15. Wahlperiode

Drucksache **15/2500**

HESSISCHER LANDTAG

30. 03. 2001

Neunundzwanzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt am 31. Dezember 2000
nach § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 30. März 2001 · Ausgegeben am 2. April 2001

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

INHALTSVERZEICHNIS

KERNPUNKTE DES 29. TÄTIGKEITSBERICHTS

1. Datenschutzinstitutionen aus dem In- und Ausland haben unter der Federführung des Datenschutzbeauftragten des Landes Schleswig-Holstein das mit öffentlichen Fördermitteln unterstützte Projekt „virtuelles Datenschutzbüro“ ins Leben gerufen. Das „virtuelle Datenschutzbüro“ dient als Informations- und Diskussionsplattform zu Datenschutzthemen. Auch Hessen ist an diesem Projekt beteiligt (Ziff. 2).

2. Derzeit wird im Parlament eine Gesetzesinitiative zum Informationszugang und zur Akteneinsicht beraten. Eine gesetzliche Regelung des Zugangs zu Informationen wird von mir nachdrücklich unterstützt (Ziff. 3).

3. Die Neuregelung in § 14 Abs. 4 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung zur Videoüberwachung durch Gefahrenabwehrbehörden erlaubt es den Kommunen nicht, nach freiem Ermessen Videokameras auf öffentlichen Plätzen zu installieren. Dies ist vielmehr nur unter engen Voraussetzungen möglich (Ziff. 4.1).

4. Wenn eine Polizeibehörde einem privaten Fernsehsender gestatten will, bei polizeilichen Maßnahmen anwesend zu sein und diese zu filmen, so muss sie zuvor mit dem Fernsehsender eine Verfahrensweise vereinbaren, die die Rechte der Betroffenen wahrt (Ziff. 6.2).

5. Der neue § 147 Abs. 6 Abgabenordnung lässt im Rahmen der Außenprüfung einen unmittelbaren Zugriff des Betriebsprüfers auf die gesamte EDV-Buchhaltung eines Unternehmens und damit deren systematische Auswertung zu. Es ist verfassungsrechtlich dringend erforderlich, dass dieser Befugnisausweitung datenschutzrechtliche Grenzen gesetzt werden, bevor sie ab 1. Januar 2002 in die Betriebsprüfung eingeht (Ziff. 8.2).

6. Bei der Verarbeitung personenbezogener Patientendaten im Rahmen des Hausarztmodells und innerhalb von Praxisnetzen muss die ärztliche Schweigepflicht eingehalten werden. Gesundheitsdaten dürfen nur mit Einwilligung der Patienten an andere Ärzte weitergegeben werden (Ziff. 9.1).

7. Beim Aufbau bundesweiter Forschungsnetze sind die Rechte der Patienten zu beachten. Personenbezogene Patientendaten dürfen vom behandelnden Arzt ohne Einwilligung des Patienten nicht an Dritte übermittelt werden. Soweit eine Übermittlung reidentifizierbarer Patientendaten an das Forschungsnetz Parkinson zur Erreichung des Forschungszwecks notwendig ist, muss ein unabhängiger Treuhänder eingeschaltet werden. Die Übermittlung personenbezogener oder pseudonymisierter Patientendaten bedarf einer schriftlichen Vereinbarung zwischen behandelndem Arzt und Forschungsnetz über die weitere Verarbeitung der Daten (Ziff. 9.2).

8. Das Hessische Sozialministerium muss sicherstellen, dass das den Patientinnen und Patienten nach dem Hessischen Krebsregistergesetz zustehende Widerspruchsrecht beachtet und korrekt umgesetzt wird (Ziff. 9.3).

9. Die neue Telekommunikations-Datenschutzverordnung lässt einige Forderungen der Datenschutzbeauftragten des Bundes und der Länder und des Landes Hessen unberücksichtigt (Ziff. 10).

10. Die Veröffentlichung von personenbezogenen Daten über ehrenamtliche Funktionsträger im Internet hat eine andere Dimension als in herkömmlichen Broschüren, da sie weltweit abgerufen werden können. Ein angemessenes Datenschutzniveau bei der Übermittlung kann nicht gewährleistet werden; einmal veröffentlichte Daten sind nicht rückholbar. An die Einwilligung zur Veröffentlichung sind besondere Anforderungen zu stellen (Ziff. 15.1).

11. Die vom Bundesrat geforderte Erweiterung der Auskünfte aus dem Bundeszentralregister für die Zuverlässigkeitsprüfung von Hundehaltern ist im beabsichtigten Umfang nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar (Ziff. 15.2).

12. Für die Bürgermeister der Kommunen oder Amtsleiter von Verwaltungsbehörden dürfen Zugriffe auf Verwaltungsdaten nur eingeräumt werden, soweit diese zu deren Aufgabenerfüllung erforderlich sind. Maßgebend sind die fachaufsichtlichen und dienstrechtlichen Befugnisse, die Bürgermeister oder Amtsleiter haben (Ziff. 15.5).

13. Verschlüsselung und verlässliche Authentizitätsprüfung gehören zu den wichtigsten Schritten, die eine moderne Verwaltung einführen muss, wenn sie das Internet als Kommunikationsmedium benutzt. Angebotene Formularsätze müssen auf ihre elektronische Verwendbarkeit geprüft werden (Ziff. 20.3).

1. Vorwort

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

- die 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 (Ziff. 4.1),
- die Vorbereitung eines Informationszugangsgesetzes (Entwurf der Fraktion Bündnis 90/Die Grünen sowie ein eigener Entwurf; Ziff. 3),
- die Änderungen des Sozialgesetzbuches Teil V, die eine grundlegende Veränderung der datenschutzrechtlichen Belange der Versicherten zur Folge haben (Ziff. 9.1),
- die starke Ausweitung des finanzbehördlichen Datenzugriffs nach der Abgabenordnung (Ziff. 8.2),
- die datenschutzrechtliche Konzeption des bundesweiten Medizinischen Kompetenznetzwerkes Parkinson-Syndrom mit der zentralen Datenbank in Marburg (Ziff. 9.2),
- das 9. Wiesbadener Forum, das sich mit den Techniken des E-Government und den daraus hervorgehenden Gefahren für das Recht auf informationelle Selbstbestimmung befasst hat.

Im Unterschied zum hessischen Gesetzgeber war der Bund bislang immer noch nicht im Stande, sein Datenschutzrecht an die neuen Anforderungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten anzupassen. Die bisher bekanntgewordene Konzeption der Neuregelung hat vor allem für die Kontrollen nicht-öffentlicher Stellen beträchtliche Auswirkungen. Materiellrechtlich treten zunehmend Überschneidungen auf, wie sich an der privaten wie öffentlichen Videoüberwachung, am zunehmenden Chipkarteneinsatz im privaten wie öffentlichen Bereich und in der Datenverarbeitung im privaten wie öffentlichen Bankwesen deutlich zeigen lässt. Die Ausweitung der datenschutzrechtlichen Aufgaben und die europäischen Rechtsgarantien für die Unabhängigkeit der Überwachungsstellen werden eine Neuorganisation der hessischen Datenschutzverwaltung erzwingen. Sollten die Aufgaben aus einem Informationszugangsgesetz mit den datenschutzrechtlichen Kontrollaufgaben gebündelt werden, wird auch von dieser Seite ein Anstoß zur Neuorganisation ausgehen. Ich trete deswegen nach wie vor dafür ein, dass das Land Hessen im Rahmen seiner förderativverfassungsrechtlichen Möglichkeiten der in immer mehr Bundesländern bereits vollzogenen Neuordnung folgt.

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 sind unter Ziff. 24 zu diesem Bericht abgedruckt, soweit sie in förmliche Entschließungen eingeflossen sind. Der in der Konferenz praktizierte Gedanken-, Erfahrungs- und Meinungsaustausch hat die in immer neuer Gestalt auftretenden Verletzungen informationeller Selbstbestimmung bewusst gemacht. Einzelfragen des Datenschutzes werden in zahlreichen Arbeitskreisen kontinuierlich erörtert und − soweit möglich − bundesweit koordiniert. Hessen hat zu dem bisherigen Vorsitz im Arbeitskreis Wissenschaft und in der ad-hoc-Gruppe Ausländerrecht den Vorsitz im Arbeitskreis Steuern neu übernommen. Die erste − sehr fruchtbare − Arbeitssitzung hat bereits in Wiesbaden stattgefunden. Primäre Ziele sind die Anpassung der Abgabenordnung an die datenschutzrechtlichen Standards und die Datensicherheit bei dem bundeseinheitlichen Verfahren der finanzbehördlichen Datenverarbeitung.

Im Jahr 2000 ist die Planung eines bundesweit tätigen „virtuellen Datenschutzbüros“ vorwärts getrieben worden. Im Spätherbst sind die geschaffenen Institutionen erstmals „ans Netz gegangen“ (Internetadressen sind für die deutsche Sektion: http://www.datenschutz.de, für die schweizer Sektion: http://www.datenschutz.ch und international: http://www.privacyservice.org). Auch Hessen war an den Vorbereitungen intensiv beteiligt, hat eigene Beiträge zum Datenschutzrecht präsentiert und ist mit mehreren Mitarbeiterinnen und Mitarbeitern in den Redaktionsstäben vertreten. Mit dem „virtuellen Datenschutzbüro“ wird der Versuch unternommen, das Medium des Internet auch für den Datenschutz und die internationale Zusammenarbeit fruchtbar zu machen (Ziff. 2).

Die im Hessischen Landtag wie in der Landesregierung in den Mittelpunkt des politischen Interesses gerückte Videoüberwachung des öffentlichen Raumes trifft ein besonderes sensibles Gebiet der informationellen Selbstbestimmung. Die Videoüberwachung erzeugt eine hohes Spannungsverhältnis zur verfassungsrechtlichen Garantie der Privatsphäre. Der Versuch, die Sicherheit im öffentlichen Raum zu steigern, führt zu einer umfangreichen Erhebung, Verarbeitung und Verwertung personenbezogener Daten. Die Umsetzung der Neuregelung im Hessischen Gesetz über die öffentliche Sicherheit und Ordnung findet vor allem in den Städten und Gemeinden statt. Nicht durchgängig werden die gesetzlichen Voraussetzungen mit der Strenge geprüft, die der Hessische Landtag mit den engen gesetzlichen Voraussetzungen des § 14 Abs. 4 geschaffen hat (Ziff. 4.2).

Die für den nachstehenden Datenschutzbericht von meinen Mitarbeiterinnen und Mitarbeitern vorbereiteten 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 Kritik 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 geben wir den Vorrang von nachträglich kritisierender Kontrolle. Oft zeigt erst die genaue Analyse das datenschutzrechtliche Gefahrenpotential. Beispielhaft mögen die Befugnisse der Finanzbehörden im Rahmen des neu geschaffenen Datenzugriffs auf die elektronische Buchhaltung der Betriebe (Ziff. 8.2), die Verkehrsüberwachung durch Videoaufzeichnung (Ziff. 4.2), die Datenverarbeitung in Praxisnetzen und beim Hausarztmodell (Ziff. 9.1), die Videoeinrichtung in den hessischen Gemeinden (Ziff. 4.2),

die Netzzugriffsrechte der Bürgermeister (Ziff. 15.5) und die aufgezeigten Möglichkeiten für anonyme Aktivitäten im Internet (Ziff. 11.4) 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 nur partiell gelösten Probleme der justiziellen Datenerhebung und Datenübermittlung. Die hier erforderlichen Rechtsgrundlagen für datenschutzrechtliche Vorgänge bei den Gerichten und Staatsanwaltschaften sind erst teilweise verabschiedet worden (Ziff. 6.1; vgl. §§ 477 ff. StPO). Zu den aus meiner Sicht immer noch nicht befriedigend gelösten Problemen gehören die Präsentation der Staats- und Kommunalverwaltungen im Internet (Ziff. 15.1), die unzureichende Bereitstellung von technischen Sicherungen für die Kommunikation mit Bürgerinnen und Bürgern (Ziff. 20.3), die Angriffe auf die Zweckbindung von Daten im Telekommunikationsbereich (Ziff. 10), die Umsetzung des Krebsregistergesetzes (Ziff. 9.3) und die datenschutzrechtlichen Probleme der umfassenden Kommunikationsstrukturen in Krankenhäusern (Ziff. 9.6) und medizinischen Forschungsnetzen (Ziff. 9.2). Weitere Probleme zeigten sich auch bei der Evaluation der Lehre (Ziff. 16.2), bei der Protokollierung von Aktivitäten im Internet (Ziff. 22.2), der Zuverlässigkeitsprüfung von Hundehaltern (Ziff. 15.2) und der polizeilichen Speicherung nach § 20 HSOG trotz erfolgen Freispruches (Ziff. 6.1). Die diesbezügliche Regelung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung ist unzureichend.

