sowie die polizeiliche Speicherung nach § 20 HSOG trotz erfolgten Freispruches. Die diesbezügliche Regelung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung ist missverständlich.

Das hessische Ausführungsgesetz zum Krebsregistergesetz, das meiner Behörde zahlreiche neue Aufgaben zugewiesen hat, wäre fast unbemerkt ausgelaufen, was zu gravierenden Datenschutzproblemen hätte führen können. Das Sozialministerium hat das Anschlussgesetz gerade noch rechtzeitig in den Gesetzgebungsgang gebracht, sodass das neue Gesetz mit den von mir vorgeschlagenen Zusätzen und Klarstellungen noch vor Jahresende verabschiedet werden konnte (GVBl. I 1999 S. 25).

Das schon in früheren Tätigkeitsberichten erhobene Postulat, meine Behörde ausreichend mit Technik und informationstechnisch geschultem Personal auszustatten, hat hinsichtlich der technischen Ausstattung im Jahr 1999 deutliche Fortschritte gemacht, da frei gewordene Haushaltsmittel für technische Verbesserungen haben eingesetzt werden können. Die personelle Umgestaltung hat ebenfalls einen ersten Schritt nehmen können, da eine Planstelle für eine informationstechnische Nachwuchskraft bereit gestellt worden ist. Eine frei gewordene Stelle für eine Verwaltungsangestellte soll derzeit mit einer technisch ausgerichteten Fachkraft neu besetzt werden. Bei Verwirklichung dieser Maßnahmen nähert sich die hessische Dienststelle in ihrer datenschutzrechtlichen und datenschutztechnischen Struktur den Entwicklungen anderer Bundesländer, die die zunehmende Technisierung und die dadurch entstehenden technischen Anforderungen schneller vollzogen haben, als Hessen. Auf diesem Wege soll das datenschutzrechtliche Know-how, das nur noch in enger Zusammenarbeit mit Informatikern zu erreichen ist, den sich immer schneller ändernden Hard- und Softwarestandards angepasst werden als bisher.

Ich nehme diesen Bericht zum Anlass, allen meinen Mitarbeiterinnen und Mitarbeitern für die im Berichtszeitraum geleistete Arbeit zu danken. Sie schlägt sich im nachstehenden Bericht nur insoweit nieder, als es sich um berichtenswerte „besondere“ Tatbestände handelt.

Ich schließe dieses Vorwort in der Hoffnung, dass der Bericht in etwa das wiedergibt, was die Vielfalt unserer Arbeit ausmacht. Gleich danke ich den Abgeordneten des Hessischen Landtages, mit denen sich stets eine fruchtbare Zusammenarbeit ergeben hat. Ich hoffe auch für die Zukunft, dass sich die wiederkehrenden Streitfragen um das Recht auf informationelle Selbstbestimmung in einer Weise lösen lassen, die dem hohen grundrechtlichen Rang gerecht wird, das der Privatsphäre zukommt. Meine Hoffnung ist darauf gerichtet, dass das Datenschutzrecht in näherer Zukunft durch ein allgemeines Akteneinsichtsrecht ergänzt und damit in den Rang eines Partizipationsrechts gehoben werden kann.

2. EG-Datenschutzrichtlinie

2.1
Stand der Umsetzung der EG-Datenschutzrichtlinie in Hessen

Hessen hat die EG-Datenschutzrichtlinie fristgerecht umgesetzt. Die Neufassung des Gesetzestextes sowie neue Durchführungsvorschriften sind inzwischen veröffentlicht.

Die durch die Umsetzung der EG-Datenschutzrichtlinie veranlassten wesentlichen Änderungen des Hessischen Datenschutzgesetzes habe ich bereits im 27. Tätigkeitsbericht unter Ziff. 2 dargestellt. Nachdem das Änderungsgesetz am 10. November 1998 in Kraft getreten ist, hat das Hessische Innenministerium am 7. Januar 1999 von seiner Ermächtigung Gebrauch gemacht und die Neufassung des gesamten Gesetzestextes veröffentlicht (GVBl. I 1999 S. 98). Der Ausführungserlass zum Hessischen Datenschutzgesetz ist ebenfalls neu gefasst (StAnz. 17/1999 S. 226).

In der Zeit seit Inkrafttreten sind mir lediglich Interpretationsfragen, aber keine wesentlichen Schwierigkeiten in der Anwendung der neuen Vorschriften bekannt geworden. Eine Ausnahme bildet der zu enge Verarbeitungsbegriff in § 2 Abs. 2 S. 1. Auch das Erheben von Daten ohne Speicherungsabsicht kann das Grundrecht auf informationelle Selbstbestimmung beeinträchtigen - z.B. durch Videoaufnahmen. Das Gesetz enthält insofern eine Regelungslücke, die - zumindest bei erheblichen Eingriffen - durch bereichsspezifische Vorschriften geschlossen werden muss. In Ziff. 3 sind einige weitere Fragestellungen und Auslegungshilfen zusammengestellt.

2.2
Stand der Umsetzung der EG-Datenschutzrichtlinie im Bundesrecht

Die Arbeiten auf Bundesebene an der Novellierung des Bundesdatenschutzgesetzes wurden im Berichtszeitraum fortgesetzt. Ich habe im Zuge einer Anhörung eine umfangreiche Stellungnahme abgegeben. Bei Redaktionsschluss lag noch kein abgestimmter Regierungsentwurf vor.

Die EG-Datenschutzrichtlinie verpflichtet die Mitgliedsstaaten, die Regelungen bis zum Oktober 1998 in nationales Recht umzusetzen. Die Bundesregierung hatte die Arbeiten bereits in der vergangenen Legislaturperiode aufgenommen, aber nicht abgeschlossen; die Frist ist inzwischen deutlich überschritten.

Die 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25/26. März 1999 hat sich mit den bis dahin vorliegenden Entwürfen befasst und die unter Ziff. 24.1 abgedruckte Entschließung einstimmig verabschiedet. Der Entwurf mit Stand vom 6. Juli 1999 stand zur schriftlichen Anhörung der Bundesressorts, der für den Datenschutz zuständigen Länderressorts, der Spitzenverbände sowie zahlreicher einschlägiger Berufsverbände. In diesem Anhörungsverfahren hat auch Hessen umfassend Stellung genommen. Nachfolgend sind meine wesentlichen Kritikpunkte wiedergegeben.

Zwar enthält der Entwurf vom 6. Juli 1999 zur Änderung des Bundesdatenschutzgesetzes (BDSG) deutliche Verbesserungen gegenüber dem Stand der Novellierung der vergangenen Legislaturperiode. Dennoch sind noch wesentliche Mängel vorhanden, die dringend beseitigt werden sollten.

1. Der neue Entwurf behält das komplizierte und unübersichtliche System der Regelungen des bisherigen Rechts bei und wird dadurch schwer verständlich. Der in § 1 niedergelegte Zweck als Gesetz zum Schutz von Bürgerrechten wird durch ein schon Juristen schwer zugängliches und vom Bürger kaum zu verstehendes Gesetz nicht erreicht. Zudem sind teilweise überzogene Generalermächtigungen vorgesehen, die dem Schutzzweck es Gesetzes nicht gerecht werden. Deshalb muss unbedingt sofort mit der - als notwendig angekündigten - vollständigen Überarbeitung des Gesetzes begonnen werden.

2. Der Entwurf verwendet - im Gegensatz zur EG-Datenschutzrichtlinie - keinen einheitlichen Verarbeitungsbegriff, sondern spricht - außerhalb der automatisierten Datenverarbeitung - von Erfassen, Verarbeiten und Nutzen. Bei der automatisierten Datenverarbeitung fällt das Erfassen und Nutzen unter den Verarbeitungsbegriff. Dadurch werden an vielen Stellen komplizierte und nicht nur sprachlich unverständliche Regelungen erforderlich, die anderenfalls entbehrlich wären (z.B. §§ 12 Abs. 4; 35 Abs. 5, 7, 8, 9; 11 Abs. 2, 3 und 4 BDSG). Sofern für das Erfassen und Nutzen besondere

Regelungen erforderlich sind, ist dies ohne weiteres möglich, weil diese Begriffe auch definiert sind.

3. Der Entwurf stellt nicht sicher, dass die verwendeten - an die heute bekannten Techniken angelehnten - Begriffe auch auf die technische Weiterentwicklung anwendbar sind, die erhebliche Gefahren für die Persönlichkeitsrechte mit sich bringt. Hier sei die Videoüberwachung genannt und an den Fall der Erfassung von Gebäuden ganzer Städte in einem Bildkataster erinnert, der in der Bevölkerung auf breite Ablehnung stößt. Von dem Entwurf sind überdies nur solche Verfahren erfasst, die „mittels einer Datenverarbeitungsanlage“ betrieben werden oder bei denen die Datensammlung unter den Dateibegriff fällt. Klarzustellen ist, dass auch konventionelle Videokameras und Videobänder den Regeln des BDSG zu unterwerfen sind. Das Gleiche gilt auch für die Aufnahme von Serienbildern mit Personenbezug. Dies bedarf der gesetzlichen Regelung, damit den Anforderungen der EG-Datenschutzrichtlinie genügt wird, denn Erwägungsgrund 14 stellt unmissverständlich klar, dass personenbezogene Bild- und Tondaten einzubeziehen sind.

4. Es fehlt eine Vorschrift, die generell die Verantwortlichkeiten bei der Datenübermittlung regelt. In eine solche Regelung würden z.B. § 4b Abs. 5 und Abs. 6 gehören, die dann bei § 4c nicht wiederholt werden müssten.

5. Bei den Rechten der Betroffenen fehlt die explizite Nennung des Rechtes, sich jederzeit und, ohne dass daraus Nachteile erwachsen, an den Bundesbeauftragten für den Datenschutz und auch an den behördlichen oder betrieblichen Datenschutzbeauftragten zu wenden (etwa entsprechend der Regelung in §§ 8 Abs. 1 Nr. 6, 28, 37 Abs. 2 und 5 Abs. 1 HDSG). Die Aufzählung der unabdingbaren Rechte ist unvollständig.

6. Soweit Forschungsprivilegien im BDSG enthalten sind, wäre eine generelle Zusammenfassung der Regelungen in einer besonderen Vorschrift zu begrüßen, wie sie sich z.B. in § 33 HDSG findet. Soweit einzelne Vorschriften beibehalten werden, ist im Übrigen jeweils darauf zu achten, dass die Grundrechte des Persönlichkeitsrechts und der freien Forschung gleichwertig sind und deshalb das Forschungsinteresse das Persönlichkeitsrecht nicht erheblich überwiegen muss. Das Wort „erheblich“ ist jeweils zu streichen, zumal Art. 5 Abs. 3 GG vorbehaltlos gewährleistet „Kunst, Wissenschaft,

Forschung und Lehre sind frei“ (z.B. § 13 Abs. 2 Nr. 5, § 14 Abs. 5 Nr. 2, § 28 Abs. 6 Nr. 2).

Die Entwicklung im Bundesrecht werde ich auch künftig in Zusammenarbeit mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder weiter begleiten.

3. Hinweise zur Anwendung des novellierten Hessischen Datenschutzgesetzes

3.1
Verfahrensverzeichnis

Zur Umsetzung der Vorschrift zum Verfahrensverzeichnis (§ 6 HDSG) hat das Hessische Ministerium des Innern und für Sport Einführungshinweise und Formulare veröffentlicht. Der Beitrag gibt einen Überblick über bisher hierzu aufgetretene Fragen.

Da das zentral bei mir geführte Dateienregister mit der Neuregelung durch das bei den datenverarbeitenden Stellen zu führende Verfahrensverzeichnis ersetzt ist, war eine Neufassung des Ausführungserlasses zum Hessischen Datenschutzgesetz (HDSG) erforderlich. Mit Erlass vom 14. April 1999 (StAnz. 17/1999 S. 226) hat das Hessische Innenministerium rechtzeitig vor Inkrafttreten dieser Bestimmung (§ 6 HDSG trat erst am 1. Juni 1999 in Kraft) Hinweise zum Verfahrensverzeichnis gegeben und die neuen Formulare veröffentlicht. Sie sind in Zusammenarbeit mit behördlichen Datenschutzbeauftragten und mir erarbeitet worden und nunmehr auch im Internet (http://www.hessen.de/hdsb/HDSG-Vz) und Landesintranet (http://www.intern.hessen.de/HDSG-Vz) verfügbar.

Die Begriffsbestimmungen des Hessischen Datenschutzgesetzes definieren den Verfahrensbegriff nicht. Allerdings ist in den Durchführungshinweisen des Hessischen Innenministeriums erläutert, was unter Verfahren zu verstehen ist: „Ein Verfahren ist die Gesamtheit aller automatisierten Verarbeitungsschritte zur rechtmäßigen Erfüllung eines bestimmten Verwaltungszweckes“. Ein Verfahrensverzeichnis ist für neue Verfahren sowie bei Änderungen zu erstellen. Für Standardverfahren, die ohne Anbindung an eine bestimmte Verwaltungsaufgabe übergreifend als „Werkzeug“ für verschiedene Aufgaben eingesetzt werden, ist es nicht erforderlich. Allerdings ist auch hierfür eine Vorabkontrolle durchzuführen (s. Ziff. 3.2).

Unsicherheit bestand in der Frage, ab *wann* Verfahrensverzeichnisse aufzustellen sind und ob zum Stichtag 1. Juni 1999 für alle eingesetzten Verfahren ein Verzeichnis nach dem neuen Muster vorhanden sein muss. Nach dem Hessischen Datenschutzgesetz sind Verfahrensverzeichnisse für alle ab dem 1. Juni 1999 neu eingeführten oder nach diesem

Zeitpunkt geänderten Verfahren aufzustellen. Es ist deshalb nicht zwingend erforderlich, dass zu diesem Stichtag für alle eingesetzten Verfahren in einer datenverarbeitenden Stelle bereits ein Verfahrensverzeichnis vorliegt; die Umstellung kann sukzessive erfolgen. Allerdings habe ich empfohlen, auch für ältere unveränderte Verfahren in absehbarer Zeit das Verfahrensverzeichnis aufzustellen, damit ein einheitlicher Überblick entsteht, der auch die Arbeit der behördlichen Datenschutzbeauftragten erleichtert.

Konkrete Fragen zu den Mustern für die Aufstellung des Verfahrensverzeichnisses wurden mir selten gestellt. Die Praxis musste sich zunächst mit den neuen *Formblätter*n vertraut machen. Wenn diese anhand eines konkreten Falles ausgefüllt wurden, geschah dies in den mir bekannt gewordenen Fällen in aller Regel sorgfältig und zutreffend. Die Stellen neigten eher dazu, zu viele Angaben zu machen als zu wenig. So wurde bei den unter Ziff. 5 abgefragten Übermittlungen häufig unter Herkunft der Daten „vom Betroffenen“ angegeben, obwohl dies nicht eine Übermittlung, sondern die Erhebung bezeichnet. Unter Empfänger der Daten wurden auch Organisationseinheiten innerhalb der datenverarbeitenden Stelle genannt, die personenbezogene Daten für den gleichen Zweck verarbeiten; das ist ebenfalls keine Übermittlung.

Die Angaben im Verfahrensverzeichnis sollen die Beurteilung erlauben, ob die Verarbeitung der personenbezogenen Daten mit dem vorgesehenen Verfahren zulässig ist. Aus diesem Grund sollten sich die in den Formularen abgefragten Angaben zum Kreis der Betroffenen (Ziff. 4), zu den Übermittlungen (Ziff. 5 und 10) sowie zu zugriffsberechtigten Personen oder Personengruppen (Ziff. 6) auf die lfd. Nr. der Art der Daten nach Ziff. 3 Bezug nehmen, wenn die Angaben nicht für alle Datenarten gleich sein können.

Die Formulare sind selbsterläuternd. Angesichts der Tatsache, dass mir nicht bekannt ist, wo noch Unklarheiten bestehen könnten, habe ich dem Anliegen aus der Praxis nach weiteren Erklärungen nur durch die Bereitstellung eines ausgefüllten Beispielsfalls, der als Orientierung dienen kann, nachkommen können. Dieser ist in mein Internetangebot inzwischen neben den Musterformularen eingestellt.

Für *Abrufverfahren* weise ich darauf hin, dass ein Verfahrensverzeichnis nach §§ 6 und 15 HDSG zu erstellen ist. Abrufverfahren sind gemeinsame Verfahren gemäß § 15 HDSG. Von der Stelle, die das Verfahren betreibt, sind zusätzlich die besonderen Muster für gemeinsame

Verfahren auszufüllen. Außerdem müssen mich die datenverarbeitenden Stellen vor der Einrichtung oder Änderung eines solchen Verfahrens einschalten und mir das Verzeichnis vorlegen. Dies gilt auch, wenn innerhalb einer datenverarbeitenden Stelle ein gemeinsames automatisiertes Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird (§ 15 Abs. 5 HDSG).

3.2
Vorabkontrolle

Da die Vorabkontrolle in Hessen neu eingeführt ist, waren Hilfen für die praktische Umsetzung erforderlich. Diese sind in Form einer Checkliste und weiterer Hinweise verfügbar.

Bei der mit § 7 Abs. 6 HDSG eingeführten Vorabkontrolle handelt es sich um ein neues Instrument.

§ 7 Abs. 6 HDSG

Wer für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung zuständig ist, hat vor dem Beginn der Verarbeitung zu untersuchen, ob damit Gefahren für die in § 1 Abs. 1 Nr. 1 geschützten Rechte verbunden sind; dies gilt in besonderem Maße für die in § 7 Abs. 4 genannten Daten. Das Verfahren darf nur eingesetzt werden, wenn sichergestellt ist, dass diese Gefahren nicht bestehen oder durch technische und organisatorische Maßnahmen verhindert werden können. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten zur Prüfung zuzuleiten.

Behördliche Datenschutzbeauftragte haben mich gebeten, ihnen Hilfestellung für die Durchführung einer solchen Vorabkontrolle zu geben. In Zusammenarbeit mit dem Hessischen Innenministerium und einigen behördlichen Datenschutzbeauftragten ist deshalb eine Checkliste erarbeitet worden, die auf die meisten Fälle angewendet werden kann. Schon wegen der Unterschiedlichkeit der denkbaren Verfahren, für die eine solche Vorabkontrolle durchzuführen ist, kann die Checkliste nur Anhaltspunkte und Beispiele auflisten und nicht

für alle denkbaren Varianten die relevanten Prüfungspunkte vollständig auflisten. Die datenverarbeitenden Stellen sollten deshalb bei jeder Vorabkontrolle überlegen, ob und welche Besonderheiten des Verfahrens vorliegen, auf die zusätzlich eingegangen werden muss. Die Checkliste und allgemeine Hinweise hierzu sind in Ziff. 25.1 abgedruckt. Diese geben auch Empfehlungen wie die Vorabkontrolle durchzuführen ist bei übergreifend als „Werkzeug“ für verschiedene Aufgaben ohne Anbindung an eine bestimmte Verwaltungsaufgabe eingesetzten Standardverfahren, für die kein Verfahrensverzeichnis zu erstellen ist. Werden personenbezogene Daten mit solchen Verfahren nicht in sensiblen Fachaufgaben (z.B. Sozialamt, Personalstelle) verarbeitet und handelt es sich auch nicht um die Verarbeitung der in § 7 Abs. 4 HDSG aufgezählten besonders geschützten Kategorien personenbezogener Daten, genügt für die Vorabkontrolle eine kurze summarische Prüfung und es werden nur wenige Festlegungen notwendig sein.

3.3
Einsichtsrecht des behördlichen Datenschutzbeauftragten in personenbezogene Daten

Im Rahmen der Novellierung des Hessischen Datenschutzgesetzes von 1998 wurden Stellung und Aufgaben des behördlichen Datenschutzbeauftragten neu definiert. Er hat ein Recht auf Einsicht in personenbezogene Daten, soweit keine gesetzliche Regelung entgegen steht. Verschiedene Anfragen haben zu einer mit dem Hessischen Innenministerium inhaltlich abgestimmten Stellungnahme zur Einsicht in Personalakten geführt. Zur Einsicht in Daten, die dem Arztgeheimnis unterliegen, habe ich eine weitere Stellungnahme abgegeben.

Die Hessische Landesregierung hat die aufgrund der EG-Datenschutzrichtlinie notwendige Überarbeitung des Hessischen Datenschutzgesetzes (HDSG) zum Anlass genommen, auch Anpassungen an die fortgeschrittene technologische Entwicklung vorzunehmen und Regelungslücken zu schließen. Die Neuregelung präzisiert und stärkt die Stellung des behördlichen Datenschutzbeauftragten und legt insbesondere die von ihm wahrzunehmenden Aufgaben konkret fest, weil in den vergangenen Jahren Unklarheiten über die Aufgaben und Kompetenzen des behördlichen Datenschutzbeauftragten Anlass zu Streitfragen gaben.

Ohne Kenntnisnahme personenbezogener Daten (außer auf der Grundlage einer Einwilligung der Betroffenen im Einzelfall) könnte der behördliche Datenschutzbeauftragte seine Aufgaben

nicht effektiv wahrnehmen. Er könnte keine systematischen Stichproben machen und nicht überprüfen, ob die Angaben in den Verfahrensverzeichnissen eingehalten werden, ob Löschungsfristen in der datenverarbeitenden Stelle eingehalten werden, Abschottungsgebote beachtet werden und ob Datensicherheitsmaßnahmen umgesetzt werden. Hiermit ist zwangsläufig auch eine Kenntnisnahme (nicht voraussehbarer) personenbezogener Daten verbunden. Anders liefe auch die Gesetzeskonzeption ins Leere, dass der behördliche Datenschutzbeauftragte der zentrale Ansprechpartner für den Hessischen Datenschutzbeauftragten sein soll. Er soll im notwendigen Umfang Sachverhalte vor Ort abklären.

§ 5 Abs. 2 HDSG

Der behördliche Datenschutzbeauftragte hat die Aufgabe, die datenverarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen und Hinweise zur Umsetzung zu geben. Zu seinen Aufgaben gehört es insbesondere

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Maßnahmen, die das in § 1 Satz 1 Nr. 1 geschützte Recht betreffen, hinzuwirken.
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
3. die datenverarbeitende Stelle bei der Umsetzung der nach den §§ 6, 10 und 29 erforderlichen Maßnahmen zu unterstützen,
4. das nach § 6 Abs. 1 zu erstellende Verzeichnis zu führen und für die Einsicht nach § 6 Abs. 2 bereitzuhalten,
5. das Ergebnis der Untersuchung nach § 7 Abs. 6 zu prüfen und im Zweifelsfall den Hessischen Datenschutzbeauftragten zu hören.

Soweit keine gesetzliche Regelung entgegensteht, kann er die zur Erfüllung seiner Aufgaben notwendige Einsicht in Akten und die automatisierte Datenverarbeitung nehmen. Vor einer beabsichtigten Maßnahme nach Satz 2 Nr. 1 ist rechtzeitig umfassend zu unterrichten und anzuhören. Wird er nicht rechtzeitig an einer Maßnahme beteiligt, ist die Entscheidung über die Maßnahme auszusetzen und die Beteiligung nachzuholen.

Aufgrund von Anfragen habe ich zu den Problemen Stellung genommen, ob und unter welchen Voraussetzungen der behördliche Datenschutzbeauftragte in Personaldaten und in Daten, die der ärztlichen Schweigepflicht unterliegen, Einsicht nehmen kann.

3.3.1
Einsichtsrecht des behördlichen Datenschutzbeauftragten in Personaldaten

Insbesondere vor dem Hintergrund der Novellierung des Hessischen Datenschutzgesetzes und der damit u.a. verbundenen Intention, die Rechtsstellung des behördlichen Datenschutzbeauftragten zu stärken, bin ich von mehreren Behörden angesprochen worden, ob und inwieweit der behördliche Datenschutzbeauftragte Einsicht in Personalakten nehmen kann.

Auszugehen ist von § 5 Abs. 2 Satz 3 HDSG, wonach der behördliche Datenschutzbeauftragte das Recht hat, die zur Erfüllung seiner Aufgaben notwendige Einsicht in Akten zu nehmen, soweit keine gesetzliche Regelung entgegen steht. § 107 Abs. 3 HBG ist eine solche gesetzliche Regelung, die den Zugang des behördlichen Datenschutzbeauftragten zu Personalakten ausschließt.

§ 107 Abs. 3 HBG

Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist...

Nur wenn eine Einwilligung des Betroffenen vorliegt, kann der behördliche Datenschutzbeauftragte Einsicht in die Personalakte nehmen.

Soweit die Dienststellenleitung Bedienstete besonders beauftragt, Personalangelegenheiten zu bearbeiten, kann sie dazu auch den behördlichen Datenschutzbeauftragten auswählen; dies

kann sich etwa dann anbieten, wenn dieser besonderen Sachverstand hinsichtlich der Aktenkontrolle hat.

Mein Kontrollrecht gegenüber der behördlichen Personalaktenführung ist durch die Rechtsstellung des behördlichen Datenschutzbeauftragten nicht berührt.

Den anfragenden Behörden habe ich meine Rechtsauffassung mitgeteilt.

3.3.2
Einsicht des behördlichen Datenschutzbeauftragten in personenbezogene Daten, die der ärztlichen Schweigepflicht unterliegen

Die Frage, ob die Regelung über die ärztliche Schweigepflicht gemäß § 203 Strafgesetzbuch (StGB) und der ärztlichen Berufsordnung einer Einsicht des behördlichen Datenschutzbeauftragten in Krankenunterlagen (Krankenakten, Krankenhauskommunikationssysteme) entgegensteht, betrifft allein personenbezogene medizinische Daten, die sich noch im Gewahrsam des Arztes befinden. Das gilt auch für Ärzte im Gesundheitsamt, in Kliniken und im sozialpsychiatrischen Dienst. Soweit die medizinischen Daten sich bereits bei der Staatsanwaltschaft, bei der Führerscheinbehörde oder der Leitung einer Strafvollzugsbehörde befinden, unterliegen sie nicht mehr der ärztlichen Schweigepflicht. Insoweit unterliegen sie der Überprüfung durch den internen Datenschutzbeauftragten.

Es bestehen keine grundsätzlichen Bedenken gegen die Zuständigkeit des Landesgesetzgebers, Regelungen zu verabschieden, die eine Offenbarung ärztlicher Daten an den internen Datenschutzbeauftragten vorsehen, auch wenn damit eine Befugnis zur Durchbrechung der ärztlichen Schweigepflicht eintritt. Dies muss allerdings in der Regelung klar zum Ausdruck kommen (Grundsatz der datenschutzrechtlichen Normenklarheit). Die Regelung des § 5 Abs. 2 Satz 3 HDSG verweist auf den Inhalt der bereits bestehenden gesetzlichen Regelungen zur Geheimhaltung. Eine Änderung des bestehenden Rechtszustandes kann daraus nicht abgeleitet werden. Nach der gegenwärtigen Rechtslage kann daher ein eigenständiges Einsichtsrecht des behördlichen Datenschutzbeauftragten nicht begründet werden.

Die behandelnden Ärztinnen und Ärzte sind verpflichtet, dafür zu sorgen, dass bei der Verarbeitung personenbezogener Patientendaten die datenschutzrechtlichen Vorschriften eingehalten, für ihren Bereich präzisiert und umgesetzt werden. Diese Aufgabe müssen sie nicht ausschließlich persönlich wahrnehmen. Sie können hierfür Mitarbeiterinnen und Mitarbeiter, die ihrer Weisung unterliegen, einschalten (§ 203 Abs. 3 StGB). Auch das führt nicht zur Offenbarung von Daten i.S.v. § 203 StGB. Die Mitarbeiterinnen und Mitarbeiter können als berufsmäßig tätige Gehilfen i.S.v. § 203 Abs. 3 StGB qualifiziert werden. Als berufsmäßig tätiger Gehilfe wird in Literatur und Rechtsprechung derjenige angesehen, der innerhalb des beruflichen Wirkungsbereichs eines Schweigepflichtigen eine auf dessen berufliche Tätigkeit bezogene unterstützende Tätigkeit ausübt, welche die Kenntnis fremder Geheimnisse mit sich bringt oder ohne Überwindung besonderer Hindernisse ermöglicht. Ein innerer Zusammenhang mit der beruflichen Tätigkeit des Arztes muss gegeben sein. Das wird bei Sekretärinnen, Sprechstundengehilfinnen, Bürovorstehern des Rechtsanwalts bejaht, nicht jedoch bei Reinigungspersonal oder Chauffeur. Ein innerer Zusammenhang mit der beruflichen Tätigkeit kann auch für den behördlichen Datenschutzbeauftragten bejaht werden, weil der Arzt aus dem Behandlungsvertrag auch eine ordnungsgemäße Dokumentation der Behandlung schuldet. Als Mitarbeiter oder Mitarbeiterin für diese Aufgabe kann die Ärztin und der Arzt auch den behördlichen Datenschutzbeauftragten auswählen. Hierfür spricht, dass gerade dieser Mitarbeiter bzw. diese Mitarbeiterin die notwendigen Datenschutzkenntnisse hat. Insoweit wird er allerdings nicht aus eigener gesetzlicher Befugnis, sondern als weisungsabhängiges ärztliches Hilfsorgan tätig.

Im Rahmen einer so begründeten Prüfungstätigkeit hat der behördliche Datenschutzbeauftragte ein Einsichtsrecht in personenbezogene Daten, das von dem Einsichtsrecht des Arztes abgeleitet ist. Der Datenschutzbeauftragte untersteht daher in vollem Umfang den Weisungen der Ärztin bzw. des Arztes bezüglich Anlass, Zweck und Umfang der Einsichtnahme in personenbezogene Daten. Die Aufgaben des behördlichen Datenschutzbeauftragten einschließlich der Einsichtnahme in personenbezogene Daten können selbstverständlich auch in genereller Form abgesprochen und festgelegt werden. So kann eine generelle Aufgabenübertragung an den behördlichen Datenschutzbeauftragten erfolgen, einschließlich der Verpflichtung, den Hessischen Datenschutzbeauftragten bei Anfragen mittels Sachverhaltsrecherchen zu unterstützen.

4. Europa

Schengener Durchführungsübereinkommen

Die Gemeinsame Kontrollinstanz für das Schengener Informationssystem hat im vergangenen Jahr ihre Arbeit fortgesetzt. Sie hat sich dafür eingesetzt, dass nach der Integration des Schengener Übereinkommens in die Europäische Union auch die Unabhängigkeit der Gemeinsamen Kontrollkommission gewahrt bleiben soll.

Im Berichtszeitraum nahm Hessen als Beauftragter aller Landesdatenschutzbeauftragten - vertreten durch eine Mitarbeiterin - an sechs Sitzungen der Gemeinsamen Kontrollkommission teil.

Auf einer Sitzung der Gemeinsamen Kontrollkommission in Florenz im Mai dieses Jahres wurde der Tätigkeitsbericht für den Zeitraum März 1998 bis März 1999 verabschiedet. Der Bericht kann beim Bundesbeauftragten für den Datenschutz angefordert oder im Internet unter <http://www.datenschutz-berlin.de> abgerufen werden.

4.1
Integration in die Europäische Union

Wichtigstes Thema im vergangenen Jahr war die Überführung von "Schengen" in die Europäische Union mit dem Inkrafttreten des Amsterdamer Vertrags am 1. Mai 1999. In einem Protokoll zu diesem Vertrag ist vorgesehen, dass die im Zusammenhang mit Schengen getroffenen Abkommen und die ergänzenden Beschlüsse und Erklärungen als "Schengen-Besitzstand" für die dreizehn Mitgliedsstaaten anwendbar sind.

Für Irland und Großbritannien, die bisher nicht am Schengener System teilnahmen, ist in einer weiteren Erklärung vorgesehen, dass einzelne Regelungen für sie auf Antrag Anwendung finden können. Island und Norwegen als nicht EU-Staaten bleiben mit den Schengen-Ländern durch Assoziierungsabkommen verbunden.

Nach den Vorgaben des Protokolls zum Amsterdamer Vertrag legt der Rat der Europäischen Union fest, welche Rechtsakte und Beschlüsse zum Besitzstand von Schengen gehören und auf welche Rechtsgrundlagen im Vertrag über die Europäische Union (EUV) und im Vertrag zur Gründung der Europäischen Gemeinschaft (EGV) diese zu stützen sind. Bisher hat der Rat die Vorschriften über die Gemeinsame Kontrollinstanz nur teilweise in den Schengen-Besitzstand aufgenommen. Nicht berücksichtigt wurden die von der Gemeinsamen Kontrollkommission seit 1995 erlassenen Beschlüsse und Empfehlungen. Die Kontrollinstanz hat deshalb in zahlreichen Gesprächen mit Mitgliedern der zuständigen Arbeitsgruppen des Rates und verschiedenen Schreiben auf eine Klärung dieses Problems gedrängt.

Sie hat dabei auch immer wieder darauf hingewiesen, dass die Integration in die Europäische Union nicht zu Lasten der Unabhängigkeit gehen darf, die für die Gemeinsame Kontrollinstanz notwendiger Bestandteil ist. Derzeit setzt sich die Gemeinsame Kontrollinstanz in zwei Bereichen für mehr Autonomie ein: Zum Einen fordert sie eine Festlegung, dass eine personelle Abschottung der für die Kontrollinstanz zuständigen Mitarbeiter innerhalb des Generalsekretariats des Rates erfolgt, in das das bisherige Schengen-Sekretariat eingegliedert wurde. Zum Anderen hält sie einen eigenen Haushaltsansatz für erforderlich, um ihre Kontrolltätigkeit effektiv ausführen zu können.

Die jetzige Einordnung der Gemeinsamen Kontrollinstanz könnte von befristeter Dauer sein. Es gibt erste Überlegungen in den zuständigen Arbeitsgruppen des Rats der Europäischen Union, alle Kontrollinstanzen - zunächst diejenigen von EUROPOL und Schengen - zusammenzuführen.

4.2
Erneuerung des Schengener Informationssystems (SIS)

Eine Erneuerung des SIS - insbesondere dessen technischer Infrastruktur - ist in zwei Schritten geplant. Bis Jahresende sollen mit dem sog. SIS-+ Sonderprobleme gelöst werden, die mit der Umstellung auf das Jahr 2000 eintreten. Gleichzeitig soll eine Teilnahme der nordischen Staaten Dänemark, Norwegen und Schweden ermöglicht werden.

Gravierende Änderungen sind mit dem sog. SIS-II geplant. Hier geht es um eine neue Generation der Informationsverarbeitung, die auf einen nochmals stark erweiterten Teilnehmerkreis zugeschnitten ist und grundlegende Änderungen in der Nutzbarkeit bzw. der Effizienz vorsieht. Die Gemeinsame Kontrollinstanz hat sich mit den von der Firma IBM erstellten Vorstudien für ein SIS-II befasst, verschiedene Fragen gestellt und Empfehlungen abgegeben. Wichtig erscheint vor allem, inwieweit eine Änderung des Schengener Durchführungsübereinkommens im Hinblick auf die angestrebte Effizienzsteigerung beabsichtigt ist.

4.3
Kontrolle des zentralen Schengener Informationssystems (CSIS)

Die Gemeinsame Kontrollkommission hat Ende April 1999 eine Kontrolle des CSIS in Straßburg durchgeführt. Der über die Prüfung angefertigte Bericht liegt derzeit dem französischen Innenministerium als der für das CSIS zuständigen Stelle vor. Der Abschlussbericht wird sich mit den Ausführungen des französischen Innenministeriums auseinandersetzen. Veröffentlicht werden können nur Auszüge dieses Berichts, da weite Teile als geheim eingestuft werden.

5. Polizei- und Strafverfolgungsbehörden

5.1
Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung

Mit der Novelle des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung sollen die Kontroll- und Überwachungsbefugnisse der Polizeibehörden erheblich ausgeweitet werden. Nicht alle beabsichtigten Maßnahmen sind aus Sicht des Datenschutzes verfassungsrechtlich unbedenklich.

Im Laufe des Sommers hat das Innenministerium einen Gesetzentwurf zur Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) vorbereitet.

Zu den Kernpunkten dieser Novellierung gehören aus Sicht des Datenschutzes Regelungen zur Videoüberwachung, die Einführung von verdachts- und ereignisunabhängigen Kontrollen (Schleierfahndung) sowie die Abschaffung der Benachrichtigung über die längerfristige Speicherung in automatisierten Dateien.

5.1.1
Einsatz von Videoaufzeichnungen durch Polizeibehörden

Zur Gefahrenabwehr und zur vorbeugenden Verbrechensbekämpfung sollen auf öffentlichen Plätzen Bildaufzeichnungen eingesetzt werden können. Dazu ist eine Ergänzung des § 14 HSOG vorgesehen, der auch jetzt schon für öffentliche Veranstaltungen, öffentliche Versammlungen und Aufzüge den Einsatz von Videogeräten zulässt, sofern konkrete Anhaltspunkte für drohende Straftaten bestehen.

§ 14 HSOG

(1) Die Polizeibehörden können personenbezogene Daten ... bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass bei oder im Zusammenhang mit der Veranstaltung oder Ansammlung Straftaten oder nicht geringfügige Ordnungswidrigkeiten drohen. Die

Unterlagen sind spätestens zwei Monate nach Beendigung der Veranstaltung oder Ansammlung zu vernichten, soweit sie nicht zur Verfolgung einer Straftat oder Ordnungswidrigkeit oder zur Strafvollstreckung benötigt werden. Eine Verwendung für andere Zwecke ist unzulässig. § 20 Abs. 7 bleibt unberührt.

(2) Die Polizeibehörden können personenbezogene Daten ... bei oder im Zusammenhang mit öffentlichen Versammlungen oder Aufzügen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass bei oder im Zusammenhang mit der Versammlung oder dem Aufzug Straftaten drohen. Die Unterlagen ...

Die im ersten Entwurf vorgesehene Regelung nannte dabei für den Einsatz der Bildaufzeichnungen als einzige Voraussetzung, dass dies zur Erfüllung polizeilicher Aufgaben erfolge. Eine so weite Ermächtigung halte ich für verfassungswidrig, da das informationelle Selbstbestimmungsrecht unverhältnismäßig eingeschränkt wird.

Sowohl Abs. 1 als auch Abs. 2 der derzeitigen Regelung setzen tatsächliche Anhaltspunkte für drohende Straftaten voraus. Es ist im Hinblick auf die in der Begründung des Entwurfs erwähnte Zielsetzung, dass „ die Videoüberwachung der Verhütung von Straftaten dienen“ soll, nicht ersichtlich, warum der neuen gesetzlichen Ermächtigung keine Zweckbestimmung wie in den Absätzen 1 und 2 beigefügt werden sollte. Da ein Grundrechtseingriff in die informationelle Selbstbestimmung vorliegt, muss dieser den rechtsstaatlichen Messbarkeitskriterien genügen. Der Verweis auf die polizeilichen Aufgaben wird im hessischen Polizeirecht wie auch sonst nicht für ausreichend erachtet. Vielmehr ist es wegen der Beschränkung der polizeilichen Befugnisse auf Fälle der konkreten Gefahrenabwehr rechtsstaatlicher Standard, in Befugnisnormen auf die abzuwehrende Gefahr oder auf die vorbeugende Bekämpfung von Straftaten abzustellen. Bestehen weder konkrete Gefahren, ein konkreter Gefahrenverdacht noch die begründete Erwartung von Straftaten, so ist eine Aufgabenerfüllung üblicherweise nur zulässig, wenn Sondergesetze das gestatten. Da zahlreiche Videoüberwachungen der Aufklärung eines Gefahrenverdachtes dienen dürften, sollte dieses in der Polizeirechtslehre heute anerkannte Institut ausdrücklich als Grund für eine Videoüberwachung erwähnt werden. Die Voraussetzungen für die Annahme eines Gefahrenverdachts gleichen denen der polizeilichen Gefahr. Mit der erstmaligen Erwähnung im HSOG würde daher nicht grundlegend Neues geschaffen, sondern Anerkanntes erstmals kodifiziert.

Die im ursprünglichen Text vorgeschlagene Formulierung schloss die Speicherung nach dem Wortlaut nicht ein. Der Zweck der Videoüberwachung durch die Polizei kann jedoch regelmäßig nur erfüllt werden, wenn eine zeitlich begrenzte Speicherung stattfindet. Deswegen müsste zur sinnvollen Umsetzung der Neuregelung auf § 20 Abs. 1 HSOG ausgewichen werden; dieser enthält eine zur Speicherung ermächtigende Befugnisnorm. Wegen der besonderen Persönlichkeitsgefahren, die aus der Überwachung folgen, habe ich gefordert, dass - wie in den Absätzen 1 und 2 - auch in Abs. 3 eine zeitliche Aufbewahrungshöchstdauer und eine Zweckbindung beigefügt werden. Auch die Zweckbindung erhobener und gespeicherter personenbezogener Daten gehört zu den Hauptanliegen jeglichen Datenschutzes und sollte grundsätzlich auch im Polizeirecht verwirklicht werden.

Ich habe daher für § 14 HSOG eine Neuformulierung angeregt:

„(3) Die Polizeibehörden dürfen zur Gefahrenabwehr, zur Aufklärung eines Gefahrenverdachts oder bei tatsächlichen Anhaltspunkten für die Annahme, dass Straftaten drohen, zur vorbeugenden Bekämpfung von Straftaten öffentlich zugängliche Orte mittels Bildübertragung offen beobachten. Abs. 1 Satz 2 und 3 gilt entsprechend."

Die entsprechende Anwendung von Abs. 1 Satz 2 und 3 stellt sicher, dass die dort vorhandenen Regelungen zur Zweckbindung und zur Löschungsverpflichtung auch bei Einsatz der Videoüberwachung beachtete werden müssen. Diese Anregungen wurden von der Landesregierung übernommen.

5.1.2

Verdachts- und ereignisunabhängige Kontrollen (Schleierfahndung)

Vorgesehen ist, auch in Hessen verdachts- und ereignisunabhängige Kontrollen einzuführen. Der Innenminister hat dies als eine Säule des neuen Sicherheitskonzeptes bezeichnet. Maßnahmen der Schleierfahndung sollen insbesondere dem Kampf gegen reisende Straftäter und grenzüberschreitende Kriminalität dienen. Zu diesem Zweck sollen die Befugnisse zur Identitätsfeststellung in § 18 Abs. 2 HSOG um eine 6. Ziffer ergänzt werden:

§ 18 Abs. 2 HSOG

Die Polizeibehörden können die Identität einer Person feststellen, wenn...
6. die Person in öffentlichen Einrichtungen des internationalen Verkehrs, auf Durchgangsstraßen (Bundesautobahnen, Europastraßen oder anderen Straßen von erheblicher Bedeutung für die grenzüberschreitende Kriminalität) sowie auf Bundeswasserstraßen angetroffen wird zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität.

Die anlassunabhängige Identitätsfeststellung auf allen öffentlichen Straßen „von erheblicher Bedeutung für die grenzüberschreitende Kriminalität“ erstreckt die polizeilichen Befugnisse letztlich auf jede Bundes- oder Landesstraße. Davon kann jeder deutsche Staatsbürger, EU-Bürger wie sonstige Ausländer betroffen sein. Dieser tiefe Eingriff in die Freiheit zu unüberwachter Bewegung des Bürgers verlangt hohe verfassungsrechtliche Legitimationsanforderungen. Mit der bloßen Aussage „zur vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität“ kann diesen Anforderungen nicht genügt werden.

Zu einer im Wesentlichen gleich lautenden Regelung in Mecklenburg-Vorpommern hat das Landesverfassungsgericht am 21. Oktober 1999 entschieden, dass eine Befugnis für die Polizei zur anlassunabhängigen Identitätsfeststellung auf Durchgangsstraßen zur vorbeugenden Bekämpfung jedweder grenzüberschreitenden Kriminalität verfassungswidrig ist. Der Gesetzgeber müsse auch zur vorbeugenden Bekämpfung grenzüberschreitender Kriminalität rechtsstaatlich präzisierte Eingriffsschwellen für Zwangseingriffe festlegen. Die vom Verfassungsgerichtshof entwickelten Maßstäbe stimmen mit meinem Grundrechtsverständnis voll überein.

Voll überzeugend führt das Gericht aus: „Die Sensibilität von Informationen kann nicht allein davon abhängen, ob sie intime Vorgänge betreffen, sondern es ist jeweils Klarheit über den Zweck sowie die Verwendungs- und Verknüpfungsmöglichkeiten zu gewinnen. Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Daher wäre die Sammlung auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken unzulässig.“ Dieser Anforderung genüge eine polizeirechtliche Ermächtigung nicht, wenn „jedermann schon deshalb, weil er sich auf einer

Durchgangsstraße befindet," die Pflicht auferlegt bekommt, die Identität zu offenbaren. Eine Vermengung von Befugnis- und Aufgabennorm wird ausdrücklich beanstandet, insbesondere wird ausgeführt, dass die gesetzliche Regelung nicht darauf beschränkt sei, „Straftaten von erheblicher Bedeutung" zur Voraussetzung von Maßnahmen der Schleierfahndung zu machen. Erforderlich sei ein ausreichender Zurechnungszusammenhang zwischen der Nutzung der Straße und dem Ziel der Identitätsfeststellung. Soweit für die Kontrollen auf kriminalistische Erfahrung und polizeiliche Lagebilder aufgebaut wird - eine tatsächliche Feststellung, die der Realität entsprechen dürfte -, „hätte der Gesetzgeber durch eine entsprechende Eingrenzung der Norm" Schranken ziehen müssen. Angesichts der Tiefe des Eingriffes dürfe „allerdings nur hinsichtlich gewichtiger Straftaten, wenn deren besondere Begehungsweise es rechtfertigt", eine Identitätsfeststellung im Rahmen der Schleierfahndung stattfinden. Der Verzicht auf einen Anfangsverdacht oder auf eine konkrete Gefahr lasse sich nur bei derartigen Straftaten rechtfertigen. Der „Ausnahmecharakter einer solchen Befugnis" gebiete, dass der Gesetzgeber Einschränkungen für die polizeilichen Befugnisse formuliert. Insbesondere müssten „die Zwecke, zu denen kontrolliert werden darf, hinreichend präzise und normenklar festgelegt, die Gefahrenlagen genau genug beschrieben sein". Schließlich müsse die Norm vorsehen, dass „der verfassungsrechtlich notwendige Zurechnungszusammenhang zwischen dem Einzelnen und der abzuwendenden (möglichen) Schädigung" bestehe. Auch § 1 Abs. 1a Bundesgrenzschutzgesetz (BGSG) sieht eine vergleichbare Voraussetzung vor, wenn dort „Lageerkenntnisse oder grenzpolizeiliche Erfahrung" als Grund für die Informationsbeschaffung genannt sind. Besonders wichtig erscheint mir dabei die Feststellung, dass es hinsichtlich der Lageerkenntnisse jeweils eines „objektiv nachvollziehbaren Verfahrens zur Ermittlung der Lage, in der sich die Polizei befugt sieht", bedürfe. In diesem Punkt stimmt die Entscheidung von Mecklenburg-Vorpommern mit einer vorausgehenden Entscheidung des Sächsischen Verfassungsgerichtshofes überein.

Mit dem Verfassungsgerichtshof ist überdies zu fordern, dass die geplante gesetzliche Regelung hinsichtlich der weiteren Verwertung und Speicherung auf die klassischen Begriffe des Polizeirechtes zurückgreifen sollte. Insbesondere sollte die weitere Verwendung der Speicherung an eine konkreten Gefahr in Bezug auf die identifizierte Person gebunden werden. Schließlich ist mit dem Landesverfassungsgericht zu fordern, dass „die Löschung der Daten bereichsspezifisch in der Weise zu regeln ist, dass sowohl dem öffentlichen Interesse als auch dem Recht auf informationelle Selbstbestimmung Rechnung getragen wird".

Verhindert werden muss „eine Informationssammlung zur Prophylaxe ohne jeglichen konkreten oder bestimmbaren Zweck“. Das setzt voraus, „den Personenkreis, von dem personenbezogene Daten verwendet werden dürfen, in einem gesetzlichen Tatbestand zu umschreiben.“

Soweit die Befugnis zur Schleierfahndung in Hessen eingeführt werden soll, müsste sie zumindest folgende Tatbestandsmerkmale enthalten:

1. Beschränkung auf besonderes schwer wiegende Straftaten oder Gefahren für Leib und Leben (Vorbild: § 15 Abs. 2 HSOG);
2. Erfordernis konkreter Anhaltspunkte für drohende Gefahren oder erhebliche Gefahren für Leib und Leben;
3. Verfahrensrechtlich formalisierte Festlegung diesbezüglicher Lageerkenntnisse durch die Polizeiführung;
4. Speicherung von personenbezogenen Erkenntnissen maximal einen Monat, sofern drohende Straftaten oder Gefahren von diesen Personen nicht ausgehen. Längerfristige Speicherung nur bei Personen, bei denen sich die bestehenden Anhaltspunkte verdichtet haben.

Eine entsprechende Überarbeitung des Entwurfes habe ich beim Hessischen Innenminister und den Fraktionen des Hessischen Landtags angeregt.

5.1.3
Wegfall der Benachrichtigung gemäß § 20 Abs. 9 HSOG

Der Gesetzentwurf sieht auch vor, dass die Pflicht, Betroffene über die Speicherung ihrer Daten zu informieren, zukünftig entfallen soll.

§ 20 Abs. 9 HSOG

Werden personenbezogene Daten länger als drei Jahre in automatisierten Dateien gespeichert, so ist die betroffene Person darüber zu unterrichten, sobald die Aufgabenerfüllung dadurch

nicht mehr gefährdet wird und die Anschrift der betroffenen Person ohne erheblichen Verwaltungsaufwand ermittelt werden kann.

Begründet wird die Aufhebung dieser Vorschrift mit dem Aufwand, der durch die Benachrichtigung entstehe. Die vorgesehene Streichung von § 20 Abs. 9 widerspricht datenschutzrechtlichem Standard, der nicht ohne zwingende Gründe verlassen werden sollte. Nach § 18 Abs. 1 Hessisches Datenschutzgesetz (HDSG) ist der Betroffene *unverzüglich* von der Speicherung zu unterrichten. Die Regelung des HSOG weicht von diesem datenschutzrechtlichen Standard bereits deutlich zu Lasten der Betroffenen ab. Die Reduktion auf eine Dreijahresfrist erleichtert den Gefahrenabwehr- und Polizeibehörden die sonst üblichen Mitteilungspflichten sehr. Eine weitere Einschränkung der Rechte der Betroffenen erscheint - vor allem im Vergleich mit dem allgemeinen Datenschutzrecht - nicht gerechtfertigt.

Die Vorschrift hat sich in der Vergangenheit bewährt. Nachdem die geltende Fassung des § 20 Abs. 4 als Voraussetzung für eine Speicherung nicht mehr an die Prognose gebunden ist, dass der Betroffene auch künftig Straftaten begehen wird, kommt es zu umfangreichen Speicherungen. Maßgebend ist allein der irgendwann entstandene Verdacht, eine Straftat begangen zu haben. Damit gestattet jede andere Art der Verfahrensbeendigung als ein Freispruch wegen erwiesener Unschuld die Speicherung. Ich hatte auf diese Problematik schon bei der letzten Novellierung des HSOG hingewiesen (27. Tätigkeitsbericht, Ziff. 5.2.5).

§ 20 Abs. 4 HSOG

Die Polizeibehörden können ... personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten gewonnen haben, zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten speichern, verändern oder sonst verwenden. Die Speicherung, Veränderung oder sonstige Verwendung in automatisierten Dateien ist nur zulässig, soweit es sich um Daten von Personen handelt, die verdächtig sind, eine Straftat begangen zu haben; entfällt der Verdacht, sind die Daten zu löschen

Die Dreijahresfrist des geltenden Rechts stellt eine Mindestsicherung für die betroffene Person dar, denn die Mitteilung eröffnet die subjektivrechtliche abgestützte Möglichkeit, eine Löschung der erfassten Vorwürfe oder Vermutungen zu beantragen und erforderlichenfalls

gerichtlich durchzusetzen. Die bisherige Staatspraxis hat zu etwa 1.400 Rückfragen im Jahr bei den Polizeibehörden oder bei mir geführt. Häufig lagen dem Sachverhalte zu Grunde, in denen die Staatsanwaltschaft das Verfahren eingestellt hatte. Die Bürger konnten davon ausgehen, dass sich die Angelegenheit für sie erledigt hatte. In einer großen Zahl von Fällen hat die Nachfrage der Betroffenen zur Löschung der Speicherung geführt. Diese Rechtsschutzmöglichkeit sollte nicht ohne Not aufgegeben werden.

Für die Polizeibehörden kommt der Dreijahresfrist eine Warnfunktion zu. Auch deswegen ist die Streichung durch den anfallenden Arbeitsaufwand nicht zu rechtfertigen.

Die Beratungen des Gesetzentwurfes waren zum Redaktionsschluss dieses Berichtes noch nicht abgeschlossen.

5.2
Durchführung von DNA-Analysen

Die hessische Praxis, bei DNA-Analysen zum Zwecke zukünftiger Strafverfolgung von der Einholung der richterlichen Anordnung abzusehen, wenn der Betroffene in das Verfahren eingewilligt hat, steht mit den gesetzlichen Vorgaben nicht im Einklang.

5.2.1
Keine DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

Die Anwendung der Regelungen des § 81g StPO zur Durchführung der DNA-Analyse zum Zwecke der Identitätsfeststellung für künftige Strafverfahren ist umstritten (vgl. 27. Tätigkeitsbericht, Ziff. 5.1).

§ 81g StPO

(1) Zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren dürfen dem Beschuldigten, der eine Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens,

eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung verdächtig ist, Körperzellen entnommen und zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersucht werden, wenn wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen einer der vorgenannten Straftaten zu führen sind.
...
(3) § 81a Abs. 2 und § 81f gelten entsprechend.

Streitpunkt ist, ob die nach diesen Vorschriften durchzuführenden Analysen immer nur auf Grund einer richterlichen Anordnung oder auch auf Grundlage einer Einwilligung der zu untersuchenden Person durchgeführt werden dürfen. In ihrer Stellungnahme zu meinem 27. Tätigkeitsbericht (LT-Drucks. 15/356 S. 2) hat die Landesregierung die bis dahin vertretene Auffassung aufgegeben und dargelegt, dass sie die Einwilligungslösung für zulässig erachtet. Dabei stellt die Landesregierung allerdings nur auf die Erhebung der Daten ab. So wird festgestellt, dass die §§ 81f und 81g StPO die Erhebung der Identifizierungsdaten nur insoweit unter den Vorbehalt der richterlichen Anordnung stellen, als der körperliche Eingriff ohne den Willen des Betroffenen erfolge. Dieser Auffassung kann ich auch weiterhin nicht folgen.

Nach meiner Einschätzung sieht die Strafprozessordnung Einwilligungen nur im Rahmen des § 81a Abs. 1 StPO vor. Die Einwilligung erlaubt nur die Entnahme des Untersuchungsmaterials, nicht die DNA-Analyse, die sich an eine Entnahme von körpereigenen Stoffen anschließen muss. Da auch in § 81g Abs. 3 nur auf § 81a Abs. 2, nicht auf Abs. 1 Bezug genommen wird, halte ich eine Ersetzung der Vorschriften der Strafprozessordnung durch Einwilligung für unzulässig. Eine Einwilligung in den gesamten Verfahrensablauf müsste dann auch die Prognose einschließen, dass gegen den Einwilligenden zukünftig erneut wegen einer Straftat von erheblicher Bedeutung zu ermitteln sein wird. Denn ohne eine solche Prognose sind die gesetzlichen Voraussetzungen für die Einstellung des Ergebnisses in die vom Bundeskriminalamt (BKA) zu führende DNA-Datei nicht gegeben. In aller Regel wird niemand freiwillig für sich selbst eine solche Prognose erstellen und dokumentieren.

Nach Einschätzung des Justizministers liegt ein Eingriff in das informationelle Selbstbestimmungsrecht nicht vor, wenn der Betroffene einwilligt. Ein Eingriff finde nur statt, wenn dem Betroffenen die eigene Disposition über die ihn betreffenden Daten genommen sei. Eine Entscheidung, freiwillig sich dem Verfahren des § 81f StPO zu unterziehen, sei damit möglich. Bei dieser Sicht verkürzt sich das Problem auf die Frage, ob eine wirksame Einwilligungserklärung vorliegt.

Meines Erachtens greift diese Argumentation zu kurz. Mit der Unterschrift unter ein Formular, auf dem darauf hingewiesen wird, dass zum Zwecke künftiger Strafverfolgung eine Speicherung in eine Datei beim BKA erfolgt, wird der Betroffene in aller Regel überhaupt nicht die Vorstellung verbinden, dass er damit für sich selbst die schwerwiegende Prognose abgibt, dass es Gründe geben wird, gegen ihn auch zukünftig wegen Straftaten von erheblicher Bedeutung zu ermitteln. Ein weiteres Problem stellt der Umstand dar, dass die Entscheidungsfreiheit von Strafgefangenen durch die Inhaftierung eingeschränkt sein wird.

Auch die 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung (vgl. 24.13) nochmals ihren Standpunkt bekräftigt, dass DNA-Analysen zur künftigen Strafverfolgung nur mit richterlicher Anordnung zulässig sind.

5.2.2
Handhabung der DNA-Analysen zum Zwecke der Identitätsfeststellung beim Landeskriminalamt

Im Laufe des Jahres habe ich die Handhabung der DNA-Analysen durch das LKA überprüft. Die technische Durchführung der Laboranalysen, das notwendige Codierungsverfahren und der Umgang mit dem Untersuchungsmaterial waren nicht Gegenstand der Kontrolle, da sich diese seit der Einfügung des § 81f Abs. 2 StPO und den daraufhin vom LKA erlassenen Richtlinien nicht geändert haben (vgl. 26. Tätigkeitsbericht, Ziff. 6.1). Das Labor des LKA wird als Sachverständiger tätig. Die Entscheidung, ob eine Identitätsfeststellung und ggf. eine Speicherung beim BKA erfolgen soll, hat die jeweilig ermittelnde Polizeidienststelle bzw. Staatsanwaltschaft zu treffen. Dort erfolgt auch die Zuordnung des Analyseergebnisses zu den Personalien des Betroffenen. Der Schwerpunkt lag daher auf der Behandlung der

unterschiedlichen Fallgruppen, in denen beim LKA Proben untersucht werden, und den Speicherungen in der DNA-Datei beim BKA.

Das LKA hat für dieses Verfahren eine Richtlinie erlassen. Dabei bin ich nicht beteiligt worden. Dies hatte zur Folge, dass nunmehr Nachbesserungsbedarf besteht.

In den Richtlinien werden für die Verfahrensweise nach verschiedene Fallgruppen differenziert:

- Behandlung von Spurendaten: Diese werden gespeichert, bis die Person des Spurenlegers bekannt ist bzw. der Täter ermittelt wurde, dann wird das DNA-Muster dieser Person zugeordnet.

- Die Daten der Opfer werden wie Spurendaten behandelt. Allerdings erfolgte die Speicherung nur mit deren Einwilligung.

- Werden in einem laufenden Verfahren mehrere Personen als Spurenleger verdächtigt, und willigen diese nicht in eine Analyse ein, wird für alle die richterliche Entscheidung eingeholt. Sie werden mit der positiven richterlichen Entscheidung zu Beschuldigten, da § 81a StPO an den Beschuldigtenstatus anknüpft. Wenn die Untersuchung ergibt, dass ein Beschuldigter nicht Spurenleger ist, darf eine Speicherung nicht stattfinden. Sollen seine Daten auf Grund des IdentG gleichwohl gespeichert werden, muss dafür eine neue richterliche Entscheidung eingeholt werden, die die Prognoseentscheidung trifft.

  Gegen diese Verfahrensweise habe ich Bedenken angemeldet. Die Tatsache, dass eine Person als Spurenleger nicht ausgeschlossen werden kann, reicht nicht aus, den Betroffenen als Beschuldigten einzustufen. Aus den Richtlinien ergibt sich nicht klar genug, dass bei Personen, die als Spurenleger ausgeschlossen worden sind, eine Speicherung nur erfolgen darf, wenn darüber eine erneute richterliche Entscheidung eingeholt worden ist.

Der in den Richtlinien vorgesehene Wortlaut von Einwilligungserklärungen für die Opfer von Straftaten war überarbeitungsbedürftig. Der vorgesehene Text machte den Betroffenen nicht deutlich, in was sie einwilligen. Es lagen keine Erläuterungen vor, die die Betroffenen vor

Abgabe der Erklärung hätten aufklären können. Eine Formulierung, “sobald diese für das anhängige Ermittlungsverfahren nicht mehr erforderlich sind“, wird kaum mit der Vorstellung verknüpft, dass die Speicherungsdauer 20 Jahre oder länger betragen kann. Hier ist zwischenzeitlich eine Änderung erfolgt.

5.3

Polizeiliche Datenspeicherung trotz Freispruch

Bei der Überprüfung einer polizeilichen Datenspeicherung habe ich festgestellt, dass Polizeibehörden die Mitteilung der Staatsanwaltschaft über einen Freispruch lediglich zur Akte nahmen, statt die Datenspeicherung zu löschen und die Akte zu vernichten. Mit der Behörde wurde abgesprochen, dass sie die Löschung und Vernichtung künftig durch organisatorische Maßnahmen sicherstellt. Da die Regelung des § 20 Abs. 4 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung mehrdeutig ist, wird eine generelle Richtlinie erarbeitet werden müssen.

Informiert durch eine Benachrichtigung nach § 20 Abs. 9 HSOG beantragte ein Frankfurter Bürger die Löschung der zu seiner Person im Hessischen Polizeiinformationssystem (HEPOLIS) gespeicherten Daten. Nachdem er zehn Wochen vergeblich auf einen Bescheid wartete, bat er mich um Hilfe.

Nach der Datenspeicherung im HEPOLIS hatte die Frankfurter Polizei insgesamt zwei Mal, und zwar in den Jahren 1995 und 1997 Ermittlungen gegen den Bürger vorgenommen. Das Delikt lautete in einem Falle "Verbreiten pornographischer Schriften“ (§ 184 StGB), im anderen Falle "Missbrauch von Abzeichen" (§ 132a StPO). Die Akte sollte bis zum Jahre 2005 aufbewahrt werden. Ebenso lange sollte die Datenspeicherung allen hessischen Polizeibehörden zum Abruf bereit stehen. Mein Mitarbeiter sah beim Polizeipräsidium Frankfurt die zur Person geführte Kriminalakte ein.

Wie es zu dem Vorwurf der Verbreitung pornographischer Schriften gekommen war, war der Akte nicht zu entnehmen. Zwar befanden sich in der Akte zwei Kopien von Fotos aus einem ausländischen Bildmagazin. Auf dem einen Foto war ein Brustbild eines Mannes zu sehen, auf dem zweiten Foto zwei Männer in kurzen Hosen. Ob die Bilder zum Nachweis seiner

Unschuld oder aus welchem sonstigen Grund zur Akte genommen worden waren, war nicht ersichtlich. Jedenfalls konnten sie, ebenso wie der sonstige Akteninhalt, den strafrechtlichen Vorwurf nicht belegen. Auch war nicht nachvollziehbar, weshalb die Staatsanwaltschaft die Strafsache nur gegen Zahlung einer Geldbuße einstellen wollte. Jedenfalls nahm der Betroffene das Angebot der Staatsanwaltschaft "Einstellung des Verfahrens gegen Zahlung einer Geldbuße" nicht an. Es kam zur Anklage. Das Gericht sprach ihn frei, weil es sich gar nicht um pornographische Schriften handelte.

Der Sachverhalt führte zu folgenden Datenspeicherungen: Zunächst hatte das Fachkommissariat den Sachverhalt beurteilt. Es stufte den Vorgang als einen "Fall geringer Bedeutung" ein und verfügte, ausgehend vom Verfügungsdatum, eine Aussonderungsprüffrist von drei Jahren. Abgesehen davon, dass die Polizei im vorliegenden Falle auch ganz auf eine Datenspeicherung zu präventiven Zwecken hätte verzichten und die Informationen nur zur Vorgangsdokumentation teilanonymisiert hätte aufbewahren können, war dies aus verschiedenen Gründen falsch. Zum einen verlangte die damaligen Rechtslage gemäß § 20 Abs. 4 HSOG eine sog. Negativprognose (die mittlerweile gegen mein Bestreben entfallen ist - s. 27. Tätigkeitsbericht, Ziff. 5.2.5). Für die Prognose, dass die Besorgnis der Begehung weiterer Straftaten besteht, war der Akte nichts zu entnehmen.

Zum andern ist für die Berechnung der Frist nicht das Datum der Verfügung maßgebend, sondern gemäß § 5 Abs. 1 der Verordnung über Prüffristen bei gefahrenabwehrbehördlicher und polizeilicher Datenspeicherung (Prüffristenverordnung) das die Speicherung begründende Ereignis - also der angenommene Tatzeitpunkt -. Dieser lag im konkreten Fall fünf Monate zurück. Bei großen Polizeibehörden, wie dem Polizeipräsidium Frankfurt, gibt das Fachkommissariat den Vorgang zur Datenspeicherung in das HEPOLIS an eine andere Organisationseinheit (Fallanalyse) ab. Diese Abteilung erkannte zwar den Fehler bezüglich der Fristenberechnung, machte dafür aber einen Neuen: Sie stufte den Fall nicht mehr als einen "Fall geringer Bedeutung" ein, sondern verfügte gemäß § 2 Abs. 1 der Prüffristenverordnung - jetzt ausgehend von der angenommenen Tatzeit - eine Frist von zehn Jahren.

§ 2 Abs. 1 Prüffristenverordnung

Bei Daten tatverdächtiger Personen betragen die Prüffristen:

1. bei Kindern zwei Jahre,
2. bei Jugendlichen fünf Jahre,
3. bei Personen über siebzig Jahre fünf Jahre,
4. bei anderen Personen zehn Jahre.

Bei Fällen von geringer Bedeutung verkürzt sich die Prüffrist bei Kindern auf ein Jahr, bei Jugendlichen auf zwei Jahre, im Übrigen auf drei Jahre.

Dies war gegenüber dem Ermittlungsergebnis nicht sachgerecht. Richtig war, falls überhaupt eine personenbezogene Datenspeicherung erfolgt und eine Negativprognose zu stellen gewesen wäre, eine Einstufung als "Fall geringer Bedeutung". Eine Abstimmung mit dem Fachkommissariat, welches diese Einschätzung getroffen hatte, erfolgte nicht. So kam es, dass der im Jahre 1995 entstandene Vorwurf bis zum Jahre 2005 gespeichert werden sollte und der Betroffene nach drei Jahren gemäß der ebenfalls zur Disposition stehenden Vorschrift des § 20 Abs. 9 HSOG (s. Ziff. 5.1.3) über die Datenspeicherung benachrichtigt wurde.

Doch damit nicht genug: Im Oktober 1996 hatte die Staatsanwaltschaft das Polizeipräsidium über den Freispruch informiert. Das Schreiben war der Akte kommentarlos beigeheftet. Die Datenspeicherungen waren nicht korrigiert worden. Spätestens zu diesem Zeitpunkt hätte die personenbezogene Datenspeicherung gelöscht und nur noch ein der Vorgangsdokumentation (§ 20 Abs. 8 HSOG) dienender teilanonymisierter Datensatz aufbewahrt werden dürfen. Denn mit diesem Freispruch war – nach alter wie nach neuer Rechtslage - der Tatverdacht ausgeräumt und der personenbezogenen Datenspeicherung die Rechtsgrundlage entzogen.

Auch der zweite "Fall" verlief aus Sicht des Betroffenen unglücklich: Er hatte sich eine amerikanische Polizeiuniform beschafft und sie stolz seinem Freund auf dessen Arbeitsstelle vorgeführt. Dies war nicht klug, denn der Freund war Polizeibeamter und tat Dienst auf einem Frankfurter Polizeirevier. Ein anderer Polizeibeamter, der die beiden beobachtete, zeigte ihn wegen eines Verstoßes nach § 132a StGB an.

§ 132a Abs. 1 Nr. 4 StGB

Wer unbefugt ...
inländische oder ausländische Uniformen, Amtskleidungen oder Amtsabzeichen trägt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Zwar waren sich diesmal in Bezug auf die Bedeutung des Sachverhaltes alle einig: Die Staatsanwaltschaft sah gemäß § 153 StPO von der Verfolgung ab. Das Fachkommissariat und die Fallanalyse stuften den Vorgang als "Fall geringer Bedeutung" ein. Aber: Da der Betroffene schon einmal wegen Verbreitens pornographischer Schriften aufgefallen war, lag ein Anhaltspunkt für eine Negativprognose vor. Auch lag kein förmlicher Freispruch vor. Der Verdacht war also nicht entfallen. Außerdem fiel die in Frage kommende Aussonderungsprüffrist von drei Jahren nicht ins Gewicht, denn die Tatzeit lag im Dezember 1997. Da immer die längste Frist gilt, war die Speicherdauer von drei Jahren in der im ersten Fall verfügten Frist bereits eingeschlossen. Bei aufmerksamer Durchsicht der Akte wären die Fehleinschätzungen im ersten "Fall" erkannt worden und der zweite "Fall" unter einem ganz anderen Licht erschienen.

Mitte 1999 war auf dem Löschungsantrag des Betroffenen die Beurteilung abzugeben (§ 27 Abs. 2 Nr. 2 HSOG), ob die weitere Aufbewahrung der Unterlagen zur rechtmäßigen Aufgabenerfüllung der Polizei erforderlich ist. Ich habe auf eine sofortige Löschung aller zur Person des Betroffenen gespeicherten Daten gedrängt. Die Polizei kam dem Verlangen nach. Sie verfügte die Löschung des Datensatzes und die Vernichtung der Kriminalakte. Außerdem sagte sie zu, den Betroffenen über die vollzogene Löschung zu informieren.

Über den Einzelfall hinausgehende Konsequenzen:

Das Polizeipräsidium Frankfurt hat zugesagt sicherzustellen, dass Verfahrens- und Beweislagemängel der beschriebenen Art durch interne Organisationsmaßnahmen entgegengewirkt werden kann. Im Einzelnen soll darauf geachtet werden:

- Die Fristenberechnung muss sich an der Tatzeit und nicht am Verfügungsdatum orientieren.
- Wenn die "Fallanalyse" eine andere Einschätzung zur Bedeutung einer Strafsache vornimmt als das Fachkommissariat, muss eine Abstimmung zwischen den beiden Stellen stattfinden.
- Die Mitteilung der Staatsanwaltschaft über den Ausgang eines Verfahrens darf nicht einfach zur Akte genommen, sondern muss auch inhaltlich ausgewertet werden. Ein förmlicher Freispruch, in dem festgestellt wird, dass keine Straftat vorlag, muss immer zur

Löschung führen. Auch eine Verfahrenseinstellung kann im Einzelfall zur Löschung führen.

Die tatsächliche Umsetzung dieser Zusagen werde ich beobachten. Dazu hat mir eine Frankfurter Justizbehörde eine Auswertung des Datenbestandes der Justiz zur Verfügung gestellt. Anhand der Auswertungsergebnisse, es handelt sich um eine Liste mit allen in einem bestimmten Zeitraum ergangenen Freisprüche, werde ich feststellen, ob es sich bei der Missachtung der Freispruchsmitteilung um einen Einzelfall handelte, oder ob solche Fallgestaltungen öfter vorkommen. Diese Prüfung dauert an.

Mit der Beschreibung dieses Einzelfalles soll zugleich die hohe Bedeutung der Benachrichtigung des Betroffenen betont werden. Mit der beabsichtigten Novelle zum HSOG soll § 20 Abs. 9 HSOG dennoch aufgehoben werden. Bislang wurden Löschungsanträgen von Betroffenen, die auf die jährliche Benachrichtigungsaktion des Landeskriminalamtes folgen, in beträchtlicher Zahl von der Polizei entsprochen.

5.4
Datenübermittlung der Polizei an private Dritte zu Zwecken der Sicherheit im Luftverkehr

Zum Zwecke der Abwehr von Gefahren für die Sicherheit im Luftverkehr darf die Polizei mit Einverständnis der Betroffenen einem im Luftverkehr tätigen Transportdienst mitteilen, ob sie gegen die Einstellung eines Bewerbers Bedenken erhebt oder nicht.

Mit dem Polizeipräsidium Frankfurt wurde die Frage erörtert, ob es zulässig ist, dass das Polizeipräsidium mit einer Tochtergesellschaft der Frankfurter Flughafen AG im Vorfeld der Einstellung von Mitarbeitern zusammenarbeitet und dabei bekannt gibt, ob es gegen die Einstellung eines Bewerbers Bedenken erhebt oder nicht. Bedenken sollten geäußert werden, wenn in den letzten fünf Jahren wiederholt gegen den Betroffenen wegen des Verdachts der Begehung eines Eigentums-, Vermögens- oder Urkundendeliktes oder eines Verstoßes gegen das Waffen- oder das Betäubungsmittelgesetz ermittelt wurde. Hintergrund dieser Zuverlässigkeitsüberprüfung ist der vorgesehene Einsatz der Bewerber im Bereich des internationalen Transportdienstes innerhalb des Flughafens. Das besondere Bedürfnis der

Sicherheit des Luftverkehrs begründet die Tochtergesellschaft in einem Merkblatt, welches die Bewerber ausgehändigt bekommen und in dem die Prüfung ausführlich und präzise beschrieben ist. Jeder Bewerber muss sein Einverständnis zu der Überprüfung erteilen; ansonsten kann er nicht im internationalen Transportdienst eingesetzt werden.

Aus datenschutzrechtlicher Sicht ist problematisch, dass personenbezogene Daten, die zur Erfüllung von Aufgaben der Polizei erhoben und gespeichert worden sind, nun, wenn auch nur in pauschaler Form (Bedenken/keine Bedenken), zu Zwecken eines privaten Unternehmens übermittelt werden sollen. Der Zweck der Datenübermittlung, der Schutz vor Gefahren für die Sicherheit des Luftverkehrs, ist im Luftverkehrsgesetz (§ 29d) geregelt. Die dort vorgesehene Sicherheitsüberprüfung erfasst allerdings nur den Einsatz von Personen, die Zugang zu Bereichen erhalten sollen, die förmlich als nicht allgemein zugänglich oder sicherheitsempfindlich eingestuft sind. Der Transportdienst ist auch außerhalb dieser Bereiche tätig. Aufgrund der hohen Anforderungen an die Sicherheit des Luftverkehrs habe ich gegen die vorgesehene Verfahrensweise keine Einwände erhoben. Die Datenübermittlung dient neben den Zwecken der privaten Tochtergesellschaft der Flughafen AG auch der Aufgabenerfüllung der Polizei, Gefahren für die Sicherheit im Luftverkehr abzuwehren (§ 23 Abs. 1 Nr. 1 HSOG).

§ 23 Abs. 1 Nr. 1 HSOG

Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies zur
1. Erfüllung gefahrenabwehrbehördlicher oder polizeilicher Aufgaben ... erforderlich ist.
...

Die Schwachstelle der Begründung liegt darin, dass im Zeitpunkt der Datenübermittlung keine konkrete Gefahr besteht. Es ist daher zu fordern, dass derartige Sicherheitsüberprüfungen und die dazu erforderlichen Datenübermittlungen gesetzlich geregelt werden. Die schlichte Bezugnahme auf die polizeilichen Aufgaben reicht nicht aus. Die Befugnisnorm ist schärfer zu fassen.

6. Justiz und Strafvollstreckung

Elektronische Fußfessel

Der Einsatz der elektronischen Fußfessel im Rahmen von richterlichen Weisungen gemäß § 56c Strafgesetzbuch ist grundsätzlich nicht ausgeschlossen. Solange keine bundesrechtliche Regelung verabschiedet ist, kann der Einsatz nur mit Einwilligung des Verurteilten erfolgen. Einzelheiten der im Rahmen der Überwachung vorgesehenen Verarbeitung personenbezogener Daten sind noch klärungsbedürftig.

In Frankfurt soll im Rahmen eines Modellversuches der Einsatz der elektronischen Fußfessel beim Amts- und Landgericht erprobt werden. Einbezogen werden sollen vor allem Verurteilte, für die nur auf Grund der zusätzlichen Überwachungsmöglichkeit eine Bewährungsstrafe ausgesprochen werden kann. Die elektronische Überwachung kommt in Betracht, wenn eine Strafaussetzung nur bei strenger Überwachung für angemessen erachtet wird. Unter dieser Voraussetzung soll der Verurteilte im Rahmen einer Weisung gemäß § 56c Strafgesetzbuch (StGB) zum Tragen des Senders verpflichtet werden. Zu verknüpfen ist diese Weisung mit einer detaillierten Festlegung zur Ausgestaltung des Tagesablaufes in Zusammenhang mit der Wahrnehmung einer Arbeitsstelle, einer gemeinnützigen Arbeit oder ähnlichem. Die elektronische Überwachung soll das Einhalten eines geregelten Tagesablaufs unterstützen.

§ 56c StGB

(1) Das Gericht erteilt dem Verurteilten für die Dauer der Bewährungszeit Weisungen, wenn er dieser Hilfe bedarf, um keine Straftaten mehr zu begehen. Dabei dürfen an die Lebensführung des Verurteilten keine unzumutbaren Anforderungen gestellt werden.

(2) Das Gericht kann den Verurteilten namentlich anweisen,
1. Anordnungen zu befolgen, die sich auf Aufenthalt, Ausbildung, Arbeit oder Freizeit oder auf die Ordnung seiner wirtschaftlichen Verhältnisse beziehen,
2. sich zu bestimmten Zeiten bei Gericht oder einer anderen Stelle zu melden,
3. ...

Im Rahmen des Modellversuchs sollen die Probanden auf Vorschlag der am Verfahren beteiligten Staatsanwälte, Anwälte oder Richter ausgewählt werden. Zur Vorbereitung der Entscheidung in der Hauptverhandlung soll die Gerichtshilfe beauftragt werden, die Geeignetheit der Beschuldigten für die elektronische Überwachung abzuklären. Darüber ist ein Bericht zu erstellen. Die schriftliche Erläuterung soll den Ablauf erklären, Informationen über den Umgang mit den anfallenden Daten geben und die Frage beantworten, wer aus dem Umkreis der Betroffenen von der Beteiligung an dem Projekt zu informieren ist. Diese Aufklärungsmaßnahmen sollen sicherstellen, dass später eine wirksame Einwilligung erfolgt. Einbezogen werden sollen alle Bewohner der Wohnung der Verurteilten.

Die notwendige Einverständniserklärung soll im Rahmen der Hauptverhandlung eingeholt werden, wenn am Ende der Beweisaufnahme ein entsprechendes Urteil möglich erscheint. Die Weisung, eine elektronische Fußfessel zu tragen, ergeht im Bewährungsbeschluss gemäß § 268a Strafprozessordnung (StPO). Teil des Beschlusses ist ein mit den Verurteilten abgesprochener Wochenplan, der ein Zeitschema mit den Kategorien „muss anwesend sein“, „Freizeit“ und „kann abwesend sein“ umfasst.

Vorgesehen ist, dass die gesamte technische Abwicklung in Zusammenarbeit mit der Hessischen Zentrale für Datenverarbeitung (HZD) erfolgt. Bei der HZD erfolgt die Verarbeitung der anfallenden Daten auf einem Stand-Alone-Rechner, der nur für dieses Projekt eingesetzt wird. Zumindest in der Erprobungsphase werden technische Fehler nicht ausgeschlossen. Für diese Fälle ist ein ständiger Bereitschaftsdienst der HZD geplant.

Die Überwachten werden mit einem Sender ausgestattet, der Signale an eine an das Telefon angeschlossene Data-Box gibt. Geplant ist ein Rhythmus von einer Meldung pro Minute. Die in der Box aufgelaufenen Signale werden in festzulegenden Abständen (vermutlich mehrmals die Stunde) über Telefon von einem Rechner der HZD abgefragt. Wenn das abgefragte Signal nicht mit der Vorgabe des Wochenplans (zwingende An- oder Abwesenheit) übereinstimmt, löst der Rechner eine Alarmmeldung bei der HZD aus. Die HZD benachrichtigt den Sozialarbeiter. Wenn der Sender wieder die Anwesenheit meldet, erfolgt eine erneute Benachrichtigung des Sozialarbeiters, der die Ursache für die Meldung klärt. Verstöße gegen

den Wochenplan werden an den Richter weitergemeldet. Dieser kann den Bewährungsbeschluss ändern. Auch eine Änderung des Wochenplans ist, auch kurzfristig, möglich, etwa im Falle eines Krankenhausaufenthalts eines nahen Angehörigen.

Nähere Festlegungen darüber, welche (zusätzlichen) Informationen bei welcher Stelle wie lange vorrätig sein müssen, sind noch nicht erfolgt. Langfristig sollte eine Konzeption entwickelt werden, die mit einer „passiven“ Abfragetechnik arbeitet. Die Beschränkung auf Stichproben wäre zudem zu erwägen. Dem Überwachungszweck wäre genügt, wenn erst nach einer Alarmmeldung eine volle Überwachung einsetzt. Der datenschutzrechtliche Rahmen ist inzwischen mit dem Justizministerium und mir abgesprochen worden:

- Die HZD erhält nur die Personalien, die zur Zuordnung des Senders zu einer Person und damit zur Zuordnung der zuständigen Gerichtshelfer notwendig sind. Ggf. kann dies auch eine laufende Nummer sein. Die Details hängen u.a. davon ab, wie der Bereitschaftsdienst der Sozialarbeiter organisiert ist.

- Für den Bereitschaftsdienst der Gerichtshilfe (nachts und am Wochenende) muss es ein Mindestmaß an Informationen über alle am Projekt Beteiligten geben. Dazu gehören die Wochenpläne, Angaben zur Person und ggf. zu weiteren Personen im Haushalt und Besonderheiten, wie etwa festgestellte und noch nicht beseitigte technische Störungen. Diese Informationen müssen den Bereitschaftsdienst in die Lage versetzen zu entscheiden, wie er auf eine Alarmmeldung durch die HZD reagiert: Anruf, Aufsuchen vor Ort usw. Über Details wird noch nachgedacht.

- Alarmmeldungen und die dadurch veranlassten Maßnahmen werden Teil der Bewährungsakte und mit dieser aufbewahrt.

- Für die bei der HZD auflaufenden Alarmmeldungen ist eine Vollprotokollierung vorgesehen. Diese soll in regelmäßigen Zeitabständen ausgewertet werden, aufgeschlüsselt nach überwachten Personen. Diese Aufstellung kann der jeweils für die Überwachung zuständige Richter erhalten, damit er kontrollieren kann, ob er über alle relevanten Vorfälle unterrichtet worden ist.

- Die einzelnen durch den Rechner abgefragten Signale können relativ kurzfristig überschrieben werden. Die Protokollierung der Alarmmeldungen stellt sicher, dass in allen anderen Fällen keine Abweichungen vom Wochenplan registriert worden sind. Für die konkreten Fristen soll nochmals mit der HZD gesprochen werden, dabei sind auch die technischen Möglichkeiten der Protokollierung näher zu klären.

Derzeit wird ein Gesetzentwurf des Bundesrates beraten (BR-Drucks. 14/1519), der durch eine Änderung des Strafvollzugsgesetzes den Ländern die Möglichkeit geben soll, eine vom Gericht bestimmte Freiheitsstrafe nicht mehr in der Justizvollzugsanstalt, sondern im Wege des elektronisch überwachten Hausarrestes in der Wohnung des Verurteilten zu vollstrecken. Auch diese Maßnahme, die die Bundesländer im Wege einer Rechtsverordnung umsetzen können, setzt dann die schriftliche Einwilligung des Verurteilten und sämtlicher im Haushalt lebender erwachsener Personen voraus. Diese Regelung soll auf vier Jahre befristet werden, um mit dem neuen Instrument Erfahrungen zu sammeln und dann ggf. endgültig über die Tauglichkeit eines Einsatzes im Rahmen der strafrechtlichen Sanktionen entscheiden zu können.

Dieses Vorhaben ist derzeit umstritten. Einigen Kritikern ist diese Art der Vollstreckung einer Freiheitsstrafe zu großzügig, sie verwenden etwa das Bild des Strafvollzuges auf dem Sofa mit der Bierflasche. Anderen greift die Kontrolle durch die elektronische Überwachung zu sehr in das Persönlichkeitsrecht der Beteiligten ein.

Sollte die geplante Erprobung der elektronischen Fußfessel vom Bundestag abgelehnt werden, ist nach meiner Auffassung eine Fortsetzung des Frankfurter Modellversuchs nicht möglich – auch nicht auf freiwilliger Basis mit Zustimmung der Betroffenen.

7. Rundfunk

7.1
Vierter Rundfunkänderungsstaatsvertrag

Die Regierungschefs der Länder haben am 31. August 1999 die Unterzeichnung des Vierten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge abgeschlossen (4. Rundfunkänderungsstaatsvertrag). Der Vertrag, der noch von den Länderparlamenten ratifiziert werden muss und im Wesentlichen am 1. April 2000 in Kraft treten soll (Art. 8 Abs. 2), bringt u.a. mit der Änderung des Rundfunkstaatsvertrages eine Neuregelung des Datenschutzes für den privaten und öffentlich-rechtlichen Rundfunk (Art. 1 Nr. 16 - §§ 47, 47a - 47f). Die Novellierung beruht weitgehend auf Vorschlägen der Datenschutzbeauftragten und orientiert sich größtenteils an den Datenschutzvorschriften des Mediendienste-Staatsvertrages von 1997 (GVBl. I S. 134).

7.1.1
Digitalisierung der Fernseh- und Hörfunkübertragung

Im Zuge der digitalen Übertragung von Fernseh- und Radioprogrammen lässt sich feststellen, welcher Zuschauer oder Hörer wann welche Sendung eingeschaltet hat. Anbieter von entgeltlichen Programmen können so für unterschiedliche Sendungen unterschiedliche Preise festlegen und mit ihren Kunden gezielt die Vergütung einzelner Sendungen vereinbaren. Die Anbieter von digitalem Fernsehen oder Radio könnten mit Hilfe dieser Technik aber auch das individuelle Mediennutzungsverhalten ihrer Kunden registrieren. Deshalb überrascht es nicht, dass besonders die Auswirkungen der Digitalisierung der Fernseh- und Hörfunkübertragung Auslöser für die Neuregelung des Datenschutzes im Rundfunkstaatsvertrag waren.

7.1.2
Datenvermeidung und Datensparsamkeit

Was der Mediendienste-Staatsvertrag von 1997 (GVBl. I S. 134) den Mediendiensten auferlegt hat, verlangt der Rundfunkstaatsvertrag nun auch von den Rundfunkveranstaltern:

Sie müssen bereits bei der Gestaltung und Auswahl der Übertragungstechnik Vorsorge treffen, dass bei der Nutzung keine oder zumindest so wenige personenbezogene Kundendaten wie möglich anfallen (§ 47 Abs. 5 Rundfunkstaatsvertrag). Außerdem müssen die Nutzer die Programmangebote anonym oder unter Pseudonym in Anspruch nehmen und bezahlen können (§ 47a Abs. 1 Rundfunkstaatsvertrag).

§ 47 Abs. 5 Rundfunkstaatsvertrag

Die Gestaltung und Auswahl technischer Einrichtungen für die Veranstaltung und den Empfang von Rundfunk haben sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.

§ 47a Abs. 1 Rundfunkstaatsvertrag

Der Veranstalter hat dem Nutzer die Inanspruchnahme einzelner Angebote und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

Mit dieser Strategie des Systemdatenschutzes wird der Persönlichkeitsschutz bereits in die Technikgestaltung integriert. Anbieter von digitalen Rundfunkdiensten können sich nicht einfach darauf berufen, die Technik erfordere eben eine Verarbeitung personenbezogener Daten. Die Technik selbst steht nunmehr auf dem Prüfstand. Der Rundfunkveranstalter muss das System auswählen, das ohne oder mit den wenigsten personenbezogenen Daten auskommt und das eine anonyme oder pseudonyme Nutzung erlaubt. Solche Systeme sind durchaus auf dem Markt. Vorausbezahlte Wertkarten wären eine Möglichkeit, um eine anonyme Nutzung zu gewährleisten.

7.1.3
Nutzungsprofile

Auf Datenschutz durch Technikgestaltung setzt der Staatsvertrag auch bei der Lösung des Problems der Nutzungsprofile. Nimmt ein Nutzer Rundfunkleistungen verschiedener Veranstalter in Anspruch, müssen die anfallenden personenbezogenen Daten getrennt verarbeitet werden. Sie dürfen grundsätzlich nur zu Abrechnungszwecken zusammengeführt werden (§ 47a Abs. 2 Nr. 4 Rundfunkstaatsvertrag).

Den Konflikt zwischen dem legitimen Interesse der Rundfunkveranstalter an der Auswertung der Inanspruchnahme ihrer Programmangebote und dem Interesse der Kunden an unbeobachteter Nutzung entschärft der Staatsvertrag durch einen Kompromiss: Nutzungsprofile sind nur unter Verwendung von Pseudonymen zulässig (§ 47a Abs. 4 Rundfunkstaatsvertrag). Die Verwendung von Pseudonymen führt nicht zu einer vollen Anonymisierung der Nutzungsprofile. Die Daten können individualisiert verarbeitet werden, aber bestimmten Nutzern ohne Kenntnis der Zuordnungsregeln nicht zugeordnet werden. Ein Pseudonym kann eine Kurzbezeichnung sein, die aus sich heraus die Identität der Nutzer nicht preisgibt. Eine Reidentifizierung ist im Rahmen der Auswertungsbefugnis nach § 47a Abs. 2 Nr. 4 nicht zulässig.

7.1.4
Datenschutz-Audit

Der Gedanke des Systemdatenschutzes liegt auch dem Datenschutz-Audit zugrunde, das § 47e Rundfunkstaatsvertrag vorsieht. Rundfunkveranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter auf freiwilliger Basis prüfen und bewerten lassen und das Gutachten veröffentlichen. Als Instrument der Selbstregulierung soll das Datenschutz-Audit die Rundfunkveranstalter dazu bewegen, sich Marktvorteile zu verschaffen, indem sie ein hohes Datenschutzniveau anstreben. Übernommen wurde die Idee aus dem Umweltschutz, wo das Audit vor einigen Jahren aufgrund einer EG-Richtlinie eingeführt worden ist. Die nähere Ausgestaltung des Datenschutz-Audits überlässt der Rundfunkstaatsvertrag einem noch zu schaffenden besonderen Gesetz, da sowohl die Festlegung der Anforderungen an die Prüfung und Bewertung als auch das Verfahren und die Auswahl der Gutachter grundrechtseinschränkenden Charakter haben.

7.1.5
Elektronische Einwilligung

Rundfunkveranstalter dürfen personenbezogene Nutzerdaten nur verarbeiten, wenn der Rundfunkstaatsvertrag oder eine andere Rechtsvorschrift dies zulassen oder der Betroffene eingewilligt hat. Im Unterschied zum allgemeinen Datenschutzrecht kann die Erklärung, mit welcher der Nutzer in die Verarbeitung seiner Daten einwilligt, auch elektronisch erfolgen. Elektronische Erklärungen sind allerdings mit besonderen Risiken verbunden, da ihnen sowohl eine Verkörperung, wie bei der Schriftform, als auch eine biometrische Kennzeichnung, wie bei der eigenhändigen Unterschrift, fehlen. Darauf reagiert der Staatsvertrag mit einer Reihe von Verfahrensanforderungen (§ 47 Abs. 8).

Eine wirksame elektronische Einwilligungserklärung kann nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgen. Damit soll der Nutzer vor einer übereilten Einwilligung geschützt werden. Durch die Flüchtigkeit des im Bildschirm Angezeigten und den einfachen Mausklick oder Knopfdruck, der zudem nicht zwischen wichtigem und unwichtigem Handeln unterscheidet, könnte es leicht zu unüberlegten Erklärungen kommen. Als autorisiert kann eine Einwilligung z.B. dann angesehen werden, wenn ein Übermittlungsbefehl bestätigend wiederholt wird und gleichzeitig die Einwilligungserklärung mindestens auszugsweise auf dem Bildschirm erscheint. Der Rundfunkveranstalter muss außerdem durch technische Verfahren sicherstellen, dass die Einwilligung nicht unerkennbar verändert werden kann und ihr Urheber sich eindeutig identifizieren lässt. Die Einwilligung muss mit Tag, Uhrzeit und Inhalt protokolliert werden und der Inhalt vom Nutzer jederzeit abgerufen werden können.

Die elektronische Einwilligungserklärung hat freilich einen gewichtigen Nachteil. Sie macht ein Speichern des Nutzungsverhaltens erforderlich, da die funktionsbezogene Einwilligung untrennbar mit der Information über das genutzte Angebot, den Nutzer und einem Zeitstempel verbunden ist.

7.2

Datenspeicherung bei der Gebühreneinzugszentrale
Nichteinhaltung von Löschungsfristen

Bei bestimmten Fallkonstellationen war die Gebühreneinzugszentrale auf Grund von Verfahrensmängeln nicht in der Lage, Rundfunk-Teilnehmerkonten innerhalb vorgeschriebener Fristen zu löschen. Aufgrund meiner Intervention wurden die Daten gelöscht.

Zwei Lebenspartner beendeten ihre getrennte Haushaltsführung. Beide hatten bis dahin ihre Rundfunkgeräte unter jeweils eigenem Namen gemeldet und wurden bei der Gebühreneinzugszentrale (GEZ) in Köln mit jeweils einem eigenen Teilnehmerkonto geführt. Die in einem Fall erfolgte Abmeldung des Teilnehmerkontos wurde von der GEZ schriftlich bestätigt. Später verzog das Paar nach Hessen und teilte der GEZ die neue Anschrift mit.

Gleichwohl erhielt die Betroffene Post von der GEZ. In ihr war auf das alte Teilnehmerkonto Bezug genommen. Dabei handelte es sich um eine "Information zur Datenspeicherung". Nach den Verfahrensvorschriften der GEZ zur Sperrung und Löschung von Daten hätten ihre Teilnehmerdaten gelöscht sein müssen. Danach sind die Daten abgemeldeter Rundfunkteilnehmer nach einem Jahr, beginnend mit dem Ende des Jahres, in dem die Abmeldung erfolgt ist, zu löschen. Diese Frist war deutlich überschritten.

Die GEZ führt mittlerweile mehr als 37 Millionen Teilnehmerkonten. Die Bearbeitung dieser Datenmengen zwingt zum Einsatz komplexer Hard- und Software. Löschungsprozeduren erfolgen in der Regel automatisiert und zu Zeitpunkten, die in den Programmen festgelegt sind. Voraussetzung für die Löschung ist u.a. ein ausgeglichenes Konto. Außerdem darf in der Zwischenzeit keine "Bewegung" der Daten stattgefunden haben; dazu gehört jede Veränderung (z.B. Aktualisierung).

In dem gerügten Fall führte eine sog. "Mailing-Aktion" dazu, dass der Zeitpunkt der Löschung fälschlich hinausgeschoben wurde. Sie diente der Überprüfung, ob trotz der Abmeldung wieder Rundfunkgeräte zum Empfang bereitgehalten werden. Dieser Brief wurde vom System als sog. "Datenbewegung" eingeordnet. Deswegen wurde die automatische Löschung des Teilnehmerkontos ausgesetzt. Das führte dazu, dass die neue Adresse der

Betroffenen mit dem Konto verknüpft wurde, das eigentlich hätte gelöscht werden müssen. Als ihr das mitgeteilt worden war, wurde die Angeschriebene hellhörig und schaltete mich ein.

Auf meine Anfrage hin hat mir die GEZ mitgeteilt,

a) dass der aufgetretene Verfahrensmangel kein Einzelfall ist. Diese Fallkonstellation könne eine unbekannte Anzahl weiterer Teilnehmer treffen,

b) dass eine sofortige Löschung der Teilnehmerdaten der Betroffenen nicht erfolgen könne. Hierfür stehe kein spezielles Programm zur Verfügung,

c) dass künftig eine Modifizierung des Löschverfahrens erfolgen solle. So sollen bei einer regelmäßig jährlich anstehenden Löschungsprozedur die vakanten Datensätze beseitigt werden.

Eine gezielte, individuelle Löschung des Teilnehmerdatensatzes der Betroffenen sei mit dem vorhandenen DV-Verfahren nicht zu bewerkstelligen gewesen. Als "Sofortmaßnahme" und Übergangslösung sagte die GEZ jedoch zu, das abgemeldete Teilnehmerkonto mittels eines provisorischen, manuellen Verfahrens so zu bearbeiten, dass der Datensatz nicht mehr über eine Auskunftstransaktion abgerufen oder auf andere Weise bearbeitet werden konnte. Nach Angaben der GEZ erfolgte die endgültige Löschung im November 1999.