Besonderen Beratungsbedarf hat das Medizinische Kompetenznetzwerk Parkinson-Syndrom e.V. geschaffen. Sitz des Vereins ist Marburg. Da der Entwicklungsstand dieses Zweiges der Kompetenznetze am weitesten fortgeschritten ist, ist den Beratungsaufgaben des Landes Hessen besonderes Gewicht zugekommen. Vergleichbare Probleme haben die datenschutzrechtlichen Sicherungen der Praxisnetze und Hausarztmodelle aufgeworfen, die sich aufgrund der Neuregelung im Sozialgesetzbuch V derzeit etablieren.

Das schon in früheren Tätigkeitsberichten formulierte Postulat, meine Behörde ausreichend mit Technik und informationstechnisch geschultem Personal auszustatten, hat hinsichtlich der informationstechnischen Ausstattung im Jahr 2000 abermals deutliche Fortschritte gemacht. Auch haben frei gewordene Stellen und Haushaltsmittel für Umwidmungen eingesetzt werden können. Mit der 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 zum Teil schneller vollzogen hatten. Ich bemühe mich, dass das datenschutzrechtliche Know-how, das nur noch in enger Zusammenarbeit mit Informatikern zu erreichen ist, für alle Dienststellen des Landes und Gemeinden fruchtbar gemacht wird. Auch wenn die Beratungstätigkeit vorzüglich unter datenschutzrechtlichen Aspekten erfolgt, kann damit gerechnet werden, dass auch im Übrigen hilfreiche Anstöße vermittelt werden können.

Im Rahmen der präventiven Aufgaben datenschutzrechtlicher Sicherheit habe ich im vergangenen Jahr verschiedene Musterverträge entwickelt, die für die wichtigsten datenschutzrechtlichen Verwaltungsaufgaben Vertragstypen bereitstellen, die die rechtlichen Probleme aufarbeiten, die im Zuge von typischen Vertragsverhältnissen auftreten. Musterverträge liegen inzwischen zur Datenverarbeitung im Auftrag (28. Tätigkeitsbericht, Ziff. 25.2), zur Fernwartung (Ziff. 22.1) und zu einfachen Wartungsarbeiten an EDV-Anlagen (Ziff. 11.3) vor. Die überarbeitete Broschüre zum Datenschutz in Wissenschaft und Forschung wird nunmehr von Berlin und Hessen gemeinsam herausgegeben. Sie ist zusammen mit dem Landesbeauftragten für Datenschutz des Landes Berlin redigiert und inzwischen veröffentlicht worden. Sie kann auch im Internet abgerufen werden: http://www.datenschutz.hessen.de.

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 besonders hervorhebenswerte Tatbestände handelt.

Ich schließe dieses Vorwort mit dem Dank an die Abgeordneten des Hessischen Landtages, mit denen sich stets eine fruchtbare Zusammenarbeit ergeben hat. Auch die Zusammenarbeit mit der Landesregierung war von Sachlichkeit und problemangemessener Argumentation geprägt, auch dort, wo divergente Auffassungen aufgetreten sind. Ich hoffe auch für die Zukunft, dass das Recht auf informationelle Selbstbestimmung ein gemeinsames Anliegen bleiben wird, das dem hohen grundrechtlichen Rang gerecht wird, der der Privatsphäre zukommt.

2. Das virtuelle Datenschutzbüro

Datenschutzinstitutionen aus dem In- und Ausland haben unter der Federführung des Datenschutzbeauftragten des Landes Schleswig-Holstein das mit öffentlichen Fördermitteln unterstützte Projekt „virtuelles Datenschutzbüro“ ins Leben gerufen. Das „virtuelle Datenschutzbüro“ dient als Informations- und Diskussionsplattform zu Datenschutzthemen. Auch Hessen ist an diesem Projekt beteiligt.

2.1 Problemstellung

Datenschutzfragen sind in unserer vernetzten Welt zunehmend schwieriger zu lösen. Oft sind verschiedene Aspekte und verschiedene Rechtsmaterien parallel zu betrachten. Laien, aber auch Experten sind darauf angewiesen, sich schnell und zutreffend zu informieren, um den mit der modernen Informationsgesellschaft verbundenen Risiken und Gefahren rechtzeitig und wirksam begegnen zu können. Experten und Interessierte brauchen ein Forum, um Positionen auszutauschen, Denkanstöße geben zu können, insgesamt Themen offen zu diskutieren. Nur auf dieser Basis können sachgerechte und gesellschaftlich akzeptierte Lösungen entwickelt werden. Die neuen Informations- und Kommunikationsstrukturen müssen konsequent genutzt werden, um mit dem rasanten Entwicklungstempo der Informationstechnologie Schritt halten zu kön-

nen. Das „virtuelle Datenschutzbüro“ will auf Basis von Information und Kommunikation mit moderner Technik Lösungen für Bürger, Datenschutzinstanzen und die Politik anbieten.

2.2
Ziele des virtuellen Datenschutzbüros

Das Projekt „virtuelles Datenschutzbüro“ verfolgt folgende Ziele:
- Bereitstellung von Informationen zum Thema Datenschutz für jedermann im Internet
- Verbesserung der Öffentlichkeitsarbeit der Datenschutzinstitutionen, z.B. durch ein verbessertes Informationsangebot, Bereitstellung transparenter Arbeitsergebnisse und Diskussionsforen
- Verbesserung der Zusammenarbeit und Leistungsfähigkeit der Institutionen z.B. durch Arbeitsteilung, Einbindung externen Sachverstandes und Durchführung gemeinschaftlicher Projekte
- Erweiterte Servicefunktionen der Bundes- und Landesbeauftragten für Datenschutz gegenüber Bürgerinnen, Bürgern und Unternehmen (gemeinsame Anlaufstelle)

Das virtuelle Datenschutzbüro soll den Gefahren für die Privatsphäre, die das grenzüberschreitende Internet mit sich bringt, begegnen. Zugleich soll mit der Kooperation im virtuellen Datenschutzbüro durch Schwerpunktbildung und systematische Bündelung ihrer Ressourcen die Effizienz der Datenschutzbeauftragten gesteigert werden.

2.3
Partner im virtuellen Datenschutzbüro

Die Satzung unterscheidet Projektpartner und Kooperationspartner. Projektpartner sind die Datenschutzbeauftragten des Bundes und der meisten Länder in Deutschland, Datenschutzbehörden aus der Schweiz, den Niederlanden und Kanada sowie der Datenschutzbeauftragte der katholischen Kirche in Norddeutschland. Das Projekt ist für weitere Partner offen − sowohl für solche, die das Projekt mittragen, als auch für solche, die lediglich Beiträge liefern, Informationen einspeisen und abrufen wollen. Kooperationspartner können Institutionen und Unternehmen sein, die besondere datenschutzrechtliche Interessen verfolgen und dem virtuellen Datenschutzbüro Informationen zur Verfügung stellen wollen.

2.4
Angebote im virtuellen Datenschutzbüro

Unter den Internetadressen für die deutsche Sektion: http://www.datenschutz.de, für die schweizer Sektion: http://www.datenschutz.ch und international: http://www.privacyservice.org können Informationen verschiedenster Art zu Datenschutzthemen abgerufen werden. Die Wissensdatenbank befindet sich noch im Aufbau. Ständig kommen neue Informationen hinzu und müssen für eine effektive Recherche aufbereitet werden. Zur Bewältigung dieser Aufgabe haben die Mitarbeiterinnen und Mitarbeiter der Beteiligten die Moderation einzelner Themenbereiche übernommen.

2.5
Beitrag des Hessischen Datenschutzbeauftragten zum virtuellen Datenschutzbüro

Zunächst musste für dieses innovative Gemeinschaftsprojekt der rechtliche Rahmen festgelegt werden. An der Schaffung der Geschäftsordnung, die Beteiligung, Mitwirkung und die konkrete Zusammenarbeit regelt, hat Hessen intensiv mitgewirkt.

Für die Zusammenarbeit ist auch die technische Plattform geschaffen worden, die für die Projekt- und Kooperationspartner einen vertraulichen Informationsaustausch trotz sehr unterschiedlicher technischer Voraussetzungen bei den einzelnen Beteiligten möglich macht und unterstützt.

Die Aufbereitung der einzelnen Informationen durch Moderatoren hat Hessen für folgende Themenbereiche übernommen:
- Wissenschaft und Forschung
- Elektronische Patientenakte
- Personalwesen
- Schengener Informationssystem
- Mobile Computing
- Chipkarten

Das virtuelle Datenschutzbüro wird auch in den kommenden Monaten und Jahren meine Mitarbeit erfordern. Seine Zukunft lebt davon, ständig mit aktuellen Informationen gespeist zu werden und die technischen Möglichkeiten datenschutzgerechter Kommunikation anzubieten und zu nutzen.

Die Finanzierung der Anlaufphase ist durch Sondermittel gesichert, die dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein zur Verfügung stehen. Kosten für persönliche Leistungen, die bei den Beteiligten entstehen, werden von diesen getragen. Vertraglich ist abgesichert, dass vor der Eingehung von Umlagepflichten die haushaltsrechtlichen Voraussetzungen gewahrt werden.

3. Gesetz über den Informationszugang und die Akteneinsicht

Derzeit wird im Parlament eine Gesetzesinitiative zum Informationszugang und zur Akteneinsicht beraten. Eine gesetzliche Regelung des Zugangs zu Informationen wird von mir nachdrücklich unterstützt.

3.1
Grundlagen

3.1.1
Sachstand bei den Bundesländern und im Bund

Die Bundesländer Brandenburg, Berlin und Schleswig-Holstein haben bereits Gesetze zu Informationszugang und Akteneinsicht geschaffen. In Nordrhein-Westfalen hat die Fraktion der CDU einen Gesetzentwurf zur Förderung der Informationsfreiheit eingebracht. Die Bundesregierung hat in der Koalitionsvereinbarung die Schaffung eines Informationszugangsgesetzes noch in dieser Legislaturperiode vorgesehen; einen Gesetzesentwurf gibt es aber noch nicht.

3.1.2
Sachstand im Ausland

Im europäischen Raum haben die Länder Schweden, Finnland, Dänemark, Norwegen und die Niederlande Regelungen zur Informationsfreiheit getroffen. Darüber hinaus gibt es Informationszugangsregelungen in den USA und Kanada.

3.1.3
Sachstand in Hessen

In Hessen hat die Fraktion Bündnis 90/Die Grünen einen Gesetzentwurf eingebracht (LTDrs. 15/1474 vom 17. August 2000), der am 19. September 2000 im Hessischen Landtag behandelt und an den Hauptausschuss verwiesen wurde. Zur Unterstützung der Initiative der Schaffung eines Informationszugangsgesetzes habe ich von meinem im Hessischen Datenschutzgesetz verankerten Rederecht im Parlament Gebrauch gemacht. Alle Fraktionen haben im Landtag ihr Interesse an einer intensiven und sachlichen Auseinandersetzung über das Thema bekundet und eine größere Transparenz der Verwaltung befürwortet. Der Hauptausschuss hat in seiner Sitzung am 17. Oktober 2000 eine Anhörung der Hessischen kommunalen Spitzenverbände, der Innenressorts und der Beauftragen für das Recht auf Informationszugang bzw. Akteneinsicht der Länder Brandenburg, Berlin und Schleswig-Hostein, des Hessischen Datenschutzbeauftragten sowie weiterer Sachverständiger beschlossen. Die Frist für die schriftlichen Stellungnahmen zur Anhörung lief bis zum 31. Dezember 2000. Der Hauptausschuss hat beschlossen, die Sachverständigen auch mündlich anzuhören.

3.2
Stellungnahme

Bereits in früheren Tätigkeitsberichten hatten meine Amtsvorgänger für die Einführung eines allgemeinen Informationszugangsrechtes plädiert (z. B. 14. Tätigkeitsbericht für das Jahr 1985, Ziff. 11; 15. Tätigkeitsbericht für das Jahr 1986, Ziff. 10; 20. Tätigkeitsbericht für das Jahr 1991, Ziff. 17.2). Die Schaffung eines Informationszugangsgesetzes wird von mir weiterhin nachdrücklich unterstützt.