Der Fall verdeutlicht einmal mehr die Tücken maschineller Verfahren. Die Verwaltung großer Datenvolumen kann nur noch unter Einsatz komplexer Verarbeitungsprogramme erfolgen. Die einzelnen Schritte, die bestimmte Aktionen auslösen sollen, bedürfen daher stetiger Überprüfung und Anpassung. Nur so können Missstände unterdrückt werden, an deren Auftreten bei Abfassung des Programms nicht gedacht worden ist. Die Einschaltung des Datenschutzes hat daher weit über den Einzelfall hinausreichende Bedeutung.

8. Gesundheit

8.1
Gesundheitsreform 2000

Der im Sommer 1999 vorgelegte Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung gab Anlass zu einer kritischen Stellungnahme. Ein Teil der kritisierten Regelungen wurde nicht verabschiedet. In die verabschiedeten Regelungen wurden datenschutzrechtliche Verbesserungen aufgenommen.

Die geplante Gesundheitsreform 2000 hat zu umfassenden öffentlichen Kontroversen geführt. In erster Linie ging es hierbei um die Frage der Einführung eines Globalbudgets. Weniger öffentliche Beachtung fanden die mit den Plänen verbundenen datenschutzrechtlichen Regelungsaspekte. Sie sind jedoch von zentraler Bedeutung für die Entwicklung des Patientendatenschutzes, insbesondere auch deshalb, weil etwa 90% der Bevölkerung des Bundesgebietes der gesetzlichen Krankenversicherung angehören (ca. 70 Millionen Versicherte).

8.1.1
Der Entwurf des Bundesministeriums für Gesundheit vom Juni 1999

Der Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreform 2000) - BTDrucks. 14/1245/23. Juni 1999) wurde u.a. von den Verbänden und von der Selbstverwaltung der Leistungserbringer sowie von anderen Institutionen - teilweise auch unter gegensätzlichen Aspekten - kritisiert. Gesundheitspolitische, berufliche und institutionelle Gesichtspunkte standen hier im Vordergrund. Aus datenschutzrechtlicher Sicht war insbesondere von Bedeutung, dass der Gesetzentwurf die Aufgaben und die Befugnisse zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Krankenkassen - einschl. des MDK, der neu vorgesehenen Datenannahmestellen und der neu vorgesehenen Arbeitsgemeinschaften zur Datenaufbereitung - gegenüber der derzeitigen Regelung des SGB V wesentlich erweiterte und die korrespondierenden Pflichten der Leistungserbringer umfassender formulierte. Eine weit gehende Zentralisierung der Speicherung und Auswertung personenbezogener Daten der

Patientinnen und Patienten und der (Zahn-)Ärzte war vorgesehen. Mit dieser Erweiterung der Verarbeitung personenbezogener Daten sollte erheblich stärker in das Recht der Patientinnen und Patienten auf informationelle Selbstbestimmung eingegriffen werden als mit der bisherigen Regelung im Sozialgesetzbuch (SGB) V.

Auch wenn im Grundsatz anzuerkennen ist, dass es Aufgabe des demokratisch legitimierten Gesetzgebers ist, für die bestehenden Probleme der Entwicklung der gesetzlichen Krankenkassen innerhalb des verfassungsrechtlich zulässigen Rahmens Lösungskonzepte zu entwickeln und ihm hierfür geeignet erscheinende Maßnahmen gesetzlich festzulegen, war aus datenschutzrechtlicher Sicht die Erforderlichkeit neuer Datenbestände bei neuen Behörden kritisch zu würdigen. Insbesondere war zu rügen, dass die vorgesehene erweiterte Verarbeitung einschließlich der Übermittlung personenbezogener Daten der Versicherten und der (Zahn-)Ärzte für die von ihm dargelegten Ziele tatsächlich nicht erforderlich und unverhältnismäßig sind. Der Entwurf begründete nicht, ob die Ziele des Gesetzgebers nicht mit der Verarbeitung anonymisierter oder zumindest pseudonymisierter Daten erreicht werden können bzw. durch andere, weniger weit reichend in das Recht der Betroffenen auf informationelle Selbstbestimmung eingreifende Maßnahmen erreicht werden können. Fragwürdig war, dass die in Anbetracht des Umfangs und der Sensibilität der Daten gebotenen angemessenen Datensicherheitsmaßnahmen nicht hinreichend festgelegt waren.

Unter diesen Aspekten habe ich gegenüber dem Hessischen Sozialministerium eine kritische Stellungnahme abgegeben. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich kritisch zu dem Entwurf geäußert (Ziff. 24.6). Im Einzelnen war folgendes hervorzuheben:

8.1.1.1
Erweiterung der Aufgaben und Befugnisse der Krankenkassen zur Verarbeitung personenbezogener Daten

Der in § 284 Abs. 1 SGB V E festgelegte Katalog der Aufgaben, zu deren Erfüllung die Krankenkassen Sozialdaten erheben, speichern und nutzen dürfen, sollte u.a. um die Aufgabe der Prüfung der Erbringung von Leistungen an Versicherte sowie um die Aufgabe der Beratung, Aufklärung und Information der Versicherten erweitert werden.

Mit den in Abs. 1 vorgesehenen Neuregelungen sollten die Aufgaben und Befugnisse der Krankenkassen zur Verarbeitung personenbezogener Versichertendaten wesentlich erweitert werden. Unklar war, wie die Prüfung der Erbringung von Leistungen mit der Zuständigkeit der Vertragsärzte und Krankenhäuser zur Festlegung der notwendigen Versorgung vereinbar ist und wie die neu vorgesehene Aufgabe der Beratung, Aufklärung und Information der Versicherten von den Aufgaben anderer Gesundheitsberufe und Leistungserbringer, die Versicherten zu beraten, abzugrenzen ist.

Da diese Aufgaben in § 284 Abs. 1 Nr. 4 SGB V E zusätzlich aufgenommen werden sollten, sollte damit offensichtlich eine intensivere Einwirkung auf die Patientenversorgung verbunden sein. Auch von Patientinnen und Patienten nicht initiierte, steuernde Beratungen sollten ermöglicht werden. Diesem erweiterten Einwirkungsbereich sollte die stark ausgedehnte, umfassende zusätzliche Verarbeitung personenbezogener Versichertendaten dienen. Der Entwurf ließ nicht erkennen, welche Konsequenzen damit für Patientinnen und Patienten und Ärzte verbunden sein können. Wenn vom Gesetzgeber eine lenkende, Kosten senkende Wahrnehmung von Beratungsaufgaben durch die Krankenkassen angestrebt wird, besteht die Gefahr, dass der Erfassungs- und Verarbeitungsbedarf so zunimmt, dass der individuelle Gesundheitszustand des Versicherten umfassend offen gelegt wird. Eine Präzisierung und Eingrenzung der Aufgaben und der Erhebungs- und Speicherungsbefugnisse durch den Gesetzgeber war daher zwingend erforderlich, um den „gläsernen“ Patienten im Langzeitprofil nicht entstehen zu lassen.

8.1.1.2
Neuregelung des Abrechnungsverfahrens: Errichtung kassenübergreifender Datenannahmestellen und Arbeitsgemeinschaften zur Erstellung von Datengrundlagen, Übermittlung versichertenbezogener Daten an die Krankenkassen

Gemäß § 294 Abs. 2 und 3 SGB V E sollten die Spitzenverbände der Krankenkassen verpflichtet werden, Datenannahmestellen zu bilden. Diese Datenannahmestellen sollten kassenübergreifend unverschlüsselt die personenbezogenen Patientendaten aller Leistungserbringer erhalten und sie auf ihre Richtigkeit und Rechtmäßigkeit überprüfen, ferner anhand des Versichertenverzeichnisses hinsichtlich der Leistungspflicht der

Krankenkassen. Anschließend sollten die Datenannahmestellen die Daten unverzüglich den zuständigen Krankenkassen übermitteln sowie nach partieller Verschlüsselung der versichertenbezogenen Daten an die nach § 303a Abs. 1 SGB V E von den Krankenkassen zu bildenden Arbeitsgemeinschaften. Letztere sollten die Daten zusammenführen und zur Erstellung von Datengrundlagen für die in § 303a Abs. 2 SGB V E aufgeführten Zwecke aufbereiten. Das sollte der Durchführung der im SGB V vorgesehenen Prüfungen sowie der Erfüllung von Steuerungsaufgaben der Krankenkassen und ihrer Verbände und der Unterstützung politischer Entscheidungsprozesse zur Weiterentwicklung der gesetzlichen Krankenversicherung und der Strukturen der medizinischen Versorgung und der Gesundheitsberichterstattung dienen.

Aufgrund dieser geplanten Neuregelung wären bei einigen wenigen Datenannahmestellen in großem Umfang Dateien mit kassenübergreifenden medizinischen personenbezogenen Daten über alle Versicherten entstanden. Auf datenschutzrechtlichen Druck war durchgesetzt worden, dass die Datenannahmestellen bzw. Datenverteilstellen der Krankenkassen lediglich verschlüsselte medizinische Daten von Versicherten erhalten und keinen Versichertenbezug herstellen können. Der im Entwurf vorgesehene Umfang der zentralen Verarbeitung personenbezogener Versichertendaten hätte eine entscheidende Steigerung der Datenverarbeitung im Gesundheitsbereich dargestellt. Es fehlte im Entwurf eine Begründung, warum eine konsequente Umsetzung der bisher bereits gesetzlich vorgesehenen Kontrollmechanismen, die keine vergleichbare Errichtung zentraler personenbezogener medizinischer Datenbestände bedingen, ungeeignet sein soll, die Wirtschaftlichkeit und Qualität der Leistungserbringung sicherzustellen.

Für den Fall, dass die zentrale Zusammenführung und Aufbereitung der personenbezogenen Versichertendaten vom Gesetzgeber für die Erreichung der Reformziele als unerlässlich angesehen würde, habe ich gefordert, dass die Speicherungsdauer der personenbezogenen Daten bei den Datenannahmestellen in jedem Fall zeitlich begrenzt wird. Die Daten sind jeweils nach den Datenübermittlungen an die Krankenkassen bzw. an die Arbeitsgemeinschaften umgehend zu löschen.

Gemäß § 294 Abs. 2 SGB V E sollten die Arbeitsgemeinschaften die Versichertendaten von den Datenannahmestellen "verschlüsselt" erhalten. Der Gesetzesbegründung zufolge sollte der Datenschutz durch ein Anonymisierungsverfahren gewährleistet werden, das den Zugriff auf

personenbezogene Daten ausschließt. Im Widerspruch dazu sollten versichertenbezogene Auswertungen - auf der Grundlage einer eindeutig verschlüsselten Versicherungsnummer - jedoch möglich bleiben, z.B. zur Bestimmung von Wirtschaftlichkeitsreserven im Arznei- und Heilmittelbereich nach Budgetregelung, der Vereinbarung von differenzierteren Richtgrößen, der Beratung von Vertragsärzten, der Qualitätssicherung, der Gesundheitsberichterstattung und der Prüfungsaufgaben nach § 303a Abs. 2 Nr. 1 SGB V E.

Aufgrund der bei den Arbeitsgemeinschaften vorhandenen umfangreichen detaillierten Informationen war das vorgesehene "Anonymisierungsverfahren" datenschutzrechtlich nicht durchführbar. Die vorgesehene Identifizierung einzelner Versicherter für die Zwecke des § 303a Abs. 2 1 SGB V E enthielt die Möglichkeit der vollständigen Entschlüsselung. Zusätzliche Sicherungen des Datenschutzes, wie z.B. im Statistikrecht bekannt, waren daher zu fordern, d.h. insbesondere ein explizites Reidentifizierungsverbot außerhalb der Zwecke des § 303a Abs. 2 Nr. 1 SGB V E sowie eine Protokollierung der vorgenommenen Auswertungen. Ferner habe ich gefordert, dass eine strikte Trennung der verschlüsselten und der reidentifizierbaren Versichertendaten rechtlich zwingend vorgeschrieben und technisch sichergestellt wird.

Gemäß § 295 Abs. 2 SGB V E sollten die Krankenkassen künftig die Diagnosen aus der ambulanten (zahn-)ärztlichen Behandlung nicht mehr wie bisher lediglich fallbezogen, sondern versichertenbezogen erhalten. Dies war eine wesentliche Abänderung des bisherigen Datenschutzkonzepts. Konsequenz wäre gewesen, dass bei den Krankenkassen erstmals umfassende und nach Krankheitsbildern aufgegliederte personenbezogene medizinische Patientendatenbestände aufgebaut werden. Aufgrund der gesetzlichen Verpflichtung der Leistungserbringer, die Diagnose nach dem ICD-10 zu codieren, wären die medizinischen Information über die einzelnen Patientinnen und Patienten - z.B. auch im Bereich der Psychologie - sehr detailliert gewesen. Die Krankenkassen hätten langfristige Gesundheitsprofile über jeden Versicherten gespeichert. Die in der Begründung angeführten Gründe - Unterrichtung der Versicherten über in Anspruch genommene Leistungen nach § 305 Abs. 1 SGB V E, Kontrolle der Einhaltung der zweijährigen Gewährleistung der Zahnärzte nach § 136b Abs. 2 SGB V E und die Unterstützung der Versicherten bei Behandlungsfehlern nach § 66 SGB V E - rechtfertigen diese umfassende Ausweitung der Übermittlung personenbezogener Versichertendaten an die Krankenkassen nicht.

Meine Forderung war, dass die Krankenkassen zunächst sämtliche Versichertendaten verschlüsselt erhalten und lediglich berechtigt sind, im Einzelfall - soweit konkrete Aufgaben i.S.v. § 284 SGB V E das gebieten - Versichertendaten für die genannten Zwecke in einem nachprüfbaren Verfahren zu entschlüsseln.

8.1.1.3

Hausärztliche Versorgung und integrierte Versorgungsformen:
Neuer Umfang von Datenerhebungen und -übermittlungen, Freiwilligkeit der Einwilligung der Patientinnen und Patienten

Gemäß § 73 Abs. 1b SGB V E sollte ein Hausarzt berechtigt sein, mit Einwilligung des Versicherten bei Leistungserbringern, die einen seiner Patientinnen oder Patienten behandeln, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zweck der Dokumentation und der weiteren Behandlung erheben. Die Leistungserbringer sollten verpflichtet werden, den Versicherten nach dem ihn behandelnden Hausarzt zu fragen und diesem mit Einwilligung des Versicherten Behandlungsdaten und Befunde zu übermitteln; die behandelnden Leistungserbringer sollten ferner berechtigt sein, mit Einwilligung des Versicherten die für die Behandlung erforderlichen Behandlungsdaten und Befunde bei dem Hausarzt und anderen Leistungserbringern zu erheben.

Mit der vorgesehenen Neuregelung sollten die Dokumentationsbefugnisse des Hausarztes erheblich erweitert und umfangreiche Datenübermittlungen personenbezogener Daten über den Versicherten eingeführt werden. Aus datenschutzrechtlicher Sicht war von zentraler Bedeutung, dass diese Datenübermittlungen ausschließlich mit Einwilligung des Versicherten erfolgen sollten. Dies entspricht auch den gegenwärtigen Regelungen des § 203 StGB und der ärztlichen Berufsordnung, den Landeskrankenhausgesetzen etc. Entscheidend war allerdings die weder im Gesetzestext noch in der Begründung beantwortete Frage, zu welchem Zeitpunkt auf welche Weise die Einwilligung des Versicherten eingeholt werden soll. Würde dem Versicherten lediglich zugestanden, einmal zu Beginn der Behandlung pauschal für alle künftigen Behandlungsfälle und für alle in Betracht kommenden Datenempfänger seine Einwilligung zu erteilen - etwa im „Kleingedruckten“ des Aufnahmeantrages in Krankenhäusern oder bei erstmaliger Begründung des Patientenverhältnisses - so würde dies den allgemein anerkannten und datenschutzrechtlich normierten Anforderungen an

Einwilligungserklärungen diametral widersprechen. Das mit einer Einwilligungsmöglichkeit generell verbundene Gestaltungs- und Entscheidungsrecht der Betroffenen wäre weitgehend in Frage gestellt. Die Betroffenen müssten einwilligen, ohne dass klar ist, welchen Inhalt und Umfang die damit initiierten Datenflüsse haben und sie hätten keine Übersicht darüber, wer wann welche Daten über sie verarbeitet und könnten eine differenzierte Verbreitung ihrer Daten nicht vorsehen. Dies ist keineswegs nur, aber in besonderem Maße problematisch im Hinblick auf Daten über psychotherapeutische Behandlungen. Zu befürchten ist darüber hinaus auch, dass Leistungserbringer bei fehlender Erteilung der Einwilligung die Behandlung des Betroffenen ablehnen und damit die scheinbar gewährleisteten Rechte der Versicherten vollständig leer laufen.

Ich habe daher gefordert, dass die Einwilligung der Betroffenen sich in diesem Bereich wie in anderen Bereichen an dem konkreten Behandlungsfall orientiert, sodass der Betroffene entsprechend allgemein anerkannten Rechtsgrundsätzen erst dann seine Einwilligung erteilt, wenn klar ist, in welchem Umfang auf welche Weise eine Verarbeitung seiner personenbezogenen Daten vorgesehen ist. Das kann die Patientin oder der Patient erst nach Abschluss des jeweiligen Behandlungsabschnitts und nur für diesen sinnvoll beantworten.

Gemäß § 170a Abs. 2 SGB V E war vorgesehen, dass die Teilnahme der Versicherten an den integrierten Versorgungsformen freiwillig ist. So weit die in § 170b und 170d vorgesehenen Verträge zu integrierten Versorgungsformen die Erhebung, Verarbeitung und Nutzung personenbezogener Daten vorsehen oder zulassen, sollten sie verpflichtet sein, hierzu die schriftliche Einwilligung der betroffenen Versicherten einzuholen.

Unklar blieb in dem Gesetzestext und auch in der Begründung, worauf genau sich die Einwilligung des Versicherten beziehen sollte. So weit sich die Einwilligung auf grundsätzliche Aspekte der Arbeitsweise der Vertragspartner bezieht, war die Regelung angemessen. Aus datenschutzrechtlicher Sicht war es jedoch keinesfalls angemessen, dass der Versicherte auf diese Weise ohne jede Differenzierungsmöglichkeit und ohne jede Transparenz einmal pauschal für sämtliche späteren Behandlungsanlässe in alle notwendig gehaltenen Übermittlungen personenbezogener medizinischer Informationen einwilligen soll.

Gemäß § 140b Abs. 24 Satz 3 SGB V E sollten die Vertragspartner verpflichtet werden, die Zusammenarbeit der Netzbeteiligten sicherzustellen einschließlich einer ausreichenden

Dokumentation, die allen an der integrierten Versorgung Beteiligten im jeweils erforderlichen Umfang zugänglich sein muss. Gegen eine Verlagerung der Entscheidung über den Umfang der Verarbeitung personenbezogener Daten der Patientinnen und Patienten auf die Vertragspartner habe ich aus verfassungsrechtlichen Gründen Bedenken geäußert. Der Gesetzgeber muss den Rahmen der Datenverarbeitung selbst festlegen; möglich wäre allenfalls eine konkret zeitlich begrenzte Experimentierklausel.

Den Patientinnen und Patienten muss die Möglichkeit eröffnet werden, die Diagnose- und Behandlungsdaten nur insoweit für andere Leistungserbringer verfügbar zu machen, wie es ihnen sachgerecht erscheint. Sie dürfen nicht zum Objekt eines Netzwerks gemacht werden, sondern müssen die Entscheidung über die Offenbarung ihres Gesundheitszustandes und den individuellen Behandlungsbedarf behalten.

8.1.2
Das Gesetzgebungsverfahren

Der Deutsche Bundestag hat in seiner Sitzung am 4. November 1999 in zweiter und dritter Lesung den Entwurf der durch die BTDrucks. 14/1245 und 14/1977 geänderten Fassung verabschiedet, in der eine Reihe der von den Datenschutzbeauftragten unterbreiteten Vorschlägen für datenschutzrechtliche Verbesserungen aufgenommen wurden. Zwar wurde die Einrichtung von Datenannahmestellen beibehalten. Alle Leistungserbringer sollten den Datenannahmestellen ihre Abrechnungsdaten versichertenbezogen übermitteln. Festgelegt wurde aber, dass die Datenannahmestellen die versichertenbezogenen Daten vor der Weiterleitung an die Krankenkassen pseudonymisieren müssen. Eine Reidentifikation der betroffenen Versicherten darf nur durch eine von der Datenannahmestelle räumlich und organisatorisch getrennte Stelle und ausschließlich in den vom Gesetz bestimmten Fällen erfolgen. In dieses Verfahren der Pseudonymisierung sollten auch diejenigen Leistungserbringer einbezogen werden, die den Krankenkassen bisher personenbezogene Daten übermitteln mussten (z.B. Krankenhäuser). Das Konzept wurde in Abstimmung zwischen dem Bundesministerium für Gesundheit, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und den Datenschutzbeauftragten entwickelt und konkretisiert (s. auch die 2. Entschließung der Datenschutzbeauftragten zur Pseudonymisierung der Versichertendaten, abgedruckt unter Ziff. 24.12). Die Aufgabe der Krankenkassen, die

Versicherten zu beraten, wurde im Gesetz konkretisiert und auf besondere Einzelfälle beschränkt. Für die Berater wurde eine persönliche Schweigepflicht vorgesehen. Die Rechte der Patientinnen und Patienten im Rahmen der integrierten Versorgung wurden gestärkt.

Der Bundesrat hat am 26. November 1999 den Gesetzesbeschluss des Bundestags zur Gesundheitsreform 2000 abgelehnt. Auch im Vermittlungsausschuss konnte keine Einigung erzielt werden (vgl. BRDrucks. 732/99). Das Gesetz wurde daher u.a. ohne die (zustimmungspflichtigen) Regelungen über den Aufbau der Datenannahmestellen und die neu zu bildenden Arbeitsgemeinschaften und ohne erweiterte Beratungsaufgaben der Krankenkassen verabschiedet. In den (nicht zustimmungspflichtigen) Vorschriften zur hausärztlichen Versorgung (§ 73) und zur integrierten Versorgung (§ 140a) wurde entsprechend meinen Forderungen und den Forderungen der Konferenz der Datenschutzbeauftragten das Erfordernis der Einwilligung der Patientinnen und Patienten in Datenübermittlungen eindeutig und differenziert geregelt (BGBl. I 1999 S. 2626).

8.2
Einsatz von Chipkarten im Gesundheitsbereich

Gegenwärtig wird über eine evtl. Einführung einer neuen Krankenversichertenkarte, die über die gegenwärtig vorhandene Ausweisfunktion hinaus weitere Funktionen erfüllen könnte, öffentlich diskutiert. Wenn eine solche Karte eingeführt wird, bedarf es einer gesetzlichen Regelung, die die datenschutzrechtlichen Aspekte hinreichend berücksichtigt.

Im Rahmen der Novellierung des Bundesdatenschutzgesetzes ist eine Novellierung der datenschutzrechtlichen Regelungen im Sozialgesetzbuch (SGB) X vorgesehen. Neu aufgenommen werden soll eine Regelung zu „mobilen personenbezogenen Speicher- und Verarbeitungsmedien“. Sie soll insbesondere sicherstellen, dass bei der Verarbeitung personenbezogener Daten auf diesen Medien Transparenz für die Betroffenen gewährleistet ist (s. Ziff: 2.2.). Dazu rechnen auch Chipkarten. Konkrete Regelungen zu der Frage, ob und ggf. in welchen Bereichen und mit welchen Inhalten Chipkarten im Gesundheits- und Sozialbereich eingesetzt werden sollen, sind noch nicht getroffen worden.

Bisher wurde im Gesundheitsbereich in der gesetzlichen Krankenversicherung die Krankenversichertenkarte als Krankenscheinersatz in Chipkartenform eingeführt. Die Regelung des § 291 SGB V legt zum Schutz des Versicherten fest, dass diese Karte keine medizinischen Daten enthalten darf. Sie darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen sowie für die Abrechnung mit den Leistungsträgern verwendet werden. In der Bundesrepublik Deutschland sind seit 1993 von verschiedenen Organisationen mit unterschiedlichen Zielsetzungen darüber hinausgehende Möglichkeiten des Einsatzes von maschinenlesbaren Patientenkarten diskutiert, in begrenzten lokalen Einsatzbereichen sogar erprobt worden. Diese Chipkarten enthalten auch medizinische Daten, z.B. Notfallkarten, Karten für besondere Patientengruppen, wie etwa Dialysepatienten und Krebskranke, Röntgenkarten, Apothekenkarten sowie allgemeine Patientenkarten mit wesentlichen Angaben zur Krankengeschichte. Da für diesen Einsatz keine rechtlichen Regelungen vorliegen, kann eine Verwendung derartiger Patientenkarten derzeit nur auf der Grundlage einer freiwilligen Einwilligung der Patientin und des Patienten verantwortet werden. Die Datenschutzbeauftragten des Bundes und der Länder haben schon in ihrer Entschließung vom 9./10. November 1995 die datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen und die mit dem Einsatz von Patientenkarten verbundenen Probleme aufgezeigt (s. 25. Tätigkeitsbericht, Ziff. 5.3; 24. Tätigkeitsbericht, Ziff. 4.1 und Ziff. 20.15; 26. Tätigkeitsbericht, Ziff. 7.2).

Vor dem Hintergrund der internationalen Diskussionen über die Verbesserung der Kommunikationsbedingungen und die Notwendigkeit weiterer Rationalisierung innerhalb des Gesundheitsbereichs wird z.Z. verstärkt eine Weiterentwicklung der gesetzlichen Krankenversichertenkarte auf der Grundlage einer Änderung des § 291 SGB V diskutiert. Wann eine erweiterte Krankenversichertenkarte eingeführt wird, ist gegenwärtig nicht absehbar. Auf einige zentrale datenschutzrechtlichen Aspekte einer evtl. Speicherung medizinischer Informationen auf der Krankenversichertenkarte ist jedoch bereits jetzt hinzuweisen. Eine derartige Datenspeicherung hätte erhebliche Auswirkungen auf die Kommunikationsstrukturen im Gesundheitsbereich. Datenschutzrechtlich ist zwingend, dass die Rechte der Betroffenen auf jeden Fall in angemessener Weise gewährleistet werden müssen.

Bei den aktuellen Diskussionen über medizinische Informationen auf der Krankenversichertenkarte geht es nicht ausschließlich um Notfalldaten, sondern um einen

Kerndatensatz. Dieser sollte aus medizinischer Sicht bei jeder (Erst-)Behandlung einer Patientin und eines Patienten dem behandelnden Arzt vorliegen, um eine adäquate Behandlung sicherzustellen und Behandlungsfehler bzw. Behandlungskomplikationen zu vermeiden. Es geht insbesondere um Angaben über Blutgruppe und Rhesusfaktor, Allergien, chronische Krankheiten, bösartige Neubildungen, chirurgische Eingriffe, kontinuierliche Behandlungen sowie Impfungen. Diskutiert wird ein europaweit abgestimmter Kerndatensatz (Interoperability-Data-Set) sowie evtl. weitere Behandlungs- und Arzneimitteldaten. Die Speicherung von medizinischen Informationen wird auch unabhängig von dem Einsatz von Chipkarten in anderen Bereichen diskutiert, z.B. im Zusammenhang mit der Vernetzung von Arztpraxen.

Die medizinischen Gründe für die Vorlage eines Kerndatensatzes bei jeder (Erst-)Behandlung einer Patientin und eines Patienten sind grundsätzlich nachvollziehbar. Allerdings ist zu bedenken, dass keineswegs bei jeder Behandlung sämtliche medizinischen Informationen eines Kerndatensatzes zur Durchführung der Behandlung erforderlich sein werden. Dies gilt umso mehr, je mehr Krankheiten und Behandlungen erfasst und je größer der auf der Karte gespeicherte medizinische Datensatz ist. Die bisher bei jeder Behandlung bestehende Entscheidungsfreiheit der Patientin und des Patienten, welchem Arzt sie oder er für welche Zwecke welche persönlichen Informationen offenbart, muss auch weiterhin gegeben sein. Deswegen bedarf es einer Sicherstellung der Entscheidungsrechte der Patienten. Dies ist in verschiedener Weise denkbar. Der Abruf medizinischer Informationen auf der Krankenversichertenkarte sollte - wie die Speicherung - in jedem Fall auf freiwilliger Basis erfolgen. Die Einwilligung der Patientin und des Patienten ist schriftlich einzuholen. Zuvor muss über den Zweck der Speicherung, den Inhalt des Datensatzes, das Zugriffsverfahren, die Zugangsberechtigungen sowie Datensicherheitsmaßnahmen in angemessener Weise aufgeklärt werden. Die Entscheidungsrechte der Patienten dürfen nicht auf die Frage beschränkt bleiben, ob medizinische Informationen auf der Krankenversichertenkarte gespeichert werden sollen. Den Patienten muss eine differenzierte und sektorale Steuerung der Verbreitung ihrer medizinischen Informationen zugestanden werden. Die technische Ausgestaltung der Karte muss dies sicherstellen. Anders kann den Anforderungen der Beschlüsse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den Chipkarten im Gesundheitswesen nicht genügt werden (s. 24. Tätigkeitsbericht, Ziff. 20.15).

Eine differenzierte Zugriffssteuerung durch die Patientin und den Patienten könnte dadurch sichergestellt werden, dass eine (partielle oder volle) Freigabe der medizinischen Daten auf der Krankenversichertenkarte im Einzelfall durch die Patientin und den Patienten gesichert werden. Die Identifikation könnte mittels PIN oder biometrischem Verfahren erfolgen. Auf keinen Fall darf es durch den Einsatz einer medizinischen Patientenkarte dazu kommen, dass Patienten überall im Gesundheitswesen pauschal ihre medizinischen Daten offenbaren müssen.

Vor der Speicherung medizinischer Informationen auf der Krankenversichertenkarte muss in jedem Fall geklärt sein, wie die Verantwortlichkeit der jeweils einspeichernden Ärztin und des jeweils einspeichernden Arztes für die Richtigkeit der Daten sichergestellt wird. Es muss zu Beweiszwecken nachvollziehbar sein, wer wann welche Daten oder Datenänderungen auf der Karte abgespeichert hat (Protokollierung). Dies ist für Patienten wie für behandelnde Ärzte von zentraler Bedeutung. Ferner wären insbesondere der konkrete Verfahrensablauf bei Zugriffen und weitere Fragen der Datensicherheit klärungsbedürftig.

Solange kein überzeugendes Konzept zur Sicherstellung der Entscheidungsrechte der Patienten entwickelt worden ist, muss die Speicherung medizinischer Informationen auf der Krankenversichertenkarte abgelehnt werden. Speicherungen auf einer zweiten zusätzlichen Karte dürfen nur mit vorausgehender Einwilligung der Versicherten stattfinden.

8.3
Verarbeitung personenbezogener Daten im Auftrag hessischer Krankenhäuser

Eine stichprobenhafte Überprüfung ergab, dass die Krankenhäuser die rechtlichen Vorgaben des Hessischen Datenschutzgesetzes für die Auftragsdatenverarbeitung nur unzureichend beachten.

Ausgehend von der Berichterstattung in den Medien, dass immer mehr Krankenhäuser dazu übergehen, eigene Aufgaben an Dritte, auch an Private, zu übertragen und hiermit oftmals die Weitergabe personenbezogener Daten an Dritte verbunden ist, habe ich, beginnend Anfang Juni 1999, mir bei zwölf hessischen Krankenhäusern einen Einblick über den derzeitigen Stand der Datenverarbeitung im Auftrag verschafft. Zunächst habe ich von den Kliniken

Informationen über die von ihnen vergebenen Aufträge angefordert. Zusätzlich habe ich einige Kliniken besucht und Informationsgespräche geführt.

8.3.1
Rechtliche Vorgaben für die Auftragsdatenverarbeitung

Maßstab für meine Überprüfungen waren die rechtlichen Vorgaben des § 4 Hessisches Datenschutzgesetz (HDSG). Nach dieser Vorschrift dürfen personenbezogene Daten unter bestimmten Voraussetzungen durch öffentliche oder private externe Stellen im Auftrag verarbeitet werden. Da § 12 Abs. 1 des Hessischen Krankenhausgesetzes (HKHG) ausdrücklich auf die Anwendung des HDSG - als auch auf § 4 - verweist, gilt diese Vorschrift auch für die hessischen Krankenhäuser. Bei einer Vergabe eines Auftrages sind von den Krankenhäusern insbesondere die folgenden rechtlichen Vorgaben des § 4 zu beachten und schriftlich festzuhalten:

- Der Auftraggeber bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Er erteilt dem Auftragnehmer die Weisungen, der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten.

- Gegenstand und Umfang der Datenverarbeitung, die vom Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen (§ 10 HDSG) sowie der Ausschluss bzw. die evtl. Zulässigkeit der Vergabe von Unterauftragsverhältnissen sind im Einzelnen vom Auftraggeber festzulegen. Gemäß § 10 HDSG sind technische und organisatorische Maßnahmen erforderlich, soweit der damit verbundene Aufwand unter Berücksichtigung der Art der personenbezogenen Daten und ihrer Verarbeitung zum Schutz des Rechts auf informationelle Selbstbestimmung angemessen ist. Der Auftraggeber hat daher bei der Festlegung der zu treffenden technischen und organisatorischen Maßnahmen insbesondere zu berücksichtigen, ob der Auftrag die Verarbeitung von Daten umfasst, die besonderen Amts- oder Berufsgeheimnissen unterliegen und die als besonders sensible Daten i.S.v. § 7 Abs. 4 HDSG einzustufen sind.

- Einsichts- und Kontrollrechte des Auftraggebers sowie sein Recht zur fristlosen Kündigung bei Nichteinhaltung der datenschutzrechtlichen Vorgaben durch den Auftraggeber sollten schriftlich festgelegt werden.

- Sofern die Vorschriften des Hessischen Datenschutzgesetzes auf den Auftragnehmer keine Anwendung finden, muss sich der Auftragnehmer vertraglich verpflichten, die Vorschriften des Hessischen Datenschutzgesetzes einzuhalten und sich der Kontrolle des Hessischen Datenschutzbeauftragten zu unterwerfen. Der Auftraggeber hat den Hessischen Datenschutzbeauftragten vorher über die Beauftragung zu unterrichten.

- Für die Vergabe von Aufträgen an nicht-öffentliche Stellen werden in § 4 Abs. 3 Satz 4 HDSG weitere rechtliche Vorgaben festgelegt. An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen oder Berufs- oder besondere Arztgeheimnisse noch überwiegende schutzwürdige Belange entgegen stehen. Da § 12 HKHG ausdrücklich auf die Vorschriften des Hessischen Datenschutzgesetzes verweist, steht die ärztliche Schweigepflicht einer Weitergabe der Patientendaten an einen Auftragnehmer nicht entgegen, insoweit liegt eine spezialgesetzliche Rechtsgrundlage für die Offenbarung der Patientendaten an einen Auftragnehmer vor. Vom Krankenhaus muss aber in jedem Fall an Hand der Umstände des Einzelfalls geprüft werden, ob der Vergabe des Auftrags schutzwürdige Belange des Patienten entgegen stehen, z.B. weil zu viele oder zu viele personenbezogene sensible Daten Dritten zur Kenntnis gelangen, das Risiko einer Kenntnisnahme der Daten durch Unbefugte zu groß ist etc..

8.3.2
Prüfungsergebnisse

Die Ergebnisse meiner Überprüfung waren unter datenschutzrechtlichen Gesichtspunkten leider ganz überwiegend nicht zufriedenstellend.

In den von mir überprüften Krankenhäusern wurden insbesondere die folgenden Aufgaben an private Dritte übertragen:

- Archivierung von Krankenakten
- Schreibarbeiten (Arztbriefe, OP-Berichte)
- Mikroverfilmung von Krankenunterlagen
- Bewirtschaftung der Küche
- Sicherheitsdienst (z.B. Besetzung der Pforte)
- Vernichtung von Datenträgern
- DV-Wartung (einschließlich Fernwartung).

Die Verträge wurden überwiegend schriftlich vereinbart, teilweise aber auch ausschließlich mündlich. In den mir zur Verfügung gestellten Unterlagen (Vereinbarungen, Vertragsauszüge, Aufträge, Erklärungen), sind Regelungen zum Datenschutz und zur Datensicherheit nur in Einzelfällen enthalten. Ganz überwiegend sind die Regelungen rudimentär oder fehlen völlig. Es war auch vielfach nicht nachvollziehbar, durch wen und auf welche Weise vom Krankenhaus vor der Auftragsvergabe geprüft wurde, ob die Datensicherheit beim Auftraggeber gewährleistet ist.

8.3.3
Mustervertrag für die Auftragsdatenverarbeitung

Aus Anlass der von mir festgestellten Probleme bei der Vergabe von Aufträgen durch die Krankenhäuser ist von mir ein Mustervertrag für die Vergabe von Aufträgen zwischen öffentlichen Stellen und öffentlichen oder nicht-öffentlichen Auftragnehmern erarbeitet worden. Er ist in diesem Tätigkeitsbericht unter Ziff. 25.2 abgedruckt und kann auch unter www.datenschutz.hessen.de abgerufen werden. Da sehr verschiedene Aufgaben durch öffentliche Stellen an Auftragnehmer übertragen werden, ist der Inhalt des Vertrags im Einzelfall aufgabenspezifisch anzupassen. Diesen Mustervertrag habe ich auch den von mir geprüften Krankenhäusern zur Verfügung gestellt und werde sie bei der Anpassung ihrer Verträge beraten.

8.4
Videoüberwachung in einem hessischen Krankenhaus

Eine verdeckte Videoüberwachung des Personals eines Krankenhauses ist nicht zulässig.

Aus dem Mitarbeiterkreis eines Krankenhauses erhielt ich die telefonische Mitteilung, dass im Wirtschaftsbereich des Krankenhauses über einen längeren Zeitraum verdeckte Video-Kameras zur Beobachtung des Personals installiert waren. Die Ortsbesichtigung ergab, dass die Rechte von Patienten sowie deren Besuchern in keiner Weise tangiert waren. Die versteckte Videoüberwachung wurde lediglich in einigen Fluren des Wirtschaftstraktes durchgeführt, zu denen Patienten und deren Besucher keinen Zugang haben. Die Krankenhausleitung war im Gespräch sehr kooperativ, beharrte aber darauf, dass die zeitlich begrenzte verdeckte Videoüberwachung notwendig sei. Sie war der Auffassung, dass ein geordneter Krankenhausbetrieb gefährdet sei, da Diebstähle von Krankenhausmaterialien sowie Sachbeschädigungen in ganz erheblichem Umfang über einen längeren Zeitraum stattfanden. Die entstandenen Schäden wurden als im sechsstelligen Bereich liegend beziffert. Die Menge der gestohlenen Krankenhausmaterialien haben zudem zu dem Verdacht geführt, dass an den Diebstählen mehrere Beschäftigte des Krankenhauses beteiligt gewesen seien.

Seit Mitte 1998 wurden seitens des Krankenhauses wegen der Diebstähle und der Sachbeschädigungen mehrere Anzeigen bei der Polizei erstattet. Die polizeilichen Ermittlungen seien ohne Ergebnis geblieben. Als letzte Möglichkeit zur Eindämmung bzw. Aufklärung insbesondere der Diebstähle wurde die Möglichkeit einer verdeckten Videoüberwachung ergriffen - und zwar auf Anregung eines Polizeibeamten. Auch der Arbeits-Sicherheits-Ausschuss des Krankenhauses habe die Videoüberwachung empfohlen. Die Installation der Anlage sei weitgehend unbemerkt geblieben. Insgesamt wurden über einen Zeitraum von knapp zwei Monaten eine Kamera sowie über einen Zeitraum von knapp einem Monat fünf Kameras installiert.

Die hier durchgeführte Maßnahme war nach den Bestimmungen des § 12 Abs. 1 Hessisches Datenschutzgesetz (HDSG) nicht zulässig, da sie verdeckt durchgeführt wurde und für die Betroffenen daher keine Möglichkeit zur Kenntnisnahme der Videoüberwachung bestand.

§ 12 Abs. 1 HDSG

Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. Werden Daten nicht über eine bestimmte Person, sondern über einen bestimmbaren

Personenkreis, etwa durch Videoüberwachung, erhoben, dann genügt es, wenn er die seinen schutzwürdigen Belangen angemessene Möglichkeit zur Kenntnisnahme hat.

Darüber hinaus wurde auch die Personalvertretung nicht in dem für eine derartige Maßnahme erforderlichen Umfang informiert und um Zustimmung gebeten. Die Krankenhausleitung hat es auch versäumt, mit dem internen Datenschutzbeauftragten des Krankenhauses die beabsichtigte Maßnahme der verdeckten Videoüberwachung zu besprechen. Die Modalitäten für eine Videoüberwachung hätten auch mit meiner Dienststelle im Vorfeld abgeklärt werden können.

Inzwischen haben weitere Gespräche im Krankenhaus unter meiner Beteiligung stattgefunden. Der Beratungsdienst der Kriminalpolizei wurde eingeschaltet. Eine Schwachstellen- und Sicherheitsanalyse wird für das gesamte Krankenhaus durchgeführt. Ich habe auf Bitte des Krankenhauses zugesagt, dass ich nach Abschluss der Analyse das Krankenhaus hinsichtlich der datenschutzrechtlichen Zulässigkeit der in Betracht kommenden Maßnahmen beraten werde.

8.5
Videoüberwachung in einem gentechnischen Institut

Zur Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für das Leben kann eine Videoüberwachung zulässig sein.

In einem gentechnischen Institut waren mehrere Brandanschläge und die Beimischung gesundheitsgefährdender Substanzen in ein Getränk eines dort tätigen Professors zu verzeichnen. Die Ermittlungen der Polizei führten zu keinem greifbaren Ergebnis. Da im Nachhinein nicht festgestellt werden konnte, wer die Räumlichkeiten betreten hatte und auch zukünftig solche Vorkommnisse nicht auszuschließen waren, wurde ich gebeten zu prüfen, ob die Installation einer Videoüberwachungsanlage für den Zugangsbereich dieses Instituts datenschutzrechtlich zulässig ist. Technische Maßnahmen, die den Zutritt von unbefugten Personen verhindern, waren aufgrund notwendiger Baumaßnahmen und der nicht vorhandenen Haushaltsmittel nicht umzusetzen, zumal das Institut in den nächsten zwei Jahren in ein neues Gebäude umziehen soll.

Die Prüfung der Angelegenheit hat ergeben, dass in diesem Fall die Installation einer Videoüberwachungsanlage nach § 12 Abs. 3 Hessisches Datenschutzgesetz (HDSG) nicht zu beanstanden gewesen ist, weil die abzuwehrende Gefahr für Leib und Leben Beschränkungen des Rechts auf informationelle Selbstbestimmung rechtfertigt.

§ 12 Abs. 3 HDSG

Beim Betroffenen und bei Dritten außerhalb des öffentlichen Bereichs dürfen Daten ohne seine Kenntnis nur erhoben werden, wenn der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies im Einzelfall gebietet oder eine Rechtsvorschrift dies vorsieht oder, soweit es sich um eine Rechtsvorschrift des Bundes handelt, zwingend voraussetzt.

Da auch Daten von Bediensteten, die befugt das Gebäude betreten, aufgezeichnet werden, wurde mit dem Personalrat eine Vereinbarung getroffen, in der festgelegt wurde, wer wann und zu welchem Zweck auf diese Daten zugreifen darf. Eine Auswertung zum Zweck der Personaldatenverarbeitung wurde ausgeschlossen. Zugriffsberechtigt sind nur die Staatsanwaltschaften oder die Polizeibehörden bei Vorkommnissen, die eine präventiv oder repressiv angelegte Überprüfung notwendig machen. In Absprache mit der Dienststelle wurde festgelegt, dass mit einem Hinweisschild an der Eingangstür auf die Videoüberwachung aufmerksam gemacht wird. Seit der Videoüberwachung haben die Anschläge im Institut aufgehört.

9. Internet

9.1

Internet-Nutzung in Hochschulen:
- Auskunftsansprüche der Nutzer
- Löschungsfristen für Nutzungsdaten

Hochschulen, die ihrem Personal und den Studierenden einen Internet-Zugang zur Verfügung stellen, speichern personenbezogene Daten über die Nutzung des Zugangs. Soweit diese Daten ausschließlich zum Zwecke der Datensicherung oder Datenschutzkontrolle gespeichert werden, haben die Betroffenen keinen Auskunftsanspruch. Die Hochschulen dürfen die Daten nicht länger als drei bis sechs Monate aufbewahren. Dies ist das Ergebnis eines Gutachtens, welches ich auf Wunsch des Arbeitskreises der Datenschutzbeauftragten der hessischen Hochschulen erstellt habe.

9.1.1
Auskunftsansprüche

Sowohl § 7 des Teledienstedatenschutzgesetzes (TDDSG) als auch § 18 Abs. 3 des Hessischen Datenschutzgesetzes (HDSG) gewähren Betroffenen ein Recht auf Auskunft über die zu ihrer Person gespeicherten Daten. § 18 Abs. 4 HDSG schließt allerdings einen Auskunftsanspruch aus, wenn es sich um personenbezogene Daten handelt, die ausschließlich zum Zwecke der Datensicherung oder der Datenschutzkontrolle gespeichert worden sind. Diese landesrechtliche Einschränkung gilt auch für den bundesrechtlichen Auskunftsanspruch nach § 7 TDDSG.

§ 7 TDDSG

Der Nutzer ist berechtigt, jederzeit die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten unentgeltlich beim Diensteanbieter einzusehen. Die Auskunft ist auf Verlangen des Nutzers auch elektronisch zu erteilen. Das Auskunftsrecht ist im Falle einer

kurzfristigen Speicherung i.S.d. § 33 Abs. 2 Nr. 5 des Bundesdatenschutzgesetzes nicht nach § 34 Abs. 4 des Bundesdatenschutzgesetzes ausgeschlossen.

§ 18 Abs. 3 HDSG

Datenverarbeitende Stellen, die personenbezogene Daten automatisiert speichern, haben dem Betroffenen gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie
3. die Herkunft der Daten und die Empfänger übermittelter Daten, soweit dies gespeichert ist...

§ 18 Abs. 4 HDSG

Abs. 1 und Abs. 3 gelten nicht ...für solche Daten, die ausschließlich zum Zwecke der Datensicherung oder Datenschutzkontrolle gespeichert werden.

9.1.1.1

Hochschulen als Anbieter von Telediensten

Auf welcher Rechtsgrundlage die Nutzer des von den Hochschulen zur Verfügung gestellten Internet-Zugangs Auskunft über die zu ihrer Person gespeicherten Daten verlangen können, hängt davon ab, ob die Hochschulen gegenüber ihrem nicht-wissenschaftlichen und wissenschaftlichen Personal sowie im Verhältnis zu den Studierenden als Teledienstanbieter auftreten. Nur wenn das der Fall ist, gilt das Teledienstedatenschutzgesetz, nur dann kommt ein Auskunftsanspruch nach § 7 TDDSG in Betracht und nur dann stellt sich das Problem des Verhältnisses von § 7 TDDSG zu § 18 HDSG.

Das Teledienstegesetz (TDG) zählt Angebote zur Nutzung des Internets zu den Telediensten (§ 2 Abs. 3 Nr. 3). Die Hochschulen bieten ihren Mitgliedern die Möglichkeit, das Internet zu

nutzen. Sie stellen ihnen einen Zugang zu sämtlichen Internet-Diensten (www, e-mail, usenet, telnet, ftp usw.) zur Verfügung. Das macht die Hochschulen jedoch nicht zwangsläufig zum Anbieter eines Teledienstes. Die Anwendbarkeit des Teledienstedatenschutzgesetzes hängt vielmehr davon ab, ob die Hochschule den Netzzugang nur für dienstliche und hochschulrechtliche Zwecke zur Verfügung stellt oder auch private Nutzung erlaubt.