Die jetzt beratene Gesetzesinitiative stellt einen wesentlichen Schritt in Richtung auf eine umfassende Verankerung der Bürgerrechte dar. Das Recht auf freien Informationszugang zielt auf eine größere Transparenz der öffentlichen Verwaltung. Im Zuge der Umstellung auf eine elektronische Staats- und Kommunalverwaltung ist hinreichende Transparenz zwingend erforderlich, um Bürgerinnen und Bürgern die Möglichkeit zu eröffnen, sich auf sie interessierende Verwaltungsverfahren effektiv vorzubereiten. Das ist zur Aufbereitung eigener Verwaltungsbeziehungen, aber auch zur Wahrnehmung bürgerschaftlicher Selbstverwaltung und Partizipation, vor allem in den Gemeinden unabdingbar.

Die nach dem Verwaltungsverfahrensrecht und dem Datenschutzgesetz bestehenden Informationsrechte schaffen für Bürger und Unternehmen noch keine ausreichende Transparenz. Sie setzen voraus, dass die Verwaltung bereits eine Handlung vorgenommen hat, von der Bürger bzw. Unternehmen betroffen sind oder sein werden. Außerdem muss im Verwaltungsverfahrensrecht ein berechtigtes Interesse an der Information nachgewiesen werden. Auch nach dem Umweltinformationsgesetz ist der Zugang nur zu eng eingegrenzten Informationen möglich. Informationen über Verwaltungsabläufe, programmatische Einzelentscheidungen und die gängige Verwaltungspraxis sind bisher dem Bürger nicht zugänglich. Eine genaue Kenntnis vorausgehender Entscheidungen, Richtlinien und Verwaltungsplanungen würde es erleichtern, sachgerechte Anträge stellen zu können. Die mit solchen Vorabinformationen entstehende Transparenz staatlichen Handelns ist ein Spiegelbild für das neue Verständnis der Verwaltung als Dienstleistungsinstrument des Staates.

Naturgemäß kann das Recht auf freien Informationszugang nicht uneingeschränkt geltend gemacht werden. Interessenkonflikte zum informationellen Selbstbestimmungsrecht über personenbezogene Daten und zur Wahrung von Betriebs- und Unternehmensgeheimnissen müssen sachgerecht gelöst werden. Auf eine konkrete Entscheidung wird sich eine Auskunft immer nur beziehen können, wenn sie anonymisiert worden ist. In der Formulierung des Gesetzes wird auf die Wahrung von Datenschutz und Betriebsgeheimnissen besonders zu achten sein.

Den Landtagsfraktionen habe ich für Ihre Beratungen eine Gegenüberstellung der bereits in Deutschland bestehenden Regelungen angefertigt und einen eigenen Gesetzesvorschlag unterbreitet. Den weiteren Gang des Gesetzgebungsverfahrens werde ich mit Interesse verfolgen.

4. Videoüberwachung

4.1
Videoüberwachung in Kommunen nach der Neuregelung des § 14 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung

Die Neuregelung in § 14 Abs. 4 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung zur Videoüberwachung durch Gefahrenabwehrbehörden erlaubt es den Kommunen nicht, ohne weiteres Videokameras auf öffentlichen Plätzen zu installieren. Dies ist vielmehr nur unter engen Voraussetzungen möglich.

In meinem 28. Tätigkeitsbericht, Ziff. 13.3 hatte ich darauf hingewiesen, dass eine Überwachung des öffentlichen Raums durch Videokameras unter Bezug auf die allgemeine Datenverarbeitungsnorm des § 11 Hessisches Datenschutzgesetz unzulässig ist. Ich hatte deshalb die Installierung einer Videoüberwachungsanlage durch eine hessische Kommune datenschutzrechtlich noch für unzulässig erklärt. Gleichwohl zeigte die damalige Diskussion, dass unter Umständen durchaus das Bedürfnis nach Überwachungsmaßnahmen dieser Art bestehen kann. Auch im kommunalen Bereich kann es erforderlich sein, öffentliche Plätze, an denen besonders häufig Straftaten begangen werden, oder gefährdete öffentliche Einrichtungen, die besonders zu schützen sind, mit Hilfe von Videokameras zu überwachen. Ich hatte deshalb im Rahmen der Diskussion über die Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) angeregt, dass in § 14 HSOG eine präzise gefasste Regelung aufgenommen wird, die es neben der Polizei auch den Behörden der Gefahrenabwehr erlaubt, bei besonderen Gefahrenlagen Bildaufzeichnungen offen durchzuführen.

4.1.1
Videoüberwachung auf öffentlichen Straßen und Plätzen

Die in der öffentlichen Diskussion besonders umstrittene Befugnis, öffentliche Straßen und Plätze zu überwachen, ist mit der Novelle unter strikte Voraussetzungen gestellt und deutlich enger gefasst worden als die Befugnisse der Polizei gem. § 14 Abs. 3 HSOG. Voraussetzung ist nach § 14 Abs. 4 Nr. 1 HSOG, dass an den zu überwachenden Orten wiederholt Straftaten begangen worden sind und dass tatsächliche Anhaltspunkte für die Begehung weiterer gleicher Straftaten bestehen. Die Installierung von Videoüberwachungsanlagen − wie auch deren Beibehaltung nach Installation − setzt den mit den üblichen Beweismitteln zu führenden Nachweis voraus, dass der behördlichen Entscheidung eine Kette von Straftaten vorausgeht und dass eine durch tatsächliche Anhaltspunkte belegbare Gefahr von weiteren Straftaten an demselben Ort besteht. Die Gefahr muss für die nahe Zukunft vorausgesagt werden, wie es der konkrete Gefahrenbegriff fordert. Die gesetzlichen Voraussetzungen gelten gleichermaßen für die Beobachtung durch ein „verlängertes Auge“ ohne Aufzeichnung wie für die Aufzeichnung. Die Geltung der Norm für das reine Beobachten war nach Inkrafttreten des Gesetzes zunächst umstritten; streitig war auch, ob die Erhebungsvorschrift des § 13 Abs. 1 HSOG auf Videobeobachtung anzuwenden ist. Nach eingehender Erörterung hat der Landtag mit Gesetz vom 22. Dezember 2000 (GVBl. I S. 577 ff.) die Vorschrift geändert, so dass kein Interpretationsspielraum mehr bleibt.

§ 14 Abs. 4 HSOG

Die Gefahrenabwehrbehörden können mittels Bildübertragung offen bobachten und aufzeichnen:
1. zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen,
2. zum Schutz besonders gefährdeter öffentlicher Einrichtungen,
3. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen.

Gefahrenabwehrbehörde im Sinne der Nr. 2 ist auch der Inhaber des Hausrechts.

Wesentlicher Bestandteil einer der vorbeugenden Verbrechensbekämpfung dienenden Videoüberwachung ist, dass der betroffene Personenkreis die Möglichkeit zur Kenntnisnahme der Aufnahme erhält, z. B. durch ein Hinweisschild.

Im Übrigen gilt für alle Maßnahmen, dass allgemeine Erwägungen, Videoüberwachungsanlagen könnten die öffentliche Sicherheit erhöhen, für die Rechtfertigung einer Videoüberwachung keinesfalls ausreichen. Ohne präsente Eingriffskräfte laufen Überwachungsmaßnahmen in Kürze ins Leere und erweisen sich als ungeeignet.

4.1.2
Videoüberwachung von besonders gefährdeten öffentlichen Einrichtungen

Für besonders gefährdete öffentliche Einrichtungen sind die rechtlichen Voraussetzungen für die Installierung von Videokameras deutlich weiter gefasst worden, da bestimmte Anlagen konstanten Gefährdungen ausgesetzt sein können. Gedacht ist hier z. B. an kern- oder gentechnische Anlagen von Universitäten, ferner Museen oder Kassenanlagen. Auch diese Form der Überwachung hat ihre Begrenzung und zwar in dem Begriff der „besonderen“ Gefährdung der genannten Einrichtungen. Nicht jede von Zeit zu Zeit auftretende Gefahr − wie Klebekolonien an Bushaltestellen − rechtfertigt eine dauerhafte Überwachung; denn diese „normalen Störungen“ gehen über das allgemeine Risiko, dass öffentliche Einrichtungen beschädigt werden können, nicht hinaus, erfüllen damit also nicht das Kriterium der „besonderen“ Gefährdung.

4.1.3
Videoüberwachung als Ausfluss des Hausrechts

Eine Besonderheit enthält Satz 2 des Abs. 4 insofern, als er den Kreis der Gefahrenabwehrbehörden über den des § 1 Abs. 1 HSOG erweitert hat. Der Schutz von Museen, Hochschuleinrichtungen etc. obliegt traditionell nicht den Gefahrenabwehrbehörden, sondern den Inhabern der öffentlichen Sachherrschaft, also den Hausherren. Damit erscheint es folge-

richtig, ihnen das Recht der Überwachung einzuräumen. Es ist aber bei der Auslegung der Vorschrift zu beachten, dass mit ordnungsrechtlichen Mitteln nicht die Rechte aus dem privatrechtlichen Hausrecht verteidigt werden können, sondern nur die Integrität der öffentlichen Sache.

4.1.4
Videoüberwachung zur Steuerung des Straßenverkehrs

Videoüberwachungsanlagen zur Steuerung des Straßenverkehrs gehören seit langem zur Realität, wurden aber in der Vergangenheit durchweg ohne Rechtsgrundlage betrieben. § 14 Abs. 4 Nr. 3 HSOG legalisiert diese Anlagen, formuliert aber strikte Zweckbindungen, die die Möglichkeiten dieser Befugnisnorm stark eingrenzen.

Zulässig sind lediglich beobachtende, keine aufzeichnenden Überwachungseinrichtungen, denn Verkehrslenkung setzt keine über den Augenblick hinaus reichenden Nachweise voraus. Zulässig sind ferner nur Überblicksaufnahmen, mit denen ein Bild über die Verkehrslage gewonnen werden kann; diese von den Datenschutzbeauftragten des Bundes und der Länder geforderte Begrenzung der Überwachungsbefugnis (vgl. Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000) ist in § 14 Abs. 4 Nr. 3 HSOG zwar nicht ausdrücklich formuliert worden, ergibt sich aber aus der gesetzlichen Zweckbestimmung flexibler Verkehrssteuerung.

Für den Regelfall ist auch der Einsatz von Zoomkameras ausgeschlossen, mit denen einzelne Verkehrsteilnehmer erfasst werden können. Soll ein multifunktionaler Einsatz erfolgen, etwa durch Mitbenutzung durch Strafverfolgungsbehörden, bedarf das der Aufnahme in das zu erstellende Verfahrensverzeichnis. Außerdem müssen für jeden Einzelfall die besonderen Ermächtigungsgrenzen der §§ 81b und 100c Strafprozessordnung (StPO) eingehalten werden. Im Übrigen erlaubt die datenschutzrechtliche Zweckbindung keine über die ursprünglichen Anordnungsgründe hinausreichende Verwendung.

4.1.5
Fazit

Der Einsatz von Videoüberwachungskameras im öffentlichen Raum darf durch die Gefahrenabwehrbehörden nur erfolgen, wenn es sich um einen Kriminalitätsschwerpunkt handelt, zur Sicherung besonders gefährdeter öffentlicher Einrichtungen und zur Verkehrslenkung. Die Formulierungen des Abs. 4 geben sowohl den Verwaltungsgerichten als auch dem Datenschutzbeauftragten rechtliche Instrumente an die Hand, befürchteten Entwicklungen zur flächendeckenden Überwachung nach englischem Vorbild entgegen zu treten.

4.2
Verkehrsüberwachung durch Videoaufzeichnungen

Dauerhafte Verkehrsüberwachungen durch ununterbrochen laufende Videokameras, bei denen auch ordnungsgemäß fahrende Verkehrsteilnehmer aufgezeichnet werden, sind unzulässig.

Aus Presseberichten und aus mir übergebenen Aufzeichnungen eines privaten Fernsehsenders habe ich entnommen, dass die Polizei in einer hessischen Großstadt Verkehrskontrollen mit einer Videokamera durchgeführt hat, die mit einer Geschwindigkeitsmessanlage gekoppelt waren. Mit der Videokamera wurden ununterbrochen Aufzeichnungen vorgenommen, aus denen sich nicht nur Geschwindigkeitsübertretungen, sondern das gesamte Geschehen auf der Straße ergaben. Dabei wurden überwiegend Personen erfasst, die sich ordnungsgemäß verhielten. Die ununterbrochene Aufnahme wurde angeordnet, um alle Arten von Verkehrsverstößen im nachhinein ermitteln zu können. Ich konnte mich davon überzeugen, dass sich auf diesen Aufnahmen sowohl die Gesichter und Fahrzeugkennzeichen als auch sonstige Verhaltensweisen (Gurtanlegung, Telefonieren) einwandfrei identifizieren ließen.

Diese Art der Verkehrsüberwachung ist unzulässig, da hierbei unterschiedslos Verkehrssünder und sich ordnungsgemäß verhaltende Verkehrsteilnehmer aufgenommen werden. Die angewandte Technik ist datenschutzrechtlich zu beanstanden. Der aufnehmende Beamte muss die Kamera zwischenzeitlich abschalten, solange er visuell keine Ordnungswidrigkeiten wahrnimmt. Eine Datenerhebung auf Vorrat nach dem Muster, irgendwas werde sich schon finden, ist unzulässig. Für den Nachweis von Verkehrsverstößen im Geschwindigkeitsbereich müssen Kameraeinrichtungen verwendet werden, die sicherstellen, dass ordnungsmäßig fahrende Verkehrsteilnehmer nicht im Klarbild aufgezeichnet werden. Da alle Bänder zu Beweiszwecken in verkehrsrechtlichen Ordnungswidrigkeitenverfahren aufgehoben werden müssen, sind bei Verwendung von Klarbildern zwangsläufig auch die Bilder der sich ordnungsgemäß verhaltenden Verkehrsteilnehmer gespeichert. Das ist unzulässig, da deren Aufzeichnung weithin vermeidbar ist.

Ununterbrochene Aufnahmen gehen über das erforderliche Maß an Personenerfassung hinaus. § 81b Strafprozessordnung (StPO) sieht die Möglichkeit vor, Lichtbilder von Beschuldigten gegen deren Willen für die Zwecke der Durchführung des Strafverfahrens anzufertigen. Der Begriff des Beschuldigten setzt jedoch voraus, dass ein Anfangsverdacht gegen den Betroffenen besteht. Ein solcher Anfangsverdacht scheidet bei den oben beschriebenen flächendeckenden Aufnahmen hinsichtlich der Mehrzahl der Personen aus, da sie sich keiner Straftat oder Ordnungswidrigkeit verdächtig gemacht haben.

Gem. § 100c Abs. 1 StPO dürfen auch ohne Wissen des Betroffenen Lichtbilder und Bildaufzeichnungen hergestellt werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder erschwert wäre. Da jedoch bereits in diesem Teil der Ermächtigungsnorm auf den Täter Bezug genommen wird, dürfen Personen, die keine Täter sind, nicht in ein Bildaufzeichnungsverfahren einbezogen werden. Dasselbe ergibt sich aus § 100c Abs. 2 Satz 1 StPO, wo es heißt, dass Maßnahmen nur gegen den Beschuldigten gerichtet werden dürfen. Gegen sonstige Personen sind Maßnahmen nur zulässig, wenn die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesent-

lich erschwert wäre. Bei den durchgeführten Verkehrsüberwachungen durch Videokameras ist eine derartige Erschwerung nicht gegeben, so dass flächendeckende Aufnahmen auch gegenüber Nichtbeschuldigten nicht gerechtfertigt sind. Eine wesentliche Erschwerung kommt insbesondere dort nicht in Betracht, wo durch individuelle Videoaufnahmen eine Selektion möglich ist.

Nach § 100c Abs. 3 StPO sind nur unvermeidbare Nebenaufnahmen hinzunehmen. Dies betrifft Fahrer, die im Hintergrund eines Verkehrssünders zwangsläufig mit aufgezeichnet werden. Diese Unvermeidbarkeit rechtfertigt jedoch keinesfalls ununterbrochene Bildaufzeichnungen.

Ich habe mich − neben der Rüge gegenüber dem Polizeipräsidium − inzwischen mit dem Hessischen Ministerium des Innern und für Sport in Verbindung gesetzt, um eine generelle Änderung der Verfahrensweise zu erreichen. Unabhängig davon habe ich zu dem mir vom Hessischen Ministerium des Innern und für Sport übersandten Erlassentwurf zur Regelung der Verkehrsüberwachung durch örtliche Ordnungsbehörden Stellung genommen.

In dieser Stellungnahme habe ich darum gebeten, die von mir in diesem Beitrag ausführlich geschilderte, rechtlich zulässige Verfahrensweise in den Erlass aufzunehmen.

4.3
Die Videoüberwachung in Schulen

Unter bestimmten rechtlichen Voraussetzungen erlaubt der neu in Kraft getretene § 14 Abs. 4 HSOG die Videoüberwachung im Schulbereich.

Eine hessische Schule bat mich um rechtliche Beratung bei der Frage, ob sie den Fahrradständer in der Schule durch eine Videoanlage überwachen dürfe. Ziel der geplanten Überwachung war die Vermeidung von Fahrraddiebstählen. Dabei sollte lediglich der auf den Fahrradständer reduzierte Blickbereich aufgezeichnet und jeweils zwei Tage später wieder gelöscht werden, sofern kein Diebstahl gemeldet wurde.

Die Anfrage fiel zeitlich mit der gerade neu in Kraft getretenen Vorschrift des § 14 Abs. 4 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) zusammen, die den hessischen Gefahrenabwehrbehörden den Einsatz eines Videogerätes zur Gefahrenabwehr unter bestimmten Vorraussetzungen erlaubt.

§ 14 Abs. 4 HSOG

Die Gefahrenabwehrbehörden dürfen offen Bildaufzeichnungen anfertigen:
1. Zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen,
2. zum Schutz besonders gefährdeter öffentlicher Einrichtungen,
3. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrs nicht entgegenstehen.

Gefahrenabwehrbehörde im Sinne der Nr. 2 ist auch der Inhaber des Hausrechtes. Abs. 1 Satz 2 und 3 gilt entsprechend.

Eine Besonderheit dieser Vorschrift, an deren Zustandekommen ich im parlamentarischen Beratungsverfahren beteiligt war, liegt darin, dass die Befugnis zum Einsatz einer Videoanlage auf alle hessischen Behörden ausgeweitet wurde, soweit sie das Hausrecht der betroffenen gefährdeten öffentlichen Einrichtung innehaben (siehe oben letzter Satz). Dabei kann als öffentliche Einrichtung auch das Dienst- oder Verwaltungsgebäude angesehen werden. Das Hausrecht übt der Schulleiter hinsichtlich des gesamten Schulgeländes aus, auf dem sich auch der betroffene Fahrradständer befindet. Somit ist eine der rechtlichen Vorraussetzungen erfüllt. Weiterhin verlangt § 14 Abs. 4 Nr. 2 HSOG, dass die öffentliche Einrichtung „besonders“ gefährdet ist. Dazu zählt auch die Möglichkeit, dass tatsächliche Anhaltspunkte dafür bestehen, dass dort Straftaten begangen werden können. Diese Bedingung sah ich bei der betroffenen Schule insoweit als erfüllt an, als dort immer wieder Fahrräder gestohlen oder stark beschädigt wurden. Die angestrebte Prävention verlangt natürlich, dass potentielle Täter gerade durch einen deutlich sichtbaren Hinweis auf die Videoüberwachung vom betreffenden Tun abgehalten werden sollen. Deshalb spricht § 14 Abs. 4 Satz 1 HSOG von „offen“. Einen solchen Hinweis verlangt auch der ansonsten geltende § 12 Abs. 1 Satz 2 HDSG.

§ 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.

Im Rahmen des Ermessens, wie der Videoeinsatz gestaltet wird, ist das Prinzip der Erforderlichkeit zu beachten. Dieses gebietet eine Einschränkung des Beobachtungsfeldes auf den Fahrradständerbereich. Das Umfeld darf nicht gefilmt werden.

Hinsichtlich der formalen Anforderungen war auf die Notwendigkeit einer vorherigen Errichtungsanordnung hinzuweisen (künftig: Verfahrensverzeichnis) nach § 28 Abs. 1 HSOG. Außerdem musste eine sog. Vorabkontrolle nach § 7 Abs. 6 HDSG stattfinden, die der datenschutzrechtliche Sicherung der aufgezeichneten Daten dient.

Nicht zu beanstanden war die geplante Löschungsfrist von zwei Tagen. Sie liegt innerhalb des von § 14 Abs. 1 Satz 2 HSOG vorgegebenen Rahmens und orientiert sich an dem Erforderlichkeitsprinzip.

§ 14 Abs. 1 HSOG

...
die Unterlagen sind spätestens zwei Monate nach Beendigung der Veranstaltung oder Ansammlung zu vernichten, soweit sie nicht zur Verfolgung einer Straftat oder auch Schutzwürdigkeit oder zur Strafvollstreckung benötigt werden.

Ich habe die Schule gebeten, mich über die Wirkung des Videoeinsatzes zu informieren, um hier praktische Erfahrungen auch für Anfragen anderer Schulen zu sammeln. Außerdem muss nach Ablauf von Einsatzperioden die Erforderlichkeit fortdauernder Überwachung erneut überprüft werden. Der Geeignetheit der Überwachungseinrichtung für die gesetzten Ziele kommt dabei besondere Bedeutung zu.

5. Justiz

Speicherung von Entscheidungstexten auf Richterarbeitsplätzen

Die längerfristige Speicherung von Entscheidungsentwürfen auf den PCs der Richterinnen und Richter − aber auch die Aufbewahrung von Kopien aller Entscheidungen in Papierform − zur Verwendung in zukünftigen vergleichbaren Verfahren ist mangels Rechtsgrundlage nur in anonymisierter Form zulässig.

Im Rahmen des vermehrten Einsatzes von PCs im Bereich der Gerichte durch Richterinnen und Richter ist mit mir erörtert worden, ob und wie lange die von den Richterinnen und Richtern verfassten Entscheidungen unabhängig von den jeweiligen Verfahren auf ihren Rechnern gespeichert werden dürfen.

Aus den Reihen der Richterinnen und Richter werden verschiedene Gründe für eine solche (unbefristete) Aufbewahrung genannt. Bei nachfolgenden Verfahren mit vergleichbaren Sachverhalten vereinfacht sich das Erstellen von Entscheidungstexten, wenn auf frühere Texte zurückgegriffen werden kann. Teilweise möchten Richterinnen und Richter auch einen Überblick über Streitigkeiten zwischen Parteien behalten, die sich häufig vor Gericht gegenüberstehen. Schließlich können solche älteren Entscheidungen für andere Mitglieder eines Spruchkörpers Hilfestellungen bei der Einarbeitung in spezielle Materien sein. Bei nicht wenigen Gerichten ist es auch üblich, Kopien aller Entscheidungen in Ordnern in der Gerichtsbibliothek aufzustellen, so dass zumindest jedes Mitglied des Gerichts und alle Referendare Zugriff nehmen können.

Für alle hier genannten Fälle ist nach meiner Auffassung eine Verwendung von Entscheidungstexten nur zulässig, wenn eine Anonymisierung stattfindet. Für personenbezogene Speicherungen ist wegen der beabsichtigten nachfolgenden Zweckänderung eine Rechtsgrundlage nicht gegeben. Da in Deutschland eine Kennzeichnung von Entscheidungen mit dem Namen des Klägers und des Beklagten unüblich ist, kann die personenbezogene Auswertung so nicht gerechtfertigt werden.

Jede Verarbeitung von personenbezogenen Daten außerhalb der anhängigen Streitverfahren stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Entsprechend der Rechtsprechung des Bundesverfassungsgerichtes ist dazu eine gesetzliche Grundlage nötig. Außerdem ist die Erforderlichkeit der Zweckänderung in jedem Einzelfall zu prüfen. Die Verfahrensordnungen sehen diese Art der Verwendung von Urteilen bislang nicht vor. Ein Fall der zulässigen Zweckänderung gem. § 13 Abs. 2 i.V.m. § 12 Abs. 2 und Abs. 3 Hessisches Datenschutzgesetz (HDSG) ist ebenfalls nicht gegeben.

§ 13 Abs. 2 HDSG

Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, dann ist dies nur aus den in § 12 Abs. 2 und 3 genannten Gründen zulässig. Besondere Amts- oder Berufsgeheimnisse bleiben unberührt.

§ 12 HDSG

(2) Bei öffentlichen Stellen dürfen Daten im Einzelfall ohne seine Kenntnis nur erhoben werden, wenn
1. eine Rechtsvorschrift dies vorsieht, zwingend voraussetzt oder der Betroffene eingewilligt hat,
2. die Bearbeitung eines vom Betroffenen gestellten Antrags ohne Kenntnis der Daten nicht möglich ist oder Angaben des Betroffenen überprüft werden müssen; der Betroffene ist darauf hinzuweisen, bei welchen Personen oder Stellen seine Daten erhoben werden können,
3. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit und persönliche Freiheit dies gebietet,
4. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder
5. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(3) 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.