§ 2 Nr. 1 TDDSG definiert Diensteanbieter als natürliche oder juristische Personen oder Personenvereinigungen, die Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln. Nutzer ist gemäß § 2 Nr. 2 TDDSG eine Person, die Teledienste nachfragt. Unerheblich ist, ob die Nutzung ganz oder teilweise unentgeltlich oder gegen Entgelt möglich ist. Zwischen Hochschule und Mitgliedern müsste also ein Anbieter-Nutzer-Verhältnis bestehen. Da niemand sich selbst etwas anbieten kann, müssen folglich Anbieter und Nutzer verschiedene Personen oder Stellen sein. Die nicht-wissenschaftlichen Bediensteten, das wissenschaftliche Personal und die Studierenden sind jedoch Mitglieder oder Beschäftigte der öffentlich-rechtlichen Körperschaft Hochschule. Als solche haben sie einen hochschulrechtlichen Anspruch, alle Einrichtungen der Hochschule im Rahmen der Benutzungsordnung zu nutzen (§ 8 Abs. 1 Satz 2 HHG). Ermöglicht die Hochschule einen Internet-Zugang, haben alle ihre Mitglieder grundsätzlich ein Nutzungsrecht. Steht den Mitgliedern der Hochschule der Internet-Zugang nur zur dienstlichen und/oder hochschulrechtlich festgelegten Aufgabenerfüllung in Forschung, Lehre und Verwaltung zur Verfügung und ist die private Nutzung ausdrücklich ausgeschlossen, erfolgt die Nutzung nicht durch von der Hochschule verschiedene Personen, sondern durch Mitglieder der Institution im Rahmen der gesetzlich festgelegten Aufgaben der Hochschule. Es handelt sich daher nicht um ein Anbieter-Nutzer-Verhältnis. Für die Datenverarbeitung sind demnach nicht die Regelungen des Teledienstedatenschutzgesetzes, sondern das allgemeine Datenschutzrecht und die für die Hochschulen geltenden datenschutzrechtlichen Sondervorschriften maßgeblich.

Ein Blick auf die Pflichten, die das Teledienstedatenschutzgesetz den Teledienstеanbietern auferlegt, lässt ebenfalls erkennen, dass die Hochschule gegenüber ihren Mitgliedern und Angehörigen nicht als Diensteanbieter auftritt, soweit die Nutzung des Internets ausschließlich für Zwecke der Hochschulverwaltung und der Forschung und Lehre ermöglicht wird. § 4 Abs. 1 TDDSG verlangt von den Diensteanbietern, dass sie den Nutzern die Möglichkeit bieten, den Teledienst anonym oder pseudonym in Anspruch zu nehmen. Das

wäre für die Hochschule jedoch unzumutbar. Es gibt keinen Grund, hier anders zu verfahren als bei der Erfassung von Telefondaten. So wie die Hochschule nicht verpflichtet ist, den Bediensteten und Studenten die anonyme Nutzung des Telefons zu ermöglichen, so wenig hat sie eine Verpflichtung, einen anonymen Zugang zum Internet zur Verfügung zu stellen. Sie kommt für die Betriebskosten auf und muss daher zumindest in der Lage sein, die Kosten einzelnen Nutzerkonten zuzuordnen.

Erlaubt die Hochschule den Beschäftigten und Studierenden auch die private Nutzung des Internet-Zugangs, so wird sie insoweit zum Anbieter eines Teledienstes.

Ist eine technische Unterscheidung zwischen der privaten Nutzung einerseits und der Nutzung für Zwecke der Hochschulverwaltung sowie Zwecke der Forschung und Lehre andererseits nicht möglich, muss für die gesamte Nutzung das Teledienstedatenschutzgesetzes gelten.

9.1.1.2
Protokollierung der Internet-Nutzung

Die Nutzung des Internets für dienstliche Zwecke oder für Zwecke der Lehre und Forschung darf im Rahmen des § 34 HDSG (Personal) bzw. § 69 Abs. 4 HHG und der Verordnung über die Verarbeitung personenbezogener Daten und über das Verfahren der Immatrikulation an den Hochschulen des Landes Hessen vom 23.01.1995 (Studierende) sowie des § 10 Abs. 1 und 2 HDSG (Datenverarbeitung zum Zwecke der Datensicherung und Datenschutzkontrolle) und zur Sicherstellung des ordnungsgemäßen Betriebs des Internet-Zugangs (§ 11 Abs. 1 HDSG) protokolliert werden. Der Umfang der Protokollierung kann je nach betroffener Personengruppe unterschiedlich sein. Eine Vollprotokollierung aller Einzelzugriffe im www ist jedoch unverhältnismäßig. Bei der Auswertung der Protokolldaten ist außerdem die in §§ 13 Abs. 5 und 34 Abs. 6 HDSG vorgeschriebene strikte Zweckbindung zu beachten.

§ 13 Abs. 5 HDSG

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer

Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

§ 34 Abs. 6 HDSG

Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

Die private Nutzung des Internets darf die Hochschule protokollieren, soweit dies für die Inanspruchnahme des Teledienstes oder für Abrechnungszwecke erforderlich ist (§ 6 Abs. 1 TDDSG). Darüber hinausgehende Protokollierungen sind nur mit Einwilligung der Betroffenen zulässig (§ 3 Abs. 1 TDDSG). Weder Nutzungs- noch Abrechnungsdaten dürfen längere Zeit gespeichert werden. Nutzungsdaten, d.h. personenbezogene Daten, die dem Nutzer die Nachfrage nach Telediensten ermöglichen, also Daten, die während der Nutzung eines Teledienstes, z.B. bei der Interaktion eines Nutzers mit dem Diensteanbieter, entstehen, müssen spätestens unmittelbar nach Ende der jeweiligen Nutzung gelöscht werden, soweit es sich nicht um Abrechnungsdaten handelt. Abrechnungsdaten, das sind Daten, die für die Abrechnung eines Dienstes erforderlich sind, müssen gelöscht werden, sobald sie für Abrechnungszwecke nicht mehr benötigt werden (§ 6 Abs. 2 TDDSG). Ausgenommen von der sofortigen Löschung sind außerdem Nutzungsdaten, die zum Zwecke der Datensicherung und Datenschutzkontrolle gespeichert worden sind (vgl. dazu unten Ziff. 9.1.2).

9.1.1.3
Auskunft gemäß § 18 HDSG

Ist die private Nutzung des Internet-Zugangs ausgeschlossen, gilt das Teledienstedatenschutzgesetz nicht. Der Anspruch der Betroffenen auf Auskunft über ihre im Zusammenhang mit der Nutzung des Internet-Zugangs gespeicherten personenbezogenen Daten richtet sich daher allein nach den Bestimmungen des Hessischen Datenschutzgesetzes (§ 18 Abs. 3). Daten, die ausschließlich zum Zwecke der Datensicherung oder Datenschutzkontrolle gespeichert worden sind, unterliegen gemäß § 18 Abs. 4 HDSG keinem

Auskunftsanspruch. Wegen der strikten Zweckbindung, die für diese Daten gemäß § 13 Abs. 5 HDSG gilt, besteht nach Ansicht des Gesetzgebers kein anerkennenswertes Informationsinteresse der Betroffenen. Außerdem würde eine Bekanntgabe der Daten möglicherweise den mit der Speicherung verbundenen Sicherheitszweck gefährden. Die Hochschule muss in diesem Fall den Bediensteten und Studierenden Protokollierungen nicht mitteilen. Dagegen unterliegen personenbezogene Daten, die zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen, dem Auskunftsanspruch gemäß § 18 Abs. 3 HDSG.

9.1.1.4
Auskunft gemäß § 7 TDDSG

Anders ist die Rechtslage, wenn die Hochschule die private Nutzung des Internet-Zugangs erlaubt. Da die Hochschule, soweit sie den Internet-Zugang zur privaten Nutzung zur Verfügung stellt, als Diensteanbieter auftritt, ist das Teledienstedatenschutzgesetz anwendbar. Dieses sieht in § 7 ein Auskunftsrecht der Nutzer vor. Das Auskunftsrecht ist nicht auf Bestandsdaten i.S.v. § 5 TDDSG beschränkt, sondern erstreckt sich auch auf Nutzungs- und Abrechnungsdaten gemäß § 6 Abs. 1 TDDSG. Die Nutzer sind demnach berechtigt, jederzeit die zu ihrer Person gespeicherten Daten bei der Hochschule einzusehen. Das gilt ebenso, wenn eine technische Unterscheidung zwischen privater Nutzung und Nutzung zu dienstlichen Zwecken bzw. Zwecken der Forschung und Lehre nicht möglich ist. Bei dieser Mischnutzung erstreckt sich der Auskunftsanspruch nach § 7 TDDSG auch auf die im Zusammenhang mit der dienstlichen Nutzung sowie der Nutzung für Forschungs- und Lehrzwecke erfolgte Datenspeicherung.

Die Frage des Verhältnisses des Auskunftsanspruchs nach § 7 TDDSG zu den in § 18 Abs. 4 HDSG enthaltenen Einschränkung des Auskunftsanspruchs stellt sich somit nur, wenn die Hochschule die private Nutzung des Internet-Zugangs erlaubt.

9.1.1.5
Verhältnis von § 7 TDDSG zu § 18 Abs. 4 HDSG

§ 1 Abs. 2 TDDSG stellt klar, dass für Teledienste subsidiär die allgemeinen Datenschutzvorschriften gelten. Die Auskunftsregelung in § 7 TDDSG ist nicht abschließend, sondern ergänzt und erweitert die im Bundesdatenschutzgesetz (§§ 19 und 34) oder den Landesdatenschutzgesetzen (§ 18 HDSG) normierten allgemeinen Auskunftsansprüche. Anders als nach dem Bundesdatenschutzgesetz oder den Landesdatenschutzgesetzen sind danach auch Daten mitzuteilen, die zu einem Pseudonym des Nutzers gespeichert sind. Die Auskunft muss auf Verlangen elektronisch erfolgen und der Auskunftsanspruch erfasst auch Daten, die nur kurzfristig gespeichert werden. Würde allein § 7 Teledienstedatenschutzgesetz gelten, wäre der Auskunftsanspruch gegenüber einem Teledienstеanbieter im Vergleich zu Auskunftsansprüchen gegenüber sonstigen datenverarbeitenden Stellen jedoch verkürzt, denn im Unterschied zu den allgemeinen Datenschutzgesetzen bestimmt das Teledienstedatenschutzgesetz z.B. nicht, dass über die Herkunft der Daten und die Empfänger regelmäßiger Übermittlungen Auskunft gegeben werden muss. Die Begründung zum Gesetzentwurf weist ausdrücklich darauf hin, dass die Auskunftsvorschriften des Bundesdatenschutzgesetzes weiterhin anwendbar bleiben (BT-Drucks. 13/7385 vom 9. April 1997, S. 25, zu § 7). Für die nicht erwähnten Auskunftsbestimmungen der Landesdatenschutzgesetze kann sinnvollerweise nichts anderes gelten.

Das bedeutet freilich andererseits, dass die Beschränkungen, die in den allgemeinen Datenschutzgesetzen für Auskunftsansprüche enthalten sind, auch für Ansprüche gegenüber Teledienstеanbietern gelten, soweit das Teledienstedatenschutzgesetz keine abweichenden Regelungen trifft. Von den in § 34 Abs. 4 i.V.m. § 33 Abs. 2 BDSG enthaltenen Einschränkungen schließt § 7 Satz 3 TDDSG nur § 33 Abs. 2 Nr. 5 aus, d.h. Teledienstеanbieter können nicht wie andere datenverarbeitende Stellen die Auskunft mit dem Hinweis verweigern, es handle sich lediglich um kurzfristig gespeicherte Daten. § 33 Abs. 2 Nr. 2 BDSG, wonach Daten, die ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen, keinem Auskunftsanspruch unterliegen, bleibt folglich anwendbar. Das Teledienstedatenschutzgesetz erwähnt zwar nur Ansprüche gegenüber nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen. Es ist aber kein Grund ersichtlich, weshalb die für die Ansprüche gegenüber öffentlichen Stellen des Bundes gleichlautenden Einschränkungen des § 19 Abs. 2 BDSG nicht gelten sollten. Gleiches gilt für die in den Landesdatenschutzgesetzen enthaltenen entsprechenden Einschränkungen der Auskunftsansprüche. Soweit hessische öffentlich-rechtliche Stellen Teledienste anbieten, gelten daher die Einschränkungen des § 18 Abs. 4 HDSG. Die Nutzer der Dienste haben

folglich keinen Auskunftsanspruch über Daten, die ausschließlich zum Zwecke der Datensicherung oder Datenschutzkontrolle gespeichert werden.

Dagegen unterliegen Nutzungsdaten, die nicht für Zwecke der Datensicherung oder Datenschutzkontrolle gespeichert werden, sowie Abrechnungsdaten dem Auskunftsanspruch nach § 7 TDDSG.

Fazit: Auch soweit die Hochschule die private Nutzung des Teledienstes ermöglicht, muss sie den Nutzern keine Auskunft geben über personenbezogene Daten, die ausschließlich zum Zwecke der Datensicherung oder Datenschutzkontrolle gespeichert werden.

9.1.2
Löschungsfristen

Erfolgt die Nutzung des Internets für Zwecke der Hochschulverwaltung sowie der Forschung und Lehre, ist für die Löschung der in diesem Zusammenhang gespeicherten personenbezogenen Daten § 19 Abs. 3 HDSG maßgeblich. Die Daten sind grundsätzlich unverzüglich zu löschen, sobald feststeht, dass sie für den ursprünglichen Speicherungszweck bzw. die zulässige Weiterverarbeitung nicht mehr erforderlich sind. Für Protokollierungen zum Zwecke der Datensicherung und Datenschutzkontrolle ist eine Aufbewahrungsdauer von drei bis maximal sechs Monaten ausreichend. Danach müssen die Daten gelöscht werden.

Wird die private Nutzung des Internet-Zugangs zugelassen, ist die Hochschule insoweit Diensteanbieter, sodass für die Löschung der Nutzungsdaten § 6 Abs. 2 Nr. 1 TDDSG gilt. Die Löschungsvorschrift des Teledienstedatenschutzgesetzes ist außerdem für Datenspeicherung im Zusammenhang mit der Nutzung des Internet-Zugangs zum Zwecke der Hochschulverwaltung, Forschung und Lehre anzuwenden, wenn eine technische Unterscheidung zur privaten Nutzung nicht möglich ist. Gemäß § 6 Abs. 2 Nr. 1 TDDSG muss der Diensteanbieter Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung löschen, soweit es sich nicht um Abrechnungsdaten handelt, für die Abs. 2 Nr. 2 eine längere Speicherungsdauer erlaubt. Das Teledienstedatenschutzgesetz enthält nur für Nutzungsdaten, die Abrechnungszwecken dienen, eine Sonderregelung, indem es eine längere Aufbewahrung der Daten gestattet. Nutzungsdaten, die für Zwecke der

Datensicherung und der Datenschutzkontrolle gespeichert werden, erwähnt das Gesetz nicht. Dem Wortlaut des § 6 Abs. 2 TDDSG zufolge müssten diese Nutzungsdaten daher unmittelbar nach Ende der jeweiligen Nutzung gelöscht werden. Das würde eine Datensicherung und Datenschutzkontrolle jedoch unmöglich machen, denn beide setzen voraus, dass die Daten für eine gewisse Zeit nach der Nutzung aufbewahrt werden. Da das Teledienstedatenschutzgesetz zweifellos keine Schwächung der Datenschutzkontrolle bei Telediensten anstrebt und § 1 Abs. 2 TDDSG ausdrücklich die subsidiäre Geltung der allgemeinen Datenschutzgesetze anerkennt, ist deshalb davon auszugehen, dass Nutzungsdaten nicht nur für Abrechnungszwecke, sondern auch für Zwecke der Datensicherung und der Datenschutzkontrolle für die o.g. Dauer aufbewahrt werden dürfen.

9.2
Präsentation von Kommunen im Internet

Auch Stadtverordnete, Vereinsvorsitzende oder Gewerbetreibende haben einen Anspruch auf Privatheit. Die Veröffentlichung ihrer Privatanschrift und privaten Telefonnummer ist nur mit ihrer ausdrücklichen Einwilligung zulässig. Darauf habe ich zahlreiche Kommunen im vergangenen Jahr hingewiesen, die die Veröffentlichung derartiger Daten im Internet planten.

Kommunen geben, um über ihre verschiedenen Service-Leistungen, Veranstaltungen etc. zu informieren, häufig Broschüren heraus. Inzwischen nutzen die Kommunen zusätzlich oder als Ersatz häufig das Internet als Informationsplattform. Solange diese Informationen rein sachbezogen sind, z.B. Kulturangebote, Müllkalender, Öffnungszeiten verschiedener kommunaler Einrichtungen etc., bleiben sie datenschutzrechtlich völlig unproblematisch. Auch die Einstellung von Daten, die aus öffentlich zugänglichen Quellen entnommen worden sind, ist datenschutzrechtlich nicht zu beanstanden (§ 3 Abs. 4 HDSG).

Im Grundsatz gilt das Gleiche für die Namen der Stadtverordneten. Solange sich deren Veröffentlichung lediglich auf die Funktion der Stadtverordneten - auch mit entsprechender Parteizugehörigkeit - bezieht, ist das zulässig. Dieser Personenkreis nimmt ein öffentliches Amt wahr und kann sich als Hoheitsträger nicht auf den grundrechtlichen Datenschutz berufen. Insoweit kann der Schutz der Privatsphäre und der privaten Handlungsfreiheit nicht

eingefordert werden. Bei Amtsträgern tritt die Person hinter der Funktionsausübung zurück. Soweit die Veröffentlichung sich auch auf die Privatanschrift und die private Telefonnummer erstreckt, ist das nur mit ausdrücklicher Einwilligung der Betroffenen zulässig. Diese Daten haben mit der Amtsträgerfunktion nichts zu tun, sondern sind der Privatsphäre zuzurechnen.

Gleiches gilt für die Veröffentlichung der Privatanschriften von Vereinsvorsitzenden. Auch hier ist jeweils die Einwilligung der Betroffenen einzuholen. Diese rechtlichen Schranken gelten sowohl für die Veröffentlichung in einer kommunalen Broschüre als auch für die Veröffentlichung im Internet.

In zwei Fällen wurde ich gefragt, ob die Präsentation von Daten der örtlichen Gewerbetreibenden im Internet zulässig sei. Geplant war die Angabe der Grunddaten aus der Gewerbeanzeige (Name, betriebliche Anschrift, angemeldetes Gewerbe). § 14 Abs. 8 Gewerbeordnung (GewO), der die Übermittlung von Daten aus der Gewerbeanzeige an nicht-öffentliche Stellen regelt, macht die Herausgabe auch dieser Grunddaten vom Vorliegen eines berechtigten Interesses des Empfängers abhängig. Werden die Daten im WorldWideWeb zur Verfügung gestellt, kann dieses berechtigte Interesse der einzelnen weltweiten Nutzer nicht geprüft werden. Deswegen ist auch hier vor der Einstellung der Daten ins Netz die Einwilligung der Gewerbetreibenden einzuholen.

9.3
Antragstellung bei Kommunen via Internet

Wenn Kommunen auf ihrer Homepage Formulare für ihre Bürgerinnen und Bürger zur Verfügung stellen, die diese ausgefüllt per E-Mail an die Verwaltung zurückschicken können, müssen die Kommunen an gut lesbarer Stelle darauf hinweisen, dass die Daten ungeschützt über das Netz geschickt werden, sofern keine Verschlüsselungsoption vorhanden ist und genutzt wird.

Viele Kommunen bieten inzwischen auf ihren Homepages als besonderen Bürgerservice Antragsformulare für verschiedene kommunale Leistungen an. So können Personenstandsurkunden angefordert, Kindergartenplätze beantragt, Bewerbungen für einen städtischen Bauplatz abgegeben oder die Ausleihfrist für ein Buch aus der Stadtbibliothek

verlängert werden. Diese Formulare können am Bildschirm ausgefüllt werden. Anschließend können sie ausgedruckt und per Brief an die Verwaltung geschickt werden, was datenschutzrechtlich völlig unproblematisch ist. Die ausgefüllten Formularsätze können aber auch per E-Mail an die Verwaltung geschickt werden.

Wegen der damit verbundenen Gefahren durch Einsichtnahme Dritter habe ich von den Kommunen gefordert, dass diese einen deutlichen Hinweis darauf geben, dass bei Nutzung der E-Mail-Funktion die Daten nur dann geschützt über das Netz geschickt werden, wenn eine Verschlüsselungsoption benutzt wird. Gibt es keine Verschlüsselungsoption, muss den Benutzerinnen und Nutzern dieses Services klar gemacht werden, dass bei dieser Art der Versendungsform das Risiko besteht, dass völlig unbeteiligte Dritte höchst sensible personenbezogene Daten mitlesen (nähere Ausführungen zu den Risiken bei der Nutzung von E-Mail siehe auch Tz. 10.1). Wer sich für diese schnelle und bequeme Möglichkeit der Antragstellung ohne Verschlüsselung entscheidet, geht dieses Risiko bewusst und selbstbestimmt ein. Deshalb muss ein aufklärender Hinweis an gut lesbarer Stelle angebracht werden (s. das unten abgedruckte Beispiel). Bei der Überprüfung der Homepage einer nordhessischen Stadt befand sich der Hinweis ganz am Ende des Formularsatzes, und zwar nach den Feldern "Ausdrucken" oder "Jetzt abschicken". Wer nicht ganz bis zum Ende dieser Seite blätterte, wofür bei der Gestaltung der Seite gar kein Anlass bestand, konnte den Hinweis gar nicht wahrnehmen. Hier habe ich eine sachgerechtere Anordnung gefordert.

@Grafik Nr. 6 einfügen@

9.4
Kraftfahrzeug-Zulassung über Internet

Im Kreis Odenwald und in der Landeshauptstadt Wiesbaden können Kraftfahrzeughändler die Zulassung von Neuwagen, Kraftfahrzeugum- und -abmeldungen sowie das Aussuchen von Wunschkennzeichen per Internet erledigen. Die Überprüfung ergab, dass die datenschutzrechtlichen Vorgaben bei der Ausgestaltung der Verfahren ausreichend berücksichtigt wurden.

Viele hessische Kommunen haben mittlerweile ein mehr oder weniger ausführliches Angebot im Internet eingerichtet, mit dem sie sich interessierten Nutzern vorstellen, Informationen bereit stellen sowie Unterlagen und Antragsformulare übermitteln. Dabei handelte es sich bislang um einen einseitigen Datenfluss vom Anbieter zum Nutzer, ohne dass ein virtueller Dialog - also Datenaustausch - stattfand. Die Entwicklung der technischen Möglichkeiten und das Bemühen, die Wirtschaftlichkeit zu erhöhen, führten zu Überlegungen, auch eine Bearbeitung von Vorgängen im Dialog zu ermöglichen. Unter dem Stichwort "Vorverlagerte Stadtverwaltung" reichen die Ideen von der Einrichtung von Heimarbeitsplätzen mit Zugriff auf die Einwohnermeldedatei zur Erteilung von Meldeauskünften über die Erteilung von Gewerbedatenauskünften und sonstigen Nutzungserlaubnissen bis zur Zulassung von Kraftfahrzeugen. Die Aufzählung ist nicht abschließend.

9.4.1

Rechtliche Vorgaben

Ich habe im Berichtsjahr drei verschiedene Vorhaben im Kraftfahrzeug-Zulassungsbereich nach den vorgelegten Unterlagen und den Präsentationen jeweils anhand folgender Vorgaben geprüft:

Aus datenschutzrechtlicher Sicht:

a) Nur die nach Straßenverkehrsrecht zulässigen und erforderlichen Daten dürfen von den Händlern verarbeitet werden (z.B. keine Personalausweisnummer oder Passnummer zur Identifikation).

b) Hoheitliche Aufgaben dürfen nicht auf private Dritte übertragen werden. Für eine Übertragung des Zulassungsaktes auf Kraftfahrzeughändler existiert im Zulassungsrecht keine Gesetzesgrundlage.

c) Es muss auch weiterhin die Möglichkeit bestehen, das Auto selbst anzumelden.

d) Die Auswahl der Autohäuser, die als Nutzer Zugriffsberechtigung erhalten, muss sich auch am Grundsatz der Zuverlässigkeit orientieren.

Aus datenschutztechnischer und organisatorischer Sicht:

a) Die von den Händlern eingegebenen Daten sollten auf einen separaten Rechner auflaufen, um eine Gefährdung des Echtdatenbestandes des Behördennetzes zu vermeiden. In jedem Fall ist sicherzustellen, dass lesende und schreibende Zugriffe nur auf die für die jeweilige Transaktion erforderlichen Daten erfolgen. Zugriffe auf sonstige Datenbanken und Computer des Behördennetzwerkes müssen ausgeschlossen sein.

b) Zur Zugangs- und Zugriffskontrolle sind entsprechende Sicherheitsmaßnahmen zu installieren, z.B. Einsatz eines Firewall-Systems.

c) Eine eindeutige Identifizierung und Authentifizierung des Nutzers muss sichergestellt werden. Die Wahl der jeweiligen Mittel (z.B. Chipkarte) hängt von der gewählten Verbindungsart ab.

d) Die Übertragung der Antrags- und Zulassungsdaten ist durch den Einsatz kryptographischer Verfahren vor unbefugter Kenntnisnahme zu schützen.

e) Alle schreibenden Zugriffe durch Dritte sind zu Nachweis- und Kontrollzwecken zu protokollieren.

f) Vorkommnisse, die die Sicherheit betreffen, wie fehlerhafte Anmeldeversuche, sind zu protokollieren und abzuklären.

g) Die privaten Nutzer sind zu verpflichten, geeignete Maßnahmen nachzuweisen, damit die auf ihrem EDV-System verarbeiteten Daten sowie die Antragsunterlagen vor unbefugtem Zugriff geschützt werden. Die Einhaltung von vertraglich auferlegten Sicherheitsauflagen ist zu überprüfen.

h) Der Kreis der zugriffsberechtigten Nutzer und ihrer Mitarbeiter und Mitarbeiterinnen ist jeweils konkret zu regeln und auf das notwendige Maß zu beschränken.

9.4.2
Konkrete Umsetzung und Bewertung der einzelnen Verfahren

Die Entwicklung des ersten Projekts erfolgte durch die Kommunale Informationsverarbeitung Hessen (KIV), Niederlassung Darmstadt. Das Verfahren läuft seit 20. September 1999 als Pilotprojekt beim Landrat des Odenwaldkreises zunächst befristet auf sechs Monate. Es nehmen sechs Autohäuser sowie ein Zulassungsdienst teil. Die erforderlichen Daten zur Zulassung, Umschreibung oder Änderung technischer Angaben eines Fahrzeuges werden jeweils in einer Bereitstellungsdatei bei der Zulassungsstelle abgelegt. Zu diesem Zeitpunkt kann ein Wunschkennzeichen beantragt werden. Die Daten werden von der Zulassungsstelle aufgerufen, kontrolliert und anschließend in den Bestand des Kraftfahrzeugverfahrens überspielt. Die Datenübertragung erfolgt dabei verschlüsselt. Die eigentliche Zulassung, Umschreibung u.s.w. erfolgt ausschließlich durch die Zulassungsstelle. Die Vorsprache bei der Zulassungsstelle mit den üblichen Unterlagen während der allgemeinen Öffnungszeiten ist weiterhin erforderlich. Die abschließende Bearbeitung erfolgt mit Übernahme der Daten in den Echtfahrzeugbestand und Ausdrucken der Fahrzeugpapiere, sobald die vollständigen Unterlagen bei der Zulassungsstelle eingehen. Eine Firewall sichert vor unbefugten Zugriffen. Die Identifizierung und Authentifizierung des Nutzers erfolgt durch Chipkarte. Die Berechtigten haben mit dem Landrat des Odenwaldkreises jeweils eine schriftliche Vereinbarung geschlossen, in der Zweck und Sicherheitsstandard geregelt sind. Unter Datenschutzgesichtspunkten war das zur Umsetzung bestimmte Konzept des Verfahrens nicht zu beanstanden.

Bei dem zweiten Projekt handelte es sich um ein Vorhaben der Stadt Wiesbaden, die mich rechtzeitig und ausführlich informierte. Dort wird seit 1. Oktober 1999 ein bereits im Saarland angewandtes Verfahren eines privaten Anbieters eingesetzt. Das Verfahren wird in Hessen von der Firma TÜV-Online GmbH vermarktet, einem elektronischen Internetdienst, der die Zusammenarbeit zwischen Zulassungsstelle und gewerblichen Kunden auf der Basis von Internetkommunikation anbietet. Auch hier gibt der Nutzer im Autohaus die notwendigen Daten zur Zulassung inkl. eines Wunschkennzeichens aus einer vorgelagerten Kennzeichendatenbank auf einen Informationsserver ein, der über die Firma TÜV-Online betrieben wird. Die Datenübertragung erfolgt auch hier verschlüsselt. Nach Benutzerauthentifikation beginnt die Transaktion. Nach Abschluss aller Eingabe- und Plausibilitätsprüfungen werden die Daten weiter verarbeitet und in der Datenbank

gespeichert. Ab diesem Zeitpunkt können die Daten vom Autohaus nicht mehr geändert werden. Die Zulassungsstelle kann jetzt die Daten vom Informationsspeicher auf einen Arbeitsplatz abrufen. Die Datenübertragung erfolgt verschlüsselt. Kontrolliert und protokolliert werden die Zugriffe von einem Firewall-System in der Zulassungsstelle, das externe Zugriffe abwehrt. In der Zulassungsstelle wird der Vorgang mit den entsprechenden, eingereichten Originalunterlagen abgeglichen und die Daten dem Echtdatenbestand der Zulassungsstelle zugeführt. Die Autohäuser können den erreichten Status einer Transaktion (erfolgreich ausgeführt/abgelehnt) abfragen und die Abholung der Unterlagen effektiv gestalten. Nach Abschluss des Zulassungsverfahrens werden die Daten auf dem Informationsserver gelöscht. Zur Abwicklung des Verfahrens bestehen Einzelvereinbarungen mit den beteiligten Händlern. Derzeit nehmen zwei Autohäuser und ein Zulassungsdienst daran teil. Auch hier habe ich unter Datenschutzgesichtspunkten keine Bedenken gegen das Konzept erhoben.

Vom dritten Vorhaben erfuhr ich nur durch einen telefonischen Hinweis eines Mitarbeiters einer betroffenen Gemeinde. Der damalige Landrat des Rheingau-Taunus-Kreises beabsichtigte binnen weniger Wochen als einer von sechs hessischen Landkreisen an einem achtwöchigen Modellversuch teilzunehmen, der darauf zielte, die Zulassung von Neufahrzeugen direkt in den Geschäftsräumen der Autohändler zu ermöglichen. Auf Rückfrage wurde erläutert, dass zwei ausgewählte Autohäuser die für den Zulassungsbetrieb notwendige EDV-Ausstattung inklusive ISDN-Anbindung zur Verfügung stellen, während der Kreis den notwendigen Zulassungsdrucker, eine parallele Schnittstelle sowie die Terminal-Emulation bereitstellt. Das Kommunale Gebietsrechenzentrum (KGRZ) Wiesbaden sollte die entsprechenden Server-Verbindungen online herstellen. Geringfügig Beschäftigte des Rheingau-Taunus-Kreises sollten in Geschäftsräumen der beiden Firmen die anfallenden Kraftfahrzeugzulassungen, -ummeldungen sowie -abmeldungen bearbeiten. Die Kosten der Beschäftigten sollten von den Autohäusern an den Rheingau-Taunus-Kreis erstattet werden. Die Firmen sollten für die amtlichen Unterlagen und Gerätschaften einen Tresor der Sicherheitsstufe D oder einen abschließbaren Bereich innerhalb eines solchen Tresors zur Verfügung stellen. Nähere Darlegungen zu Sicherungsmaßnahmen, etwa zu einem Projektkonzept, konnten weder der Kreis noch das KGRZ geben. Trotz Aufforderung wurde eine prüffähige Beschreibung nicht vorgelegt. Eine ausreichende Trennung zwischen der Tätigkeit der eingesetzten Bediensteten und den Geschäftsinteressen der Firma war nicht gewährleistet. Schließlich konnte auch nicht geklärt werden, ob eine Übernahme der

Amtstätigkeiten durch Mitarbeiter der Firmen geplant war. Datenschutzrechtliche Bedenken wurden somit bisher nicht ausgeräumt. Nachdem auch das Hessische Ministerium für Wirtschaft, Verkehr und Landesentwicklung Bedenken gegen die Zulässigkeit des Verfahrens angemeldet hatte, wurde der Rheingau-Taunus-Kreis gebeten, zunächst von der bevorstehenden Umsetzung des Pilotprojekts Abstand zu nehmen. Er wurde aufgefordert, ein prüffähiges Konzept vorzulegen. Das Vorhaben wurde bisher nicht weitergeführt.

9.5
Persönliche Daten schulischer Lehrkräfte im Internet

Private Daten schulischer Lehrkräfte wie etwa Adresse und Geburtsdatum dürfen im Internet ohne deren Zustimmung nicht veröffentlicht werden.

Die Anfrage einer Lehrkraft an einem Gymnasium vermittelte einen Eindruck der vielfältigen Nutzungsvarianten des Internet im Schulbereich. Der Abiturjahrgang 1999 eines Gymnasiums beabsichtigte, ebenso wie der Abiturjahrgang 1998, das sog. Abiturbuch im Internet zu veröffentlichen. Das Abiturbuch sollte neben den Beiträgen einzelner Schüler über ihre schulischen Erlebnisse und Eindrücke auch Name, Vorname, Adresse, Telefonnummer und Geburtsdatum einzelner Lehrkräfte enthalten, die den Jahrgang unterrichteten. Die betroffenen Lehrkräfte waren über diese Art der Veröffentlichung jedoch nicht informiert. Als Quelle der Daten kam die Lehrerstammdatei der Schulverwaltung in Betracht.

In § 34 Abs. 2 Hessisches Datenschutzgesetz (HDSG) sind die rechtlichen Voraussetzungen einer Übermittlung von Beschäftigtendaten an Personen und Stellen außerhalb des öffentlichen Rechts - als auch für Veröffentlichungen - festgelegt.

§ 34 Abs. 2 HDSG

Abweichend von § 16 Abs. 1 ist eine Übermittlung der Daten von Beschäftigten an Personen und an Stellen außerhalb des öffentlichen Bereiches nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Die Übermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

§ 34 Abs. 2 HDSG findet keine Anwendung, soweit der Bedienstete "nur" als Amtswalter, also als Teil des Staats, betroffen ist (vgl. auch 25. Tätigkeitsbericht, Ziff. 8.3). Dies ist z.B. der Fall, wenn Daten der Lehrerinnen und Lehrer im schulischen Wirkungskreis preisgegeben werden. Soweit aber die Veröffentlichung der Daten nicht der Ausübung der dienstlichen Funktion dient, sind die Lehrerinnen und Lehrer nicht als Amtswalter betroffen, sondern als Privatperson. Dies gilt auch für die Veröffentlichung von Namen, Adressen und Geburtsdaten im Abiturbuch, das im Internet abrufbar ist. Im konkreten Fall lagen die in § 34 Abs. 2 HDSG festgelegten Voraussetzungen für eine Übermittlung nicht vor. Ohne Einwilligung der betroffenen Lehrkräfte ist eine derartige Veröffentlichung daher nicht zulässig. Der Lehrkraft bleibt es dabei unbenommen, diese Einwilligung sogar pauschal für alle Übermittlungsfälle zu erklären, soweit sie schulischen Bezug haben.

10. Entwicklungen im Bereich der Technik

10.1
Fallstricke bei der Benutzung von E-Mail

Eine der meist genutzten Anwendungen der neuen Kommunikationstechniken ist die elektronische Post (E-Mail). Sie erlaubt es, schneller als mit normalen Briefen Nachrichten zu versenden. Auch gegenüber dem Telefax hat sie - in der Regel - Vorteile. So können vom Arbeitsplatz aus Nachrichten und andere elektronische Dokumente versandt, eingehende Post gelesen und ohne Medienbruch weiter bearbeitet werden. Diesen Vorteilen stehen aber auch datenschutzrechtliche Risiken gegenüber, die Gegenmaßnahmen erfordern.

10.1.1
Ablaufskizze

Um die im folgenden Abschnitt beschriebenen Gefahren verstehen zu können, sind die Abläufe und die eingesetzte Technik kurz zu skizzieren: Um über einen Kommunikations-Anbieter E-Mails versenden zu können, benötigt ein Teilnehmer einen sog. Account, dies entspricht in etwa einer Kundennummer, mit dem er sich am Rechner des Anbieters anmeldet, und ein Passwort, mit dem er sich als berechtigte Person ausweist. Diesem Account können eine oder mehrere E-Mail-Adressen zugeordnet sein. Die Verbindung mit dem Rechner des Anbieters bauen besondere Programme auf, sog. E-Mail-Clients. Beispiele für derartige E-Mail-Clients sind Microsoft Outlook, Netscape Messenger, Eudora Pro oder vom Anbieter gestellte Programme wie bei T-Online.

Einfache Mitteilungen können mit dem E-Mail-Client erstellt werden. Sollen ansprechend aufbereitete Schreiben, Bilder oder schon vorhandene Dokumente versandt werden, kann einer E-Mail ein Anhang mit Dateien hinzugefügt werden.

Zum Versand nimmt der E-Mail-Client mit dem Zentralrechner Kontakt auf, auf dem der Anbieter die E-Mails speichert: dem Mailserver. Die E-Mail wird im Ausgangsbereich des Postfachs (Mailbox) gespeichert, das der Zentralrechner bereitstellt. Anschließend bereitet der Mailserver die Weiterleitung vor. Dazu stellt er an Hand der Adresse des Empfängers fest,

welcher Mailserver für den Empfänger zuständig ist. Jetzt wird die E-Mail über das Netzwerk an den Zielrechner geleitet. Dabei kann es vorkommen, dass die E-Mail noch auf weiteren Rechnern zwischengespeichert wird. Am Ende des Vorgangs befindet sich die E-Mail auf dem Mailserver des Empfängers in dessen Mailbox.

Um die E-Mail abzufragen, muss der Empfänger am Mailserver angemeldet sein. Dieser zeigt die eingegangenen E-Mails an. Die vom Empfänger ausgewählten E-Mails werden dann vom Mailserver zum Empfängerrechner übertragen.

10.1.2
Gefahren und Gegenmaßnahmen

In diesen Abläufen gibt es typische Gefahren, die aus Schwachstellen der Technik oder der Organisation hervorgehen. Die Risiken müssen durch geeignete Gegenmaßnahmen reduziert werden.

E-Mails unterliegen insbesondere während der Übertragung Gefahren, die sich allerdings nicht von denen unterscheiden, die generell bei einer Kommunikation über Netze vorhanden sind (vgl. 22. Tätigkeitsbericht, Ziff. 21). Dabei gibt es zu den meisten Gefahren Entsprechungen bei der Briefpost. Annäherungsweise ist eine E-Mail mit einer offen versandten Postkarte vergleichbar, die in Druckbuchstaben mit einem Bleistift geschrieben wurde. Abhilfe bieten Sicherheitsmaßnahmen wie Verschlüsselung und elektronische Unterschrift, die das Schutzniveau erheblich verbessern. Teilweise kann sogar eine höhere Sicherheit erreicht werden als bei der Briefpost.

Die E-Mail selbst kann für den Empfänger Gefahren bedingen, wenn beispielsweise Viren oder andere Schadprogramme (vgl. Ziff. 10.1.2.7) übertragen werden. Durch ausgehende E-Mails kann der Absender ungewollt Informationen preisgeben, die an sich nicht versandt werden sollten (vgl. Ziff. 10.1.2.8).

10.1.2.1
Unbefugte Kenntnisnahme des Passwortes

Beim Abhören der Kommunikation gibt es zwei Problembereiche. Zum einen können Unbefugte E-Mails während der Übertragung oder auf dem Server selbst zur Kenntnis nehmen (s. Ziff. 10.2.2); zum anderen können Unbefugte das Passwort abhören, mit dem sich der Nutzer auf dem Mailserver anmeldet.

Hat ein Unbefugter sich das Passwort beschafft - dies ist natürlich auch im Fall von innerbetrieblicher E-Mail denkbar -, so kann er irreführend als Urheber auftreten und statt des Nutzers E-Mails schreiben und lesen.

Die Möglichkeiten, sich dagegen zu schützen, hängen von der eingesetzten Technik ab. Die Art und Weise wie zwischen dem PC und dem Mailserver Daten ausgetauscht werden, hängt von dem verwendeten Protokoll ab. Weit verbreitet sind derzeit das POP3 (Post-Office-Protocol 3) oder das IMAP (Internet Mail Access Protocol). IMAP erlaubt es standardmäßig, das Passwort zu verschlüsseln. Die Option "Passwort verschlüsseln" muss nur "angekreuzt" werden. POP3 beinhaltet hingegen keine Verschlüsselung des Passworts. POP3 benötigt dazu Zusatzprogramme auf dem Server und dem PC, die nicht als Standard festgelegt sind. Es erfordert viel Aufwand zwischen dem Kunden und dem Betreiber, eine geeignete Software auszuwählen.

Empfohlene Gegenmaßnahmen

- Nutzen der Verschlüsselung des IMAP Protokolls.
- Festlegen und nutzen von Zusatzprogrammen zur Verschlüsselung beim POP3 Protokoll.

10.1.2.2

Unbefugte Kenntnisnahme der E-Mail während der Übertragung oder der Speicherung auf den Servern

Durch Verschlüsselung lässt sich verhindern, dass Unbefugte die E-Mail lesen. Für Privatpersonen ist das Programm PGP (Pretty Good Privacy; vgl. 23. Tätigkeitsbericht, Ziff. 27) zurzeit am weitesten verbreitet. Es ist auch möglich mir verschlüsselte E-Mails zuzusenden. Auf der Homepage (http://www.datenschutz.hessen.de) ist der öffentliche Schlüssel abrufbar. Der Fingerprint ist:

6868 99B3 032D D020 999A CDE4 BFAD 38F7

Neben PGP gibt es andere Verschlüsselungsstandards. Beispiele sind PEM, S/MIME oder MailTrusT. Darauf aufbauende Programme sind aber oft nicht interoperabel, weshalb derzeit versucht wird, einen einheitlichen Standard zu erarbeiten. Im Rahmen des Pilotversuchs SPHINX haben die Bundesverwaltung und einige andere Institutionen auf dem MailTrusT-Standard basierende Programme getestet. Nach Anfangsproblemen funktionierte die Verschlüsselung.

Ein Nachteil soll aber nicht verschwiegen werden: Wenn E-Mails verschlüsselt werden, ist eine Virenprüfung nicht mehr auf dem Mailserver oder an der Firewall möglich, sondern nur noch auf dem einzelnen PC.

Empfohlene Gegenmaßnahme

- Verschlüsseln der E-Mail.

10.1.2.3
Unbefugtes Löschen von Nachrichten

Eine E-Mail kann auf einem der Mailserver gelöscht werden, sodass sie nie den Empfänger erreicht. Diese Gefahr ist nicht nur theoretischer Natur. Verträge mit Anbietern können eine Klausel enthalten, wonach E-Mails ohne Rückfrage gelöscht werden, wenn sie nicht innerhalb einer vorgegebenen Zeit abgerufen wurden oder wenn der zugeteilte Plattenplatz ausgeschöpft ist. Gleichwohl hat der Absender die Meldung erhalten, die E-Mail sei abgeliefert. Damit scheint für ihn alles Notwendige vollzogen zu sein. Der Empfänger erhält die E-Mail jedoch nicht zur Kenntnis.

Empfohlene Gegenmaßnahmen

- Keine vertragliche Regelung akzeptieren, die es dem Anbieter gestattet, ohne Wissen und Wollen des Kunden E-Mails zu löschen.
- Bei wichtigen E-Mails die Absendung telefonisch ankündigen.
- Zur ergänzenden Absicherung eine Bestätigung vom Empfänger fordern und, wenn diese nicht erfolgt, nachfragen.

10.1.2.4
Unbefugte Modifikation der Daten

Auf dem Weg vom Absender zum Empfänger kann der Inhalt der E-Mail verändert werden.

Falls die E-Mail mit einer elektronischen Unterschrift (vgl. 24. Tätigkeitsbericht, Ziff. 17 und 25. Tätigkeitsbericht, Ziff. 20) versehen wird, kann der Empfänger erkennen, wenn die E-Mail nicht vom genannten Absender stammt. Um den technischen Möglichkeiten einen rechtlichen Rahmen zu geben, wurde das Gesetz zur digitalen Signatur am 22. Juli 1997 erlassen. Mittlerweile gibt es erste gesetzeskonforme Produkte. PGP bietet zwar mit der Möglichkeit Daten elektronisch zu unterschreiben, eine Lösung, die in vielen Fällen ausreichend ist, jedoch genügt sie nicht dem Signaturgesetz. Die Unterschiede liegen sowohl in der Technik, insbesondere in dem Vertrauen in die technische Implementierung, als auch in der Sicherheitsinfrastruktur, an die das Signaturgesetz hohe Ansprüche stellt. Während der Inhalt einer normalen E-Mail leicht manipuliert werden kann, ist dies bei digital signierten E-Mails sehr viel schwieriger. Der Empfänger einer E-Mail sollte sich aber in jedem Fall ein gesundes Misstrauen bewahren und sich in Zweifelsfällen trotz einer elektronischen Unterschrift beim Absender rückversichern.

Zurzeit findet eine Überarbeitung zur Anpassung an die EU-Richtlinie statt. Ferner gibt es Ansätze, die elektronische Unterschrift sowohl im Privatrecht als auch im öffentlichen Recht unter bestimmten Rahmenbedingungen der handschriftlichen Unterschrift gleichzusetzen.

<u>Empfohlene Gegenmaßnahmen</u>

- Einsetzen einer elektronischen Unterschrift.
- Bei wichtigen Nachrichten oder unerwarteten Äußerungen eines Kommunikationspartners rückfragen.

10.1.2.5
Vortäuschen einer fremden Identität

Im Kopf einer E-Mail, der allerdings oft nicht angezeigt bzw. ausgedruckt wird und nur schwer verständliche Informationen enthält, gibt es eine Reihe von Angaben, die Rückschlüsse auf den echten Absender zulassen. Die elektronische Unterschrift bietet jedoch eine bessere Gewähr, die Identität eines Absenders nachzuweisen oder eine Täuschung zu erkennen.

Empfohlene Gegenmaßnahme

- Elektronische Unterschrift fordern.

10.1.2.6
Leugnen einer Kommunikationsbeziehung

Ein Absender kann behaupten, eine beim Empfänger eingegangene E-Mail nicht abgesandt zu haben. Ein Empfänger kann abstreiten, eine an ihn versandte E-Mail erhalten zu haben.

In beiden Fällen kann versucht werden, über aufwendige Auswertungen von Protokollen Nachweise zu führen. Analog zur Briefpost gibt es jedoch Grenzen der Nachweisbarkeit. Wenn dem Empfänger eine elektronisch unterschriebene E-Mail zugeht, kann der Empfänger davon ausgehen, dass die E-Mail vom Absender stammt. Der Nachweis des Zugangs kann so allerdings nicht erleichtert werden.

Empfohlene Gegenmaßnahme

- Eine elektronische Unterschrift fordern.
- Zugangsbestätigung anfordern, am besten durch anderes Medium (Telefon, Fax, Brief) oder Doppelversand durch anderes Medium.

10.1.2.7
Schadprogramme

In vielen Fällen wird einer E-Mail als Anhang eine Datei hinzugefügt. Diese Datei kann ein beliebiges Format haben (Textverarbeitung, Tabelle, Grafik oder Programm). Derartigen Anhängen kann ein ausführbarer Programmcode so hinzugefügt werden, dass dieser gestartet

wird, sobald das Dokument zum Lesen geöffnet wird. Der Programmcode kann auch vom Empfänger unerwünschte Funktionen beinhalten (Viren, trojanische Pferde oder Würmer).

Viren sind seit vielen Jahren als Problem bekannt (vgl. 19. Tätigkeitsbericht Ziff. 15.4 oder 23. Tätigkeitsbericht, Ziff. 28) und ein aktuelles Virenschutzprogramm sollte zur Ausstattung eines jeden PC gehören. Verstärkt treten sog. Macro-Viren auf, die in einem unverdächtigen Dokument, zum Beispiel eine Word-Datei oder eine Excel-Tabelle, versteckt sind. Wird das Dokument geöffnet, so wird der Virus aktiviert. Besonders ärgerlich ist in diesem Zusammenhang, wenn die automatische Ausführung von Macros unterbunden werden soll, was sinnvoll wäre, auf der anderen Seite aber Macros genutzt werden, um Abläufe zu automatisieren. Mittlerweile können auch in HTML-Format [HyperTextMarkupLanguage; Format vieler Internet-Seiten] erstellte Anhänge aktive Inhalte wie Active-X haben. Je nach Einstellung des Browsers können dann Schadensroutinen ablaufen. Zum ersten Mal ist 1999 ein Virus aufgetreten, der nicht im Anhang versteckt war, sondern bereits beim Öffnen der E-Mail selbst ausgeführt wurde. Es mussten dazu aber bestimmte Active-X-Komponenten aktiviert sein.