Diese Regelungen gelten auch für Richterinnen und Richter; dem steht die richterliche Unabhängigkeit nicht entgegen.

§ 25 DRiG

Der Richter ist unabhängig und nur dem Gesetz unterworfen.

Der richterlichen Unabhängigkeit gem. § 25 Deutsches Richtergesetz (DRiG) trägt das HDSG insoweit Rechnung, als die Kontrollrechte des Hessischen Datenschutzbeauftragten gem. § 24 Abs. 1 S. 3 sich nur auf die Tätigkeiten der Gerichte bezieht, die nicht der richterlichen Unabhängigkeit unterliegen.

§ 24 Abs. 1 HDSG

Der Hessische Datenschutzbeauftragte überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den datenverarbeitenden Stellen. Zu diesem Zwecke kann er Empfehlungen zur Verbesserung des Datenschutzes geben; insbesondere kann er die Landesregierung und einzelne Minister sowie die übrigen datenverarbeitenden Stellen in Fragen des Datenschutzes beraten. Die Gerichte unterliegen der Kontrolle des Hessischen Datenschutzbeauftragten, soweit sie nicht in richterlicher Unabhängigkeit tätig werden. Der Hessische Datenschutzbeauftragte kontrolliert die Einhaltung der Datenschutzvorschriften auch bei den Stellen, die sich und soweit sie sich nach § 4 Abs. 3 Satz 1 seiner Kontrolle unterworfen haben.

Aus der Beschränkung der Kontrollrechte des Hessischen Datenschutzbeauftragten kann aber nicht abgeleitet werden, dass das Gesetz in materiellrechtlicher Hinsicht nicht zur Anwendung käme. Dem entspricht auch die Parallelregelung im Bundesdatenschutzgesetz (BDSG): Dort sind in § 2 Abs. 1 u. 2 die Organe der Rechtspflege ausdrücklich als Adressat der Regelungen benannt.

§ 2 BDSG

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform …

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

Die weitere Verarbeitung der personenbezogenen Daten aus den Entscheidungsentwürfen lässt sich nicht auf § 11 Abs. 1 HDSG stützen.

§ 11 Abs. 1 HDSG

Die Verarbeitung personenbezogener Daten ist nach Maßgabe der nachfolgenden Vorschriften zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Die Erforderlichkeit einer Datenübermittlung muss nur bei einer der beteiligten Stellen vorliegen.

§ 11 HDSG kommt nicht in Betracht, da der Erforderlichkeitsgrundsatz voraussetzt, dass ohne Zweckänderung eine Aufgabe nicht oder nicht vollständig erfüllt werden könnte. Soweit die Verarbeitung dieser Daten nur zweckmäßig und arbeitserleichternd, aber nicht unbedingt erforderlich ist, ist sie unzulässig.

Die gleichen Grundsätze gelten selbstverständlich auch für die Verwendung von Entscheidungskopien in Papierform.

6. Polizei- und Strafverfolgungsbehörden

6.1
Mangelnde Verwertung des Verfahrensergebnisses bei Datenspeicherungen durch die Polizei

Nicht immer kommt die Justiz ihrer Pflicht nach, die Polizei über den Ausgang eines Ermittlungsverfahrens zu informieren. Erfolgt die Information, ist sie oft unzureichend. Die Polizei wiederum unterlässt es gelegentlich, eine Mitteilung zur Kenntnis zu nehmen oder auszuwerten. Der Eingang der Verfahrensabschlussmitteilung wird oft nicht zum Anlass genommen, Datenspeicherungen zu prüfen. Mitteilungen über Freisprüche werden oft nur zu den Akten genommen. Bei Auskünften an Dritte wird nicht darüber informiert, dass Verfahren abgeschlossen und eingestellt sind.

6.1.1
Verweigerung begehrter Berichtigung

Eine Frau aus dem Wetteraukreis wurde in einer zivilrechtlichen Auseinandersetzung vom gegnerischen Rechtsanwalt wegen Nötigung, Verleumdung, falscher Verdächtigung, Schuldnerbegünstigung, Pfandkehr und Verstrickungsbruch angezeigt. Die Staatsanwaltschaft Gießen stellte das Verfahren nach § 170 Abs. 2 Strafprozessordnung (StPO) ein.

§ 170 StPO

(1) Bieten die Ermittlungen genügend Anlass zur Erhebung der öffentlichen Klage, so erhebt die Staatsanwaltschaft sie durch Einreichung einer Anklageschrift bei dem zuständigen Gericht.

(2) Andernfalls stellt die Staatsanwaltschaft das Verfahren ein. Hiervon setzt sie den Beschuldigten in Kenntnis, wenn er als solcher vernommen worden ist oder ein Haftbefehl gegen ihn erlassen war; dasselbe gilt, wenn er um einen Bescheid gebeten hat oder wenn ein besonderes Interesse an der Bekanntgabe ersichtlich ist.

Im beschriebenen Falle enthielt die der Betroffenen übersandte Einstellungsverfügung der Staatsanwaltschaft die Feststellung „Es besteht kein begründeter Tatverdacht mehr“. Die zunächst Beschuldigte wollte sich darüber versichern, dass sie bei der Polizei auch tatsächlich nicht mehr mit einer Datenspeicherung belastet ist. Sie legte ihrem Schreiben an die Polizei die Einstellungsverfügung bei und bat um Bestätigung der Löschung. Die Polizeidirektion antwortete ihr, die weitere Speicherung der Daten sei zur polizeilichen Aufgabenerfüllung erforderlich und diene der vorbeugenden Verbrechensbekämpfung. Daten, die in strafrechtlichen Ermittlungsverfahren gewonnen worden seien, dürften nach § 20 Abs. 4 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) ohne weiteres in automatisierten Dateien gespeichert werden, wenn die Person verdächtig ist, eine Straftat begangen zu haben. Der Ausgang des Ermittlungsverfahren sei für die weitere Speicherung irrelevant.

§ 20 Abs. 4 HSOG

Die Polizeibehörden können, soweit Bestimmungen der Strafprozessordnung oder andere gesetzliche Regelungen nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten gewonnen haben, zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten speichern oder sonst verarbeiten. Die Speicherung oder sonstige Verarbeitung in automatisierten Verfahren ist nur zulässig, wenn es sich um Daten von Personen handelt, die verdächtig sind, eine Straftat begangen zu haben; entfällt der Verdacht, sind die Daten zu löschen.

Die Betroffene berief sich auf diese Regelung und verwies auf die Feststellung der Staatsanwaltschaft, es habe kein begründeter Tatverdacht mehr bestanden. Sie drängte erneut auf Löschung. Die Polizei wertete dies als Widerspruch gegen ihre Entscheidung, gab den Vorgang zuständigkeitshalber an die Aufsichtsbehörde zur weiteren Entscheidung ab und bat, von weiteren Sachstandanfragen abzusehen. Nach einer Wartezeit von einigen Monaten − dies war kurz vor Redaktions-

schluss dieses Berichtes − wandte sie sich an mich. Ich habe die zuständige Polizeidirektion ob der mit § 20 Abs. 4 HSOG unvereinbaren Datenspeicherung aufgefordert, die Löschung vorzunehmen. Eine Entscheidung ist noch nicht getroffen.

6.1.2
Nicht aktualisierte Auskünfte

Nach Abgabe eines Verfahrens aufbewahrte Daten werden auch zu anderen Zwecken verwendet. Insbesondere bei Zuverlässigkeitsprüfungen teilt die Polizei anderen Stellen ihre Informationen mit. Diese müssen auf neuestem Stand sein. Das ist oft nicht der Fall. Dazu zwei Beispiele aus dem Berichtszeitraum.

6.1.2.1
Auskunft zu gaststättenrechtlichen Zwecken

Ein Gastwirt aus dem Frankfurter Umland beantragte eine Änderung seiner Gaststättenerlaubnis. Im Zuge der Prüfung seiner Zuverlässigkeit nach dem Gaststättenrecht informierte die Polizei die Ordnungsbehörde über fünf angeblich laufende Ermittlungsverfahren der Staatsanwaltschaft Frankfurt. Daraufhin wurde die Gaststättenerlaubnis versagt. Dass die Ermittlungsverfahren bereits seit Jahren abgeschlossen und von der Staatsanwaltschaft nach § 170 Abs. 2 StPO eingestellt worden waren, teilte die Polizei der Ordnungsbehörde nicht mit. Erst auf meine Anforderung hin erfolgte eine Korrektur der fehlerhaften Mitteilung. Unvollständige Datenübermittlungen dieser Art können die Betroffenen in gleicher Weise belasten wie Informationen, die von vornherein falsch sind. Alle Datenspeicherungen müssen auf den neuesten Stand gebracht werden, bevor eine weitere Verarbeitung erfolgt. Übermittlungen sind zu unterlassen, solange eine Berichtigung oder Aktualisierung nicht möglich ist.

6.1.2.2
Auskunft zu Zecken der Luftverkehrssicherheit

Ein Mitarbeiter der Frankfurter Flughafen AG sollte nach § 29 Luftverkehrsgesetz (LuftVG) auf seine Zuverlässigkeit geprüft werden. Die Zertifizierung des Hessischen Wirtschaftsministeriums ließ auf sich warten. Der Betroffene fürchtete bereits um seinen Arbeitsplatz. Er beantragte beim Landeskriminalamt Auskunft über eventuell gespeicherte Daten und bat gleichzeitig, eventuell gespeicherte Daten zu löschen. Ein scheinbar aussichtsloses Unterfangen: Vierzehn Mal hatten in den vergangenen zehn Jahren verschiedene Polizeibehörden wegen z. T. schwerer Delikte immer wieder Ermittlungen gegen ihn gerichtet. Allerdings waren alle Verfahren abgeschlossen. Nie wurde er verurteilt.

Das Hessische Landeskriminalamt kam in seinem Bescheid über den Löschungsantrag zu dem Ergebnis, die Einzelfallüberprüfung der Unterlagen habe ergeben, dass eine weitere Speicherung zur polizeilichen Aufgabenerfüllung nicht erforderlich ist. Es hat die Löschung aller Datenspeicherungen und die Vernichtung aller Kriminalakten veranlasst. Das Wirtschaftministerium erhielt eine korrigierte Antwort auf die Zuverlässigkeitsanfrage. Der Betroffene wurde als „zuverlässig“ im Sinne von § 29 LuftVG eingestuft. Er konnte seinen Arbeitsplatz behalten.

6.1.3
Unterbleibende Löschung trotz Freispruch

Ein Verdacht, der die weitere Speicherung von Daten rechtfertigt, entfällt bei Freispruch und vergleichbaren Verfahrenseinstellungen. Dennoch unterbleibt die Löschung immer wieder.

Im 28. Tätigkeitsbericht (Ziff. 5.3) hatte ich einen Sachverhalt geschildert, in dem die Polizei die Mitteilung über den Freispruch des Angeklagten lediglich zur Akte genommen hatte. Obwohl das Gericht festgestellt hatte, dass überhaupt keine Straftat vorlag, behielt die Polizei ihre Datenspeicherung bei. Um festzustellen, ob es sich dabei um einen Einzelfall handelte oder ob regelmäßig so verfahren wird, hat mir eine Frankfurter Justizbehörde durch Auswertung ihres Datenbestandes eine Aufstellung von Fällen angefertigt, in denen Angeklagte vom Gericht freigesprochen worden waren. Ich nahm eine Stichprobe und bat das Polizeipräsidium Frankfurt um die Vorlage von dreizehn durch mich ausgewählten Akten.

Zu sechs Personen verfügte die Polizei über keinerlei Informationen. Ob Datenspeicherungen und Akten nie vorhanden gewesen oder vorhanden gewesen und mittlerweile gelöscht waren, konnte nicht mehr festgestellt werden. In zwei Fällen − die Angeklagten wohnten nicht in Frankfurt − war nicht auszuschließen, dass die Frankfurter Polizei nie beteiligt war. In den anderen vier Fällen ist davon auszugehen, dass vorhanden gewesene Akten vernichtet und gespeicherte Daten gelöscht worden waren.

Die sieben vorgelegten Kriminalakten hatten eines gemeinsam: In allen Fällen hatte die Polizei nicht nur wegen des Sachverhaltes ermittelt, in dem der Betroffene freigesprochen worden war, sondern auch in Zusammenhängen, in denen es nicht zu Freisprüchen gekommen war. Die Ermittlungen betrafen zum Teil schwere Delikte. In einem Fall lag der Polizei keine Mitteilung über den Freispruch vor, in sechs Fällen war die Mitteilung über den Freispruch nur zu den Akten geheftet. Warum die Betroffenen freigesprochen worden waren, war der Polizei in keinem Falle bekannt. Dies ging nicht aus den Mitteilungen hervor. Die unzureichende Überprüfung der Datenlöschung wurde gerügt.

6.1.4
Unzureichende Sachstandsmitteilung durch die Staatsanwaltschaft

Ebenfalls im Zusammenhang mit einer ordnungsbehördlichen Zuverlässigkeitsprüfung informierte eine Polizeibehörde in Südhessen das Landratsamt über drei anhängige Ermittlungsverfahren der Staatsanwaltschaft beim Landgericht Darmstadt. Auch hier lagen die Verfahren bereits einige Zeit zurück und sind schon vor mehreren Jahren von der Staatsanwaltschaft

eingestellt worden. Der Verfahrensausgang war der Polizei nicht mitgeteilt worden. Die Staatsanwaltschaft erklärte dazu, in einem Falle habe es sich um ein Versehen gehandelt. Im zweiten Fall sei die Mitteilung unterblieben, weil die Polizei die Mitteilung über den Verfahrensausgang nicht mit dem zur Rückgabe vorgesehenen Vordruck formularmäßig angefordert habe. Zum dritten Falle führte sie an, die Polizei sei nicht im Sinne der Übermittlungsvorschrift mit der Angelegenheit „befasst“ gewesen.

Art. 32 Justizmitteilungsgesetz

(1) Die Staatsanwaltschaft teilt der Polizeibehörde, die mit der Angelegenheit befasst war, ihr Aktenzeichen mit.

(2) Sie unterrichtet die Polizeibehörde in den Fällen des Absatzes 1 über den Ausgang des Verfahrens durch Mitteilung der Entscheidungsformel, der entscheidenden Stelle sowie des Datums und der Art der Entscheidung. Die Übersendung eines Abdrucks der Mitteilung zum Bundeszentralregister ist zulässig. Im Falle des Erforderns auch des Urteils oder einer mit Gründen versehenen Einstellungsentscheidung.

Zwar habe sie den Beschuldigten auf Ersuchen der Staatsanwaltschaft vernommen, „Befasstsein“ im Sinne der Übermittlungsvorschrift sei aber nur gegeben, wenn die Polizei von Amts wegen oder auf Anzeige Ermittlungen aufnehme. Das Justizministerium habe ich zu dieser Rechtsauffassung um eine Stellungnahme gebeten. Die Antwort steht noch aus.

6.1.5
Die Rechtslage

Schließt die Polizei ihre Ermittlungen in einer Strafsache ab, so gibt sie das Ergebnis nebst den dabei entstandenen Unterlagen und Beweismitteln zur weiteren strafrechtlichen Beurteilung und Verfolgung an die zuständige Staatsanwaltschaft ab. Die Informationen, die sie während der Aufklärung der Straftat gewonnen hat, benötigt sie zu diesem Zweck in der Regel nicht mehr. Sie hat aber ein Interesse daran, die Daten später zu anderen Zwecken, nämlich zur Verhütung von Straftaten oder zur Aufklärung anderer Straftaten zu verwenden. Die Rechtsgrundlage einer Datenspeicherung nach Verfahrensabschluss ist § 20 Abs. 4 HSOG (Zitat s. 6.1.1). Das setzt voraus, dass der Verdacht fortbesteht, eine Straftat begangen zu haben. Entfällt der Verdacht, muss gelöscht werden. Trifft die Staatsanwaltschaft in ihrer Einstellungsverfügung die Feststellung, dass kein begründeter Verdacht besteht, steht auch der Polizei kein Ermessensspielraum mehr zur Verfügung. Das gleiche gilt für gerichtliche Freisprüche, die Ablehnung, das Hauptverfahren zu eröffnen und für die Einstellung des Verfahrens wegen Gesetzesänderung. Die Polizei muss in diesen Fällen auf eine weitere Datenspeicherung verzichten. Mit dem letzten Halbsatz des § 20 Abs. 4 HSOG ist eine Löschungspflicht beim Vorliegen einer bestimmten Bedingung (Wegfall des Verdachts) gegeben.

Umgekehrt bedeutet dies aber nicht, dass die Datenspeicherung immer zulässig ist, solange der Verdacht besteht. Auch dann muss eine Abwägung getroffen werden zwischen dem öffentlichen Interesse zu Zwecken der Strafverfolgung, Strafvollstreckung, Gefahrenabwehr oder Gefahrenvorsorge auf polizeiliche Erkenntnisse zurückgreifen zu können und dem Interesse des Einzelnen, Einwirkungen der öffentlichen Gewalt nicht ausgesetzt zu sein.

Für diese Abwägung ist der Ausgang des Verfahrens von großer Bedeutung. Kommt es beispielsweise zu einer Verurteilung zu einer Freiheits- oder Geldstrafe, ist das öffentliche Interesse an der Aufbewahrung der Information höher als das Interesse des Einzelnen an der Löschung seiner Daten. Gleiches gilt, wenn der Betroffene einen Strafbefehl der Staatsanwaltschaft annimmt. Weiterhin kann von einem überwiegendem öffentlichen Interesse an der Aufbewahrung der Daten ausgegangen werden, wenn die Staatsanwaltschaft ein Verfahren gegen eine Auflage z.B. das Ableisten von gemeinnütziger Arbeit oder das Bezahlen einer Geldauflage einstellt (§ 153a StPO). Bei allen sonstigen, in der Praxis durchaus häufig vorkommenden Fällen ist die Abwägung schwieriger. So kann die Staatsanwaltschaft ein Verfahren einstellen, wenn die Schuld des Täters als gering anzusehen wäre und kein öffentliches Interesse an der Verfolgung besteht (§ 153 StPO). Wenn kein öffentliches Interesse an der Verfolgung einer Tat besteht, an der der Beschuldigte nur eine geringe Schuld trägt, ist das öffentliche Interesse an der weiteren Aufbewahrung der gespeicherten Informationen fraglich und in jedem Einzelfall sorgfältig zu prüfen. Schwierig ist auch die Einordnung von Freisprüchen aus Mangel an Beweisen. Sofern das Gericht verbleibende Verdachtsmomente im Urteil anführt, bestätigt es damit, dass Ermittlungen zu Recht geführt worden sind. Trotzdem ist der staatliche Anspruch auf Strafverfolgung mit der Rechtskraft des Urteils verwirkt. Deswegen muss eine Entscheidung über die weitere Aufbewahrung von Daten unter genauer Auswertung der Urteilsgründe getroffen werden. Das Gleiche gilt, wenn die Staatsanwaltschaft ein Verfahren aus Mangel an Beweisen (§ 170 Abs. 2 StPO) einstellt oder wenn sie einen Kläger auf den Privatklageweg verweist.

Hilfestellung sollen die Richtlinien für kriminalpolizeiliche Sammlungen des Hessischen Landeskriminalamtes (sog. KPS-Richtlinien) geben. Diese sehen allerdings die Löschung von Daten nach Einstellung eines Verfahrens nur für den Fall vor, dass gar keine Straftat vorliegt oder − wie bereits gesetzlich geregelt − ein Verdacht ausgeräumt wurde. Selbst bei einem Freispruch ist die Löschung nur für den Fall vorgesehen, dass er wegen erwiesener Unschuld erfolgt ist. Für die Polizeibehörden ist diese − dringend erneuerungsbedürftige − Richtlinie verbindlich. Es ist daher nicht mit einer Löschung zu rechnen, wenn ein strafrechtlicher Vorwurf weder erwiesen noch ausgeräumt wurde. Auch bei einem Freispruch aus Mangel an Beweisen ist nicht mit einer Löschung zu rechnen. Hinzu treten die Fälle, in denen die Staatsanwaltschaft es unterlässt, die Polizei über die Einstellung eines Verfahrens zu informieren. Letzteres passiert nicht selten.

6.1.6
Fazit

Zum einen muss der Informationsfluss zwischen Justiz und Polizei verbessert werden. Die Justiz muss sicherstellen, dass die Polizei auch tatsächlich über die Art des Abschlusses eines Ermittlungsverfahrens informiert wird. Ob diese Information stattfindet oder nicht, darf nicht davon abhängen, ob die Polizei der Staatsanwaltschaft dafür einen Vordruck zur

Verfügung stellt. Die Mitteilung muss als Regelverhalten vorgesehen werden; es ist problematisch, ob dazu überhaupt eine Einzelfallentscheidung getroffen wird. Mit dem fortschreitenden Einsatz der Datenverarbeitung in der Justiz durch die Einführung des Verfahrens MESTA (**Me**hrländer-**St**aatsanwaltschafts-**A**utomation) ist an sich auszuschließen, dass die Mitteilung an die Polizei in Vergessenheit gerät (s. 27. Tätigkeitsbericht, Ziff. 6.3). Das Verfahren sieht eine automatische Information der Polizei vor.

Des Weiteren muss sichergestellt werden, dass die Information in den Polizeibehörden auch tatsächlich verwertet wird. In den von mir überprüften Fällen hätte die Polizei, nachdem sie über einen Freispruch informiert worden war, auf die weitere Speicherung ihrer Informationen verzichten und die Akten bereinigen müssen. Im Zweifelsfalle hätte sie beim Gericht weitere Informationen über die Gründe des Freispruchs einholen müssen. Keinesfalls ist das einfache Abheften der Mitteilung ohne weitere Prüfung sachgerecht. Jeder Freispruch eines Gerichtes beinhaltet die Regelvermutung, dass der Verdacht gegen den Angeklagten nicht aufrecht zu halten ist. Daraus folgt für den Regelfall eine Löschungspflicht. Das gilt auch für die Einstellung von Verfahren. Die Informationen, die zu solchen Verfahren zusammengetragen worden waren, dürfen regelmäßig zur Verdachtsschöpfung oder Verdachtsverdichtung für evtl. künftig aufzuklärende Taten nicht mehr herangezogen werden.

Vor jeder Weitergabe von Informationen über Ermittlungsverfahren muss die Polizei die Daten aktualisieren. Ist das nicht möglich, weil aus Zeitgründen eine Eilauskunft gegeben werden muss, ist dieser die einschränkende Aussage hinzuzufügen, dass die Polizei keine Kenntnis vom Ausgang des Verfahrens hat und dass der Empfänger zu näherer Aufklärung verpflichtet ist.

Die KPS-Richtlinien sagen dazu teilweise nichts, teilweise Gegensätzliches aus. Bei der wegen der Änderungen in den §§ 477 ff. StPO ohnehin dringlichen Novellierung der Richtlinien müssen die datenschutzrechtlichen Belange der Betroffenen besser berücksichtigt werden. Das zuständige Ministerium ist auf den Anpassungsbedarf hingewiesen worden.

6.2
Medienpräsenz bei behördlichen Kontrollen und polizeilich angeordneten Maßnahmen

Wenn eine Polizeibehörde einem privaten Fernsehsender gestatten will, bei polizeilichen Maßnahmen anwesend zu sein und diese zu filmen, so muss sie zuvor mit dem Fernsehsender eine Verfahrensweise vereinbaren, die die Rechte der Betroffenen wahrt.

Unter Ziff. 4.2 habe ich bereits ausführlich zur Frage der Verkehrsüberwachung mittels Videoaufzeichnungen Stellung genommen. Unabhängig von der Unzulässigkeit dieser Aufzeichnungen liegen mir darüber hinaus Videoaufnahmen privater Fernsehsender vor, deren Mitarbeiter in Absprache mit einem Beamten des Frankfurter Polizeipräsidium bei polizeilichen Maßnahmen anwesend waren und diese filmten.

Im konkreten Fall hatte − bereits zum zweiten Mal − ein privater Fernsehsender mit dem Polizeipräsidium vereinbart, dass ein Aufnahmeteam des Fernsehsenders bei Verkehrskontrollen der Polizei anwesend sein kann. Die Überwachung fand durch Videokameras statt. Diesen Vorgang durfte der Sender filmen. Anschließend wurden die Aufnahmen der Polizei in Gegenwart eines Aufnahmeteams elektronisch ausgewertet. Das Aufnahmeteam filmte auch die Auswertung. Gegen ein solches Vorgehen der Polizeibehörden habe ich rechtliche Bedenken, da sich ein solches Vorgehen der Polizeibehörden der Weitergabe von Daten im Sinne des § 23 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) nähert. Diese Vorschrift regelt die Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs. Zwar werden die Daten in diesem Fall nicht von den Polizeibehörden, sondern von den privaten Fernsehsendern erhoben, jedoch gestatten die Polizeibehörden durch die Anwesenheit privater Aufnahmeteams Aufzeichnungen, wie sie durch gleichartige Videoaufnahmen seitens der Polizei gefertigt würden.