Weiterhin sind sog. "trojanische Pferde" besonders im letzten Jahr der Öffentlichkeit als Problem beschrieben worden (z.B. Netbus, SubSeven und Back-Orifice). Mit diesen Programmen kann ein Außenstehender einen Computer ausspionieren und sogar jeden Tastenanschlag des Benutzers (inklusive der Passwörter) protokollieren. Das geht soweit, dass der Außenstehende den Computer fernsteuern kann. Der Benutzer kann sogar vom eigenen Computer ausgesperrt werden. Diese Programme sind oft nicht von Anwendungen zur Fernadministration und Fehlerbehebung zu unterscheiden. Der entscheidende Unterschied ist, dass sich die Schadprogramme ohne Wissen und Wollen des Anwenders installieren und dann ablaufen. Gute Virenschutzprogramme sollten auch "trojanischen Pferde" erkennen und abwehren.

Handelt es sich um eine E-Mail von einem unbekannten Absender, ist besondere Vorsicht geboten. Dateien sollten dann nur ausnahmsweise geöffnet werden. Selbst wenn der Absender bekannt ist, sollte vor dem Öffnen von Dateien die E-Mail genauer betrachtet werden. Wenn es sich um einen Bekannten aus Deutschland handelt, ist Misstrauen angesagt, wenn der Text der E-Mail in Englisch verfasst ist. Einige Schadprogramme wie "Melissa" haben jeder E-

Mail-Adresse eines befallenen Rechners einen englischen Text geschickt mit der Aufforderung, das im Anhang befindliche komprimierte Programm zu starten.

Empfohlene Gegenmaßnahmen

- Einen Virenscanner einsetzen, der in kurzen Abständen aktualisiert wird.
- Vor dem ersten Aufruf einer E-Mail sollte eine Prüfung mit einem aktuellen Virenscanner erfolgen. Falls E-Mails verschlüsselt werden, kann die Prüfung nur auf dem PC des Empfängers - nicht auf dem Server oder durch eine Firewall - erfolgen.
- E-Mail vor dem Versand auf Viren prüfen.
- Einstellungen des Browsers auf sichere Stufen stellen.
- Automatische Ausführung von Macros bei E-Mails unterbinden.
- Mit dem Kommunikationspartner abstimmen, welche Austauschformate genutzt werden sollen.
- Wenn möglich, Formate ohne aktive Inhalte zum Datenaustausch wählen.
  Beispiele: rtf- (Rich Text Format) oder pdf-Format
- Kein automatisches Öffnen der Anlagen einer E-Mail vorsehen.

10.1.2.8
Überschüssige Informationen in E-Mails

10.1.2.8.1
Verborgene Informationen in Dokumenten

Im letzten Jahr gab es Eingaben, in denen allgemein nicht bekannte Fallstricke im Umgang mit E-Mails aufgetreten sind. Die Beispiele zu den folgenden Ausführungen beziehen sich auf Text-Dokumente, die mit Word 97 von Microsoft erstellt wurden. Es sind aber auch andere Dokumentenformate betroffen. Deshalb muss jeder Nutzer in seinen Umfeld entsprechende Vorsicht walten lassen, wenn er Dokumente elektronisch verschickt.

Ein Bürger hatte per E-Mail ein Word-Dokument von einem Bekannten zur Kenntnis erhalten. Er öffnete es mit einem Editor und war dadurch in der Lage, den Text der für ihn bestimmten Nachricht zu lesen. Gleichzeitig konnte er aber auch nachlesen, was der Bekannte seinem Sohn an Vorhaltungen gemacht hatte, da Teile eines alten Schreibens enthalten waren.

Dies liegt an der Eigenschaft von Word-Dokumenten, auch gelöschte Daten zu speichern, ohne sie am Bildschirm anzuzeigen. Bei den folgenden Grafiken handelt es sich um Anzeigen bzw. Ausschnitte von Dokumenten, die auch im Internet unter „www.datenschutz.hessen.de“ abrufbar sind.

Ansicht eines unter Word 97 erfassten Schreibens

@Grafik 1@

Teilansicht dieses Schreibens mit dem Editor Note-Pad

@Grafik 2@

Anschließend wurde das Schreiben mit „Speichern unter“ unter einem anderen Namen gespeichert, der alte Text gelöscht und der folgende Text erfasst.

Ansicht des neuen Schreibens unter Word 97

@Grafik 3@

Unter Note-Pad sind folgende Informationen sichtbar (die Trennzeichen zwischen den Buchstaben des neuen Textes sind keine Blanks)**:**

Teilansichten des neuen Schreibens unter Note-Pad

@Grafiken 4 und 5@

Dieses Beispiel zeigt, dass mit Dokumenten ungewollt Informationen preisgegeben werden können, weil Teile des Textes und sonstige Informationen verborgen mit übertragen werden. Es gibt Formate, bei denen diese Schwachstelle nicht oder weniger ausgeprägt ist.
Das rtf-Format (Rich Text Format) wird von den meisten Textverarbeitungsprogrammen verstanden. Es ist gut geeignet, um Texte auszutauschen.
Kompliziertere Dokumente können im pdf-Format ausgetauscht werden. Der zum Lesen erforderliche Acrobat-Reader ist kostenlos verfügbar, jedoch gibt es Probleme, das Dokument weiterzuverarbeiten. Das Erstellen von Dokumenten im pdf-Format wird nur von wenigen Textverarbeitungsprogrammen unterstützt. Meist müssen zusätzliche, kostenpflichtige Programme angeschafft werden.

Gegenmaßnahmen

- Nutzen eines Austauschformats, in dem außer Formatinformationen keine verborgenen Informationen enthalten sind.
- Wenn kein Austauschformat ohne überschüssige Informationen genutzt werden kann, müssen organisatorische Maßnahmen die Gefahr minimieren. Die Mitarbeiter müssen darauf hingewiesen werden, wie vermieden werden kann, dass in Dokumenten unerwünschte verborgene Informationen weitergeleitet werden. So ist beispielsweise bei Word-Dokumenten anzuraten, ein Dokument neu anzulegen und dann den Text zu erfassen. Falls Teile aus anderen Dokumenten kopiert werden sollen, dürfen nur exakt diese Abschnitte kopiert werden!

10.1.2.8.2
Umfangreiche Adressverteiler

In einem anderen Fall erreichte mich eine E-Mail mit einer Größe von über 50 Kilobyte, die das E-Mail Programm nur mit Mühe anzeigen konnte. Die eigentliche Nachricht war die vierzeilige Einladung zu einer Sitzung, die fünf Institutionen betraf, also erheblich weniger als ein Kilobyte. Der Rest war das komplette Adressbuch des Absenders, fast 500 Kommunikationspartner, für die die Sitzung in aller Regel aber unwichtig war. Als Folge hatte der Empfänger einen Überblick über den Bekannten- und Kollegenkreis des Absenders, was je nach Absender auch für die Partner unangenehm sein kann.

Gegenmaßnahme

- Erstellen von Adressverteilern, die auf den jeweiligen Adressatenkreis eingegrenzt sind.

10.1.3
Ärgernisse

Neben den Gefahren gibt es noch Ärgernisse, die für den Absender oder den Empfänger Aufwand verursachen, ohne unmittelbar datenschutzrechtlich relevant zu sein.

10.1.3.1
Nicht lesbares Format

Wenn es keine Abstimmung zwischen Sender und Empfänger gibt, kann es immer wieder geschehen, dass der Empfänger die E-Mail oder die Dokumente im Anhang nicht lesen kann. Es sind dann Rückfragen erforderlich, evtl. müssen andere Programme installiert werden oder der Absender muss die Informationen auf einem anderen Weg oder in anderem Format übermitteln.

10.1.3.2
Aufgeblähte oder unerwünscht zugesandte E-Mails

Sofern aufgeblähte, insbesondere unaufgefordert zugesandte E-Mails (unerkannte Werbung) abgerufen werden müssen, kostet das den Empfänger Zeit und Geld.

10.1.3.3
Nicht organisierte Verteilung in der Behörde/Institution

Bei Empfang von E-Mails durch Behörden oder andere Institutionen muss festgelegt werden, wie die E-Mails im Geschäftsgang zu behandeln sind.

10.1.3.4
Fehlende Regelungen zur privaten Nutzung

Unabhängig hiervon gilt es noch für Arbeitgeber oder andere Institutionen, Regelungen darüber zu treffen, ob und wenn ja mit welchen Rahmenbedingungen eine private Nutzung der E-Mail zulässig ist. Problematisch ist insbesondere der mögliche Zugriff des Arbeitgebers auf private E-Mails (Briefgeheimnis).

10.1.4
Hinweise, wie die Sicherheit bei der Nutzung von E-Mails verbessert werden kann

Die folgenden Hinweise sollen in Form einer Checkliste zusammenfassen, wie den oben beschriebenen Gefahren und Ärgernissen begegnet werden kann.

1. Ist gewährleistet, dass ein aktueller Viren-Scanner eingesetzt wird?
2. Ist sichergestellt, dass ein Viren-Scanner jeden Anhang, auch verschlüsselte, überprüft, bevor diese geöffnet werden?
3. Ist sichergestellt, dass die Anhänge einer E-Mail nicht automatisch geöffnet werden?
4. Welche Austauschformate sind verfügbar?

4.1 Sind mit den Partnern, mit denen regelmäßig E-Mails ausgetauscht werden, Austauschformate vereinbart?

4.2 Werden zum Informationsaustausch Dateiformate verwendet, die keine überschüssigen Informationen enthalten?

4.3 Werden Austauschformate genutzt, die keine aktiven Inhalte umfassen?

4.4 Ist geregelt, wie Dokumente erstellt werden müssen, die per E-Mail versandt werden sollen?

5. Wird ein Verschlüsselungsprogramm eingesetzt, wenn vertrauliche Informationen versandt werden sollen?

6 Werden E-Mails elektronisch unterschrieben?

7. Sind Adressverteiler vorhanden und werden diese gepflegt?
8. Ist geregelt, wie mit E-Mails im Geschäftsgang zu verfahren ist?
9. Wird das Passwort zum Mailserver verschlüsselt übertragen?

10. Ist gewährleistet, dass eine E-Mail nicht ohne Zustimmung des Empfängers auf dem Mailserver gelöscht wird?
11. Prüfen Sie den Inhalt einer E-Mail auf Stichhaltigkeit und fragen Sie bei Zweifeln nach?
12. Rückfragen, ob E-Mail angekommen, am besten über anderes Medium, sofern rechtliche Folgen davon abhängen.

10.2

Fernadministration und Fernwartung von Firewalls

Das Angebotsspektrum von EDV- Dienstleistungen hat sich in den letzten Jahren um die Fernadministration und Fernwartung von Firewalls erweitert. Dadurch ergeben sich Risiken, die durch eine planvolle, kontrollierte Vorgehensweise begrenzt werden müssen.

Im letzten Jahr wurden mir im Zusammenhang mit dem Betrieb von Firewalls verschiedene Formen der Kooperation mit externen Dienstleistern geschildert. Für solche Dienste findet § 4 HDSG Anwendung, der die Zulässigkeitsvoraussetzungen für eine Auftragsdatenverarbeitung festlegt.

In einem Fall überlegte eine Kommune, sich über eine Firewall, die von einem privaten Dienstleister betrieben wird, an das Internet anzuschließen. Eine ähnliche Situation entsteht, wenn sich die Firewall bei einem Kommunalen Gebietsrechenzentrum oder der Hessischen Zentrale für Datenverarbeitung befindet. Gemäß § 4 Abs. 2 HDSG muss im Vertrag genau festgelegt werden, welche technischen und organisatorischen Vorkehrungen durch den Anbieter geschaffen und umgesetzt werden müssen. Der Auftraggeber muss kontrollieren, ob entsprechend den vereinbarten Vorgaben verfahren wird. Anhaltspunkte, welche Dienste die Firewall wie filtern soll, sind der Orientierungshilfe "Internet" (27. Tätigkeitsbericht, Anhang 2 oder Internet www.datenschutz.hessen.de) zu entnehmen.

Komplizierter wird die Rechtslage, wenn die datenverarbeitende Stelle die Firewall selbst betreibt, die Administration und Wartung aber aus Kapazitätsgründen durch eine externe Firma vornehmen lässt. Diese Dienstleistung wird von spezialisierten Firmen angeboten. In einem Fall betreibt eine Firma vier Zentren in Europa, von denen aus die Fernadministration

der Firewalls aller ihrer Kunden vorgenommen wird. Die besondere Brisanz dieser Lösung besteht darin, dass unbefugte Personen sich nur auf wenige Stellen konzentrieren müssen, um durch Ausnutzen von Sicherheitslücken in den Zentren oder unsichere Übertragungswege zwischen den Zentren und den Firewalls in die Netze vieler Kunden eindringen zu können. Deshalb ist bei den Verträgen sowie bei der Planung und Realisierung der Fernadministration besondere Umsicht geboten.

Die grundsätzlichen Risiken und datenschutzrechtlichen Vorgaben bei Fernwartungen sind auch bei dieser Konstellation zu beachten (vgl. 24. Tätigkeitsbericht, Ziff. 17.4 und 19.2). Die Forderungen an die technische und organisatorische Absicherung sind aber höher anzusetzen als bei einer normalen Fernwartung, um die Risiken überschaubar zu halten. Wenn der Kunde in seinem Netz sensible Daten verarbeitet, für die die Fernadministration ein untragbares Risiko darstellt, ist unbedingt auch zu prüfen, ob es nicht geboten ist, den dazugehörigen Rechner oder Server vom Internet zu trennen.

10.2.1
Grundsätzliche Forderungen

Wenn die Administration oder die Wartung der Firewall durch einen externen Dienstleister vorgenommen werden soll, müssen folgende Grundsätze beachtet werden:

- Der Betreiber ist und bleibt für die Sicherheit des Netzes sowie aller Daten und Verfahren verantwortlich. Er muss den ihm obliegenden Datenschutz und die Datensicherheit gewährleisten. Das ist vertraglich im Einzelnen sicherzustellen (vgl. Mustervertrag, Ziff. 25.2).

- Die Administration oder die Wartung muss auf seine konkrete Weisung hin erfolgen. Sie darf nur mit seinem Wissen und Wollen vorgenommen werden.

- Der Betreiber muss in der Lage sein, die Durchführung der Fernadministration oder -wartung technisch und vom Wissen her zu kontrollieren. Er darf sich nicht des Know-Hows begeben, das für die Kontrolle erforderlich ist. Er darf nicht in Abhängigkeit vom

Dienstleister geraten.

- Es müssen die nach § 10 Abs. 2 HDSG erforderlichen Sicherungsmaßnahmen ergriffen und vertraglich vereinbart werden.

- Die Zugriffsrechte des Wartungspersonals sind auf ein Minimum zu beschränken. Die strikte Trennung von Datenbeständen anderer Kunden ist vertraglich abzusichern.

- Die Wartung muss detailliert protokolliert werden, um revisionsfähig zu sein.

10.2.2
Umsetzung der Forderungen

Von den Abläufen her können drei Phasen mit verschiedenen Aktivitäten unterschieden werden.

Die Planung der Fernadministration und Fernwartung:

- Die Rechte und Pflichten des Auftraggebers und Auftragnehmers müssen verbindlich festgelegt werden (vgl. Mustervertrag, Ziff. 25.2).

- Der Umfang der Zugriffsrechte ist zu bestimmen.

- Die Systemverwalter sind zu schulen.

- Technische Maßnahmen zur Verringerung des Netzrisikos bei der Fernadministration oder Fernwartung müssen ergriffen werden.
- Die gegenseitige Authentisierung der beteiligten Kommunikationspartner muss angesichts der Wichtigkeit der Aufgabe sicher erreicht werden. Hierzu müssen kryptografische Verfahren wie Challenge-Response-Verfahren oder vergleichbar sichere Systeme gewählt werden. Alle Daten, die im Rahmen der Dienstleistung übertragen werden, müssen mit einem ausreichend sicheren Verfahren verschlüsselt werden.

- Es müssen technische Maßnahmen beim Rechner umgesetzt werden, die gewährleisten, dass ausschließlich zugelassene Personen arbeiten können. Die übliche Identifikation und Authentisierung von Benutzern mit Passwörtern sollte um eine Komponente ergänzt werden, die den Besitz einer Chipkarte voraussetzt oder ein biometrisches Merkmal abfragt.

- Zugriffe auf Daten und Programme dürfen nur innerhalb des vertraglich festgelegten Rahmens erfolgen.

- Die Revisionsfähigkeit muss gegeben sein. Dazu ist eine vollständige Protokollierung der Aktivitäten unabdingbar.

Beim Ablauf der jeweiligen Maßnahmen der Fernwartung ist sicherzustellen:

- Die Fernadministration darf allein vom Betreiber eingeleitet werden.

- Die systemseitigen Sicherungsmaßnahmen des Betreibers müssen vom Wartungspersonal des Fernadministrators durchlaufen werden.

- Die einzelnen Schritte der Fernadministration sind vom Betreiber zu überwachen. ID-Systeme könnten hier eine Unterstützung bieten (vgl. Ziff. 10.3). Er muss wissen, welche Aktionen auf seinem Rechner vorgenommen werden, bei Unregelmäßigkeiten die Fernadministration abbrechen.

Die Revision der Fernwartung:

- Dem Betreiber muss bekannt sein, wer wann von wo mit welchen Mitteln was veranlasst hat und worauf zugegriffen worden ist. Dazu müssen Auswertungsprogramme zur Verfügung stehen.

10.3
Intrusion Detection Systeme

Behörden, Firmen und andere Institutionen hängen immer mehr von dem korrekten Funktionieren ihrer Informationstechnik ab. Die Vertrauenswürdigkeit der Ergebnisse muss insbesondere durch Maßnahmen zur IT-Sicherheit erreicht werden. Als eine Komponente, die noch an Bedeutung gewinnen dürfte, werden "Intrusion Detection Systeme" (IDS) eingesetzt. Das sind Systeme, die das Eindringen Unberechtigter feststellen. Diese Systeme verarbeiten Daten von Beschäftigten. Ihr Einsatz ist dann datenschutzkonform, wenn die Daten nur zu Zwecken der Datenschutzkontrolle und nicht zu Leistungs- oder Verhaltenkontrollen genutzt werden.

10.3.1
IT-Sicherheit und Intrusion Detection Systeme

In einer Studie zur Informationssicherheit, die von den Unternehmen PricewaterhouseCoopers und InformationWeek vorgenommen wurde (Ausgabe 17-18/99 der InformationWeek), wurden die Antworten von über 2700 IT-Managern und Sicherheitsverantwortlichen aus 49 Ländern ausgewertet. Ein Ergebnis der Studie war u.a. eine Übersicht über die ergriffenen Abwehrmaßnahmen.

Maßnahmen	**Deutschland** in %	**weltweit** in %
Anti-Viren-Software	95	95
Firewall	69	76
Automatisches Backup	63	55
Intrusion Detection System	15	37
Virtual Private Network	17	27
Evaluierungs-Software	9	16

Es ist auffallend, dass es zwischen dem Einsatz von Intrusion Detection Systemen (IDS oder ID-Systeme) in Deutschland und weltweit die größten Unterschiede gibt. Die Antwort auf eine weitere Frage, wie die Verantwortlichen von einer Sicherheitsverletzung erfahren haben, lässt ebenfalls aufhorchen.

Alarmauslöser	**1998** in %	**1999** in %
Kollege	47	48
Analyse von Logdateien	40	45
Intrusion Detection System	29	41

Daten-/Materialschaden	41	37
Kunden/Zulieferer	14	15

Die Zahlen lassen darauf schließen, dass ID-Systeme gut geeignet sind, um die Sicherheit der IT-Installationen zu erhöhen. Angesichts der Zahlen gehe ich davon aus, dass die Zahl der Installationen und die Bedeutung von ID-Systemen in Deutschland in den nächsten Jahren zunehmen wird. Gleichwohl sollten ID-Systeme nicht isoliert von anderen Bausteinen zur Verbesserung der IT-Sicherheit gesehen werden. Sie gehören zusammen mit einer Firewall, Systemen zur Kontrolle von Kommunikationsinhalten (Virenschutz, Blockieren von aktiven Inhalten usw.), zur Verschlüsselung und zur Authentisierung zu den Komponenten, die Netzwerke absichern helfen.

10.3.2
Funktionsweise von Intrusion Detection Systemen

ID-Systeme können je nach technischem Ansatz Eindringversuche erkennen, während sie stattfinden, oder sie weisen im Nachhinein erfolgreiche Angriffe nach. Es lassen sich drei Funktionsweisen unterscheiden.

Die erste Funktionsweise, zu der Produkte auf dem Markt verfügbar sind, orientiert sich an bekannten Angriffsmustern und den dazugehörigen Merkmalen, an denen sie erkannt werden können. Dazu untersucht das ID-System laufend den Kommunikationsverkehr in einem Netzwerk und die Abläufe auf den zugehörigen Rechnern.
Es erfolgt ein Abgleich zwischen Protokollen und einer Datenbank, in der zu möglichen Angriffen die Merkmale hinterlegt sind. Hier gibt es eine Analogie zu Virenscannern. Das IDS reagiert entsprechend den Vorgaben (Policy) auf erkannte Vorfälle. Die Güte des Systems steht und fällt mit den in der Musterdatenbank gespeicherten Merkmalen, da nur auf bekannte Strukturen reagiert werden kann. Dieser Ansatz erlaubt es, Eindringversuche festzustellen, während sie stattfinden.

Eine weitere Funktionsweise besteht darin, unzulässige Veränderungen an Dateien zu erkennen. Die Erfahrung hat gezeigt, dass erfolgreiche Angriffe mit Änderungen an Systemdateien und an bestimmten anderen Stellen einhergehen. Bei diesem Verfahren werden die Dateien definiert, die kontrolliert werden sollen. Zu jeder Datei werden mehrere

Hashwerte erzeugt. Zu vorgegebenen Zeitpunkten werden dann zu den Dateien wieder die Hashwerte berechnet. Weichen die errechneten und die alten Hashwerte von einander ab, so ist das ein Hinweis auf einen möglichen Angriff. Bei dieser Methode werden Angriffsversuche hingenommen. Man kann aber feststellen, ob Attacken stattgefunden haben. Es gibt Produkte, die diesen Ansatz verfolgen.

Eine dritte Funktionsweise, zu der mir keine marktgängigen Produkte bekannt sind, basiert auf der Idee, das Verhalten von Benutzern oder Systemen zu registrieren. Es wird Alarm geschlagen, wenn Abweichungen von dem bisherigen Verhalten auftreten. Der Vorteil dieses Ansatzes liegt darin, dass auch ein Angriff mit unbekanntem Muster erkannt wird. Hierdurch findet eine laufende Verhaltenskontrolle statt.

ID-Systeme können auch danach klassifiziert werden, an welchen Stellen Informationen gewonnen werden und wo Komponenten installiert werden müssen. Man unterscheidet netz- und hostbasierte Systeme.

Die netzbasierten Systeme greifen wie ein Netzscanner auf den Datenstrom zu, der im Rahmen der Kommunikation in einem Netz stattfindet. Die dort übertragenen Datenpakete werden analysiert. Auch wenn die Daten in der Regel keine Benutzerkennungen, sondern die Netzwerkadressen der Rechner umfassen, handelt es sich doch um personenbezogene Daten, da vom Rechner auf die Person geschlossen werden kann. Die gespeicherten Daten lassen folglich Rückschlüsse auf die Tätigkeit von Mitarbeitern zu.

Viele Netzwerke sind in kleine und kleinste Teilnetze aufgegliedert, die jeweils nur die für das Teilnetz bestimmten Datenpakete erhalten. Die Komponenten, die dies bewerkstelligen, sind sogenannte Switche. In einem derartigen Netzwerk gibt es außer bei den Switchen selbst keine Stelle, an der die Kommunikation von mehr als einem Teilnetz abgehört werden kann. Ein Zugriff auf die Daten muss sich daher auf die Switche konzentrieren, die oft keine entsprechenden Schnittstellen haben. Ein weiterer Flaschenhals entsteht durch das große Datenvolumen, das kontrolliert werden muss. Bei Netzen mit hohen Datenraten kann es schwierig sein, die Daten in Echtzeit zu verarbeiten. Eine Auswertung von Daten mehrerer Teilnetze erfordert also eine vorherige Filterung. Schließlich sind meist Rechner mit unterschiedlichen Betriebssystemen vernetzt. Bei der Definition der Angriffsmuster kann es

Probleme geben, da ein Systemverhalten in einem System normal, im anderen Fall als Angriff zu werten ist.

Hostbasierte Systeme nutzen bei den derzeit verfügbaren Systemen die bereits systemseitig vorhandenen Protokolldaten. Dabei werden u.a. Benutzerkennungen und Aktionen erfasst. Die Alarmierungs- und Auswertungskomponente ist hier der wesentliche Vorteil eines IDS.

10.3.3
Datenschutzrechtliche Wertung

Die ausgewerteten personenbezogenen Daten sind entweder Protokolldaten, die auf Rechnern zur Datenschutzkontrolle oder zur Systemkontrolle gespeichert wurden, oder Daten, die als Ergebnis der Filterung des gesamten Datenverkehrs im Netz angefallen sind. Der Einsatz darf nur zu dem Zweck erfolgen, die Sicherheitsziele aus § 10 Abs. 2 HDSG zu erreichen, insbesondere die Benutzerkontrolle und die Datenverarbeitungskontrolle.

Die Kehrseite der Systeme liegt darin, dass aus den Daten Aussagen zur Leistung oder zum Verhalten von Beschäftigten und anderen berechtigten Nutzern abgeleitet werden können. Vor allem wenn Verhaltensprofile zu Personen erstellt werden, wie es das dritte Funktionsprinzip explizit vorsieht, entstehen laufend fortgeschriebene Bestände an sensiblen Daten. Aus datenschutzrechtlicher Sicht ist die Zweckbindung dieser Daten besonders wichtig. Für die von ID-Systemen erzeugten und ausgewerteten Daten findet die spezielle Zweckbindungsregelung des § 13 Abs. 5 HDSG Anwendung.

§ 13 Abs. 5 HDSG

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

Die Verarbeitung von Mitarbeiterdaten wird durch § 34 Abs. 6 HDSG stark eingeschränkt. Danach dürfen Daten der Beschäftigten, die im Rahmen der Durchführung der technischen

und organisatorischen Maßnahmen nach § 10 Abs. 2 gespeichert werden, nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden. Für Zwecke der Strafverfolgung können die Daten allerdings genutzt werden.

10.3.4
Anwendungskriterien

Die datenschutzrechtlichen Vorgaben müssen durch technische und organisatorischen Maßnahmen umgesetzt werden. Eine Maßnahme besteht darin, gezielte Auswertungen nach Personen nur nach dem 4-Augen-Prinzip vorzunehmen und festzulegen, wie der Personalrat und der behördliche Datenschutzbeauftragte in das Verfahren eingebunden sind.

Bei ausreichender Sicherheit gegen Leistungs- und Verhaltenskontrollen gibt es keine datenschutzrechtlichen Hindernisse gegen den Einsatz. Im Gegenteil. Als Teil eines Gesamtsystems können ID-Systeme die Sicherheit bei der Verarbeitung von Daten verbessern und damit auch den personenbezogenen Datenschutz fördern.

Informationen zu technischen Details und Anforderungen können beispielsweise beim BSI abgerufen werden.: www.bsi.bund.de.

10.4
SAP R/3

An den Hessischen Hochschulen wird die kaufmännische Buchführung eingeführt. Zur Unterstützung wurde das Programm SAP R/3 ausgewählt. Eine verbesserte Ablauforganisation wird dadurch erwartet, dass weitere Funktionsbereiche durch die in SAP R/3 integrierten Module unterstützt werden. Dies betrifft beispielsweise die Personalwirtschaft. In dem Projekt muss eine Vorabkontrolle vorgenommen werden. Die dazu begonnenen Aktivitäten begleitet meine informationstechnische Abteilung.

10.4.1

Die Entscheidung der Hochschulen für SAP R/3

Die Hessische Landesregierung ist bestrebt, eine moderne und leistungsfähige Verwaltung aufzubauen. Eine Komponente ist die Einführung eines kaufmännischen Rechnungswesens. Die Hochschulen sind in diesem Bereich die Vorreiter. Sie sollen ein leistungsorientiertes Budgetsystem auf Basis der doppelten Buchführung mit Kosten- und Leistungsrechnung, ergänzt um ein internes und externes Berichtswesen mit Controlling, erhalten. Zur Unterstützung der Ziele wurde ein DV-System ausgeschrieben. Als Ergebnis wurde das Verfahren SAP R/3 (**S**ysteme, **A**nwendungen und **P**rodukte in der Datenverarbeitung; **R**ealtime"; "**3**" steht für die Nutzung von Anlagen der mittleren Datentechnik als Hardwareplattform) mit den Modulen FI, FM, CO, MM und HR ausgewählt. Dieses Produkt der Firma SAP ist im Bereich der betriebswirtschaftlichen Standardsoftware auf dem Weltmarkt führend.

Die Einführung wird im Rahmen des Projektes "Modellprojekt Hochschul-Programmhaushalt" im Teilprojekt HR/3 vorgenommen.

Vor der Einführung des Verfahrens SAP R/3 muss nach § 7 Abs. 6 HDSG untersucht werden, ob Gefahren für die Rechte der Betroffenen auf informationelle Selbstbestimmung existieren. Nur wenn die Gefahren nicht bestehen oder durch technische und organisatorische Maßnahmen verhindert werden können, darf das Verfahren eingesetzt werden. Diese Untersuchung wird von meinen informationstechnischen Mitarbeiterinnen und Mitarbeitern begleitet. Dies betrifft auch die Frage, ob die rechtlichen Rahmenbedingungen eingehalten werden, und die Erstellung eines Sicherheitskonzeptes.

10.4.2
Technik von SAP R/3

SAP R/3 nutzt eine Client-Server-Technik (vgl. 25. Tätigkeitsbericht, Ziff. 20.2), bei der die Datenbanken auf den dafür vorgesehenen Servern laufen, während an den Arbeitsplätzen PCs zum Einsatz kommen. SAP R/3 unterstützt verschiedene Betriebssysteme. Häufig werden Windows NT und UNIX-Derivate eingesetzt. Zur Datenhaltung werden relationale Datenbanken genutzt, die die Daten in Tabellenform speichern. Es werden die

Datenbankmanagementsysteme verschiedener Hersteller unterstützt, wie ORACLE, IBM, Software AG oder Microsoft.

Das Gesamtsystem ist sehr umfangreich und nur mit einer ausgiebigen Schulung zu verstehen. Die Komplexität soll durch einige Zahlen verdeutlicht werden. In der Datenbank sind über 10.000 Tabellen, jede mit zahlreichen Datenfeldern definiert, die selbst teilweise aus logischen Tabellen bestehen. Diese logischen Tabellen sind zwar R/3 bekannt, das Datenbanksystem kann sie aber nicht unterscheiden. So besteht die Tabelle ATAB aus 2000 logischen Tabellen. Eingegebene Daten werden gleichzeitig an vielen Stellen verarbeitet. Nach dem Stand der Version 4.5B wird in 1822 Modulen der Kundenstamm angesprochen, in 1621 Fällen der Lieferantenstamm, in 2496 Fällen die Adressverwaltung der Firmendaten. Die Personalnummer eines Bediensteten taucht 431 mal auf, der Name eines Benutzers 554 mal und der Benutzername 112 mal. Wenn die Felder der Personalstammdaten (PA0*) mit ihrer Kurzbeschreibung ausgedruckt werden, ergeben sich ca. 660 Seiten und ca. 4600 Seiten zusammen mit der Felddokumentation.

Das System kann in weitem Rahmen den Bedürfnissen der Dienststellen angepasst werden. Dazu wird aufbauend auf den Vorgaben ein Referenzmodell erstellt, das dann Grundlage der Verarbeitung wird.

10.4.3
Sicherheitskonzepte zum Betrieb von SAP R/3

10.4.3.1
Allgemein

Es gibt eine Reihe von Leitfäden, die die Firma SAP bzw. Kundenarbeitskreise erarbeitet haben, um die Erstellung von Sicherheitskonzepten zu unterstützen. Besonders soll hier auf den "SAP Sicherheitsleitfaden R/3", den "Leitfaden Datenschutz für SAP R/3" und den "SAP-Prüfleitfaden R/3 FI" hingewiesen werden.

Das Beratungsunternehmen, das die Hochschulen unterstützt, hat darüber hinaus einen Leitfaden zum Thema Datenschutz und Datensicherheit erstellt, der auf die Anforderungen der Hochschulen abgestimmt war. Die Aussagen bezogen sich auf die Themen

- Benutzerauthentifizierung
- R/3-Berechtigungskonzept
- Netzwerk-Infrastruktur
- Schutz des Betriebssystems
- Schutz der Zugriffe auf die Datenbank
- Schutz des Produktivsystems
- Remote Communications
- Secure-Store-&-Forward Mechanismen (SSF) und digitale Signaturen
- Protokollierung und Prüfung und
- Spezielle Themen

An dieser Stelle können nicht alle Punkte angesprochen werden, die wichtig sind und zu denen ich Stellung genommen habe. Ich will mich auf die folgenden Feststellungen beschränken, die weitgehend mit den Aussagen des Beratungsunternehmens übereinstimmen:

- Die von SAP standardmäßig vorgenommenen Einstellungen zur Benutzerauthentifizierung müssen aus datenschutzrechtlicher Sicht teilweise geändert werden. Dies gilt z.B. für die Mindestlänge und die Gültigkeitsdauer des Passwortes (vgl. 19. Tätigkeitsbericht, Ziff. 15.5.4).

- Im Berechtigungskonzept muss festgelegt werden, welche Benutzer welche Aufgaben ausführen. Danach sind die Berechtigungen zu vergeben. Die Fortschreibung ist ein stetiger Prozess.

- Die Aufgaben, die bei der Pflege der Berechtigungen anfallen, müssen auf mehrere Verwalter aufgeteilt werden. Die Empfehlungen unterscheiden sich im Zuschnitt der Aufgaben, wenn manuell oder programmtechnisch unterstützt die Berechtigungen gepflegt werden. Der Leitfaden schlägt in beiden Fällen eine Verteilung auf drei Verwalter vor. Der Vorschlag beinhaltet auch eine detaillierte Aufgabenzuordnung.

- In einem Revisionskonzept, das Teil des Sicherheitskonzepts sein kann, muss beschrieben werden, wer wann welche Protokolle und Informationen wie kontrolliert.
  Als Hilfsmittel stehen das "Infosystem Berechtigungen", das "Audit-Informationssystem (AIS)", das "Security-Audit-Log", die Systemprotokolle, die "Tagesstatistik im CCMS" und die Protokollierung von spezifischen Aktivitäten zur Verfügung.
  Das AIS wurde von SAP speziell zur Unterstützung der Datenschutzkontrolle und verwandter Funktionen entwickelt. Es gibt Informationen über Systemkonfiguration, Repository, Security-Konfiguration und Berechtigungen.
  An spezifischen Protokollen gibt es die Anwendungsprotokollierung, die Protokolle beim Ausführen des Workflow, Protokolle über Änderungsbelege, Protokolle über Datenänderungen in Tabellen sowie Protokolle über Änderungen an Benutzerstammsätzen, Profilen und Berechtigungen. Das letzte Protokoll erlaubt es, die Dokumentation im Rahmen der Benutzer- und der Zugriffskontrolle vorzunehmen, während die ersten vier Protokolle Grundlage der Verantwortlichkeitskontrolle sein können.

- Sachgerecht ist eine Netzwerktopologie, bei der die R/3-Anwendungsserver und die Datenbankserver in einem eigenen Subnetz betrieben werden. Für Systeme mit verschiedenen Sicherheitsgraden sollten separate lokale Netze eingerichtet werden. Der Zugriff soll nur über Router/Paketfilter und den SAProuter erfolgen können. Hinweise zum Einsatz von Firewalls werden ebenfalls gegeben.

- Zum Schutz der Daten bei der Übertragung im Netz wird eine Verschlüsselung vorgeschlagen.

- Zur Sicherheit von R/3 unter Windows-NT sollte eine Domäne für Clients und eine Domäne für die Server und Systembetreuer eingerichtet werden.

- Damit die Zugriffsschutz- und Protokollierungsmechanismen von SAP greifen, dürfen nur die R/3-Werkzeuge genutzt werden, um Anpassungen an der Datenbank vorzunehmen.

- Um das Produktivsystem gegen beabsichtigte und unbeabsichtigte Programmänderungen zu schützen, müssen getrennte Test-, Qualitätssicherungs- und Produktionssysteme

existieren. Die Vorgehensweise, wie Programme in Produktion übernommen werden können, ist detailliert zu regeln.

10.4.3.2
Umsetzung durch die Hochschulen

Die Hessischen Hochschulen sehen in ihren IT-Konzepten einen unterschiedlichen Ansatz zum Betrieb von SAP R/3 bei den Universitäten und den Fachhochschulen vor. Während die Universitäten dezentral in ihrem eigenen Rechenzentrum das SAP-System betreiben wollen, haben die Fachhochschulen ein gemeinsames Rechenzentrum eingerichtet. Die Server befinden in der FH Darmstadt. Stellvertretend für alle Fachhochschulen hat die FH Darmstadt ein Sicherheitskonzept erstellt, das von den anderen Hochschulen mit entsprechenden Anpassungen übernommen werden kann.

10.4.3.2.1
Das Sicherheitskonzept der Fachhochschulen

Den Mitarbeitern der Verwaltungen wird im Rahmen der Einführung von SAP R/3 der Zugriff auf den SAP-Server am Standort der FH Darmstadt ermöglicht. Die Verbindung der Standorte erfolgt über unsichere Netze. Da es sich grundsätzlich um sensible Daten handelt, müssen die Verwaltungsnetze geschützt und die Daten verschlüsselt übertragen werden.
Bei der Erstellung des Sicherheitskonzeptes wurden die Kommunikationsanforderungen und die Sicherheitsanforderungen der beteiligten Fachhochschulen untersucht und auch die mittelfristige Entwicklung der FH-System- und Anwendungslandschaft in Betracht gezogen.

Durch geeignete Migrationspfade, Ausnutzung von Synergieeffekten, Investitionsschutz und Vermeidung von Insellösungen, die nicht problemlos ausgeweitet werden können, wird der Aufwand für Investitionen und den Betrieb minimiert.

Am Beispiel der Sicherung der Kommunikation und der Sicherung der Rechner sollen die Ansätze des Sicherungskonzepts erläutert werden.

Sicherung der Kommunikation

Eine Absicherung der Kommunikation über unsichere Netze kann nur durch Verschlüsselung erfolgen. Hier können drei verschiedene Verfahren zum Einsatz kommen:

a) Gateway to Gateway-Verschlüsselung
Bei diesem Verfahren werden Systeme mit verschiedenen Sicherheitsgraden und unterschiedlicher Schutzbedarf in Gruppen gleicher oder ähnlicher Systeme in eigenen Netzsegmenten zusammengefasst. Die Kommunikation erfolgt kontrolliert über Firewallsysteme (Anforderungen an Firewall s. 27. Tätigkeitsbericht, Anhang 2). Zwischen derartig kontrollierbaren Netzen kann mittels Verschlüsselungstechnologie ein Tunnel hergestellt werden. Dieses Verfahren ist sehr zu empfehlen, da die sicherheitstechnische Relevanz hauptsächlich auf der "Firewall" und der verwendeten Verschlüsselungstechnologie liegt. Die Administrierbarkeit ist überschaubar, da nicht beliebig viele Systeme einer Gefährdung ausgesetzt sind.

b) Client to Gateway-Verschlüsselung
Die Verschlüsselung wird zwischen einem einzelnen Host und dem Client-Rechner aufgebaut. Hier ist lediglich die Kommunikation geschützt. Der Client selbst ist nicht geschützt und befindet sich im ungünstigsten Fall permanent im unsicheren Netz. Vorteile dieser Lösung liegen lediglich in der großen Flexibilität auf der Clientseite und den niedrigen Kosten.

c) Client to Serverebene
Eine weitere Sicherheit bietet die Einführung einer Applikationssicherheit, das bedeutet starke Authenisierung und Verschlüsselung auf der Applikationsebene. Der Tunnel endet dann nicht am Firewall, sondern direkt am SAP R/3 System.

Hinsichtlich der technischen Realisierung der Kommunikation kommen die Varianten a) und c) zum Einsatz. Im Regelfall wird die Variante c) genutzt. Nur in den Fällen, in denen ein reines Verwaltungsnetz vorhanden ist, das durch eine Firewall geschützt wird, kommt die Variante a) zum Tragen.

Sicherung der Rechner

Neben der Sicherung der Kommunikation müssen insbesondere die Arbeitsplatzrechner sicher betrieben werden. Die Rechner selbst müssen sicher konfiguriert werden. Folgende Maßnahmen werden bei dem Konzept vorgesehen.

Grundkonfiguration des Rechners

durch:

- Bootschutz des Rechners durch Vergabe eines Bios-Passwortes
- Physikalischer Zugangsschutz zum Rechner (Schlüssel, Identifikationstechnik)
- Zugriffskontrolle mittels Smart-Card

Grundkonfiguration Betriebssystem

- Einsatz von Windows-NT in der jeweils aktuellen Version mit neuestem Service-Pack
- Einstellung der Rechner auf C2-Security

Grundkonfiguration der Softwareausstattung

- Zentral administrierbare Virenschutzsoftware wird eingesetzt und ständig aktualisiert
- Durch Anpassen der Registry wird verhindert, dass der Endanwender selbst Programme installieren kann.
- Es dürfen nur vorgegebene Programme installiert werden.

Administrative Vorgaben

Es werden Richtlinien erstellt, wie die IT-Struktur verwendet werden darf. Die Anwender erhalten diese zur Kenntnis.

10.4.3.2.2
Ist-Zustand

Eine Umsetzung der unter 10.4.3.1 dargestellten Vorschläge ist wegen der Besonderheiten an einzelnen Hochschulen nicht vollständig möglich. Zu Details verschiedener Sicherungsmaßnahmen dauert die Diskussion mit den beteiligten Stellen an.

10.4.3.3
Ausblick

Derzeit gibt es keine Anhaltspunkte, dass ein datenschutzkonformer Betrieb von SAP R/3 an den Hochschulen unmöglich ist. Die rechtliche Bewertung der vorgelegten Feinkonzepte zeigte keine Probleme, solange ein adäquates Sicherheitskonzept umgesetzt wird. Das bereits bestehende Sicherheitskonzept kann von der jeweiligen Hochschule als Grundlage für die zusätzlich nötigen Sicherungsmaßnahmen gewählt werden. Es würde dann auch Basis der Vorabkontrolle sein, die jede Hochschule durchführen muss. Hierzu gehört insbesondere, die Restrisiken abzuschätzen.

11. Ausländer

11.1
Smart-Card für Asylbewerberinnen und -bewerber

Die im Auftrag des Bundesministerium des Innern angefertigte Machbarkeitsstudie zum Einsatz einer Smart-Card im Asylverfahren liegt den Innenministerien und Senatoren der Länder vor. Ich habe gegenüber dem Hessischen Ministerium des Innern und für Sport eine ausführliche Stellungnahme abgegeben und dabei von einer Realisierung des Einsatzes der Smart-Card in dem von der Studie anvisierten Umfang dringend abgeraten.

Nach den Plänen des Bundesinnenministeriums soll jedem Asylbewerber obligatorisch eine Prozessor gestützte Ausweiskarte ausgehändigt werden. Die Chipkarte soll verschiedene Identifizierungsdaten, weitere Informationen zur Person, die biometrischen Daten des Fingerabdrucks, ein Lichtbild, Daten zum Asylverfahren, aber auch beispielsweise Informationen im Zusammenhang mit einer Arbeitserlaubnis, mit Leistungen nach dem Asylbewerberleistungsgesetz oder einer Gesundheitsuntersuchung enthalten. Für die verschiedenen Stellen, mit denen die Asylbewerber im Laufe der Zeit zu tun haben (Ausländerbehörden, Aufnahmeeinrichtungen, Sozialbehörden, Meldebehörden, Arbeitsämter), sind sektorale Zugriffsmöglichkeiten vorgesehen.

Meine wichtigsten Kritikpunkte gegen den Einsatz einer derartigen Smart-Card sind folgende:

11.1.1
Multifunktionalität der Karte

Die Machbarkeitsstudie sieht den Einsatz der Karte in einer Reihe verschiedener Anwendungsbereiche vor. Neben der sog. Basisanwendung, bei der es mit Hilfe des biometrischen Materials um einen Identitätsnachweis, aber auch um die Ausweisfunktion und die Dokumentation der Aufenthaltsgestattung geht, sind sog. zweckgebundene Anwendungen vorgesehen. Bei einer Reihe der Anwendungen bleibt unklar, aus welchen Gründen für Asylbewerber – anders als für Deutsche – der Einsatz der Chipkarte vorgesehen werden soll. Dies gilt beispielsweise für den Einsatz im Meldewesen, beim Zugang zum Arbeitsmarkt, der

Zuerkennung und Kontrolle von Leistungen nach dem Asylbewerberleistungsgesetz oder beim Einsatz der Smart-Card als Ersatz für den heutigen Krankenschein. Die Studie belässt es nicht bei den angeführten Verwendungsbereichen, sondern weist darauf hin, dass noch weitere zweckgebundene Anwendungen auf der Smart-Card definiert werden können.

Bei der Verwendung durch Polizeibehörden und den Bundesgrenzschutz bleibt offen, zu welchen Zwecken, welchen Voraussetzungen und in welchem Umfang gerade in diesem sensiblen Bereich ein Zugriff eingeräumt werden soll.

Für äußerst problematisch halte ich den in der Studie vorgesehenen Einsatz der Chipkarte zur Aufenthaltssteuerung. Möglich wäre eine Verpflichtung für Asylbewerber, sich mehrmals täglich bei einer Meldestelle registrieren zu lassen.

Die Fülle der zur Diskussion stehenden Informationen, die auf der Karte und dem erforderlichen Hintergrundsystem gespeichert werden sollen, laufen darauf hinaus, dass verfassungsrechtlich unzulässige Persönlichkeitsprofile erstellt werden können. Je größer der Kreis der eingebenden und abrufenden Behörden, desto größer ist die Gefahr, dass technische Zugriffssicherungen versagen. Es ist zu befürchten, dass technisch mögliche Vorkehrungen nicht in erforderlichem Maße dagegen schützen, dass unrichtige bzw. unberechtigte Eingaben und Zugriffe stattfinden.

Für keine andere Bevölkerungsgruppe besteht die Verpflichtung, eine derart multifunktionale Chipkarte bei sich zu führen und zum Zugriff für verschiedene Stellen bereitzuhalten. Deshalb drängt sich der Verdacht auf, dass es nicht nur um eine Effizienzsteigerung des Asylverfahrens geht, sondern dass über die schon existierenden Instrumente zur Kontrolle und Überwachung von Ausländern (Ausländerzentralregister, automatisiertes Fingeridentifizierungssystem) hinaus für die Gruppe der Asylbewerber ein weiterer qualitativ einschneidender Schnitt in diese Richtung unternommen werden soll.

11.1.2
Funktionsbeschränkung auf die Basisdaten

Sollte die Einführung der Karte überhaupt weiter verfolgt werden, habe ich eine Reduzierung auf die sog. Basisanwendung gefordert. Das bedeutet, dass nur die im Personalausweis üblichen Angaben, ergänzt durch elektronischen Fingerabdruck, Zuzugsdatum und zugehörige Tatsachenfeststellungen, erfasst werden.

Zusätzlich könnte allenfalls noch die Zulassung solcher zweckgebundener Anwendungen geprüft werden, die in engem Zusammenhang mit dem Asylverfahren stehen, also z.B. der Nachweis über den Verfahrensstand bei den Ausländerbehörden. Für den Fall, dass ein derartiger Einsatz der Karte geplant wird, ist allerdings darauf hinzuweisen, dass angesichts der erwarteten hohen Kosten für die Basisanwendung die Gefahr besteht, dass unter Rentabilitätsgesichtspunkten eine Ausweitung der Anwendungsbereiche versucht wird. Hier ist zu fordern, dass dies gesetzlich eindeutig ausgeschlossen wird.