Unabhängig davon, dass ich es grundsätzlich für erforderlich halte, ein Einvernehmen mit der Landesregierung herzustellen, in dem die Frage generell geregelt wird, inwieweit Polizeibehörden in dieser Form Absprachen mit privaten Fernsehsendern treffen dürfen, habe ich im konkreten Fall zunächst einen zwischenzeitlich gültigen Kompromiss vorgeschlagen.

Die nachfolgend aufgeführten Punkte habe ich als Bedingungen für die Beteiligung von Polizeibehörden an derartigen Aufnahmen formuliert. Sie müssen mit den beteiligten Fernsehsendern vor einer Maßnahme vereinbart werden:

1. Eine Person − Bürger oder Beamter − darf nicht aufgenommen werden, wenn sie nicht vorher über Umfang, Zweck und Dauer der Aufnahmen aufgeklärt wurde und ihr Einverständnis erklärt hat. Auf die Freiwilligkeit der Einwilligung ist die betroffene Person hinzuweisen, außerdem auf ihr jederzeitiges Widerrufsrecht.
2. Bilder von Personen oder andere personenbezogene Umstände (insbesondere Kennzeichen) dürfen ohne zusätzliche schriftliche Einwilligung nicht gesendet werden. Sie sind durch Schnitt zu löschen oder unkenntlich zu machen. Personenbezogenes Aufnahmematerial ist nach der Auswertung für die Sendung zu löschen. Die Löschung ist zu belegen.
3. Die Originalaufnahmen sind vor der Weiterverarbeitung von den Aufnahmeteams und den Polizeibehörden daraufhin zu überprüfen, ob sie datenschutzrechtlich unbedenklich sind. Widerspricht eine Seite, so dürfen sie nicht verwendet werden.
4. Solange keine Einwilligung vorliegt, weil der Betroffene vom Aufnahmeteam noch nicht angesprochen werden konnte, dürfen nur Übersichtsaufnahmen erstellt werden, die den Betroffenen nicht klar erkennen lassen.

Da die Polizei in gleicher Lage keine Videoaufzeichnungen machen dürfte (vgl. § 14 Abs. 3 HSOG), ist ihre Beteiligung an Aufnahmen Dritter problematisch. Es ist deshalb eine besondere datenschutzrechtliche Sorgfalt bei dem abgestimmten Vorgehen von Polizeibehörden und Aufnahmeteams geboten.

Dies gilt sowohl für die Teilnahme privater Fernsehsender an polizeilichen Maßnahmen als auch für deren Teilnahme an polizeilich angeordneten Maßnahmen.

In einem zweiten mir unterbreiteten Fall ging es darum, dass einem anderen privaten Fernsehsender gestattet wurde, außer an den verkehrspolizeilichen Alkoholkontrollen auch an den anschließend angeordneten Blutentnahmen zwecks Alkoholbestimmung teilzunehmen.

Weder die Polizeibeamten noch das Polizeipräsidium hatten eine Zuständigkeit für die Entscheidung über die Erstellung von Aufnahmen in den Praxisräumen des Arztes oder der Universität, in denen die angeordnete Blutentnahme durchgeführt werden sollte. Von diesen Stellen konnte den Aufnahmeteams daher keine Zusage für das Betreten dieser Räume und das Filmen der angeordneten Blutentnahmen in diesen Räumen gegeben werden. Dies kann nur durch den Inhaber des Hausrechts erfolgen.

Darüber hinaus besteht auch für den Amtsträger, der das Hausrecht ausübt, keine presserechtliche Verpflichtung zur Genehmigung. Selbst Behörden sind nach § 3 Abs. 1 S. 1 Hessisches Gesetz über Freiheit und Recht der Presse (PresseG) nur zur Auskunft und nicht zur Gestattung von Videoaufnahmen verpflichtet. Da die für die angeordnete Blutentnahme notwendigen Untersuchungsräume nicht „öffentlich zugänglich“ sind, bietet auch § 4 Abs. 1 des Rundfunkstaatsvertrages im Artikel 1 des Staatsvertrag über den Rundfunk im vereinten Deutschland keine Rechtsgrundlage dafür, dass privaten Aufnahmeteams der Zutritt und das Filmen in diesen Räumen gestattet wird.

Auch wenn eine Genehmigung der Filmaufnahmen erfolgt, müssen zum Schutz der Betroffenen die von mir formulierten Bedingungen eingehalten werden. Die hausrechtliche Genehmigung kann sich nur auf die Nutzung der öffentlichen Einrichtung, nicht auf die informationelle Selbstbestimmung betroffener Bürgerinnen und Bürger erstrecken.

Im vorliegenden Fall führte meine Intervention dazu, dass die ursprünglich vorgesehene Möglichkeit für den privaten Fernsehsender, Videoaufnahmen bei Verkehrskontrollen und Aufnahmen bei Blutentnahmen zwecks Alkoholbestimmung durchzuführen, zurückgezogen wurde. Einer der privaten Fernsehsender hat rechtliche Auseinandersetzungen über die Einschränkungen journalistischer Arbeit angekündigt. Ich bin gleichwohl bei meiner ursprünglichen Haltung verblieben.

6.3
Verarbeitung der Hessischen Polizeidaten beim Bundeskriminalamt im Wege der Datenverarbeitung im Auftrag

In Übereinstimmung mit den anderen Datenschutzbeauftragten halte ich eine Auslagerung der Verarbeitung wesentlicher Teile der Landesdatenbestände der Landespolizei zum Bundeskriminalamt aufgrund einer Verwaltungsvereinbarung grundsätzlich für unzulässig und darüber hinaus für verfassungsrechtlich bedenklich. § 2 Abs. 5 Bundeskriminalamtsgesetz bietet keine ausreichende Rechtsgrundlage.

Über die Entwicklung des Verfahrens „INPOL-neu“ habe ich in der Vergangenheit schon mehrmals berichtet, zuletzt im 27. Tätigkeitsbericht, Ziff. 5.3.

Die immer noch ausstehende Umsetzung der Bund-Länder-Planung hat verschiedene Ursachen. Zum einen haben sich bei der Entwicklung der notwendigen Schnittstellen zu den Landessystemen Schwierigkeiten ergeben. Zum anderen wurde in Frage gestellt, ob aus polizeifachlicher Sicht die Verwendung des gleichen Verfahrens auch für die Daten, die nicht INPOL-Relevanz besitzen und daher in landeseigenen Verfahren verarbeitet werden, sinnvoll sei. Die Einwände beruhen nicht zuletzt auf den anfallenden Kosten, wenn mehrere unterschiedliche Verfahren betreut werden müssen. Dies hat im Ergebnis dazu geführt, dass das Bundeskriminalamt (BKA) den Ländern angeboten hat, diese Datenverarbeitung für die Länder im Auftrag durchzuführen. Die Verarbeitung soll mit der gleichen Software erfolgen, die Verarbeitung der Daten einzelner Länder wird dabei nur logisch voneinander getrennt. Zudem ist vorgesehen, die Überführung der Daten in den INPOL-neu Bestand technisch so einfach wie möglich auszugestalten.

Der Termin- und Kostendruck, unter dem der Anschluss der Datenverarbeitung der Länder an INPOL-neu allmählich steht, darf weder die rechtliche Interpretation des Regelungsgehalts des § 2 Abs. 5 Bundeskriminalamtsgesetz (BKAG) steuern, noch als Begründung für eine Ausdehnung des wechselseitigen Zugriffs von BKA und Länderpolizeien auf Daten dienen, ohne dass die durch § 2 Abs. 1 BKAG bezeichnete Grenze beachtet würde.

§ 2 BKAG

(1) Das Bundeskriminalamt unterstützt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung.

(5) Das Bundeskriminalamt kann die Länder auf Ersuchen bei deren Datenverarbeitung unterstützen. Die Verarbeitung und Nutzung der Daten erfolgt nach den Weisungen der Länder und gemäß deren Vorschriften über die Datenverarbeitung im Auftrag.

Aus § 2 Abs. 1 BKAG folgt − jedenfalls bis zu einer gegenteiligen Entscheidung des Gesetzgebers − dass die Länderpolizeien grundsätzlich eigene Datenspeicher zu betreiben haben. Die Hilfskonstruktion per Auftragsdatenverarbeitung ist nur als vorübergehende Notmaßnahme zur Gewährleistung eines termingerechten Anschlusses der Länder an INPOL-neu tragbar. Nach der gegenwärtigen Rechtslage sind die Länder gehalten, eigene Anstrengungen zum Aufbau von Informationssystemen zu machen, die zum Verfahren INPOL-neu kompatibel sind. Ihre Datenbestände sind beim BKA gegeneinander so abzuschotten, wie es bei einer dezentralen Haltung der jenseits der Schwelle des § 2 Abs. 1 BKAG angesiedelten Landesdaten zwingend wäre.

In diesem Sinne hatte ich in Abstimmung mit den anderen Bundesländern zum Vertragsentwurf für die Auftragsdatenverarbeitung Stellung genommen. Gleichzeitig haben wir durch einen Konferenzbeschluss unsere Haltung bekräftigt (vgl. Ziff. 21.7).

Die Innenministerkonferenz hat im November 2000 beschlossen, dass sie die Einwände der Datenschutzbeauftragten des Bundes und der Länder nicht teilt. Sie hat sich dem Bundesinnenminister angeschlossen, der eine dauerhafte Verarbeitung der Landesdaten mit der Regelung des § 2 Abs. 5 BKAG für vereinbar hält.

Ich sehe nunmehr die Gefahr, dass noch häufiger, als bisher für INPOL-neu geplant, Daten zwischen den einzelnen Polizeien ausgetauscht bzw. in den INPOL-Verbund eingestellt werden. Ein Datenaustausch darf nur dort erfolgen, wo die INPOL-Relevanz besteht oder die gesetzlichen Vorgaben für eine Übermittlung gegeben sind. Die einfache Zugriffstechnik darf nicht zum Grund für die Durchbrechung der Bund-Länder-Schranken werden.

Gleichwohl kann ich mich zwingenden Erforderlichkeiten, im Wege einer zeitlich begrenzten Übergangslösung einen termingerechten Anschluss an INPOL-neu sicherzustellen, nicht verschließen. Das zwingt jedoch dazu, eine datenschutzkonforme Ausgestaltung der vertraglichen Grundlagen für eine übergangsweise Auftragsdatenverarbeitung zu erreichen. Dies ist bis zum Ende des Berichtszeitraumes nur teilweise gelungen. Zu den kritischen Punkten gehören dabei die Trennung der Datenbestände der einzelnen Teilnehmer, die Möglichkeiten eines länderübergreifenden Zugriffs sowie die Ausgestaltung der datenschutzrechtlichen Kontrolle.

Der bis Redaktionsschluss vorliegende Vertragsentwurf (Stand 14.11.2000) verweist für die Details auf Anlagen, die mir zu diesem Zeitpunkt nicht in endgültiger Fassung vorlagen. Dort soll auch der genaue Umfang der vom BKA zu erbringenden Leistungen festgelegt werden. Eine abschließende Bewertung konnte deswegen noch nicht erfolgen.

Die Art und Weise der logischen Trennung der Datenbestände gegenüber INPOL-neu sowie gegenüber anderen Ländern muss eine strenge Abschottung gewährleisten. Die Möglichkeit einer versehentlichen Fehlzuordnung zu einem anderen Datenbestand (insbesondere zum Verbund) muss durch hinreichende Mechanismen minimiert werden. Durch die Trennung sind auch übergreifend arbeitende Funktionalitäten wie ein Bestandsabgleich zwischen Verbund- und/oder Länderdaten auszuschließen. Aus älteren mir vorliegenden Entwürfen könnte man eher das Gegenteil schließen. Für einen solchen Bestandsabgleich gibt es aber keine Rechtsgrundlagen.