11.1.3
Gesetzliche Grundlage

Die Studie hält für die Frage, ob die Karte eingesetzt wird, eine bereichsspezifische gesetzliche Grundlage für erforderlich. Allerdings ist unzureichend geklärt, inwieweit die vorgesehenen vielfältigen Kommunikationsbeziehungen durch bestehende Gesetze (z.B. §§ 7, 8 Asylverfahrensgesetz) gedeckt sind. Zum Teil müssen dafür neue gesetzliche Regelungen geschaffen werden, zum Teil werden auch bestehende Regelungen (Sozialgesetzbuch V, s. Ziff. 8.2) zu verändern sein. Erst eine sorgfältige Prüfung wird Aufschluss darüber geben, in welchem Ausmaß Neuregelungen erforderlich werden, damit Informationen über den bisherigen Stand hinaus verarbeitet werden können.

11.1.4
Zugriffsregelungen

Die Frage von abgeschotteten Zugriffsberechtigungen wird umso wichtiger, je mehr unterschiedliche Stellen Zugang zu der Chipkarte erhalten sollen. Nach der Studie haben am Asylverfahren beteiligte Behörden Zugriff, sofern die Smart-Card die Authentisierung der Behörde und das Recht zum Zugriff auf das einzelne Datum positiv beantwortet. Da die

Zugriffsmatrix fest in die Karte eingebracht werden soll und die Festlegung nur durch das Bundesamt geändert werden kann, ist wohl davon auszugehen, dass Zugriffe für alle Behörden eröffnet werden, die zu einem bestimmten Bereich (z.B. Ausländerbehörden) gehören. Deshalb stellt sich die Frage, wie technisch garantiert werden kann, dass wirklich nur die örtlich und sachlich zuständige Behörde Zugriff auf die Karte erhält, etwa durch elektronische Signatur des Mitarbeiters oder ein Identitätskennzeichen der Behörde.

11.1.5
Protokollierung

Die Protokollierung der elektronischen Datenkommunikation ist aus Gründen der Nachvollziehbarkeit von Verarbeitungsvorgängen, zur Klärung von Verantwortlichkeiten und evtl. zur Datenrekonstruktion von großer Wichtigkeit. Umso mehr befremdet, dass die Protokollierung in der Studie nur eine marginale Rolle spielt. Wesentliche Fragen bleiben unbeantwortet: Welche Daten werden genutzt, aus welchen Anlässen, in welchem Umfang? Wie lange werden sie gespeichert? Welche Nutzung der Protokolldaten wird wem erlaubt? Aus dem Datenschema der Asyl-Card selbst ist zu entnehmen, dass eine Protokollierung auf der Karte offensichtlich nicht geplant ist.

11.1.6
Transparenz für die Betroffenen

Besonders wichtig ist, inwieweit das Verfahren für die Betroffenen transparent gestaltet werden kann. Das datenschutzrechtliche Auskunftsrecht soll dadurch realisiert werden, dass die Betroffenen Kenntnis über die auf der Karte gespeicherten Daten durch Lesegeräte erhalten können. Den Asylbewerbern sollen PINS mitgeteilt werden, die nur ihnen bekannt sind und mit der alle Daten auf der Karte auf Antrag durch den Systembetreiber freigeschaltet werden können. Die Studie gibt jedoch keine Auskunft darüber, wer den Asylsuchenden und in welcher Form die PIN mitteilt. Unklar ist auch, welche Sicherungen dagegen getroffen werden, dass Unberechtigte in Kenntnis der PIN die Daten aus der Karte auslesen. Ohne Zugriffsprotokollierung ist diese Gefahr hoch. Auch die einzelnen Modalitäten der

Datenkommunikation müssen für die Betroffenen transparent sein, deshalb sollten Unterrichtungspflichten vorgesehen werden.

Schließlich müsste sichergestellt werden, dass die Betroffenen über ihre weiteren Rechte auf Berichtigung, Sperrung und Löschung der Daten informiert werden.

Grundsätzlich bestehen bei den am Asylverfahren beteiligten Personen besondere Schwierigkeiten bei der Herstellung von Transparenz. Asylbewerber haben in der Regel keine Kenntnisse von technischen und administrativen Vorgängen, hinzu kommen Sprachprobleme, die nicht immer durch die Beiziehung von Dolmetschern ausgeräumt werden können. Angesichts eines derartig komplizierten Kommunikationsverfahrens bestehen große Zweifel, ob die Betroffenen wirklich in die Lage versetzt werden können, von ihren Rechten Gebrauch zu machen.

Das Hessische Ministerium des Innern und für Sport, das sich bisher von dem Einsatz einer Smart-Card keine Vorteile versprach, hält jetzt eine Prüfung des Projekts für sinnvoll, will sich aber an einem Pilotprojekt nicht beteiligen.

11.2
Die gleichgeschlechtliche Scheinehe

Auch ein gleichgeschlechtliches Paar, das zur Erlangung der Aufenthaltserlaubnis eines Partners oder einer Partnerin, den grundgesetzlichen Schutz von Ehe und Familie in Anspruch nehmen möchte, muss eine sog. Scheinehenüberprüfung hinnehmen, wenn die Ausländerbehörde berechtigte Zweifel am Vorliegen der eheähnlichen Beziehung hat.

Ein hessischer Bürger bat mich zu folgendem Sachverhalt um eine Stellungnahme: Bedienstete der Ausländerbehörde hätten von ihm nähere Angaben zu seinem Sexualleben erfragt. Zuvor hatte er die Polizei über eine gleichgeschlechtliche Beziehung zu einem polnischen Staatsangehörigen informiert. Damit stand in Widerspruch, dass er gegenüber der Ausländerbehörde Angaben über eine gleichgeschlechtliche Beziehung zu einem rumänischen Staatsangehörigen gemacht hatte. Er fragte mich, auf welche Weise die Ausländerbehörde

über Angaben Kenntnis erhielt, die er gegenüber der Polizei gemacht hatte. Weiterhin wollte er wissen, ob die Fragen nach seinem Sexualleben rechtens gewesen seien.

Der Sachverhalt war so widersprüchlich, dass ich bei der Ausländerbehörde und der Polizei zu allen Beteiligten - soweit vorhanden - Akteneinsicht nahm. Danach lebte der Betroffene seit Jahren mit einem rumänischen Staatsangehörigen in einer eheähnlichen Beziehung. Der Aufenthalt des Rumänen in der Bundesrepublik war nicht legal. Er sollte ausgewiesen werden. Dagegen wehrte dieser sich mit dem Argument, seine Lebensbeziehung zu dem Deutschen sei eheähnlicher Art. Er und sein deutscher Lebenspartner fühlten sich aufgrund ihrer sexuellen Neigung diskriminiert, denn wenn die Beziehung nicht gleichgeschlechtlich wäre, könnten sie heiraten. Die Ausländerbehörde stimmte dieser grundsätzlichen Argumentation zu. Sie verlangte aber, dass der Rumäne seinen Aufenthalt legalisiert. Eine Prüfung, ob der Schutz von Ehe und Familie die Erteilung der Aufenthaltsgenehmigung gebiete, setze einen legalen Aufenthalt voraus. Der Rumäne solle ausreisen und dann vom Ausland aus einen Einreiseantrag stellen. Das geschah auch.

Aus den Akten der Polizei ergab sich, dass der beschwerdeführende Bürger eine Strafanzeige gegen einen polnischen Staatsangehörigen gestellt hatte. Aus der Strafanzeige ging hervor, dass er mit dem Polen einige Zeit in seiner Wohnung in einer homosexuellen Beziehung gelebt hatte. Als diese Beziehung endete, verschwand der Pole unter Mitnahme einiger Wertgegenstände. Deshalb erfolgte die Anzeige bei der Polizei. Der Täter wurde nicht gefasst.

Eines Tages sah der Bürger den Polen zufällig in seiner Heimatstadt, ging sofort zur Polizei, machte auf die damalige Anzeige aufmerksam und wies auf den augenblicklichen Aufenthalt des Gesuchten hin. Dabei wiederholte er noch einmal seine Angaben zu der beendeten homosexuellen Beziehung zu dem Polen. Die Polizei nahm den polnischen Staatsangehörigen fest und verhörte ihn.

Wenige Tage zuvor war in einer großen deutschen Boulevardzeitung ein umfangreicher Bericht mit Namensnennung und Abbildungen des Deutschen und des Rumänen erschienen, in dem die beiden als trautes Paar dargestellt wurden. Der Artikel suggerierte, dass die Ausländerbehörde der Beziehung des Paares im Wege stehe. Zufällig wurde der Bericht auch von dem Polizeibeamten gelesen, der die Strafanzeige gegen den Polen bearbeitete. Die zutage getretenen Widersprüche veranlassten ihn, einen Auszug aus der Strafsache

anzufertigen und der Ausländerbehörde zur Verfügung zu stellen. Diese wiederum nahm die Information zum Anlass, eine sog. Scheinehenüberprüfung (25. Tätigkeitsbericht, Ziff. 13.2) vorzunehmen.

Die weitere Aufklärung machte klar, dass ich die Datenübermittlung der Polizei an die Ausländerbehörde nicht beanstanden kann. Sie war nach § 22 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung zulässig. Danach dürfen u.a. Polizeibehörden personenbezogene Daten an andere Gefahrenabwehrbehörden - hier die Ausländerbehörde - übermitteln, wenn dies zur rechtmäßigen Aufgabenerfüllung des Datenempfängers erforderlich erscheint.

Auch die nachfolgende Verwertung dieser Information durch die Ausländerbehörde - die Scheinehenüberprüfung -, war nicht zu beanstanden. Der hessische Bürger und der Rumäne hatten sich gegenüber der Ausländerbehörde als ein in eheähnlicher Beziehung lebendes Paar vorgestellt. Sie stützten den Antrag auf Aufenthaltserlaubnis auf den im Grundgesetz gewährten Schutz von Ehe und Familie und verlangten Gleichbehandlung der Beziehung mit einer ehelichen Lebensgemeinschaft. Bei begründeten Zweifeln darf die Ausländerbehörde prüfen, ob die eheliche Lebensgemeinschaft tatsächlich vorliegt und nicht - etwa nur zur Erlangung einer ausländerrechtlichen Erlaubnis - vorgegeben wird. Dies muss auch für die eheähnliche Lebensgemeinschaft gelten. Eine solche Prüfung, die die Persönlichkeitsrechte und die datenschutzrechtlichen Belange der Betroffenen erheblich tangiert, darf sie nur in Fällen vornehmen, in denen ernste Zweifel am Vorliegen einer ehelichen bzw. eheähnlichen Lebensgemeinschaft bestehen. Durch die Mitteilung der Polizei lag ein solcher Anlass vor. Deswegen musste der Betroffenen diese Erhebung und die weitere Verarbeitung seiner personenbezogenen Daten hinnehmen.

12. Melderecht

Kein Abgleich von Melderegisterdaten mit Klingel- und Haustürschildern

Die Vermutung einer mangelhaften Meldemoral vor allem unter Studierenden und die daraus resultierenden Nachteile beim Finanzausgleich rechtfertigen keinen flächendeckenden Abgleich örtlicher Klingelschilder mit den Eintragungen im Melderegister. Diese Maßnahme ist weder melderechtlich vorgesehen noch datenschutzrechtlich zulässig.

Durch die Anfrage eines Journalisten wurde ich auf folgenden Sachverhalt aufmerksam:

Der Oberbürgermeister einer hessischen Universitätsstadt stellte durch Auswertung der Bevölkerungsstatistik fest, dass nicht alle in der Stadt wohnenden Einwohnerinnen und Einwohner im Melderegister erfasst sind. Die Meldebehörde vermutete, dass insbesondere Studierende an der Universität ihrer Meldeverpflichtung nicht nachkommen. In bestimmten Wohngebieten war die Einwohnerzahl gesunken, ohne dass ein Wohnungsleerstand oder eine Wohnraumvernichtung zu verzeichnen war. Daraufhin wurde ein Mitarbeiter des Stadtbüros, das auch die einwohnermelderechtlichen Aufgaben wahrnimmt, in die betreffenden Wohngebiete entsandt, um die an Brief- und Klingelanlagen vermerkten Namen aufzunehmen. Die aus den örtlichen Überprüfungen resultierenden Namenslisten wurden im Stadtbüro mit den im Melderegister verzeichneten Einwohnerdaten abgeglichen. Konnte eine bestimmte Person nicht als gemeldet ermittelt werden, erhielt diese ein Schreiben mit der Bitte, sich mit dem Stadtbüro in Verbindung zu setzen. Auf diese Weise wurden 17 Straßen überprüft. Nach Schätzung des Oberbürgermeisters waren ca. 10.500 Wohnungen betroffen. 700 Personen wurden angeschrieben. Mit Stand vom 22. Februar 1999 wurden 59 Einwohner mit einer Anmeldung als Hauptwohnung und 197 mit einer Nebenwohnung neu erfasst.

Diese Art der Beweiserhebung findet auch im Hessischen Meldegesetz (HMG) keine förmliche Rechtsgrundlage und ist datenschutzrechtlich unzulässig. Gemäß § 1 Abs. 2 HMG darf die Meldebehörde personenbezogene Daten, die im Melderegister gespeichert werden, n u r nach Maßgabe dieses Gesetzes oder sonstiger Rechtsvorschriften verarbeiten. Die melderechtliche Datenerhebung kann entweder direkt bei den Einwohnerinnen oder Einwohner erfolgen (§ 13 Abs. 1 HMG) oder durch Auskunftsverlangen gegenüber den Wohnungsgebern (§ 20 HMG). Ferner können Tatsachen berücksichtigt werden, die von

anderen Behörden oder sonstigen öffentlichen Stellen mitgeteilt werden. Die Berichtigung unrichtiger Daten kann im Einzelfall, d.h. zielgerichtet erfolgen, wenn ein konkreter Anlass besteht (z.B. Rücklauf einer Wahlbenachrichtigung, Rücklauf von Postsendungen, Hinweis eines Wohnungsgebers oder dessen Nachbarn).

Eine flächendeckende Erhebung personenbezogener Daten ohne Kenntnis der Betroffenen sieht das Hessische Meldegesetz nicht vor, auch wenn sie auf eine Gruppe beschränkt sein sollte. Zu den nach dem Meldegesetz zugelassenen Erhebungstechniken gehört das Aufsuchen der Wohnhäuser durch städtische Bedienstete nicht. Da die Art und Weise der Datenerhebung durch die Meldebehörden im Gesetzgebungsverfahren umstritten war, kommt der beschränkenden Formulierung in § 1 Abs. 2 HMG rechtsnormativ ernstzunehmende Bedeutung zu.

§ 1 Abs. 2 HMG
Die Meldebehörden dürfen personenbezogene Daten, die im Melderegister gespeichert werden, nur nach Maßgabe dieses Gesetzes oder sonstiger Rechtsvorschriften verarbeiten.

Ich übersehe nicht, dass das mangelhafte Meldeverhalten die Qualität des Melderegisters beeinträchtigt und auch zu Nachteilen der Stadt im Finanzausgleich führen kann. Zweck und Ziel des Melderechts schließen es jedoch aus, Probleme des Finanzausgleichs über das Melderecht zu lösen (so auch Erlass des Hessischen Ministeriums des Innern vom 6. Juni 1991 – III A 31 – 23a02). Der gesetzeskonforme Weg, dem Fehlverhalten entgegenzuwirken, ist vorrangig in der Einschaltung der Wohnungsgeber zu suchen. Sie sind gemäß § 14 HMG verpflichtet, an der Anmeldung ihrer Wohnungsnehmer mitzuwirken, und müssen bei fehlender Anmeldung eine eigenständige Meldung vorzunehmen (Abs. 2). Der Verstoß gegen diese Verpflichtung ist eine Ordnungswidrigkeit. Die Vorschrift ist deswegen leicht durchsetzbar. Außerdem sind die Wohnungsgeber verpflichtet, auf schriftliche oder telefonische Anfragen durch die Stadt Auskunft zu erteilen (§ 20). Unter Hinweis auf diese Vorschrift können Wohnungseigentümer oder sonstige Berechtigte angeschrieben werden. Bei Versagen dieser üblichen Form von Auskunftsverlangen können sie auch direkt vor Ort nach dem Bestehen von Mietverhältnissen oder dem Aufenthalt nicht gemeldeter Personen befragt werden. Bei dieser Form der Sachverhaltsermittlung muss allerdings offen vorgegangen werden. Sofern bestimmte Wohnbezirke als ganze aufgesucht werden, muss der ermittelnde Bedienstete sich an den Wohnungstüren als Ermittler ausweisen, um die

betroffenen Bürger in Kenntnis über Sinn und Zweck der Ermittlungstätigkeit zu setzen. Die so aktualisierten Auskunftspflichten können notfalls mit Verwaltungszwang durchgesetzt werden.

Soweit § 1 Abs. 2 HMG eine ergänzende Heranziehung anderer Vorschriften vorsieht, kommen auch die Ermächtigungsnormen des Datenschutzgesetzes in Betracht, denn die Feststellung von Namen an Klingelschildern ist Erheben von Daten und damit eine Datenverarbeitung nach dem Hessischen Datenschutzgesetz. Zwar sind die Haus- und Klingelschilder nach außen gerichtet angebracht, um Erreichbarkeit und z.B. Postzustellung zu ermöglichen, sie dienen jedoch nicht den Zwecken einer kommunalen Überwachungsbehörde. Weiterhin werden bei der Nutzung der so gewonnenen Daten durch Abgleich mit dem Melderegister personenbezogene Daten verarbeitet. § 7 Abs. 1 Nr. 1 Hessisches Datenschutzgesetz (HDSG) macht die Zulässigkeit der Verarbeitung personenbezogener jedoch davon abhängig, dass das Spezialgesetz - hier das HMG – die Maßnahme „zwingend voraussetzt“. Diese Anforderung kann allenfalls als erfüllt angesehen werden, wenn konkrete Anhaltspunkte für ein ordnungswidriges Verhalten bereits vorliegen, bevor Sachverhaltsermittlungen vor Ort stattfinden. Für die hier vorliegende praktizierte Vorgehensweise, ganze Straßenzüge oder Stadtviertel zu erfassen und die gewonnenen Erkenntnisse einem Datenabgleich zuzuführen, fehlt es an der bei Ordnungswidrigkeiten typischen Einzelfallermittlung.

Darüber hinaus ist der datenschutzrechtlich gebotenen Transparenz des Verfahrens bei dem bisherigen Vorgehen der Stadt nicht genügt. Personenbezogene Daten sind grundsätzlich bei dem Betroffenen und mit dessen Kenntnis zu erheben (§ 12 Abs. 1 S. 1 HDSG). Auch das gebietet ein offenes Vorgehen seitens der städtischen Bediensteten. Regelmäßig wird daher ein direkter Verwaltungskontakt zwischen dem vor Ort ermittelnden Bediensteten und den betroffenen Bürgern hergestellt werden müssen.

Ich haben den Oberbürgermeister gebeten, zukünftige Datenerhebungen für das Melderegister nur im Rahmen der vorgenannten Gesetzesschranken zu veranlassen.

13. Kommunen

13.1
Umfrage zur Videoüberwachung

Eine Umfrage unter allen Städten und Gemeinden in Hessen hat ergeben, dass der Einsatz von Videoüberwachungsmaßnahmen derzeit nur in einer begrenzten Zahl stattfindet.

Im Zusammenhang mit der geplanten Einführung einer polizeilichen Videoüberwachung habe ich einen Fragebogen an die Gemeinden versandt, mit dem aufgeklärt werden sollte, wie sich die Videoüberwachung heute in tatsächlicher Hinsicht darstellt.

In dem Fragebogen, den wir versandt haben, waren folgende Fragen zu beantworten:
- Ort, Häufigkeit und Zwecksetzung von Videoüberwachungen,
- Speicherung und Speicherungsdauer,
- Auswertungsbefugnis und
- Datenschutzkonzeption
- Erstellung von Verfahrensverzeichnissen vor Beginn der Videoüberwachung.

Die Erhebung zeigte bei einem Rücklauf von 89,2 % bei Redaktionsschluss einen weithin beruhigenden Verhaltenstrend:

1. Nur 6,6 % der 378 hessischen Gemeinden, die geantwortet haben, verwenden überhaupt Videoüberwachungsanlagen. Insgesamt sind bislang 439 gemeindliche Videoanlagen angezeigt worden, wovon immerhin 142 Anlagen allein in der Stadt Frankfurt installiert worden sind. Um die Frankfurter Einrichtungen nicht in falsches Licht geraten zu lassen, sind die Einsatzformen zu erwähnen: Allein 31 Kameras dienen dem Schutz von Museen, weitere 34 Kameras der Prozessüberwachung im Abwasserbereich und 66 Kameras dem Gebäudeschutz und der Zutrittskontrolle.

2. In den meisten Gemeinden, die zur Gruppe der Anwender gehören, liegt die Zahl der installierten Anlagen unter zehn. Nur zehn Gemeinden haben zehn und mehr Anlagen aufgebaut.

3. Die meisten Videokameras sind für die Sicherung von Gebäuden, Bädern und vor allem von Parkhäusern eingesetzt. Ein weiterer Schwerpunkt liegt in der Verkehrsüberwachung, vor allem im Zusammenhang mit Geschwindigkeitsmessungen. Gerade im letztgenannten Sektor sind hinsichtlich Häufigkeit der Maßnahmen und Speicherdauer auffällige Unterschiede erkennbar.

4. Aufzeichnungen finden in etwa der Hälfte der Fälle statt. Die Speicherungszeiten liegen zwischen 24 Stunden bis zu mehreren Jahren. Die einsame Spitze im Bereich der Verkehrsüberwachung liegt in einer Rheingaugemeinde mit einer Speicherdauer von fünf Jahren.

5. Ein ausdrücklicher Hinweis auf die Tatsache der Videoüberwachung wird nur von einer Gemeinde gemeldet.

6. Das größte Erstaunen erweckte ein weiteres Ergebnis der Umfrage:
   - nur eine einzige Gemeinde hat eine Konzeption für den Datenschutz erstellt, während alle übrigen Fehlanzeige erstattet haben. Insbesondere dort, wo Aufzeichnungen und dauerhafte Speicherungen erfolgen, hätten sich die datenschutzrechtlichen Pflichten eigentlich aufdrängen müssen.

   - Verfahrensverzeichnisse, wie sie das reformierte Hessische Datenschutzgesetz (§ 6 Abs. 1) zwingend vorschreibt, existieren nur in einer einzigen Gemeinde.

7. Stärkstes Positivum der Umfrage ist der Umstand, dass eigentlich nur ein Fall Stirnrunzeln auslöst: Eine Nachbarstadt Wiesbadens hat ausgerechnet in ihrem Bürgerbüro eine Kamera installiert. Diesem Eifer werde ich nachgehen.

13.2
Gebäudeverfilmung durch eine Kommune

Die Verfilmung sämtlicher privater und öffentlicher Gebäude für die Erstellung eines kommunalen Wärmekatasters, die die Gemeinde durch ein privates Ingenieurbüro in Auftrag

gegeben hat, ist nicht zulässig. Aufgrund meiner Intervention wurde eine Verfahrensweise gewählt, die keine Erhebung personenbezogener Daten erfordert.

Aus den Videoaufnahmen sollten sich Geschosszahl, Bauvolumen, Dach- und Kellerausbau sowie Dachneigungen ermitteln lassen. Es war geplant, diese Daten anschließend für jedes Haus jeweils mit den Energieverbrauchszahlen der Versorgungsunternehmen und Messwerten der Schornsteinfeger zu verknüpfen. Aus den so zusammengetragenen Daten sollte dann nach einer Methode des Darmstädter Instituts für Wohnen und Umwelt ein Klimaschutzkonzept entwickelt werden. Auf der Grundlage dieser Ergebnisse wollte die Gemeinde interessierten Hausbesitzern gezielte Energieeinsparmöglichkeiten zur Verfügung stellen. Bei einem Teil der Bürgerinnen und Bürger dieser Stadt löste die geplante Verfilmung Unwillen aus, sie sprachen sich gegen diese Form der Datenerhebung aus und baten mich um die Bewertung der rechtlichen Zulässigkeit der Videoverfilmung und der Auswertung ihrer Verbrauchsdaten.

13.2.1
Zulässigkeit der Videoverfilmung für die Erstellung des Wärmekatasters

Anknüpfungspunkt für die datenschutzrechtliche Bewertung, ob eine Videoverfilmung in dem geplanten Umfang rechtlich zulässig ist, war die Frage nach der Erforderlichkeit dieser Art der Datenerhebung für die Verwirklichung des geplanten Wärmekatasters. Aus Gesprächen mit der Stadt wurde deutlich, dass für die Realisierung des Projekts Daten wie Gebäudealter, Geschosszahl und Dachneigungen unverzichtbar waren. Bisher waren diese Daten - wie mir die Stadt mitteilte - bei vergleichbaren Projekten durch Straßenbegehungen manuell erfasst worden.

Die Verfilmung des gesamten Häuserbestandes mit Videokameras geht als Datenerhebung weit über das hinaus, was mit den bisherigen Methoden an Daten erfasst worden war. Durch die Verfilmung werden über die formularmäßige manuelle Erfassung von Gebäudedaten hinaus weit mehr Informationen dokumentiert. Diese können im Einzelfall durchaus sensibel sein. Sie können Einblicke in Wohnbereiche oder Aussagen über Lebensgewohnheiten einzelner Bewohner geben.

Die Stadt konnte nicht rechtfertigen, dass die Videodokumentation für die Erstellung des Wärmekatasters überhaupt von zusätzlichem Nutzen sei. Orientiert an dem Grundsatz, dass

eine Datenerhebung nur in dem Umfang zulässig sein kann, in dem sie für die Aufgabenerfüllung zwingend erforderlich ist, bedeutete dies für die Gemeinde, dass die geplante Videoverfilmung aller Liegenschaften aus datenschutzrechtlichen Gründen unterbleiben musste (§ 11 HDSG).

Die Probleme lassen sich möglicherweise durch Infrarotverfilmungen, auf denen Personen nicht zu erkennen sind, vermeiden.

13.2.2
Zulässigkeit der Erhebung von Verbrauchsdaten bei den Energieversorgern und Messdaten bei den Schornsteinfegern

Das Konzept sah zudem den Abgleich mit Verbrauchsdaten vor, die von den Energieversorgern an die Stadt übermittelt werden sollten. Diese Daten sind jedenfalls bei kleineren Wohneinheiten (z.B. Einfamilienhäusern) durchaus personenbezogen. Ihre Erhebung durch die Energieversorgungsunternehmen ist zu Abrechnungszwecken erfolgt. Die Übermittlung dieser Daten für die Erstellung eines Wärmekatasters hätte eine Zweckänderung bewirkt. Die wäre nur dann zulässig, wenn eine normenklare Rechtsvorschrift dies gestattet (§§ 13 Abs. 2; 12 Abs. 2 HDSG). Zwar gibt es inzwischen eine ganze Reihe von Rechtsvorschriften, die als Regelungsziel die Förderung energiesparender Projekte und den Einsatz erneuerbarer Energien haben. Sie stellen jedoch allesamt keine Rechtsgrundlage für die Erhebung und Übermittlung personenbezogener Daten dar. Wenn neue planerische Methoden der Energieeinsparung in Zukunft verwirklicht werden sollen, muss der Gesetzgeber für gemeindliche Neuansätze eine klare gesetzliche Ermächtigung schaffen. Die Verordnungsermächtigungen des § 11 Abs. 1 S. 3 oder Abs. 2 S. 3 des Energiewirtschaftsgesetzes sind zu eng gefasst.

Indessen ist die Einbeziehung der Messdaten der Schornsteinfeger in das Konzept datenschutzrechtlich nicht zu beanstanden. § 19 Abs. 3 des Schornsteinfegergesetzes in der Fassung vom 17. August 1998 erlaubt ausdrücklich, dass die Schornsteinfeger ihre Messdaten zum Zwecke rationeller Energieverwendung an öffentliche Stellen übermitteln.

§ 19 Abs. 3 Gesetz über das Schornsteinfegerwesen

Der Bezirksschornsteinfegermeister darf die nach den Absätzen 1 und 2 erhobenen Daten aus seinen Aufzeichnungen an öffentliche Stellen übermitteln, soweit das für die Erfüllung seiner Aufgaben, die Bekämpfung der Luft-, Boden- und Gewässerverschmutzung, die rationelle Energieverwendung, die Bauaufsicht oder die Brandbekämpfung erforderlich ist. Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt worden sind. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, soweit die Daten auch dafür hätten übermittelt werden dürfen. Erfolgt die Datenübermittlung auf Ersuchen, trägt die ersuchende Behörde die Kosten der Datenübermittlung.

Die Erstellung des integrierten Klimaschutzkonzepts lässt sich hierunter einordnen.

Letztlich standen der Gemeinde zur Realisierung ihres Klimaschutzkonzeptes zwei Wege offen: Sie hätte sich dafür entscheiden können, die Videobilder und die Verknüpfung mit Verbrauchsdaten für diejenigen Hausbesitzer vorzunehmen, die ihr Einverständnis zuvor erklärt hatten. Freilich müsste die Gemeinde dann davon absehen, ein flächendeckendes Wärmekataster zu erhalten.

Als zweiter Weg stand offen, die benötigten Gebäudedaten manuell erfassen zu lassen. Außerdem hätte sich die Auswertung der Verbrauchsdaten nicht an einzelnen Haushalten, sondern an ganzen Straßenzügen orientieren müssen. So wären sie nicht mehr personenbeziehbar. Auf dieser Grundlage hätte sich nach der Methode des Instituts für Wohnen und Umwelt eine Hochrechnung vornehmen lassen, die für die Energiesparstrategie nutzbar ist. Die interessierten Hausbesitzer hätten also auf die nützliche Beratung nicht verzichten müssen- und das ohne den Einsatz einer Technologie, die viel mehr Daten erfasst, als tatsächlich für die Umsetzung des Projekts benötigt werden.

Auf meine Intervention hin hat die Gemeinde diesen zweiten Weg gewählt.

13.3
Videoüberwachung am Busbahnhof Hofheim

Die Überwachung des öffentlichen Raums durch Videokameras unter Bezug auf die allgemeine Datenverarbeitungsnorm des § 11 Hessisches Datenschutzgesetz ist unzulässig. Ich musste deshalb dem Magistrat der Stadt Hofheim mitteilen, dass die geplante Überwachung des Busbahnhofs durch den Einsatz von Videokameras datenschutzrechtlich nicht zulässig war. Fehlende bereichsspezifische Eingriffsermächtigungen für Bildspeicherungen erweisen sich insofern als rechtsstaatlich bedenkliches Defizit.

Weil die Stadt Hofheim das Gelände am Busbahnhof als unsicheren Ort ansah, plante sie den Einsatz von Videoüberwachungsmaßnahmen, um potentielle Gewalttäter abzuschrecken und dem Sicherheitsbedürfnis der Bürgerinnen und Bürger Rechnung zu tragen. Drei Kameras sollten den Platz „im Blick“ haben. Die Bilder sollten ins Rathaus übertragen und aufgezeichnet werden, ohne dass dort eine Auswertung der Bilder erfolgen sollte. Vielmehr war geplant, der Polizei im Falle eines Übergriffs/Straftat im Bereich Busbahnhof ein Auswertungsrecht der Aufzeichnungen einzuräumen.

Ich habe dem Magistrat der Stadt Hofheim daraufhin mitgeteilt, dass es sich bei den Videoaufzeichnungen um Datenerhebungen handelt, die einen nicht unerheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der von der Aufzeichnung betroffenen Bürgerinnen und Bürger darstellen. Derartige Eingriffe sind nur aufgrund einer normenklaren gesetzlichen Regelung zulässig, die gemäß § 7 Abs. 1 Hessisches Datenschutzgesetz (HDSG) entweder in einem Spezialgesetz oder im Hessischen Datenschutzgesetz selbst enthalten sein muss. Das Hessische Datenschutzgesetz selbst enthält keine Ermächtigungsnorm für einen Grundrechtseingriff dieser Intensität. Für Grundrechtseingriffe von erheblicher Bedeutung, die bei einer Überwachungsmaßnahme des öffentlichen Raums ganz sicher vorliegt, reicht die allgemeine Datenverarbeitungsnorm des § 11 HDSG als Ermächtigungsgrundlage nicht aus. Erforderlich ist vielmehr eine bereichsspezifische Sonderregelung. Soweit das Hessische Datenschutzgesetz in § 12 Abs. 1 die Videoüberwachung erwähnt, setzt es - soweit es um die Sicherung öffentlicher Straßen und Plätze geht - deren Zulässigkeit voraus. § 12 Abs. 1 HDSG regelt nur die besonderen Modalitäten der Erhebung (Offenheit, Berücksichtigung schutzwürdiger Belange betroffener Personen). Eine selbständige Ermächtigungsnorm kann daher in § 12 HDSG nicht gesehen werden.

Auch das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) enthält gegenwärtig Ermächtigungen nur für besondere Anlässe (§ 14 Abs. 1 und 2 HSOG). Dazu

gehören keine allgemeinen Überwachungsmaßnahmen. Aber selbst wenn man das Kriterium „Ansammlung“ gemäß § 14 Abs. 1 Satz 1 HSOG als erfüllt angesehen hätte, hätte die Anordnung zur Überwachung durch die Polizeibehörden erfolgen müssen, da § 14 HSOG keine Ermächtigung für die allgemeinen Behörden der Gefahrenabwehr enthält. Für eine Aufzeichnung der Daten durch die Stadt Hofheim gab es deswegen keine solche Rechtsgrundlage. Auch die Absicht, die Daten nicht durch die Stadt, sondern durch die Polizei auswerten zu lassen, änderte an dieser Einschätzung nichts; denn entscheidend für die Bewertung ist die Zuständigkeit zur Anordnung einer Videoüberwachung. Sie liegt allein bei den Polizeibehörden, soweit der öffentliche Raum erfasst werden soll.

In Zukunft wird § 14 Abs. 3 HSOG für die Polizei die Möglichkeit schaffen, zur Abwehr einer Gefahr oder wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen, öffentlich zugängliche Orte mittels Bildübertragung offen zu beobachten. Aber auch diese Regelung erlaubt es lediglich den Polizeibehörden, Videoüberwachungsmaßnahmen anzuordnen (s.a. Ziff. 5.1.1). Mit Verabschiedung des Gesetzes zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung ist damit für die Polizeibehörden mit einer ausreichenden Ermächtigungsnorm zu rechnen. Allerdings hat mir dieser Fall gezeigt, dass der Einsatz von Videoüberwachungsmaßnahmen durchaus auch in anderen Fällen geboten sein kann. Ich habe mich deshalb dafür eingesetzt, dass eine gesetzliche Regelung geschaffen wird, die es auch den allgemeinen Gefahrenabwehrbehörden ermöglicht, zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, Videokameras zu installieren, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen. Gleichwohl darf das Bedürfnis nach mehr Sicherheit nicht dazu führen, dass der Schutz der Privatsphäre völlig vernachlässigt wird. Gerade bei der Installierung von Videokameras im öffentliche Raum sind deshalb strenge Maßstäbe an die Verhältnismäßigkeit der Maßnahme zu stellen.

13.4
Datenschutz für Stadtverordnete

Stadtverordnete, die in ihrer Eigenschaft als "normale" Bürger in Kontakt zu ihrer Stadtverwaltung treten, haben Anspruch darauf, datenschutzrechtlich genau so behandelt zu werden wie alle anderen Bürgerinnen und Bürger. Gegen diesen Grundsatz haben im

vergangenen Jahr eine Bürgermeisterin und ein Bürgermeister in zwei hessischen Städten verstoßen.

In einem Fall nutzte ein Stadtverordneter das von der Kommune eingerichtete Bürgertelefon offenbar überaus häufig. Er suchte Kontakt zur Verwaltung, und zwar nicht in seiner Funktion als Stadtverordneter, sondern bewusst als ganz normaler Bürger. Dieser Umstand wurde im Rahmen einer politischen Diskussion in einer öffentlichen Sitzung der Stadtverordnetenversammlung vom Bürgermeister der Stadt offenbart.

In einem anderen Fall wurde in einer Stadtverordnetensitzung über die schrittweise Abschaffung der Grundwasserabgabe in Hessen diskutiert. In diesem Zusammenhang kamen auch die Wassereinsparprojekte der Stadt kontrovers zur Sprache. Bürgerinnen und Bürgern sind seinerzeit Regenwassertonnen kostenlos zur Verfügung gestellt worden. Ein Kritiker dieses Konzepts aus den Reihen der CDU in der Stadtverordnetenversammlung musste kurz darauf in zwei Zeitungen lesen, dass er - obwohl Kritiker des Konzepts - ebenfalls Bezieher einer derartigen Regenwassertonne sei. Diese Information war durch die „grüne“ Bürgermeisterin an die Presse gegeben worden.

In beiden Fällen waren die Stadtverordneten mit ihrer Verwaltung nicht in ihrer Funktion als Stadtverordnete, sondern als Bürger in Verbindung getreten. Das hat zur Folge, dass die Verwaltung hinsichtlich der Daten dieser Bürger genauso verpflichtet ist, die datenschutzrechtlichen Bestimmungen einzuhalten, wie im Umgang mit Daten anderer Bürgerinnen und Bürgern. Eine Veröffentlichung derartiger Daten wäre deshalb nur dann zulässig gewesen, wenn eine Rechtsvorschrift dies ausdrücklich zugelassen hätte, die Betroffenen eingewilligt hätten oder die Daten bereits anderweitig offenkundig gewesen wären. Keine dieser Voraussetzungen war erfüllt. Insofern war die öffentliche Bekanntgabe verwaltungsinterner Daten der Stadtverordneten datenschutzrechtlich unzulässig.

Deswegen habe ich hervorgehoben, dass Beteiligte an einem Verwaltungsverfahren gemäß § 30 des Hessischen Verwaltungsverfahrensgesetzes (HVwVfG) - unabhängig von ihrer beruflichen oder ehrenamtlichen Stellung - einen Anspruch darauf haben, dass Vorgänge aus Verwaltungsverfahren von den Bediensteten gegenüber der Öffentlichkeit geheim gehalten werden. Insofern lag auch ein Verstoß gegen die Geheimhaltungspflicht des § 30 HVwVfG vor. Ich habe die Verantwortlichen aufgefordert, künftig sauber darauf zu achten, dass im

Rahmen der politischen Diskussion deutlich zu unterscheiden ist, ob es sich um verwaltungsinterne Daten über die Stadtverordneten als Bürger oder um Informationen handelt, die die Stadtverordneten in dieser öffentlichen Funktion betreffen.

14. Soziales

14.1
Überprüfung von Jugendämtern durch den Rechnungshof

Die Überprüfung von Jugendämtern einschließlich der Kenntnisnahme personenbezogener Daten durch den Rechnungshof ist datenschutzrechtlich zulässig.

Das Hessische Sozialministerium hat mich um Auskunft gebeten, ob Jugendämter durch den Rechnungshof überprüft werden dürfen.

Ich habe das in Übereinstimmung mit dem behördlichen Datenschutzbeauftragten des Sozialministeriums bejaht. Zwar genießen Sozialdaten und speziell Jugendhilfedaten einen herausgehobenen gesetzlichen Schutz, aber schon im Sozialdatenschutzrecht selbst wird betont, dass es Kontrolltätigkeiten und speziell der Rechnungsprüfung nicht im Wege steht (§§ 67c Abs. 3, 69 Abs. 5 Sozialgesetzbuch X und § 61 Abs. 1 Sozialgesetzbuch VIII).

Auch das Bundesverfassungsgericht hat im Anschluss an das Bundesverwaltungsgericht darauf hingewiesen, dass im Rahmen der Rechnungsprüfung (sogar) in Patientenunterlagen eingesehen werden darf (Beschluss vom 29. April 1996 - 1 BvR 1226/89).

Die Rechtsstellung des Rechnungshofs ist verfassungsrechtlich verankert (Art. 144 Hessische Verfassung). Dessen Aufgaben und Prüfungsbefugnisse sind in der Landeshaushaltsordnung näher konkretisiert (§§ 95 ff. Landeshaushaltsordnung); hinzu kommt das Gesetz zur Regelung der überörtlichen Prüfung kommunaler Körperschaften in Hessen (ÜPKKG) vom 22. Dezember 1993 (GVBl. I S. 708).

Dessen § 5 Abs. 1 Satz 4 verfügt, dass der Präsident des Rechnungshofs mit der Wahrnehmung der Prüfungen öffentlich bestellte Wirtschaftsprüfer, Wirtschaftsprüfungsgesellschaften oder andere geeignete Dritte zu beauftragen hat. Dieser gesetzlichen Vorgabe entspricht es, dass der Präsident des Rechnungshofs das Unternehmen "Kienbaum-Management-Consultings-GmbH" mit der Rechnungsprüfung der Jugendämter betraut hat.

Dass mit Blick auf § 4 HDSG (Auftragsdatenverarbeitung, s. auch Ziff. 25.2) die Mitarbeiter des Kienbaum-Unternehmens im Rahmen ihrer Rechnungsprüfung der Jugendämter u.a. das Datengeheimnis (§ 9 HDSG) zu beachten haben und dass das Unternehmen bei seiner Rechnungsprüfung meiner Kontrolltätigkeit unterliegt, ist unter den Beteiligten zu Recht einhellige Ansicht.

14.2
Täter-Opfer-Ausgleich bei Jugendlichen

Träger der freien Jugendhilfe dürfen als Schlichtungsstellen einen Täter-Opfer-Ausgleich nur durchführen, wenn die Einwilligung von Opfer und Täter vorliegt. Der Grundsatz der Erforderlichkeit ist zu beachten.

Das Landesjugendamt hat mich darauf aufmerksam gemacht, dass Staatsanwaltschaften sich weigern, für die Träger der freien Jugendhilfe als Schlichtungsstellen für den Täter-Opfer-Ausgleich bei Jugendlichen die Daten zu selektieren, die für den Täter-Opfer-Ausgleich benötigt werden. Außerdem wird nicht gewährleistet, dass vor der Übersendung die Einwilligung der Betroffenen eingeholt wird. Das Verfahren, die Ermittlungsakte insgesamt zu übersenden, sei - so die Staatsanwaltschaften - aus Gründen der Arbeitsökonomie geboten. Ansonsten würde sich das Projekt Täter-Opfer-Ausgleich bei Jugendlichen erledigen.

Kurzfristig wurde unter der Moderation des Landesjugendamtes mit den Trägern der freien Jugendhilfe ein vorläufiges Konzept entwickelt, um den Belangen des Datenschutzes schon vor einer gesetzlichen Neuregelung besser Rechnung zu tragen:

1. Die Träger der freien Jugendhilfe holen - nachdem sie die Akten von der Staatsanwaltschaft übermittelt bekommen haben - die Einwilligung der Betroffenen für den Täter-Opfer-Ausgleich ein. Wird die Einwilligung nicht gegeben, findet ein Verfahren zum Täter-Opfer-Ausgleich nicht statt.

2. Die Träger der freien Jugendhilfe extrahieren die Akten unter dem Gesichtspunkt der Erforderlichkeit für den Täter-Opfer-Ausgleich und schicken die Akten anschließend an die Staatsanwaltschaft zurück.

Längerfristig ist zu fordern, dass die Jugendämter in das Verfahren des Täter-Opfer-Ausgleichs integriert werden. Das Kinder- und Jugendhilferecht weist den Jugendämtern die Aufgaben der Jugendgerichtshilfe und insoweit eine Mitwirkung im Jugendstrafverfahren zu (§§ 52, 61 Abs. 3 SGB VIII).

15. Banken

Zwangsanzeige des Kontostandes bei Geldausgabeautomaten

Die Zwangsanzeige des Kontostandes auf dem Display der Geldausgabeautomaten bei reinen Geldabhebevorgängen ist unzulässig, da die Gefahr einer Ausspähung durch Dritte nicht ausgeschlossen werden kann. Die Daten verarbeitende Stelle hat nach § 9 Satz 1 Bundesdatenschutzgesetz Maßnahmen zu treffen, die das verhindern sollen.

Der Kunde einer hessischen Sparkasse beschwerte sich darüber, dass bei Geldabhebungen an Geldausgabeautomaten automatisch der Kontostand angezeigt würde. Dies geschehe, ohne das er einen Einfluss darauf ausüben könne. Er wolle das im Übrigen auch nicht, da er die Gefahr der Ausspähung durch Dritte fürchte.

Ich habe mich daraufhin mit der betreffenden Sparkasse in Verbindung gesetzt und mir das Verfahren angesehen. Nach der Eingabe der PIN erscheinen auf dem Display des Geldautomaten Menüpunkte zur Saldenanzeige und zur Barabhebung. Bei Auswahl des Menüpunktes Barabhebung erscheint eine Anzahl von Geldbeträgen auf dem Bildschirm, die man auswählen und abheben kann. Nach Auswahl der gewünschten Summe und zum Ende des Bedienungsvorganges hin erscheint die ec-Karte, das Geld wird in das Ausgabefach geschoben und im Display wird der nach dem Abhebevorgang aktuelle Kontostand angezeigt.

Nach Aussage der Sparkassenvertreter wird dieses Verfahren seit etwa 1992 praktiziert. Ausgangspunkt dieser Anzeige, die jede hessische Sparkasse für ihren Organisationsbereich in Gang setzen kann, waren Überlegungen, den „Kundendurchsatz“ an stark frequentierten Ausgabegeräten zu erhöhen. Da der Kontostand automatisch nach der Abhebeprozedur angezeigt werde, brauche der Kunde weder vorher noch nachher noch einmal einen Menü-Durchgang zu starten, um seinen Kontostand zu erfragen. Damit habe er seine Geschäfte am Automaten schneller beendet und dadurch sei eine größere Kundenfrequenz möglich.

Meine Recherchen innerhalb der hessischen Sparkassenorganisation haben ergeben, dass mit Ausnahme von zwei Sparkassen alle übrigen diese automatische Anzeige in ihren Geldautomaten programmiert haben. Interessant erscheint in diesem Zusammenhang, das dieses Thema bei den Privatbanken keine Rolle spielt. Weder im Bereich der

Genossenschaftsbanken noch bei den Postbanken oder den klassischen privaten Instituten wie Deutsche Bank und anderen wird ein derartiges Verfahren angewandt. Gerade das von der Sparkasse ins Feld geführte Kostenargument (höhere Benutzerfrequenz) spielt bei den privaten Instituten offensichtlich keine Rolle.

Ich halte die vom Kunden nicht beeinflussbare Anzeige für unzulässig. Da das Hessische Datenschutzgesetz für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, nur eingeschränkt gilt, ist im vorliegenden Fall das Bundesdatenschutzgesetz (BDSG) Grundlage für die rechtliche Bewertung des Sachverhalts. Die in der Anlage zu § 9 Satz 1 BDSG fixierten Voraussetzungen für die automatisierte Verarbeitung personenbezogener Daten erfordern von der Daten verarbeitenden Stelle Maßnahmen, um Gewähr zu leisten, das „personenbezogene Daten nicht unbefugt oder nicht zufällig zur Kenntnis genommen werden".

Durch die Anzeige des Kontostandes, die der Kunde nicht ausdrücklich und auf eigene Initiative hin in Gang setzen kann, wird ein unnötiges, vom Kunden nicht gewolltes Datensicherheitsrisiko in Form einer möglichen Ausspähung ausgelöst, denn es ist häufig so, dass von anderen Kunden der Diskretionsabstand nicht eingehalten wird. Bei dem gewollten Vorgang der Kontostandsanzeige wird der Kunde i.d.R. bemüht sein, die Gefahr einer Ausspähung zu minimieren. Nicht ausgeschlossen werden kann zudem auch eine Fehlfunktion des Geldautomaten. So ist es z.B. schon passiert, dass sich der Bildschirm eines Geldautomaten nicht mehr abschaltete, der letzte Geschäftsvorgang eines Kunden am Automaten also ablesbar blieb.

Ich habe der betroffenen Sparkasse meine Rechtsauffassung mitgeteilt und um eine Änderung der bisherigen Praxis gebeten. Zudem habe ich den Sparkassen- und Giroverband Hessen-Thüringen über diesen Vorgang informiert und darum gebeten, die anderen hessischen Sparkassen über meine Rechtsauffassung zu informieren. Ein Einvernehmen hat bisher nicht erzielt werden können.

16. Personalwesen

16.1
Personalkostenbudgetierung

Vor dem Hintergrund der Personalkostenbudgetierung und des Mitbestimmungsrechts des Personalrats in Personalangelegenheiten ist es datenschutzrechtlich zulässig, wenn dem Personalrat Personalkosten mitarbeiterbezogen bekannt gegeben werden.

Die Betriebsleitung eines Kreiskrankenhauses hat mich um Auskunft gebeten, ob im Fall einer Personalkostenbudgetierung der Personalrat erfahren darf, welche Personalkosten Mitarbeiter verursachen.

Soweit es für die Aufgabenerfüllung des Personalrats erforderlich ist, Personaldaten einzelner Bediensteter bekannt zu geben, bestehen dagegen datenschutzrechtliche Bedenken grundsätzlich nicht. Der Personalrat des Kreiskrankenhauses hat selbst betont, dass es ihm um eine hinreichende Informationsgrundlage für Angelegenheiten gehe, die der Mitbestimmung unterlägen.

Im Hinblick auf das Mitbestimmungsrecht des Personalrats gemäß §§ 62, 77 Hessisches Personalvertretungsgesetz habe ich der Betriebsleitung des Kreiskrankenhauses mitgeteilt, dass es datenschutzrechtlich zulässig ist, dem Personalrat vor dem Hintergrund der Personalkostenbudgetierung die Personalkosten einzelner Bediensteter bekannt zu geben.

16.2
Bearbeitung von Beihilfeangelegenheiten durch private Versicherungen

Nach geltendem Recht ist die Bearbeitung von Beihilfeangelegenheiten durch private Versicherungen unzulässig.

Kommunen haben mich mehrfach mit dem Thema konfrontiert, ob die Beihilfebearbeitung auf private Versicherungen übertragen werden kann. Ich bin - in Übereinstimmung mit der Landesregierung - der Auffassung, dass die datenschutzrechtlichen Regelungen keine

ausreichende Ermächtigung für ein „outsourcing“ bieten. § 4 Hessisches Datenschutzgesetz (HDSG) legt die Voraussetzungen fest, unter denen personenbezogene Daten durch Dritte bearbeitet werden dürfen. Die Regelung selbst schafft jedoch keine hinreichende Ermächtigung dafür, dass der besondere Geheimnisschutz, der Personalakten nach § 107 Abs. 3 und speziell Beihilfeakten nach § 107a Hessisches Beamtengesetz (HBG) zugemessen ist, durch Vereinbarungen mit Dritten durchbrochen wird. Diese spezielle gesetzliche Regelung besitzt Vorrang gegenüber der allgemeineren datenschutzrechtlichen.

§ 107 Abs. 3 HBG

Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. ....

Zwar verpflichtet § 4 Abs. 2 Satz 4 HDSG den Auftraggeber zu prüfen, ob beim Auftragnehmer die Anforderungen erfüllt sind, die bei besonderen Amts- und Berufsgeheimnissen gewahrt bleiben müssen. Diese Norm kann jedoch nur als Prüfungsverpflichtung, nicht hingegen als Ermächtigung zur Weitergabe von Beihilfedaten interpretiert werden.

Hinzu kommt, dass § 4 Abs. 2 Satz 5 HDSG für private Versicherungen, also nicht-öffentliche Stellen, eine zusätzliche Barriere errichtet.

§ 4 Abs. 2 Satz 5 HDSG

An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen über berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen.

Vor diesem Hintergrund müsste der Landesgesetzgeber eine besondere gesetzliche Ermächtigung schaffen, die die Bearbeitung von Beihilfeangelegenheiten durch private Versicherungen deckt, wenn ihm die externe Datenverarbeitung als rechtspolitisch wünschenswert erscheint.

Ich habe den anfragenden Kommunen mitgeteilt, dass die Bearbeitung von Beihilfeangelegenheiten durch private Versicherungen nach geltendem Recht unzulässig ist.

16.3
Jahrbuch 2000

Die namentliche Nennung der leitenden Beamten und Angestellten in einem Handbuch, das eine Übersicht über die Organisationsstruktur der Ministerien und der Staatskanzlei sowie sonstiger Dienststellen der Landesregierung enthält, ist datenschutzrechtlich zulässig.

Die Hessische Staatskanzlei hat mich zu der Frage angehört, ob es zulässig ist, ein Hessen-Jahrbuch 2000 durch einen Verlag herausgeben zu lassen, das eine Übersicht über die Organisationsstruktur der Staatskanzlei und der Ministerien sowie sonstiger Dienststellen des Landes enthalten soll, in der die leitenden Beamten und Angestellten namentlich aufgeführt sind.

Die Zweifel, die gegen eine namentliche Nennung bestehen, beruhen auf § 34 HDSG und dem Grundsatz der Erforderlichkeit. Bei einem strikten Verständnis des Grundsatzes der Erforderlichkeit können die mit dem Handbuch verfolgten Zwecke an sich auch ohne Namensnennung erreicht werden, denn die Bürgerinnen und Bürger können die jeweils zuständigen Ansprechpartner z.B. mit Hilfe des Telefonverzeichnisses oder der Internetadresse der zuständigen Behörde erreichen.

Nach meiner Auffassung hat die Staatskanzlei darauf hingewiesen, dass die Namensübermittlung im Interesse der Bürgerfreundlichkeit und der schnelleren Erreichbarkeit der jeweiligen Ansprechpartner sachgerecht und deswegen datenschutzrechtlich zu rechtfertigen ist. Dahinter steht die Idee des modernen Staates, für den es keinen Grund zu übertriebener "staatlicher Geheimniskrämerei" mehr geben kann. Aus diesem Grund habe ich die Planung der Landesregierung als datenschutzrechtlich legitimierbar erachtet.

Eine ähnliche Thematik hatte ich in meinem 25. Tätigkeitsbericht bereits behandelt: Telefonverzeichnisse von Dienststellen im Internet (8.3, Seite 71 ff.). Auch in anderen

Zusammenhängen hat der Gesetzgeber explizit verfügt, dass Amtsträger bei Ausübung ihrer Ämter datenschutzrechtlich nur eingeschränkten Schutz genießen. So gelten beispielsweise die archivrechtlichen Schutzfristen nicht für Amtsträger in Ausübung ihrer Ämter, § 15 Abs. 2 Hessisches Archivgesetz.

Ich habe der Staatskanzlei mitgeteilt, dass ich gegen das angesprochene Handbuch keine datenschutzrechtlichen Einwände erhebe.

17. Schulen

OECD-Forschungsprojekt PISA

Wissenschaftliche Forschungsvorhaben, die auf der Befragung von Schülerinnen und Schülern sowie Eltern beruhen, sind nur dann datenschutzrechtlich bedenkenlos, wenn die für die schriftliche Einwilligung notwendige Aufklärung in allen Punkten dem § 7 Abs. 2 Hessisches Datenschutzgesetz entspricht.

Im Rahmen der angestrebten Qualitätssicherung der Schulen hatte sich 1998 die Kultusministerkonferenz der Länder darauf verständigt, an der von der OECD getragenen, weltweit größten Vergleichsstudie über die Leistungsfähigkeit der Bildungssysteme teilzunehmen. Dieses Programm PISA (**P**rogram for **I**nternational **S**tudent **A**ssessment) untersucht und vergleicht in 32 Ländern bei einer Stichprobe von mindestens 5.000 Jugendlichen pro Land die grundlegenden Kompetenzen in den Kernfächern Lesen, Mathematik und Naturwissenschaft und die Fähigkeit, das Wissen anzuwenden. Dem für 1999 vorgesehenen Feldtest sollen in den Jahren 2000, 2003 und 2006 die Hauptstudien folgen. Den Kern der Feldstudie bildeten zunächst die Vorauswahl der zu befragenden 15-jährigen Schülerinnen und Schüler, die Verteilung der umfangreichen Fragebögen sowie die Schülerteilnahme an Leistungstests.

Die Organisation und wissenschaftliche Datenauswertung liegt in den Händen des Max-Planck-Instituts für Pädagogik in Berlin. Dieses hatte die für das Verfahren der Feldstudie notwendige Zustimmung der für den Schulbildungsbereich zuständigen Länderministerien einzuholen. Die vom Kultusministerium erbetene Beteiligung des Hessischen Datenschutzbeauftragten war notwendig. Gemäß einer Absprache mit den anderen Datenschutzbeauftragten hatte es Hessen übernommen, eine koordinierte Stellungnahme der beteiligten Länder abzufassen, soweit der Zeitrahmen und die Anwendung der nur teilweise übereinstimmenden Datenschutzregelungen der Länder dies zuließen.

Neben organisatorischen Fragen der Datensicherheit im Testverfahren blieb als Kernfrage, inwieweit die Datenerhebung bei den Jugendlichen und deren Eltern durch die umfangreichen Fragebögen mit teilweise sensiblen Fragestellungen den datenschutzrechtlichen Bestimmungen entspricht. Da in allen Ländern schulrechtliche Normen zur Rechtspflicht an

der Teilnahme an solchen Befragungen fehlen, sah das Verfahrenskonzept die vorherige schriftliche Einwilligung der Beteiligten vor, wie es auch in § 84 Abs. 3 Satz 1 Hessisches Schulgesetz (HSchulG) vorgegeben ist.

§ 84 Abs. 2 Satz 1 HSchulG

Personenbezogene Daten dürfen für ein bestimmtes wissenschaftliches Forschungsvorhaben in der Regel nur mit der Einwilligung der Eltern oder der volljährigen Schülerinnen und Schüler verarbeitet werden. ...

Die Einwilligung ist jedoch nur rechtswirksam, wenn vor ihrer Erteilung die Voraussetzungen des § 7 Abs. 2 Satz 3 bis 5 Hessischen Datenschutzgesetz (HDSG) erfüllt sind.

§ 7 Abs. 2 Satz 3 bis 5 HDSG

... Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern und jederzeit mit Wirkung für die Zukunft widerrufen kann.

Die mir vorgelegten Entwürfe der Informationsschreiben an die Jugendlichen und ihre Eltern hatten gravierende Mängel. Die weitgehende Beseitigung der Mängel gelang erst durch klare Auflagen seitens des Hessischen Kultusministeriums. Die Erwähnung der wichtigsten Punkte erfolgt an dieser Stelle deshalb, weil das Max-Planck-Institut das Projekt PISA mit einem ähnlichen Verfahren in den nächsten Jahren fortsetzen und auch ähnliche landesübergreifende Forschungsprojekte im Schulbereich tragen wird.

Datenschutzrechtlich zu beanstanden war, dass die Einwilligungserklärung von den Eltern abgegeben werden sollte, bevor sie überhaupt Gelegenheit hatten, den Inhalt der Fragebögen zur Kenntnis zu nehmen. Damit wäre der Sinn der Einwilligung verfehlt worden, da sie die Kenntnis der Art der zu erhebenden Daten voraussetzt. Ich habe daher verlangt, dass das Informationsschreiben die Art der erfragten Informationen näher beschreibt, und den Eltern Gelegenheit gegeben wird, den Fragebogen der Schule vor Zustimmung einzusehen.

Weiterhin fehlte eine hinreichende Aufklärung über die rechtliche Bedeutung der Einwilligung als notwendige rechtliche Voraussetzung der Datenverarbeitung. Überdies fehlte der gesetzlich vorgesehene Hinweis auf die Möglichkeit, die Einwilligung jederzeit für die Zukunft widerrufen zu können. Zu kritisieren war schließlich die Aussage, die in dem Fragebogen enthaltenen Angaben seien "anonym". Eine Anonymisierung der Fragebögen war zwar insoweit vorgesehen, als sie keinen direkten Hinweis auf die betroffene Person enthielten. Die Fragebögen trugen jedoch eine Code-Nummer, die wiederum über eine separate Liste der Jugendlichen, die als Testperson ausgewählt waren, eine Re-Identifizierung nicht ausschloss. Meine Forderung, die in dem Schüler-Fragebogen erbetene Auskunft über das Geburtsdatum auf die Angaben von Monat und Jahr zu reduzieren, wurde akzeptiert.

Diese und weitergehende Forderungen konnten trotz der Kürze der verfügbaren Zeit noch vor Beginn des Feldtests erreicht werden. Für künftige Forschungsprojekte dieser Art ist zu fordern, dass die beanstandeten Mängel schon in den Konzepten vermieden werden.

18. Hochschulen

Prüfung der Technischen Universität Darmstadt

Eine Prüfung der Verwaltung der Technischen Universität Darmstadt ergab, dass verschiedene datenschutzrechtliche Verbesserungen notwendig sind.

Auch im Berichtsjahr setzte ich die Reihe der Hochschulprüfungen fort mit einem Prüfbesuch bei der Technischen Universität Darmstadt. Die begrenzten personellen Kapazitäten führten allerdings zu einer Beschränkung auf solche Verwaltungseinheiten, die in der Hochschulverwaltung zentrale Aufgaben haben. Gravierende Mängel wurden nicht vorgefunden. Gleichwohl waren nach wie vor einige Schwachstellen festzustellen, die vermeidbar gewesen wären (vgl. im Übrigen 26. und 27. Tätigkeitsbericht).

18.1
Ausgestaltung der Formulare

Im Bereich des zentralen Studentensekretariats werden für die Immatrikulation Formulare verwendet, die der erstmaligen Erhebung der notwendigen Studentendaten dienen, bevor sie automatisiert gespeichert werden. In dieser Phase ist § 12 Abs. 4 Hessisches Datenschutzgesetz (HDSG) zwingend zu beachten.

§ 12 Abs. 4 HDSG

Werden Daten beim Betroffenen mit seiner Kenntnis erhoben, dann ist er von der datenverarbeitenden Stelle in geeigneter Weise über deren Anschrift, den Zweck der Datenerhebung sowie über seine Rechte nach § 8 aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Werden Daten bei dem Betroffenen auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, dann ist er auf die Rechtsgrundlage hinzuweisen. Im Übrigen ist er darauf hinzuweisen, dass er die Auskunft verweigern kann. Sind die Angaben für die Gewährung einer Leistung erforderlich, ist er über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

In dieser novellierten Fassung des Hessischen Datenschutzgesetzes kommt zu den früheren Hinweisen noch die Information über die Rechte des Betroffenen nach § 8 HDSG hinzu. Die in Vollzug dieser Vorschrift festgestellten Defizite bei den verwendeten Formularen, insbesondere bzgl. des fehlenden Hinweises auf die Rechte aus § 8 HDSG, ließen die Annahme zu, dass auch in anderen Verwaltungsbereichen der Hochschule gleichartige Mängel existieren. Es wurde zugesagt, unverzüglich alle Hochschulformulare auf die Anwendung dieser Vorschrift zu überprüfen.

18.2
Studentensekretariat

In einigen Formularen des Studentensekretariates befanden sich Fragen, die in der einschlägigen „Verordnung über die Verarbeitung personenbezogener Daten und über das Verfahren der Immatrikulation an den Hochschulen des Landes Hessen" (GVBl. 1995, S. 79) keine rechtliche Grundlage finden und auch dem Grundsatz der Erforderlichkeit nicht genügen. So wurde im Antrag auf Zulassung als Gasthörerin oder -hörer nach der Staatsangehörigkeit gefragt. Dieses Datum sieht § 14 Abs. 1 der Verordnung nicht vor.

§ 14 Abs. 1 Verordnung über die Verarbeitung personenbezogener Daten und über das Verfahren der Immatrikulation an den Hochschulen des Landes Hessen

Der Antrag auf Zulassung als Gasthörerin oder -hörer muss folgende Angaben enthalten: Familienname, Vorname, Geburtsdatum, Geschlecht, Anschrift(en), gewünschte Lehrveranstaltungen.

Die Kenntnis der Staatsangehörigkeit ist für die Entscheidung über die Gasthörerzulassung offensichtlich nicht erforderlich. Gleiches gilt für die erfragte Telefonnummer. Keinen durchgreifenden Bedenken begegnet diese Frage, wenn ein deutlicher Hinweis in das Formular aufgenommen wird, dass es sich um freiwillige Angaben handele, von denen die Zulassung nicht abhänge.

Das Antragsformular für die Exmatrikulation sah die Frage nach dem Grund der Exmatrikulation vor. Dieses Kriterium ist in § 10 der Verordnung nicht vorgesehen.

§ 10 Verordnung über die Verarbeitung personenbezogener Daten und über das Verfahren der Immatrikulation an den Hochschulen des Landes Hessen

Für die Exmatrikulation verarbeitet die Hochschule die gespeicherten Daten sowie Angaben zur Beendigung des Studiums nach § 10 des Hochschulgesetzes.

18.3
Hochschularchiv

Das im Hause des Hessischen Staatsarchivs residierende „Hochschularchiv“ erfüllt auf Grund der sachlichen und personellen Ausstattung und der faktisch öffentlichen Nutzung wesentliche Kriterien, die für die Qualifizierung als öffentliches Archiv i.S.d. § 5 Abs. 2 Hessisches Archivgesetzes (HArchivG) notwendig sind.

§ 5 Abs. 2 HArchivG

Die Anbietungspflicht gegenüber den Staatsarchiven entfällt, wenn die betreffende juristische Person oder Vereinigung ein eigenes öffentliches Archiv unterhält, das archivfachlichen Ansprüchen genügt, oder wenn die Unterlagen bei einer dazu geschaffenen Gemeinschaftseinrichtung archiviert werden.

Neben den in dieser Vorschrift verlangten „archivfachlichen Ansprüchen“ ist eine eigenständige öffentliche Einrichtung zu fordern, die der Umfang der Nutzung durch Satzung festlegt. Für das kommunale Archiv ist dies in § 4 Abs. 1 Hessisches Archivgesetz sogar ausdrücklich geregelt.

§ 4 Abs. 1 HArchivG

Die Gemeinden, Landkreise und kommunalen Verbände regeln die Archivierung ihres Archivgutes im Rahmen ihrer Leistungsfähigkeit und nach den in diesem Gesetz vorgegebenen Grundsätzen durch Satzung.

Eine Archivsatzung fehlt bisher bei der TU Darmstadt. Die Freigabe von personenbezogenem Archivgut, etwa für die Forscher, erfolgte analog zur „Benutzungsordnung für die Hessischen Staatsarchive" (StAnz. 1997, S. 1300). Eine rechtsstaatliche Absicherung und die Nachprüfbarkeit der Entscheidungen waren jedoch damit nicht gewährleistet. Die Hochschule hat zugesagt, die Satzung umgehend zu beraten. Ihr wurde empfohlen, für die Durchführung des eigentlichen Nutzungsverfahrens eine ergänzende Benutzungsordnung, wie bei Staatsarchiven, zu erlassen.

18.4
Aufbewahrungsfrist für Akten

Bevor für Verwaltungsunterlagen die - archivrechtliche - Pflicht zur Aussonderung und zum Anbieten gegenüber dem zuständigen Archiv einsetzt, werden zu archivierende Unterlagen für bestimmte Fristen durch die Verwaltung aufbewahrt. Bei der Bestimmung der jeweiligen Aufbewahrungsfrist ist von den Hochschulen zu beachten, dass der hessische Erlass zu den „Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut des Landes Hessen“ vom 6. Dezember 1996 (StAnz. 1996, S. 4275) nur für die Akten der Auftragsverwaltung unmittelbar gilt. Wegen der weitgehenden rechtlichen Autonomie der Hochschulen wird die Beachtung des Erlasses im Übrigen nur empfohlen (s. Nr. 20 des Erlasses). Für den Bereich der Prüfungsunterlagen ist eine Frist durch das Hessische Ministerium für Wissenschaft und Kunst festgelegt worden (Erlass vom 25. Mai 1992, Abl. 1992, S. 770). Ansonsten obliegt der Hochschule die Entscheidung, inwieweit sie die Vorgaben des Erlasses von 1996 ganz oder teilweise übernimmt oder im Rahmen des Verwaltungsermessens eigene Fristen festlegt.

Ein umfassender Katalog der Aufbewahrungsfristen für alle Arten der anfallenden Verwaltungsunterlagen fehlte in der geprüften Hochschule. Ich habe daher die Hochschulleitung aufgefordert, einen solchen Fristenkatalog zu erstellen, um den Zeitraum der Aufbewahrung transparent und kontrollierbar zu machen.

19. Statistik

Fortsetzung der Prüfung von kommunalen Statistikstellen

Im Berichtsjahr habe ich die von mir begonnene Prüfserie von abgeschotteten Statistikstellen in den größeren Städten des Landes fortgesetzt und abgeschlossen(vgl. 27. Tätigkeitsbericht, Ziff. 19). Vier Statistikstellen wurden auf die Einhaltung der Vorgaben, wie sie sich aus § 12 des Hessischen Landesstatistikgesetzes vom 19. Mai 1987 ergeben, überprüft. Es handelt sich hierbei um die Stellen in den Städten Frankfurt, Wiesbaden, Hanau und Offenbach.

19.1
Statistikstelle Offenbach

Die Statistikstelle der Stadt Offenbach ist seit ihrer Einrichtung im Jahre 1989 im 12. Stock des Rathauses der Stadt untergebracht. Die formalen Organisationsverfügungen wie Dienstanweisungen, Verpflichtungserklärungen der Mitarbeiter auf das Statistikgeheimnis sowie die Satzung über die regelmäßigen Datenübermittlungen aus anderen Bereichen der Verwaltung an die Statistikstelle haben nach wie vor Gültigkeit.

Klassische Kommunalstatistik wie etwa in Form statistischer Umfragen wurde in Offenbach bislang nicht gemacht. Die Arbeit der Statistikstelle beschränkte sich auf laufende Erhebungen, die im Auftrag des Hessischen Statistischen Landesamtes (HSL) durchgeführt werden.

Die klassischen Statistikbereiche wie z.B. die Preisstatistik, Fremdenverkehrsstatistik, Bautätigkeitsstatistik oder die Landwirtschaftszählung werden manuell bearbeitet. Beim Fremdenverkehr und der Bautätigkeit übernimmt die Statistikstelle die Funktion des Verteilens und Einsammelns. Die in Papierform eingehenden und von den betroffenen Stellen ausgefüllten Unterlagen werden dann direkt nach Wiesbaden an das HSL weitergeleitet. Eigene Auswertungen, wie dies z.B. von anderen Städten im Bereich der Fremdenverkehrsstatistik gemacht wird, werden in Offenbach nicht durchgeführt.

Eine automatisierte Verarbeitung der Daten gibt es nicht. Nur die Korrespondenz mit anderen Stellen wird mittels PC durchgeführt.

Im Zusammenhang mit der Bautätigkeitsstatistik wird von der Statistikstelle eine Gebäudekartei geführt. Die Karteikarten, auf denen neben Informationen zum Gebäude auch die Straße, Hausnummer und der Name des Erstbesitzers vermerkt sind, reichen bis in die fünfziger Jahre zurück. Eine personenbezogene Aufbewahrung dieser Unterlagen ist nicht zulässig. Sie hat keine Aussagekraft und ist deswegen i.S.v. § 11 Hessisches Datenschutzgesetz (HDSG) nicht erforderlich. Die Statistikstelle kann diese Kartei zwar weiter führen, muss aber die Namen der Hauseigentümer entfernen und darf sie für die Zukunft auch nicht mehr erfassen. Ich habe die Leitung der Statistikstelle deshalb gebeten, die personenbezogenen Teile aus der Kartei zu entfernen.

Die Verfahrensweise im Bereich der Bevölkerungsstatistik entspricht den gesetzlichen Vorgaben und wurde von mir bereits an anderer Stelle im 27. Tätigkeitsbericht geschildert.

19.2
Statistikstelle Hanau

Die Statistikstelle der Stadt Hanau ist organisatorisch dem Ordnungs- und Umweltamt zugeordnet und in einem städtischen Komplex in der Steinheimer Straße 1b untergebracht. Der Zugang zu den Räumen ist verschlossen und kann nur von den Bediensteten selbst geöffnet werden. Für Besucher gibt es eine Klingel. Zur Zeit gibt es einen Sachbearbeiter, der die Statistikgeschäfte bearbeitet. In Kürze sollen weitere eineinhalb Stellen geschaffen werden. Die erforderlichen Organisationsregelungen (Verfügungen, Satzung, Dienstanweisungen etc.) entsprechen dem erforderlichen Stand.

Kommunalstatistik bzw. statistische Umfragen gibt es in Hanau bislang keine. Einige statistische Verfahren werden mit PC bearbeitet. Ein festgestellter Mangel war, dass die persönlichen Passwörter nur sechs Stellen lang waren. Eine Länge von acht Stellen halte ich für erforderlich.

Der Umgang mit Auftragsstatistiken, die für das HSL durchgeführt bzw. bearbeitet werden, entspricht den gesetzlichen Anforderungen. Im Rahmen der Einzelprüfung habe ich jedoch festgestellt, dass diverse Unterlagen nicht den Speicherfristen entsprechend, sondern z.T.

lange Zeit darüber hinaus aufbewahrt werden. So gab es beispielsweise einen Aktenordner, in dem eine Statistik über gewählte Schöffen geführt wurde. Die Meldungen über bestimmte, namentlich und mit Anschrift benannte Personen reichten bis in das Jahr 1956 zurück. Es gibt keinen Grund, diese Unterlagen über einen derart langen Zeitraum aufzubewahren.

Auch die Zählkarten von Geburts- und Sterbefällen sowie von Eheschließungen wurden zu lange gespeichert. Die Unterlagen reichten teilweise bis in den Anfang des Jahres 1998 zurück.

Aus den Monaten Januar und Mai 1997 fanden sich kopierte Bauanträge. Das Kopieren dieser Unterlagen ist nicht zulässig; sie mussten sofort vernichtet werden.

In einem Ordner befanden sich Berichtigungslisten zum Melderegister, die aus dem Jahre 1989 stammten. Auch diese mussten vernichtet werden.

Ein nicht unerheblicher Mangel war, dass die Statistikstelle einen ständigen Zugriff auf die Einwohnerdatenbank der Stadt hatte. Dies ist jedoch allenfalls temporär und auf eine bestimmte Aufgabenstellung hin zulässig. Im Rahmen einer funktionalen Trennung der Ämter innerhalb der Verwaltung ist dafür zu sorgen, dass keine unzulässige Verquickung von Aufgaben und kein unzulässiger Datenaustausch erfolgt.

19.3
Statistikstelle Wiesbaden

Die Statistikstelle ist in der Wilhelminenstraße im dritten Obergeschoss untergebracht. Für externe Besucher gibt es eine Klingel, die Bediensteten selbst haben einen Schlüssel.

Die Organisationsverfügungen aus der Zeit der erstmaligen Einrichtung dieser Organisationseinheit haben nach wie vor Geltung. Eine private Nutzung der DV-Anlage ist unzulässig und durch interne Verfügung untersagt.

Die Datenverarbeitung erfolgt über ein internes, nur die Statistikstelle betreffendes Netz. Eine externe Verbindung besteht zur Kommunalen Informationsverarbeitung (KIV - früheres

KGRZ) Wiesbaden. In absehbarer Zeit will man sich in das städtische Netz einklinken, was unter datenschutzrechtlichen Aspekten grundsätzlich möglich ist. Allerdings müssen die stringenten Abschottungskriterien, die sich aus dem Statistikrecht ergeben, eingehalten werden. Die Stadt Wiesbaden steht hier im Dialog mit mir, weil eine technische Abschottung durch eine Firewall gewährleistet sein muss, die den technischen Sicherheitsansprüchen genügt.

Wesentliche Probleme im Umgang mit Statistikdaten habe ich nicht gefunden. Das betrifft sowohl die Verfahren selbst als auch die Speicherung bzw. Aufbewahrung der Daten. In Wiesbaden werden die Instrumentarien der Kommunalstatistik genutzt. Das schließt kommunale Umfragen ebenso ein wie die Durchführung von Geschäftsstatistiken. Für eigene Auswertungen der Fremdenverkehrsstatistik hat man sich das schriftliche Einverständnis der auskunftspflichtigen Betriebe eingeholt.

Kritisch betrachte ich das generelle Kopieren von Erhebungsbogen im Zusammenhang mit der Bautätigkeitsstatistik. Weil nach Auffassung der Statistikstelle die Zahlen des HSL von Aktualität und Qualität her nicht unproblematisch seien, fährt man in Wiesbaden eine "Parallelstatistik" und verwendet in Zweifelsfällen die eigenen Daten. Dies kann so jedoch nicht bleiben, da die eigenen Auswertungen der Urdaten durch die Statistikstelle rechtlich nicht abgedeckt ist.

19.4
Statistikstelle Frankfurt

Die Zugangssicherung zur Statistikstelle entspricht den Anforderungen (Klingel, Türdrücker, Türschließer etc.). Die notwendigen Organisationsverfügungen und Verpflichtungserklärungen der Mitarbeiter waren alle vorhanden und einsehbar.

Auch in Frankfurt werden die Möglichkeiten, die sich aus dem Hessischen Landesstatistikgesetz für die Städte und Kommunen ergeben, genutzt. So werden regelmäßige Bürgerbefragungen ebenso initiiert wie die Durchführung von Geschäftsstatistiken.

Wesentliche Mängel habe ich nicht festgestellt. Das betrifft auch die Aufbewahrung bzw. Speicherung von Unterlagen. Nur in einigen wenigen Ausnahmefällen bin ich zu der Ansicht gelangt, dass die Speicherdauer überschritten ist.

In Frankfurt gibt es ein umfangreich ausgebautes internes DV-Netz, das sowohl über einen Zugang zum KIV Frankfurt verfügt als auch an das allgemeine städtische Netz angeschlossen ist. Zur Sicherung wurde eine Firewall implementiert, die von mir aber noch auf ihre Funktionalität hin überprüft werden muss.

20. Wohnungswesen

Genehmigte Zweckentfremdung von Wohnraum

Die Vorlage vollständiger Mietverträge beim Wohnungsamt zum Beweis, dass Ersatzwohnraum für zuvor zweckentfremdeten Wohnraum geschaffen worden ist, ist ohne Einwilligung der betroffenen Mieterinnen und Mieter datenschutzrechtlich nicht zulässig.

Die Universitätsklinik Frankfurt hatte bei der Stadt Frankfurt beantragt, ein ihr gehörendes Gebäude, in dem sich Wohnungen befanden, zu Verwaltungszwecken zu nutzen. Diesem Antrag wurde unter der Auflage stattgegeben, dass Ersatzwohnraum geschaffen wird. In einer Vereinbarung zwischen dem Universitätsklinikum und der Stadt war festgehalten worden, dass das Klinikum zum Beweis die Mietverträge vorzulegen hat.

Nach Fertigstellung der Wohnungen forderte die Stadt das Universitätsklinikum auf, die abgeschlossenen Mietverträge zu übersenden. Das Klinikum äußerte Bedenken hinsichtlich der datenschutzrechtlichen Zulässigkeit der Überlassung der kompletten Mietverträge. Diese Bedenken wurden von mir geteilt, während die Stadt meinte, dass eine Übermittlung der in Frage stehenden Mietvertragsdaten nach § 14 Hessisches Datenschutzgesetz (HDSG) zulässig sei. Das Zweckbindungsgebot des § 13 HDSG gelte für eine Übermittlung im öffentlichen Bereich nicht. Demgegenüber habe ich dargelegt, dass sich die Zulässigkeit der in Frage stehenden Datenübermittlung nach § 11 Abs. 1 i.V.m. § 14 HDSG richtet. Eine Privilegierung einer Datenübermittlung im öffentlichen Bereich betrifft lediglich die Frage nach der Erforderlichkeit. Grenzen sind der Übermittlung danach gezogen, wenn die Übermittlung für die übermittelnde Stelle nicht erforderlich wäre. Der Grundsatz der Zweckbindung bleibt von dieser Regelung jedoch unberührt. Die Datenübermittlung an das Amt für Wohnungswesen wäre deshalb eine zweckwidrige Datenverwendung der Universität als Vermieterin gewesen.

Auch ein Rückgriff auf § 12 Abs. 2 Nr. 5 HDSG war ausgeschlossen. Ohne Kenntnis des Betroffenen dürfen Daten danach übermittelt werden, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und wenn keine schutzwürdigen Belange des Betroffenen beeinträchtigt werden können. Diese Vorschrift setzt eine Abwägung mit den schutzwürdigen Belangen der Betroffenen voraus. Der Verwaltungsaufwand, die Vermietung über die Mieter festzustellen, ist gering. Außerdem ist

nicht auszuschließen, dass - bei einer größeren Anzahl verschiedener Mieter - durch die Übersendung kompletter Mietverträge mit allen Nebenabsprachen schutzwürdige Belange tangiert sein könnten. Eine mit § 12 Nr. 5 begründete Datenübermittlung ist deswegen nicht zulässig.

21. Ordnungswidrigkeiten

Zeugenangabe im Bußgeldbescheid

Im sogenannten Vorverfahren einer Bußgeldsache kann im Anhörungsschreiben über einen Zeugenbeweis sowohl durch die Angabe des Namens und Wohnortes des Zeugen, als auch nur unter der Angabe „Zeuge/Zeugin“ informiert werden.

Im 22. Tätigkeitsbericht hatte ich unter Ziff. 5 die Ansicht vertreten, es genüge, wenn im Bußgeldbescheid nur der Name des Zeugen - ohne weitere Angaben - aufgeführt werde. Zwar gehöre nach § 66 Abs. 1 Nr. 4 des Ordnungswidrigkeitengesetzes (OWiG) die Angabe der Beweismittel zu den Pflichtangaben des Bußgeldbescheides, doch sei interpretationsfähig, in welcher Ausführlichkeit das Beweismittel zu bezeichnen ist.

§ 66 Abs. 1 OWiG

Der Bußgeldbescheid enthält
...
4. die Beweismittel, ...

Unter Hinweis auf § 222 Abs. 1 Strafprozessordnung (StPO) und § 46 Abs. 1 OWiG vertrat dagegen die Hessische Landesregierung die Auffassung, die Angabe des Namens müsse durch die Angabe des Wohnortes des Zeugen ergänzt werden.

§ 222 Abs. 1 StPO

Das Gericht hat die geladenen Zeugen und Sachverständigen der Staatsanwaltschaft und dem Angeklagten rechtzeitig namhaft zu machen und ihren Wohn- oder Aufenthaltsort anzugeben.
...

§ 46 Abs. 1 OWiG

Für das Bußgeldverfahren gelten, soweit dieses Gesetz nichts anderes bestimmt, sinngemäß die Vorschriften der allgemeinen Gesetze über das Strafverfahren, namentlich die Strafprozessordnung, das Gerichtsverfassungsgesetz und das Jugendgerichtsgesetz.

Da das Ordnungswidrigkeitengesetz nicht näher bestimmt, wie das Beweismittel zu bezeichnen ist, drängt sich die Anwendung von § 222 StPO auf. Dem Betroffenen soll die Prüfung möglich sein, ob der gegen ihn erhobene Vorwurf beweisbar ist. Da die Einlegung eines Einspruches für den Betroffenen mit Kosten verbunden ist, muss er die Erfolgsaussichten des Rechtsbehelfs abschätzen können. Beim Zeugenbeweis wird es regelmäßig im Verteidigungsinteresse liegen, Nachforschungen über die Person des Zeugen, insbesondere für dessen Glaubwürdigkeit beachtliche Umstände, anzustellen. Ansonsten kann der Betroffene einwenden, sein legitimes Verteidigungsinteresse sei ohne ersichtlichen Grund eingeschränkt worden.

Von mir wurde bisher dahin argumentiert, die regelmäßige Angabe des Wohnortes berücksichtige nicht hinreichend den Grundsatz der Verhältnismäßigkeit, insbesondere im Hinblick auf die Bedeutung des Vorwurfes bei Verkehrsordnungswidrigkeiten, die überwiegend geringfügige Verfehlungen im Straßenverkehr betreffen. Erst im Einzelfall sei dem Informationsinteresse des Betroffenen Rechnung zu tragen, z.B. bei Rückfragen oder bei Akteneinsichtsverlangen. Hingegen sei die „per Formular“ aufgedrängte Information über den Wohnort des Zeugen im Regelfall nicht erforderlich. Auch nach der Stellungnahme der Hessischen Landesregierung zu meinem 22. Tätigkeitsbericht (LTDrucks. 13/6384) blieb der Dissens zu diesem Sachverhalt erhalten.

Auf Grund mehrerer Eingaben von Zeugen, die sich über die Angaben zu Ihrer Person im Ordnungswidrigkeitenverfahren beschwerten, habe ich mich im Berichtszeitraum mehrmals mit dem Thema beschäftigt. In der Zwischenzeit hat die Praxis ein differenziertes Verfahren entwickelt: Das Datenverarbeitungsverfahren und die für die manuelle Vorgangsbearbeitung landeseinheitlich zu verwendenden Vordrucke sehen für das Vorverfahren die Auswahlmöglichkeit vor, dass entweder der Zeuge namentlich unter Angabe des Wohnortes zu benennen ist oder es erfolgt nur die Angabe: Beweismittel "Zeuge/Zeugin". In allen Verfahren, in denen ein Verwarnungsgeld festgesetzt werden kann, kann auf Angaben über den Zeugen verzichtet werden. Wird das Verwarnungsgeld bezahlt, kommt es zu keinem Bußgeldbescheid, in dem dann die Zeugenangaben zu offenbaren wären. Dies ist die große

Mehrzahl aller Fälle. Auch wenn der Betroffene den Vorwurf schlüssig zurückweisen kann und die Ordnungswidrigkeitenbehörde das Verfahren in diesem Stadium einstellt, kommt es nicht zum Bußgeldbescheid.

Ist ein Bußgeldbescheid zu erwarten, so ist die Vernehmung des Betroffenen zu gewährleisten. Das setzt die Kenntnis der Zeugen voraus, die den Vorwurf stützen. Bei Amtsträgern ist dies kein Problem. In den übrigen Fällen führt die Abwägung zwischen den datenschutzrechtlichen Interessen der Zeugen und dem Informationsinteresse der Bußgeldadressaten zur Zurückstellung der Zeugenbelange. Der Zeuge muss „mit offenem Visier“ kämpfen und die namentliche Bezeichnung nebst der Angabe seines Wohnortes hinnehmen. Ausnahmen sind nur bei besonderer Schutzbedürftigkeit der Zeugen zu machen, etwa bei Kindern (z.B. Schülerlotsen) oder psychisch hart betroffenen Opfern.

22. Allgemeines

Verwendung von Vordrucken

Bei der Verwendung von Vordrucken sollte mehr darauf geachtet werden, dass mit allgemeinen Formulierungen Anforderungen des Datenschutzes und besondere Amtsgeheimnisse nicht unterlaufen werden (siehe auch 27. Tätigkeitsbericht, Ziff. 24).

Ein Bürger beschwerte sich, dass die Gerichtskasse Frankfurt zur Durchsetzung von Forderungen personenbezogene Daten bei kommunalen Steuerämtern abfragt. Dazu benutzte die Gerichtskasse einen Vordruck, der im Adressfeld das jeweilige Steueramt einer Stadt vorsah. Außerdem wurde u.a. nach Inhabern, Geschäftsführern und persönlich haftenden Gesellschaftern von näher bezeichneten Firmen gefragt. Ein Zweck wurde nicht angegeben. Es handelte sich zwar um Daten, die problemlos aus dem jeweiligen (öffentlichen) Gewerberegister übermittelt werden konnten. Da die Anfragen aber an das Steueramt gerichtet waren, sollten die Daten aus der Steuerdatei übermittelt werden. Diese unterliegt dem Steuergeheimnis nach § 30 Abgabenordnung (AO). Eine Offenbarungsbefugnis der kommunalen Steuerämter bestand deswegen nicht.

Einige Städte erteilten die abgefragten Auskünfte – sachgerecht - aus der Gewerberegisterdatei, weil diese dort ebenfalls beim Steueramt geführt wurden. Ich habe das für den Vordruck verantwortliche Ministerium der Justiz gebeten, den Vordruck dahingehend zu ändern. Es stellte sich jedoch zunächst auf den Standpunkt, das Steuergeheimnis würde selbst bei Auskünften aus der Steuerdatei nicht verletzt. Die abgefragten Daten fielen nicht unter den geschützten sachlichen Inhalt des Steuergeheimnisses, da sie auch im öffentlich zugänglichen Handelsregister zu finden seien. Erst nachdem das Hessische Ministerium der Finanzen bestätigte, dass derartige Auskünfte auch dem Steuergeheimnis unterliegen und seinerseits die Änderung des Vordrucks anregte, wurde im Anschriftenfeld das "Steueramt der Stadt" durch das "Gewerberegister der Stadt" ersetzt.

23. Bilanz

23.1
Medizinische Unterlagen in Ausländerakten
(27. Tätigkeitsbericht, Ziff. 11.3)

Im vergangenen Jahr hatte ich über meine bei einer Datenschutzprüfung getroffene Feststellung berichtet, wonach medizinische Unterlagen zu Ausländerakten genommen wurden, ohne sie besonders gegen unberechtigte Einsichtnahmen zu schützen. Die geprüfte Ausländerbehörde hatte die besondere Aufbewahrung aller von mir beanstandeten Fälle zugesagt. Mit dem hessischen Innenministerium konnte eine für alle Ausländerbehörden gültige zufriedenstellende Lösung erreicht werden. Das Innenministerium hat meine Anregungen aufgenommen und angeordnet, psychiatrische und psychotherapeutische, aber auch alle sonstigen ärztlichen Atteste wegen der besonderen Sensitivität der in ihnen enthaltenen Daten verschlossen zu den Ausländerakten zu nehmen. Einsichtnahmen sollen dokumentiert werden. Falls erforderlich, können wesentliche Aussagen der Atteste oder Gutachten in einem in der Akte frei zugänglichen Vermerk zusammengefasst werden. Diese - mit mir abgestimmte - Verfahrensanweisung soll in Form eines Erlasses an alle Ausländerbehörden ergehen.

23.2
Inaktuelle Ausschreibungen über Ausländerinnen und Ausländer in polizeilichen Fahndungsdateien
(27. Tätigkeitsbericht, Ziff. 11.6)

Im 27. Tätigkeitsbericht (Ziff. 11.6) wurde über einen libanesischen Staatsangehörigen berichtet, der zwei Mal ungerechtfertigter Weise, auf Grund einer nicht aktuellen Datenspeicherung im polizeilichen Fahndungssystem, verhaftet worden war. Bei der nachfolgenden Prüfung wurde festgestellt, dass es sich nicht um einen Einzelfall handelte. Die von uns deswegen veranlasste Abstimmung mit dem Innenministerium hat die folgenden Ergebnisse erzielt:

- Die Löschungsverfügungen der Ausländerbehörden, die bislang bei der Polizei verblieben waren, sollen künftig den Ausländerbehörden zurückgegeben werden. Diese haben zu überwachen, ob ein Erledigungsvermerk der Polizei innerhalb einer angemessenen Frist eingeht. Damit wird gewährleistet, dass verfügte Löschungen auch tatsächlich umgesetzt werden.

- Vorgesehen ist weiter, dass die Ausländerbehörden künftig Akten, in denen eine Fahndungsausschreibung enthalten ist, in geeigneter Weise, etwa durch eine auffällige Beschriftung oder einen Aufkleber, besonders kennzeichnen. Dadurch soll jeder Bearbeiter sofort auf eine aktuelle Fahndung hingewiesen werden, damit er sie nicht übersieht und ggf. die Fahndungslöschung veranlasst.

- Nicht nur die Behörde, die eine Fahndungsausschreibung veranlasst hat, sondern auch die Behörde, die auf Grund eines Wohnungswechsels neu zuständig geworden ist, soll die Löschung einer Ausschreibung zur Fahndung verfügen dürfen.

- Ein Ausländer muss nicht gesondert beantragen, dass ein unbefristetes Wiedereinreiseverbot nachträglich befristet wird, wenn er inzwischen als Asylberechtigter anerkannt wurde. Der Antrag auf Erteilung einer Aufenthaltserlaubnis beinhaltet regelmäßig auch den Antrag nach § 8 Abs. 2 Satz 3 Ausländergesetz.

Durch die Absprache kann weitgehend ausgeschlossen werden, dass künftig erneut Verhaftungen aufgrund inaktueller Datenspeicherungen vorgenommen werden. Die abgesprochenen Verfahrensanweisungen und rechtlichen Klarstellungen sollen per Erlass den Ausländerbehörden vorgegeben werden. Der Erlass soll im Staatsanzeiger veröffentlicht werden.

Noch keine Einigung konnte bezüglich des vorhandenen Datenbestandes erzielt werden. 30.000 Ausländer sind nach einer Schätzung des Landeskriminalamtes auf Veranlassung hessischer Ausländerbehörden zur Fahndung ausgeschrieben. Im Gegensatz zu Ausschreibungen im Schengener Informationssystem - dort müssen die Datenspeicherungen nach drei Jahren geprüft und nach sechs Jahren regelmäßig gelöscht werden - werden Fahndungsausschreibungen in INPOL regelmäßig zehn Jahre aufrecht erhalten. Die deutlich längere Speicherung in INPOL sollte dem europäischen Standard angepasst werden, denn

sachlich zu rechtfertigende Gründe für die unterschiedliche Speicherungsdauer sind nicht erkennbar.

Fahndungsausschreibungen, die nicht nach der beschriebenen neuen Verfahrensweise erfolgt sind, sollten einer Prüfung unterzogen werden. Die Fehlerquote von 7% (a.a.O.) ist zu hoch, um sie einfach hinzunehmen.

23.3
Beschränkte Kontrolle des Personalrats durch den behördlichen Datenschutzbeauftragten
(27. Tätigkeitsbericht, Ziff. 15.1)

Im 27. Tätigkeitsbericht hatte ich die Ansicht vertreten, dass der behördliche Datenschutzbeauftragte nicht das Recht hat, den Personalrat gegen dessen Willen zu kontrollieren.

Die hessische Landesregierung und ich gehen übereinstimmend davon aus, dass der behördliche Datenschutzbeauftragte nach § 5 Abs. 2 Hessisches Datenschutzgesetz (HDSG) auch den Personalrat bei der Ausführung des Hessischen Datenschutzgesetzes zu unterstützen und Hinweise zur Umsetzung der Vorschriften zu geben hat. Insbesondere hat der Datenschutzbeauftragte die in Abs. 2 Satz 2 Nr. 1 bis 5 HDSG genannten Aufgaben zu erfüllen.

Der Einblick in Vorgänge, die Personaldaten enthalten, ist ihm nach § 5 Abs. 2 Satz 3 HDSG ohne Einwilligung der Betroffenen verwehrt, da das Personalaktengeheimnis entgegen steht.

Ist das Personalaktengeheimnis nicht betroffen, so steht die Aufgabenwahrnehmung mit dem Gesetz in Einklang, wenn der Personalrat der Kontrolle durch den behördlichen Datenschutzbeauftragten zugestimmt hat. Ohne Zustimmung würde die Einsicht in Akten und Dateien des Personalrats dem Gebot der Friedenspflicht gemäß § 60 Abs. 3 Hessisches Personalvertretungsgesetz (HPVG) widersprechen. Bei fehlender Zustimmung des Personalrats wird es sich aufdrängen, dass der behördliche Datenschutzbeauftragte mich

unterrichtet, damit ich die erforderlichen Schritte zur Beachtung der datenschutzrechtlichen Vorschriften durch den Personalrat einleiten kann.

23.4

Automatisierte Abgleiche im Sozialhilferecht

Im 27. Tätigkeitsbericht (Ziff. 14.1) hatte ich mich mit der begonnenen Umsetzung von § 117 Bundessozialhilfegesetz (BSHG) befasst, der einen automatisierten Datenabgleich zwischen den Trägern der Sozialhilfe untereinander und mit den Trägern der gesetzlichen Unfall- und Rentenversicherung sowie der Bundesanstalt für Arbeit zulässt.

Auf meine Bitte hin hatte mir die Stadt Frankfurt erste Ergebnisse der Vollziehung des § 117 BSHG zugeleitet; für den Zeitraum vom 1. Januar 1998 bis 31. März 1998 konnte ein unrechtmäßiger Leistungsbezug in Höhe von 1.275.154,10 DM durch den Datenabgleich ermittelt werden.

Mittlerweile hat die Stadt Frankfurt über weitere Datenabgleiche berichtet: Im zweiten Abgleich (1. April 1998 bis 30. Juni 1998) wurde ein unrechtmäßiger Leistungsbezug in Höhe von 546.161,36 DM ermittelt, also ein deutlich geringerer Betrag als im ersten Datenabgleich. An sich wäre zu erwarten gewesen, dass sich diese Tendenz fortsetzt. Überraschend wurde im anschließenden dritten Datenabgleich (1. Juli 1998 bis 30. September 1998) ein unrechtmäßiger Leistungsbezug in Höhe von 761.975,45 DM festgestellt. Im vierten Abgleich (1. Oktober 1998 bis 31. Dezember 1998) ist die Höhe der unrechtmäßigen Leistungsbezüge wieder auf 207.200,00 DM gesunken. Nunmehr liegt auch der Bericht über das Ergebnis des ersten Quartals 1999 vor; die Höhe der unrechtmäßig bezogenen Leistungsbezüge ist wieder gestiegen, auf 341.700,80 DM.

Diese Ergebnisse rechtfertigen den Abgleich. Hinzu kommt die Präventivwirkung solcher Abgleiche. Die Stadt Frankfurt hält gerade auch deshalb die Aufrechterhaltung der Abgleiche für geboten. Dem ist nicht entgegenzutreten.

23.5

Anspruch und Wirklichkeit bei der Umsetzung des Psychotherapeutengesetzes im Hinblick auf die Nachqualifizierung von Therapeutinnen und Therapeuten

Fast 3.200 Anträge auf Erteilung der Approbation und mehr als 2.000 Anträge auf Erteilung einer bedarfsunabhängigen Zulassung wurden bis zum 31. Dezember 1998 bei den zuständigen Stellen in Hessen gestellt. Über die Handhabung der Verfahren habe ich mich im Februar und März 1999 beim Landesprüfungsamt für Heilberufe in Frankfurt am Main und bei der Kassenärztlichen Vereinigung in Frankfurt am Main stichprobenhaft informiert. Nach meinen Feststellungen wurde nur ein Teil der Unterlagen hinreichend anonymisiert.

In meinem letztjährigen Tätigkeitsbericht (27. Tätigkeitsbericht, Ziff. 7.2) hatte ich dargelegt, dass im Rahmen der Umsetzung des zum 1. Januar 1999 in Kraft getretenen Gesetzes über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichen-Therapeuten (PsychThG) auf Grund der Forderungen der Datenschutzbeauftragten ein Verfahren entwickelt wurde, das den datenschutzrechtlichen Anforderungen genügt und der Schweigepflicht i.S.v. § 203 Strafgesetzbuch (StGB) entspricht. Das datenschutzgerechte Verfahren wurde im Ausführungserlass des Hessischen Ministeriums für Umwelt, Energie, Jugend, Familie und Gesundheit zur Umsetzung des Gesetzes über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichen-Therapeuten zur Änderung des V. Buches Sozialgesetzbuch und anderer Gesetze (BGBl. I 1998 S. 1311) im Hinblick auf die Nachqualifizierungsvorschriften des Gesetzes umgesetzt.

Insbesondere ist in dem Ausführungserlass die Bestimmung enthalten, dass patientenbezogene Nachweise für die Vorlage bei der Approbationsbehörde in geeigneter Weise anonymisiert sein müssen. Dieser Grundsatz hat selbstverständlich auch für das Verfahren für die Kassenzulassung zu gelten.

Bei meinen Informationsbesuchen im Hessischen Landesprüfungsamt für Heilberufe in Frankfurt am Main sowie der Geschäftsstelle des Zulassungsausschusses der Kassenärztlichen Vereinigung Hessen in Frankfurt am Main stand die Frage der Umsetzung des Ausführungserlasses im Vordergrund.

Zunächst ist festzustellen, dass mich die Mitarbeiterinnen und Mitarbeiter der beiden Dienststellen trotz des hohen Arbeits- und Zeitdrucks auf Grund der gesetzlich festgelegten Terminvorgaben zur Erteilung der Approbation bis spätestens zum 31. März 1999 sowie der bedarfsunabhängigen Zulassung bis spätestens zum 30. April 1999 umfassend unterstützt haben.

Aufgrund des Ausführungserlasses hatte ich erwartet, dass das Landesprüfungsamt und der Zulassungsausschuss der Kassenärztlichen Vereinigung den Antragstellern konkret mitteilen, dass nur vollständig anonymisierte Patientenunterlagen vorzulegen sind. Auch war hinsichtlich der Umsetzung des Psychotherapeutengesetzes i.V.m. der ärztlichen Schweigepflicht i.S.d. § 203 StGB aufgrund einer Anfrage des Berufsverbandes Deutscher Psychologinnen und Psychologen e.V. in Bonn vom 3. September 1998 zu erwarten, dass die Antragsteller nur vollständig anonymisierte Unterlagen für die Prüfungen vorlegen. Dem umfangreichen Antragsvordruck des Hessischen Landesprüfungsamtes auf Erteilung der Approbation war in der Vergangenheit allerdings ein Zettel mit folgendem Inhalt beigefügt:

> Wichtiger Hinweis:
> Nachweise über Behandlungstätigkeiten sind für die Antragstellung nach Möglichkeit zu anonymisieren.
>
> Soweit eine Anonymisierung von Unterlagen z.B. zu aufwendig wäre und deswegen nicht erfolgt, wird selbstverständlich Amtsverschwiegenheit gewährleistet.

Dieser Hinweis gab die Rechtslage nicht korrekt wieder, denn die Therapeuten durften ihre Unterlagen ohne Einwilligung der Betroffenen nicht personenbezogen übermitteln. Es entsprach auch nicht dem im Ausführungserlass vorgesehenen Verfahren. Ich habe daher das Verfahren gegenüber dem Sozialministerium kritisiert. Das Sozialministerium hat meiner Rechtsauffassung zugestimmt.

Das Ergebnis der stichprobenhaften Überprüfung der Unterlagen war gemischt. Zum Teil waren in den Behandlungsunterlagen die Patientenangaben vollständig unkenntlich gemacht. In einem anderen Teil waren Patientennamen, Geburtsdaten, Adressen zwar geschwärzt, dies aber so unzureichend, dass die Daten durchaus noch lesbar waren. Weiter gab es

Antragsteller, die gar keine Anonymisierung von Patientendaten vorgenommen hatten. In einem Antragsfall, bestehend aus drei Ordnern, hatte ich den Eindruck, dass die kompletten Patientendateien mit Behandlungsdokumentationen dem Landesprüfungsamt übersandt wurde. Diesen Eindruck hat zudem die zuständige Sachbearbeiterin des Landesprüfungsamtes bestätigt. In diesem Fall war kein Patientendatum anonymisiert. Dass im konkreten Einzelfall sowie in anderen Fällen die Einwilligung der Patienten in die Weitergabe ihrer Daten eingeholt wurde, war nicht erkennbar.

Dass die Anonymisierung von patientenbezogenen Unterlagen zu aufwendig wäre, lässt sich einfach widerlegen, da mir Akten vorgelegen haben, in denen eine komplette Anonymisierung durchgeführt wurde. Anhand der Stichproben war eine genaue Schätzung nicht anonymisierter Akten nur schwer möglich. Sie dürfte bei etwa einem Drittel liegen. Der Einstieg in das Psychotherapeutengesetz ist daher unter datenschutzrechtlichen Gesichtspunkten nur bedingt gelungen.

Von den rund 3.200 Antragstellern auf Erteilung der Approbation durch das Landesprüfungsamt für Heilberufe haben mehr als 2.000 Antragsteller beim Zulassungsausschuss der Kassenärztlichen Vereinigung Hessen den Antrag auf bedarfsunabhängige Zulassung zum Psychologischen Psychotherapeuten oder zum Kinder- und Jugendlichen-Therapeuten gestellt. Die Anträge bei beiden Stellen mussten bis spätestens 31. Dezember 1998 vorgelegt werden. Der Zulassungsausschuss bei der Kassenärztlichen Vereinigung hatte für die bedarfsunabhängige Zulassung weitgehend die selben Antragsunterlagen zu prüfen wie das Landesprüfungsamt für Heilberufe. Die Entscheidung zur Zulassung wurde jeweils in mündlicher Verhandlung des Ausschusses getroffen. Bei Abwesenheit wurde nach Aktenlage verhandelt. Die beim Landesprüfungsamt eingereichten Unterlagen sind mit Zustimmung der jeweiligen Antragsteller vom Landesprüfungsamt an die Kassenärztliche Vereinigung abgegeben worden. Das betrifft auch die nicht anonymisierten Patientendaten.

Angesichts der Tatsache, dass das vorgesehene Verfahren der Anonymisierung nicht vollständig eingehalten worden war, war es von zentraler Bedeutung, sicherzustellen, dass die Datensicherheit beim Landesprüfungsamt und beim Zulassungsausschuss gewährleistet ist und die Unterlagen den jeweiligen Antragstellern so schnell wie möglich zurückgesandt werden. Meine Überprüfung ergab, dass beide Stellen ausreichende

Datensicherheitsmaßnahmen getroffen hatten. Über die erfolgte Zurücksendung der Unterlagen sowie über den Umgang mit Unterlagen nach abgelehnten Anträgen, im Widerspruchsverfahren und im Verwaltungsstreitverfahren habe ich mich im Herbst informiert. Beanstandungen ergaben sich nicht, insbesondere wurden die Antragsunterlagen ordnungsmäßig zurückgegeben. Aus den Akten im Widerspruchsverfahren war ersichtlich, dass eine erneute Vorlage von Behandlungsunterlagen nicht erfolgte.

24. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

24.1
Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein "Zwei-Stufen-Konzept" vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, dass das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbringung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken.

Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der Kontrolle im nicht öffentlichen Bereich muss institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z.B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substanziellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsersuchen, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

24.2

Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation

Die Bundesregierung und der Bundesrat werden demnächst über den Erlass der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnsetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, dass die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Datenschutzverordnung, dass alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbindung stattfand, kann dies in Einzelfällen dazu führen, dass die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation. Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur solange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die

Speicherung von Verbindungsdaten muss sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundinnen und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlass für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, dass diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

24.3

Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Transparente Hard- und Software

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number - PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen

und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, dass Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.

Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

24.4
Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. März 1999

Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL 98)

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFOPOL 98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, dass der entsprechende Entwurf bisher geheim gehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z.B. prepaid cards) nicht konterkariert wird.

24.5

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17. Juni 1999

Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern

Bei der Einführung der Befugnis zum "Großen Lauschangriff" hat der Gesetzgeber im Grundgesetz ein Verfahren zur parlamentarischen Kontrolle weit reichender Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung verankert (Art. 13 Abs. 6 GG). Dieses Verfahren dient nach dem Willen des Gesetzgebers der parlamentarischen Kontrolle der Normeffizienz und hebt zugleich die politische Kontrollfunktion der Parlamente gegenüber der Exekutive hervor. Auch wenn es die Überprüfung von Lauschangriffen durch die Gerichte und Datenschutzbeauftragten nicht ersetzt, hat es gleichwohl eine grundrechtssichernde Bedeutung. Jetzt ist jedoch bekannt geworden, dass einige Landesjustizverwaltungen der Ansicht sind, Art. 13 Abs. 6 GG sehe eine Berichtspflicht über Lauschangriffe zu Strafverfolgungszwecken gegenüber den Landesparlamenten nicht vor.

Im Gegensatz dazu vertritt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Auffassung, dass die Verfassung eine effektive parlamentarische Kontrolle von

Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muss. Bei Maßnahmen zur Strafverfolgung durch Landesbehörden besteht die parlamentarische Verantwortlichkeit gegenüber den Landesparlamenten. Die Landtage müssen die Möglichkeit haben, die ihnen in anonymisierter Form übermittelten Berichte der Landesregierungen öffentlich zu erörtern. Die Landesparlamente sollten deshalb durch Gesetz eine regelmäßige Berichtspflicht der Landesregierung für präventiv-polizeiliche und repressive Lauschangriffe vorsehen. Nur auf diese Weise ist eine wirksame parlamentarische Kontrolle der Ausübung dieser einschneidenden Überwachungsbefugnisse gewährleistet.

Wird durch eine solche Kontrolle deutlich, dass die akustische Wohnraumüberwachung für Zwecke der Strafverfolgung in der Praxis nicht die vom Gesetzgeber angestrebte Effizienz im Verhältnis zur Häufigkeit und Intensität der Grundrechtseingriffe zeigt, können Landesregierungen, die das Bundesrecht in eigener Verantwortung auszuführen haben, über den Bundesrat darauf hinwirken, die Befugnis für eine derartige Überwachung wieder aufzuheben oder zumindest zu modifizieren.

24.6
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1999

Gesundheitsreform 2000

Die Datenschutzbeauftragten von Bund und Ländern erklären zu dem Entwurf eines Gesetzes "Gesundheitsreform 2000":

Die Datenschutzbeauftragten haben großes Verständnis für die Bemühungen, die Kosten im Gesundheitswesen zu begrenzen und eine gute Versorgung der Patientinnen und Patienten sicherzustellen. Bei der Wahl der Mittel ist es aber Aufgabe des Gesetzgebers, beim Eingriff in das Recht auf informationelle Selbstbestimmung das Prinzip der Erforderlichkeit und der Verhältnismäßigkeit zu wahren.

Der Entwurf lässt jede Begründung vermissen, warum die bisherigen Kontrollmechanismen, die das Entstehen umfangreicher medizinischer Patientendatenbestände bei den Krankenkassen vermeiden, ungeeignet sein sollen, die Wirtschaftlichkeit und Qualität ärztlicher Leistungserbringung sicherzustellen.

Der Entwurf gibt das bisherige Konzept der Datenverarbeitung in der gesetzlichen Krankenversicherung auf. Insbesondere standen bisher aus dem ambulanten Bereich personenbezogene Abrechnungsdaten mit medizinischen Inhalten und Diagnosedaten den Krankenkassen nur ausnahmsweise zu Prüfzwecken zur Verfügung, künftig sollen diese Informationen den Krankenkassen dagegen generell versichertenbezogen übermittelt werden. Damit entstehen bei den gesetzlichen Krankenkassen vollständige personenbezogene medizinische Datenbestände der gesetzlich Versicherten mit der Möglichkeit, für jede einzelne Person umfassende Darstellungen ihres Gesundheitszustandes zu bilden. Bei den Kassen entstehen gläserne Patientinnen und Patienten. Das Patientengeheimnis wird ausgehöhlt.

Die Datenschutzbeauftragten richten an den Gesetzgeber die dringende Bitte, die bisher versäumte eingehende Prüfung von Erforderlichkeit und Verhältnismäßigkeit der weiterreichenden Datenverarbeitungsbestimmungen nachzuholen. Der Bundesbeauftragte für den Datenschutz, mit dem der Entwurf entgegen anders lautenden Äußerungen von Regierungsvertretern in der Sache bisher in keiner Weise abgestimmt wurde, sowie die Datenschutzbeauftragten der Länder stehen hierfür zur Diskussion zur Verfügung.

Insbesondere klärungsbedürftig sind folgende Punkte:

- Der Entwurf erweitert die Aufgaben der Krankenkassen auch auf eine steuernde und durch die Patientinnen und Patienten nicht geforderte Beratung über Gesundheitserhaltungsmaßnahmen und auf eine Prüfung der u.a. durch die Ärztinnen und Ärzte erbrachten Leistungen. Er sieht dafür umfangreiche Datenerhebungs- und -verarbeitungsbefugnisse vor.

Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne

rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

Wegen der vagen Aufgabenbeschreibung sind auch die damit verbundenen Datenverarbeitungs- und -zusammenführungsbefugnisse in gleicher Weise unklar und verschwommen. Eine Präzisierung und Eingrenzung ist dringend erforderlich.

Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z.B. im Bereich der Psychotherapie auch hochdifferenziert.

Die zur Begründung besonders angeführten Punkte "Unterrichtung der Versicherten über die in Anspruch genommenen Leistungen, Kontrolle der Einhaltung der zweijährigen Gewährleistungspflicht bei den Zahnärzten, Unterstützung der Versicherten bei Behandlungsfehlern" vermögen insoweit nicht zu überzeugen. Bereits jetzt können die Versicherten über die beanspruchten Leistungen und deren Kosten informiert werden und von ihrer Krankenkasse auch im Übrigen Unterstützung erbitten, sodass keine Notwendigkeit für die Anlegung derart sensibler, umfangreicher und zentraler Datenbestände ersichtlich ist.

Der Eingriff in die Rechte der Patientinnen und Patienten steht damit in keinem Verhältnis zu den angegebenen Zwecken.

Die beabsichtigte Einführung von zentralen Datenannahme- und -verteilstellen, bei denen nicht einmal klar ist, in welcher Rechtsform (öffentlich oder privat) sie betrieben werden sollen, hat eine weitere, diesmal Krankenkassen übergreifende zentrale Sammlung medizinischer personenbezogener Patientendaten zur Folge. Wegen des hohen weiteren Gefährdungspotenzials von derart umfassenden Datenbeständen müsste der Entwurf im

Einzelnen begründen, warum eine konsequente Umsetzung der schon bisher möglichen Kontrollmechanismen nicht ausreicht.

Die angesprochenen Punkte stellen besonders gewichtige, aber keineswegs die einzigen Probleme dar. Zu nennen sind hier nur beispielsweise die Verlängerung der Speicherdauer von Patientendaten beim Medizinischen Dienst der Krankenversicherung (MDK) von 5 auf 10 Jahre, unzureichende Regelungen bei den Speicherfristen, bei Umfang, Zweckbindung und Freiwilligkeit der Datenerhebung beim Hausarztmodell, der integrierten Versorgung und den Bonus-Modellen sowie unzureichende Pseudonymisierung bei den Arbeitsgemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

24.7
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16. August 1999

Angemessener Datenschutz auch für Untersuchungsgefangene

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, dass die Bundesregierung den Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft vorgelegt hat. Damit wird die seit Jahren erhobene Forderung der Datenschutzbeauftragten nach einer bereichsspezifischen gesetzlichen Regelung aufgegriffen.

Diese Regelung muss das Strafverfolgungs- und Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft berücksichtigen. Gleichzeitig sind jedoch das Persönlichkeitsrecht der Gefangenen sowie die Unschuldsvermutung und der Anspruch auf wirksame Verteidigung im Strafverfahren angemessen zur Geltung zu bringen.

Der Gesetzesentwurf der Bundesregierung trägt diesem Anliegen durch differenzierende Vorschriften teilweise Rechnung, lässt allerdings noch Raum für datenschutzrechtliche Verbesserungen. Die Stellungnahme des Bundesrates betont demgegenüber einseitig das staatliche Vollzugsinteresse und entfernt sich damit deutlich vom Ziel einer sorgfältigen Güterabwägung.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder muss die gesetzliche Regelung insbesondere folgenden Anforderungen genügen:

- Entgegen dem Vorschlag des Bundesrates, von einer inhaltlichen Überwachung nur ausnahmsweise nach dem Ermessen des Gerichts abzusehen, sollte im weiteren Gesetzgebungsverfahren an der Konzeption der Bundesregierung festgehalten werden. Der Gesetzentwurf der Bundesregierung differenziert bei der Überwachung der Unterhaltung mit Besucherinnen und Besuchern sowie bei der Kontrolle des Textes von Schriftstücken sachgerecht nach Haftgründen. Nur im Falle der Untersuchungshaft wegen Verdunkelungsgefahr sollten diese Maßnahmen unmittelbar und generell durch Gesetz vorgeschrieben werden, während sie bei Vorliegen anderer Haftgründe (z.B. Fluchtgefahr) nur im Einzelfall auf Grund richterlicher Anordnung erfolgen dürfen.

- Darüber hinaus sollte im weiteren Gesetzgebungsverfahren die Möglichkeit unüberwachter Kontakte der Gefangenen zu nahen Angehörigen mit Zustimmung der Staatsanwaltschaft auch in Fällen der Untersuchungshaft wegen Verdunkelungsgefahr erwogen werden. Stichprobenartige Überprüfungen von Schriftstücken durch die Vollzugsanstalt an Stelle einer Textkontrolle sollten nicht den gesamten Schriftverkehr einzelner Gefangener umfassen. Dies könnte sich im Ergebnis als verdachtsunabhängige Totalkontrolle ohne richterliche Entscheidung auswirken.

- Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigten muss auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot wirksamer Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen, wie vom Bundesrat befürwortet.

- Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt (z.B. Sozialleistungsträger, Ausländerbehörden) und an Forschungseinrichtungen müssen die schutzwürdigen Interessen der Betroffenen im Rahmen einer Abwägung berücksichtigt werden. Auch die Erteilung von Auskünften an die Verletzten der Straftat sollte der Gesetzgeber unter Beachtung der Unschuldsvermutung regeln.

- Die vom Bundesrat vorgeschlagene erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen im Hinblick auf den Zweck der Untersuchungshaft würde wesentliche Datenschutzrechte in einem besonders sensiblen Bereich weitgehend entwerten und ist daher abzulehnen.

24.8

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 9./10. März 1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16. August 1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss von 17. September 1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

24.9

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Täter-Opfer-Ausgleich und Datenschutz

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BRDrs. 325/99 vom 28. Mai 1999) sieht in § 155a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des "Täter-Opfer-Ausgleichs" nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als "objektive Dritte mit dem Gebot der Unterstützung jeder Partei" könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die "fachlich geleitete Auseinandersetzung" der "am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden".

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z.B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am "Täter-Opfer-Ausgleich" Beteiligten muss gesetzlich geschützt werden.

24.10

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, sodass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz

personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte
(z.B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger“ besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,

- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,

- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z.B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),

- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,

- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,

- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offengelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

24.11

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: "Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

24.12

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Patientenschutz durch Pseudonymisierung

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z.B.

Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des "gläsernen Patienten" verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

24.13

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

In der Strafprozessordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u.a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis - also ohne

richterliche Anordnung - erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z.B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflusst, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen - abweichend von den gesetzlich vorgesehenen Verfahren - systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Reglung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

24.14

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7./8. Oktober 1999

Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat

einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil auf Grund der weit reichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.
Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31. Dezember 1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern stattdessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100a StPO neu geregelt werden.

25. Materialien

25.1
Hinweise, Checkliste und Ablauf zur Vorabkontrolle nach § 7 Abs. 6 Hessisches Datenschutzgesetz

25.1.1
Grundsätzliches zur Vorabkontrolle

Vor dem Einsatz oder der wesentlichen Änderung eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten ist nach § 7 Abs. 6 HDSG die sogenannte „Vorabkontrolle“ durchzuführen. Dies ist eine Untersuchung, ob durch die beabsichtigte automatisierte Datenverarbeitung das in § 1 Abs. 1 Nr. 1 HDSG beschriebene Recht der informationellen Selbstbestimmung (das Datenschutzrecht als Persönlichkeitsrecht des Einzelnen) gefährdet wird. Die in Zusammenarbeit mit dem Hessischen Innenministerium und einigen behördlichen Datenschutzbeauftragten entwickelte inhaltliche Checkliste und das Ablaufschema bieten zwar für die meisten Fälle eine gute Orientierung, können aber nicht alle denkbaren Aspekte der Vorabkontrolle abdecken. Unterschiede in Intensität und relevanten Prüfungspunkten entstehen zwangsläufig wegen der unterschiedlichen Sensitivität der zu verarbeitenden personenbezogenen Daten, der unterschiedlichen Risikofaktoren und der unterschiedlichen Sicherheitskonzepte.

Die Checkliste und das Ablaufschema sind auf eine Vielzahl von Prüfungen automatisierter Verfahren anwendbar, z.B. wenn es um die datenschutzrechtliche Prüfung im Rahmen der Auswahl zwischen verschiedenen Softwareprodukten geht.

Nachfolgend sind besondere Fälle betrachtet, bei denen bereits vorhersehbar ist, dass eine Vorabkontrolle von diesem Schema abweichen kann:

- Bei **Verfahren**, die **speziell** für die Verarbeitung personenbezogener Daten im Rahmen einer bestimmten Aufgabenstellung **neu entwickelt** werden, ist die Checkliste parallel zur Entwicklung abzuarbeiten und dabei sind die in Betracht gezogenen Verfahrensalternativen datenschutzrechtlich zu bewerten.

- Bei **komplexen Verfahren**, die für die Verarbeitung personenbezogener Daten den Einsatz **verschiedener** Komponenten und Optionen ermöglichen (z.B. SAP/R3), wird die Vorabkontrolle nicht schon vor der prinzipiellen Entscheidung, welches Verfahren eingesetzt werden soll, erfolgen können. Sie lässt sich regelmäßig erst parallel zu Auswahl und Erprobung jener Komponenten durchführen, mit denen die personenbezogenen Daten verarbeitet werden, also wenn feststeht, welche Komponenten welche personenbezogenen Daten wie und auf welche Weise verarbeiten sollen. Auch die angebotenen Alternativen für ein Sicherheitskonzept sind von vielfältigen Randbedingungen abhängig, die nicht global, sondern nur für den konkreten Einsatz beurteilt werden können. Deshalb wird bei solchen Verfahren die Vorabkontrolle schrittweise parallel zu einer entsprechenden Konkretisierung erfolgen.

- Für **Standardverfahren, die** ohne Anbindung an eine bestimmte Verwaltungsaufgabe **übergreifend als „Werkzeug“** für verschiedene Aufgaben eingesetzt werden (z.B. einfache Telefonanlagen, Textverarbeitung), ist für die Einsatzfelder, bei denen personenbezogene Daten verarbeitet werden sollen, eine Vorabkontrolle durchzuführen. Ein Verfahrensverzeichnis ist für das Standardverfahren als solches nicht notwendig (Erlass des HMdI zu §§ 6 und 15 HDSG, StAnz 17/1999, S. 1226). Zweck der Vorabkontrolle solcher Verfahren ist festzustellen, ob der geplante Einsatz zur Verarbeitung personenbezogener Daten rechtmäßig ist; insbesondere muss sichergestellt sein, dass mögliche Risiken erkannt und durch entsprechende Sicherheitsmaßnahmen minimiert werden.

  Bei dem Einsatz einer Telefonanlage wird deshalb z.B. zu untersuchen sein, welche Daten dort und wozu gespeichert werden, ob dies von der Rechtsgrundlage gedeckt ist, wer Zugriff auf diese Daten hat und wann sie gelöscht werden müssen.

  Vor dem Einsatz eines Textprogramms, mit dem auch personenbezogene Daten verarbeitet werden (und seien es nur Anschriften in Briefen), sollte die Stelle sich klar werden, für welche personenbezogene Arbeiten die Textverarbeitung eingesetzt werden soll. Für **weniger kritische** Einsatzfelder (z.B. Einsatz in der allgemeinen Verwaltung zum Schriftverkehr mit Firmen im Rahmen der Beschaffung, Schriftverkehr mit Bürgern und Behörden, bei dem außer der Anschrift kaum personenbezogene und keine sensitiven Daten ausgetauscht werden) wird die Vorabkontrolle schnell erledigt sein:

Rechtsgrundlage der Verarbeitung ist § 11 HDSG, es sind nur geringe Risiken anzunehmen und es werden in der Regel einfache Maßnahmen der Zutritts-, Benutzer- und Zugriffskontrolle genügen.

Kritische und sensible Einsatzfelder gebieten strengere Anforderungen - z.B. im Sozialamt für die Bearbeitung von Anträgen, den Verkehr mit dem Gesundheitsamt; in der Personalabteilung für Personallisten mit Beurteilungsnoten, für Beurteilungen und Zeugnisse; in Prüfungsämtern für Zeugnisse, Beurteilungen und Notenlisten; im Krankenhaus für das Schreiben von Arztberichten und Gutachten. Die Rechtmäßigkeit ist hier sorgfältig zu prüfen und die dem höheren Risiko entsprechenden Sicherheitsmaßnahmen (z.B. Verschlüsselungen, spezieller Zugriffsschutz, spezieller Speicherort oder Netzabsicherung) und organisatorische Vorkehrungen müssen anhand des § 10 Abs. 2 HDSG im Einzelnen festgelegt werden. Für alle Anwendungskategorien sollten Löschungsfristen festgelegt werden.

Ist zu einem späteren Zeitpunkt beabsichtigt, ein Standardverfahren über das ursprüngliche Konzept hinaus für **neue** Anwendungsfelder der Verarbeitung personenbezogener Daten zu nutzen, liegt ein Fall der **Verfahrensänderung** vor. Für diese neuen Anwendungen ist eine Vorabkontrolle durchzuführen bzw. die ursprüngliche insoweit fortzuschreiben.

25.1.2
Checkliste

Die Vorabkontrolle nach § 7 Abs. 6 HDSG soll sicherstellen, dass durch die beabsichtigte automatisierte Datenverarbeitung das in § 1 Abs. 1 Nr. 1 HDSG beschriebene Recht der informationellen Selbstbestimmung (das Datenschutzrecht als Persönlichkeitsrecht des Einzelnen) nicht gefährdet wird. Diese Untersuchung stellt für die beabsichtigte automatisierte Verarbeitung personenbezogener Daten den Schutzbedarf und die Risiken fest und bewertet, insbesondere unter Berücksichtigung der technischen und organisatorischen Maßnahmen, ob Gefahren für das Persönlichkeitsrecht angemessen verhindert werden. Verfährt man nach dem nachfolgenden Schema, hat das den Vorteil, dass im Hinblick auf das ausgewählte Verfahren Doppelarbeit vermieden wird, weil bereits Festlegungen abgefragt

werden, die ohnehin für das nach § 6 HDSG zu erstellende Verfahrensverzeichnis erforderlich sind.

Sind verschiedene Verfahrensalternativen vorhanden, sollte die Vorabkontrolle mit der Angabe dieser Alternativen beginnen. Folgender Ablauf ist - ggf. für jede Alternative - zu durchlaufen:

(Die als Klammerzusatz angegebenen Nummern beziehen sich jeweils auf die Nummerierung im Formular „Verfahrensverzeichnis“)

1. Grundangaben
   - zur datenverarbeitenden Stelle (Nr. 1)
   - zur Zweckbestimmung (Nr. 2.1)
   - zur Rechtsgrundlage (Nr. 2.3)
   - zur Art der gespeicherten Daten (Nr. 3)
   - zur Schutzbedürftigkeit der Daten, insbesondere bei sensitiven Daten im Sinne von § 7 Abs. 4 HDSG oder sonst besonders schutzbedürftigen Daten
   - zum Kreis der Betroffenen (Nr. 4)
   - zur Übermittlung (Nr. 5 und 10)
   - zu den zugriffsberechtigten Personengruppen (Nr. 6)
   - zu den Fristen für die Löschung (Nr. 9)

   Dabei werden die meisten Angaben für alle Alternativen gleich sein.

2. Prüfung, ob
   - die Art der gespeicherten Daten (Nr. 3)
   - die Übermittlungen (Nr. 5 und 10)
   - die Eingrenzung der Zugriffsberechtigten (Nr. 6)
   - die Löschfristen (Nr. 9)

   von der angegebenen Zweckbestimmung und Rechtsgrundlage (Nr. 2) gedeckt sind, insbesondere auch unter Berücksichtigung des Grundsatzes der Datensparsamkeit nach § 10 Abs. 2 HDSG. Ist dies nicht der Fall, muss geprüft werden, ob Änderungen im Verfahren möglich sind, die zu einem positiven Ausgang der Prüfung führen. Falls dies nicht möglich ist, ist die Alternative auszuschließen.

3. Prüfung, ob die Rechte der Betroffenen nach § 8 HDSG gewahrt sind.
   - Können die erforderlichen Auskünfte, Berichtigungen, Sperrungen und Löschungen durchgeführt werden?
   - Ist sichergestellt, dass der Betroffene in Fällen des § 8 Abs. 3 HDSG seine Rechte

   ohne unvertretbaren Aufwand geltend machen kann?
   Auch hier ist im Negativfall die Nachbesserungsmöglichkeit zu prüfen und wenn auch diese mit negativem Ergebnis endet, ist die Alternative auszuschließen.

4. Risikofaktoren für einen Missbrauch der Daten sind zu ermitteln. Dies sind Gefahren für
   - die Vertraulichkeit
   - die Integrität
   - die Verfügbarkeit

   der Daten. Dazu gehören z.B. die Gefahr, dass Datenträger oder „Computerlisten“ während des Transports gestohlen werden, Virenbefall, Gefahr von unbefugten Zugriffen. Ggf. sind Personengruppen, die für missbräuchliche Verwendung in Frage kommen, zu benennen.

5. Beurteilung der möglichen Folgen bei missbräuchlicher Verwendung der Daten, z.B.
   - Gefahren oder Nachteile für die Betroffenen
   - Schadensersatzansprüche
   - finanzielle Schäden
   - „Vertrauensschaden"

6. Angaben zu der Technik des Verfahrens:
   - Einzelplatz (Nr. 8.1)
   - bei vernetzten Rechnern auch Angaben zur Netzstruktur und Datenhaltung (Nr. 8.2)
   - eingesetzte Software (Nr. 8.3)
   - sowie zu den technischen und organisatorischen Maßnahmen nach § 10 HDSG (Nr. 7)

7. Abgleich der Risikofaktoren unter besonderer Berücksichtigung der Schutzbedürftigkeit der personenbezogenen Daten mit den getroffenen Sicherheitsmaßnahmen und Entscheidung, ob das Restrisiko unter Anwendung des Verhältnismäßigkeitsgrundsatzes tragbar ist. Ist das Restrisiko zu hoch, ist zu prüfen, ob eine Nachbesserung der Technik des Verfahrens oder der technischen und organisatorischen Maßnahmen eine positive

Bewertung ergibt. Ist dies nicht der Fall, ist die Alternative auszuschließen. Bei vertretbarem Restrisiko endet die Vorabkontrolle dieser Alternative mit positivem Ergebnis.

Schriftlich festzuhalten ist, welche Alternativen geprüft wurden, die Risikoabwägung und die Gründe für die Auswahl der Alternative.

Das Ergebnis der Vorabkontrolle und die Begründung sind dem behördlichen Datenschutzbeauftragten zur Prüfung vorzulegen.

Anliegendes Ablaufschema soll die Reihenfolge der Schritte optisch veranschaulichen.

25.1.3
Ablauf einer Vorabkontrolle

Zunächst ist für die Prüfung der Verfahrensalternativen jeweils wie folgt zu verfahren:

@Grafik Nr. 7 und Nr. 8 einfügen@

25.2

Mustervertrag zur Auftragsdatenverarbeitung zwischen öffentlichen Stellen und öffentlichen oder nicht-öffentlichen Auftragnehmern (Stand 18. Januar 2000)

Nachfolgend wurde ein Mustervertrag für die Verarbeitung personenbezogener Daten im Auftrag gemäß § 4 HDSG entworfen. Der Inhalt des Vertrages ist im Einzelfall aufgabenspezifisch anzupassen. An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen. Soweit nicht § 4 HDSG, sondern spezialgesetzliche Regelungen für die Daten, die im Auftrag verarbeitet werden sollen, Anwendung finden, ist zunächst zu prüfen, ob eine Auftragsdatenverarbeitung grundsätzlich zulässig ist, und ggf. sind die spezialgesetzlichen Regelungen bei der Vertragsgestaltung (z.B. Personal-, Beihilfe- und Sozialdaten) zu berücksichtigen. Soweit die BVB (HessStAnz 1994, S. 2050 ff) anzuwenden sind, müssen die dort vorgesehenen Vertragstypen datenschutzrechtlich ergänzt werden. Die jeweiligen Vertragsbestimmungen sind dem Mustervertrag zu entnehmen. Gem. § 3 Abs. 3 Satz 2 hat der Auftraggeber den Hessischen Datenschutzbeauftragten vorab über die Beauftragung zu unterrichten.

V e r e i n b a r u n g

zwischen dem/der

.....

- nachstehend Auftragnehmer genannt -

und dem/der

.....

- nachstehend Auftraggeber genannt -

§ 1 Gegenstand der Vereinbarung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

(2) Der Auftrag umfasst folgende Arbeiten:

.....

(Definition der Aufgaben)

§ 2 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

(3) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Weisungsberechtigte Personen des Auftraggebers sind:

.....

Weisungsempfänger beim Auftragnehmer sind:

.....

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er verwendet die zur

Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(2) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen scharf getrennt werden.

(3) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme.

(4) Die Verarbeitung von Daten in Privatwohnungen ist nur mit Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch den Auftraggeber (§ 3 Abs. 3) vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(5) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

(6) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen.

(7) [1. Alternative]

Die Einschaltung von Subauftragnehmern ist ausgeschlossen. Die Beauftragung von Subunternehmen mit der Verarbeitung von personenbezogenen Daten ist in keinem Fall zulässig.

[2. Alternative]
Die Beauftragung von Subunternehmen ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. Der Auftragnehmer hat in diesem Falle vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 4 erfüllt hat. [Zur Zeit sind die in Anlage ..... mit Namen und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt.]

(8) Soweit für den Auftragnehmer die Vorschriften über den nicht-öffentlichen Bereich Anwendung finden, bestätigt er, dass er zum Register bei der Aufsichtsbehörde für den Datenschutz gemeldet ist. Die Ergebnisse der zuletzt vorgenommenen Überprüfung durch die Aufsichtsbehörde gemäß § 38 Abs. 2 BDSG werden dem Auftraggeber zugänglich gemacht.

(9) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

§ 4 Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß § 9 HDSG zu wahren. Er verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen (§ 4 Abs. 3 HDSG).

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(3) Auskünfte darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

§ 5 Kontrollrechte des HDSB

(1) Der Auftragnehmer verpflichtet sich, dem Hessischen Datenschutzbeauftragten und den von ihm eingesetzten Bediensteten Zugang zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle nach Maßgabe des HDSG in seiner jeweiligen Fassung.

(2) Soweit Daten in einer Privatwohnung verarbeitet werden, ist der Zugang des Hessischen Datenschutzbeauftragten und der von ihm eingesetzten Bediensteten vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer stellt sicher, dass die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

§ 6 Datensicherungsmaßnahmen (Erläuterungen s. Anhang)

(1) Zu den Regelungstatbeständen des § 10 HDSG werden folgende technische und organisatorische Maßnahmen verbindlich festgelegt:

a) Zutrittskontrolle
Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden:
.....
.....
.....
.....

b) Benutzerkontrolle
Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungsanlagen und –verfahren gehindert werden:
.....

.....

.....

.....

c) Zugriffskontrolle

Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

.....

.....

.....

.....

d) Datenverarbeitungskontrolle

Maßnahmen, damit personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden:

.....

.....

.....

.....

e) Verantwortlichkeitskontrolle

Maßnahmen, damit es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind:

.....

.....

.....

.....

f) Dokumentationskontrolle

Maßnahmen, damit durch eine Dokumentation aller wesentlichen Verarbeitungsschritte die Überprüfbarkeit der Datenverarbeitungsanlage und des -verfahrens möglich ist:

.....
.....
.....
.....

g) Organisationskontrolle
Maßnahmen, damit die innerbehördliche oder innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird:
.....
.....
.....
.....

(2) An der Erstellung der Verfahrensverzeichnisse hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

(3) Der Auftragnehmer beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

(4) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

(5) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten. Er unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht nicht befolgt zu werden, solange sie nicht durch den Auftraggeber geändert oder ausdrücklich bestätigt wird.

§ 7 Vertragsdauer

(1) Der Vertrag

- beginnt am ..... und endet am ...../

- mit Auftragserledigung /

- wird auf unbestimmte Zeit geschlossen.

Er ist mit einer Frist von ..... Monaten zum Quartalsende kündbar.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen des HDSG oder dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder des Hessischen Datenschutzbeauftragten vertragswidrig verweigert.

§ 8 Vergütung

....

§ 9 Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem HDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

§ 10 Vertragsstrafe

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... DM vereinbart.

§ 11 Nichterfüllung der Leistung

....

§ 12 Sonstiges

(1) Der Auftragnehmer übereignet dem Auftraggeber zur Sicherung die Datenträger, auf denen sich Dateien befinden, die Daten des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen.

(2) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen [Diese Klausel muss wegen § 11 Nr. 2 AGB gesondert vereinbart werden].

§ 13 Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im übrigen nicht.

Erläuterungen zu § 6 Datensicherungsmaßnahmen

In dem Vertrag müssen die technischen und organisatorischen Maßnahmen festgelegt werden, die bei der Datenverarbeitung umzusetzen sind.

Rechtsgrundlage ist § 4 Abs. 2 HDSG, in dem beschrieben ist, welche Prüfungen ein Auftraggeber vor einer Auftragsvergabe durchzuführen hat. So muss der Auftragnehmer unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Im Auftrag sind insbesondere die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Auch hat der Auftraggeber zu prüfen, ob beim Auftragnehmer die nach § 10 erforderlichen Maßnahmen getroffen werden.

Werden personenbezogene Daten verarbeitet, deren Verarbeitung für die Betroffenen keine besonderen Risiken erwarten lässt, so bietet das Grundschutzhandbuch des BSI für bestimmte technische Konstellationen einen Katalog an Sicherheitsmaßnahmen. (Das Handbuch, in dem die Maßnahmen erläutert werden, kann auf Datenträgern beim BSI bestellt werden. Tabellen, in denen Abhängigkeiten zwischen Grundschutz-Maßnahmen und den Sicherheitszielen des HDSG dargestellt werden, sind im Internetangebot des Hessischen Datenschutzbeauftragten abrufbar; www.datenschutz.hessen.de.)

a) Wenn der Auftragnehmer ein Datensicherheitskonzept besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. Die Sicherheitsziele sind in § 10 Abs. 2 HDSG genannt. Ist das Konzept nicht ausreichend, sind ergänzende Maßnahmen zu vereinbaren. Das daraus resultierende Sicherheitskonzept sollte zum Vertragsbestandteil gemacht werden. In diesem Fall kann darauf verzichtet werden, im Sicherheitskonzept genannte Maßnahmen im Vertragstext zu wiederholen.

b) Wenn der Auftragnehmer kein Datensicherheitskonzept vorlegen kann, müssen die Maßnahmen im Vertrag vereinbart werden. Dabei sind wiederum die in § 10 Abs. 2 HDSG genannten Sicherheitsziele zu erreichen. Aus dem Katalog sollten die einzelnen Maßnahmen

in den Vertrag übernommen werden. Es handelt sich um keinen abschließenden Maßnahmenkatalog. Insbesondere bei der Verarbeitung sensibler Daten sind in der Regel zusätzliche Maßnahmen erforderlich.

c) Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

- Verantwortlichkeiten: Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.
- Abschottung von Netzen: Es müssen Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern. Da meist keine absolute Sicherheit zu erreichen ist, müssen derartige Versuche erkannt werden. Technische Komponenten, die in Betracht kommen, sind Firewalls oder Intrusion Detection Systeme.
- Abhören der Kommunikation: Zum Schutz gegen unberechtigtes Abhören bietet es sich an, die Daten zu verschlüsseln.
- Abmeldeprozeduren: Die Anmeldung am System oder Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.

Organisationsplan
des Hessischen Datenschutzbeauftragten

Hessischer Datenschutzbeauftragter

Prof. Dr. Friedrich von Zezschwitz Tel. (06 11) 14 08 20

Vertretung des Hessischen Datenschutzbeauftragten und Dienststellenleitung

Ute Arlt Tel. (06 11) 14 08 22

Vorzimmer:

Ursula Gegner Tel. (06 11) 14 08 21

Gruppe A

Referat A1

Gruppenleitung, Koordinierung und Grundsatzfragen, interne Verwaltung

Ute Arlt Tel. (06 11) 14 08 22

Mitarbeiter/innen:

Christel Friedmann-Baradel Tel. (06 11) 14 08 14

Bernd Groh Tel. (06 11) 14 08 35

Karin Nitsche Tel. (06 11) 14 08 34

Referat A2

Bildung, Verwaltung von Hochschulen und anderen Wissenschaftseinrichtungen, Schulverwaltung, Schulen einschl. Forschung, Archive

Manfred Weitz Tel. (06 11) 14 08 45

Mitarbeiterin:

Karin Nitsche Tel. (06 11) 14 08 34

Referat A3
Finanzwesen, Einwohnerwesen, Verkehr, Ordnungswidrigkeiten

Cornelia Topp Tel. (06 11) 14 08 38

Mitarbeiter/innen:
Christa Kreis Tel. (06 11) 14 08 43
Helga Schaller Tel. (06 11) 14 08 41
Alfons Schranz Tel. (06 11) 14 08 32

Gruppe B

Referat B1
Gruppenleitung, Informatik I

Rüdiger Wehrmann Tel. (06 11) 14 08 37

Mitarbeiter:
Holger Weigel Tel. (06 11) 14 08 28

Referat B2
Informatik II

N.N.

Mitarbeiter:
Holger Weigel Tel. (06 11) 14 08 28

Referat B3
Informatik III

Maren Thiermann Tel. (06 11) 14 08 31

Mitarbeiter:
Holger Weigel Tel. (06 11) 14 08 28

Gruppe C

Referat C1
Gruppenleitung, Rechtsfragen der Informations- und Kommunikationstechnik, Rundfunk, Statistik, Versicherungen, Kreditinstitute, Kammern, internationaler Datenschutz

Wilhelm Rydzy Tel. (06 11) 14 08 24

Mitarbeiter:
Michael Sobota Tel. (06 11) 14 08 27

Referat C2
Verfassungsschutz, Ausländerrecht, Europarecht, Schengener Informationssystem

Angelika Schriever-Steinberg Tel. (06 11) 14 08 25

Mitarbeiter:
Alfons Schranz Tel. (06 11) 14 08 32

Referat C3

Justiz, Staatsanwaltschaften, Vollzugsanstalten, Polizei

Barbara Dembowski Tel. (06 11) 14 08 26

Mitarbeiter:
Alfons Schranz Tel. (06 11) 14 08 32

Gruppe D

Referat D1
Gruppenleitung, Gesundheitswesen, Wissenschaft und Forschung, Betreuungsrecht, Redaktion des Tätigkeitsberichts

Dr. Rita Wellbrock Tel. (06 11) 14 08 23

Mitarbeiter:
Rainer Banse Tel. (06 11) 14 08 33

Referat D2
Personalwesen, Sozialwesen

Dr. Robert Piendl Tel. (06 11) 14 08 36

Mitarbeiter:
Rainer Banse Tel. (06 11) 14 08 33
Bernd Groh Tel. (06 11) 14 08 35

Referat D3
Kommunen, Vermessungswesen, Gewerberecht, Umwelt, Landwirtschaft, Forsten und Naturschutz, Öffentlichkeitsarbeit

Ulrike Müller	Tel. (06 11) 14 08 42
Mitarbeiter/in:	
Helga Schaller	Tel. (06 11) 14 08 41
Michael Sobota	Tel. (06 11) 14 08 27

Abkürzungsverzeichnis zum 28. Tätigkeitsbericht

a.a.O.	am angegebenen Ort
ABl.	Amtsblatt des Hessische Kultusministeriums
Abs.	Absatz
AG	Aktiengesellschaft
BDSG	Bundesdatenschutzgesetz
BGSG	Gesetz über den Bundesgrenzschutz (BGBl. I, 2978) vom 19.10.94
BKA	Bundeskriminalamt
BSHG	Bundessozialhilfegesetz
CSIS	Zentrales Schengener Informationssystem
DNA	Desoxiribonucleid acid (Desoxyribonukleinsäure)
EG	Europäische Gemeinschaft
EG-Datenschutzrichtlinie	Datenschutzrichtlinie der Europäischen Gemeinschaft
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
E-Mail	Electronic Mail
EU	Europäische Union
EUROPOL	Europäisches Kriminalpolizeiamt
EUV	Vertrag über die Europäische Union
GAA	Geldausgabeautomat
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz für die Bundesrepublik Deutschland
GVBl.	Gesetz- und Verordnungsblatt des Landes Hessen
HArchivG	Hessisches Archivgesetz
HBG	Hessisches Beamtengesetz
HDSB	Hessischer Datenschutzbeauftragter
HDSG	Hessisches Datenschutzgesetz
HEPOLIS	Hessisches Polizeiinformationssystem
HessLStatG	Hessisches Landesstatistikgesetz
HHG	Hessisches Hochschulgesetz
HKHG	Hessisches Krankenhausgesetz
HMG	Hessisches Meldegesetz
HPVG	Hessisches Personalvertretungsgesetz
HSchulG	Hessisches Schulgesetz
HSL	Hessisches Statistisches Landesamt
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HTML	Hyper Text Markup Language
HVwVfG	Hessisches Verwaltungsverfahrensgesetz
i.S.d.	im Sinne des/der
IdentG	DNA-Identitätsfeststellungsgesetz vom 07.09.1998, BGBl. S. 2646
IDS	Intrusion Detection System

ID-System	Intrusion Detection-System
IMAP	Internet Mail Access Protocol
INPOL	Informationssystem der Polizei
IT	Informations Technik
KGRZ	Kommunales Gebietsrechenzentrum
LKA	Landeskriminalamt
LTDrucks.	Landtagsdrucksache
Nr.	Nummer
OWiG	Ordnungswidrigkeitengesetz
PGP	Pretty Good Privacy
PIN	Persönliche Identifikationsnummer
PISA	Program for International Student Assessment
POP 3	Post-Official-Protocol 3
PsychThG	Gesetz über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichen-Therapeuten
rtf	Rich Text Format
s.	siehe
S.	Seite
SAP/R3	Systeme, Anwendungen und Produkte in der Datenverarbeitung, Realtime "3"
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
StAnz.	Staatsanzeiger für das Land Hessen
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
u.a.	unter anderem
z.B.	zum Beispiel
Ziff.	Ziffer

Sachwortverzeichnis zum 28. Tätigkeitsbericht