Darüber hinaus ist nach der mir derzeit bekannten Ausgestaltung für den Abrufenden vor Ort nicht erkennbar, ob es sich um einen Datensatz aus dem Verbund oder aus dem Landesdatenbestand handelt. Für die Bewertung einer Auskunft aus dem Informationssystem ist dies aber notwendig. Bei der heutigen Verfahrensweise gibt es dieses Problem nicht, da eine deutliche Trennung zwischen den Anfragen an das HEPOLIS-System und an INPOL erfolgt.

Der ältere Entwurf zur Vertragsanlage, in der der Funktionsumfang des Auftrages beschrieben werden soll, sieht eine gegenüber dem heutigen Stand ausgeweitete Datennutzung unter den Stichworten „Überwindung der regionalen Trennung von Landesgrenzen“ vor. Hier muss sichergestellt worden, dass immer eine „echte“ Entscheidung durch die hessische Polizei getroffen wird, ob und inwieweit die Polizei eines anderen Bundeslandes auf hessische Daten zugreifen darf, bevor technische Mechanismen zum Tragen kommen. Die Ausführungen im Entwurf sind insoweit zumindest missverständlich. So ist u. a. ausdrücklich vorgesehen, dass „Beziehungen“ zwischen Bundes- und Landesdaten hergestellt werden dürfen.

Auswertungen, Abgleiche und Referenzierungen dürfen lediglich in den nach den landesrechtlichen Vorschriften im berechtigten Zugriff anderer Länder stehenden Datenbeständen durchgeführt werden. Diese Zugriffe müssen getrennt vom Verbund INPOL-neu stattfinden. Länderübergreifende Auswertungen mit dem Ziel einer Überführung in den Bundesbestand, sobald Treffer in mehreren Ländern auftreten, wären mit der rechtlich unabdingbaren Trennung der Datenbestände nicht vereinbar. Dies würde die bereits gegen § 2 Abs. 1 BKAG verstoßende Erweiterung des Kriminalaktennachweises (KAN) um die „kriminelle Historie“ wiederum ausweiten (s. dazu auch die Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15.03.2000 zum unzulässigen Speicherungsumfang in „INPOL-neu“, Ziff. 21.5).

Nicht mit der Rechtslage vereinbar ist m. E. auch die Regelung zur Datenschutzkontrolle. § 4 Abs. 2 und 3 Hessisches Datenschutzgesetz (HDSG) verlangt, dass ein Auftragnehmer, der nicht dem Geltungsbereich des HDSG unterliegt, sich vertraglich meiner Kontrolle unterwirft.

§ 4 HDSG

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen; dabei sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen. Für ergänzende Weisungen gilt Satz 2 entsprechend. Der Auftraggeber hat zu prüfen, ob beim Auftragnehmer die nach § 10 erforderlichen Maßnahmen getroffen und die erhöhten Anforderungen bei der Verarbeitung von Daten, die besonderen Amts- oder Berufsgeheimnissen unterliegen sowie der in § 7 Abs. 4 genannten Daten eingehalten werden. An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen.

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzgesetzes unterwirft. Der Auftraggeber hat den Hessischen Datenschutzbeauftragten vorab über die Beauftragung zu unterrichten.

Der Vertragstext sieht vor, dass die Kontrolle der Tätigkeit des Auftragnehmers (BKA) ausschließlich durch den Bundesbeauftragten für den Datenschutz erfolgt.

Eine abschließende Bewertung der Datenverarbeitung im Rahmen von INPOL-neu hängt selbstverständlich auch von dem dazu notwendigen Sicherheitskonzept ab. Das Landeskriminalamt Hessen bleibt auch dann, wenn es Daten im Rahmen der Auftragsdatenverarbeitung durch andere verarbeiten lässt, für die ordnungsgemäße Datenverarbeitung verantwortlich. Auch bei einer Integration der Landesdatenhaltung in das Sicherheitskonzept von INPOL-neu muss gewährleistet sein, dass die landesrechtlichen Anforderungen an technisch-organisatorische Maßnahmen zur Datensicherheit vollständig erfüllt werden. Da dieses Konzept noch nicht vorliegt, kann insoweit noch keine Bewertung erfolgen.

Eine Protokollierung hat ausschließlich nach den rechtlichen Vorgaben und Weisungen des Landes als Auftraggeber stattzufinden. Wegen der auf den eigenen Datenbestand begrenzten Auswertungsbefugnis der Länder muss eine strikte Trennung der Protokolldatenbestände des INPOL-neu-Verbundes und der jeweiligen Landesdatenhaltungen stattfinden. Darüber hinaus ist sicherzustellen, dass eine Verarbeitung und Nutzung dieser Protokolldaten ausschließlich nach landesrechtlichen Vorgaben stattfindet. Insbesondere ist eine gemeinsame Verarbeitung mit den Daten aus der Protokollierung von INPOL-neu auszuschließen.

7. Verfassungsschutz

Prüfung der Aufbewahrungsdauer von personenbezogenen Daten beim Hessischen Landesamt für Verfassungsschutz

Beim Hessischen Landesamt für Verfassungsschutz habe ich die Einhaltung der Vorschriften über die Aufbewahrungsdauer von personenbezogenen Daten kontrolliert. Es ging mir vor allem darum festzustellen, ob seit der im Jahre 1997 erfolgten Prüfung Verbesserungen zu verzeichnen sind. Dies ist der Fall.

Im 26. Tätigkeitsbericht, Ziff. 14.1 habe ich von einer Prüfung des Landesamtes für Verfassungsschutz berichtet. Ich hatte damals festgestellt, dass bei der Festsetzung der Aufbewahrungsfristen für die vom Landesamt für Verfassungsschutz gespeicherten personenbezogenen Informationen sowie bei der vorgesehenen Überprüfung bzw. Löschung erhebliche Mängel bestehen. Durch neuerliche Prüfung habe ich festgestellt, dass die Mehrzahl der Mängel behoben ist.

7.1
Festlegung des Datums der letzten relevanten Erkenntnis (EK-Datum)

Wichtig ist dieses Datum deshalb, weil mit dem Zeitpunkt der Vergabe die Aufbewahrungsfristen in Gang gesetzt werden. Die Durchsicht von ca. 55 Akten aus ausgewählten Aktensachgruppen ergab, dass das EK-Datum überwiegend korrekt vergeben wird. Anders als bei der letzten Prüfung im Jahr 1997 gab es nur noch einen Fall, in dem es in der Akte kein dem EK-Datum korrespondierendes Ereignis gab. Die Mitarbeiter des Landesamtes für Verfassungsschutz räumten die fehlerhafte Vergabe des Datums ein, bewerteten allerdings den der Speicherung zugrunde liegenden Sachverhalt für so gravierend, dass eine Verlängerung der Wiedervorlagefrist vorgenommen wurde.

In ca. 25 Fällen hatte das EK-Datum zum letzten relevanten Sachverhalt Bezug, war aber ungenau festgelegt und differierte bis zu mehreren Monaten sowohl zu Gunsten als auch zu Lasten des Betroffenen. Es wurde Einvernehmen mit dem Landesamt für Verfassungsschutz erzielt, dass das EK-Datum exakt das Datum des letzten relevanten Ereignisses angeben muss.

In allen von meinen Mitarbeitern eingesehenen Fällen war die erforderliche Begründung für die Vergabe des EK-Datums − wie es nach der letzten Prüfung im Jahre 1997 vom Landesamt für Verfassungsschutz verfügt wurde − in der Akte zu finden.

Insgesamt hat sich das Verfahren der Vergabe des EK-Datums auf der Grundlage meiner Vorschläge deutlich verbessert.

7.2
Zeitnahe Prüfung der weiteren Speicherung oder Löschung

Breiten Raum bei meiner Prüfung nahm weiterhin die Frage ein, ob das Landesamt für Verfassungsschutz in angemessenen Zeitabständen die vom Bundesamt für Verfassungsschutz erstellten Listen der Datensätze abarbeitet, die zur Prüfung oder Löschung anstehen. Bei meiner letzten Prüfung hatte ich festgestellt, dass die vorgesehenen Fristen zur Überprüfung der Erforderlichkeit einer weiteren Speicherung teilweise bis zu einem Jahr überschritten wurden. Insgesamt lässt sich sagen, dass sich auch hier das Verfahren deutlich verbessert hat.

8. Finanzwesen

8.1
Keine Patientendaten für das Finanzamt zur Umsatzsteuerbefreiung

Die Entscheidung über die Befreiung von der Umsatzsteuer eines ambulanten Pflegedienstes zwingt im Regelfall nicht dazu, dem Finanzamt den vollen Namen, die Anschrift und die Diagnosen aller gepflegten Personen zu offenbaren.

Die Eingabe eines Abrechnungsinstitutes für die privaten Gesundheitsdienste machte mich auf einen problematischen Umgang mit Sozial- und Medizindaten bei der Umsatzsteuerbefreiung aufmerksam.

Gemäß § 4 Nr. 16e Umsatzsteuergesetz sind Pflegeeinrichtungen, die nur vorübergehend pflegebedürftige Personen aufnehmen oder ambulante Pflege leisten, von der Umsatzsteuer befreit, wenn die Pflegekosten in mindestens 40 % der Fälle von Sozialversicherungsträgern oder Sozialhilfe ganz oder zum überwiegenden Teil getragen worden sind. Um diese Voraussetzungen zu prüfen, verlangen die Finanzämter aufgrund eines BMF-Schreibens vom 14. November 1997 (Az.: IV C 4 − S 7171 − 41/86)

- die Darlegung der angefallenen Kosten,
- die Namen und Anschriften aller gepflegten Personen,
- den Nachweis ihrer Pflegebedürftigkeit,

- die voraussichtliche Dauer der Pflegebedürftigkeit durch eine Bestätigung der jeweiligen Kasse, des Gesundheitsamtes oder durch ärztliche Verordnung,
- den Nachweis des Entgelts für die gesamte Pflegeleistung und
- die Höhe des Kostenersatzes durch den Träger der Sozialversicherung oder Sozialhilfe.

In der Praxis bedeutet das, dass die Pflegeeinrichtungen für namentlich genannte Personen mitteilen müssen, ob und wie lange diese krank bzw. pflegebedürftig waren (dazu ist die Diagnose notwendig) und ob sie Krankenkassenleistungen oder Sozialhilfe erhalten.

Die Übermittlung dieser umfangreichen Pflege- und Sozialdaten ist für die Entscheidung der Finanzämter nicht erforderlich. Weil die Umsatzsteuerbefreiung überhaupt nur greift, wenn in 40% der Fälle die Sozialversicherung oder die Sozialhilfe als Kostenträger auftritt, ist eine darüber hinausreichende Prüfung der sensiblen Sozialmedizindaten durch die Finanzämter nicht mehr notwendig. Die Pflegeversicherung erfasst inzwischen nahezu alle Pflegebedürftigen in Deutschland. Allein die Bestätigung des Kostenträgers, dass eine Krankheit oder Pflegebedürftigkeit vorliegt, die eine Inanspruchnahme des Pflegedienstes begründet, reicht zur Prüfung des § 4 Nr. 16e Umsatzsteuergesetz aus. Es ist weder notwendig, Name und Anschrift des Betroffenen, noch dessen Gesundheitsstatus zu offenbaren. Die Prüfung der erforderlichen Informationen kann ohne weiteres anhand von pseudonymisierten Daten erfolgen. Im Fall begründeter Zweifel an der Steuererklärung der Dienste können die Daten mit den jeweiligen Einzelpersonen wieder verbunden werden. Namen und Anschriften aller pflegebedürftigen Personen sind zum Zwecke der Beurteilung der Umsatzsteuerbefreiung nicht notwendig. Sie könnten nur dann für Finanzämter erheblich werden, wenn die Steuererklärung der gepflegten Person selbst mit diesen Daten abgeglichen werden soll. Für eine solche weitergehende Nutzung der Daten gibt es jedoch keine gesetzliche Grundlage. Sie beinhaltet eine Zweckänderung, die das Umsatzsteuergesetz nicht vorsieht. Allenfalls kann erwogen werden, ob wie bei der Führung eines Fahrtenbuches bei Ärzten verfahren werden soll. Hier wird eine Trennung zwischen sachbezogenen und personenbezogenen Daten durch verschiedene Verzeichnisse zugelassen. Das personenbezogene Verzeichnis wird von den Finanzbehörden nur dann eingesehen, wenn Zweifel an der Richtigkeit der Erklärung bestehen und alle anderen Beweismittel erfolglos ausgeschöpft sind. Eine entsprechende Vorgehensweise beim Nachweis der Voraussetzungen zur Umsatzsteuerbefreiung würde verhindern, dass die Pflegedienste gezwungen werden, sensible Daten Dritter routinemäßig zu offenbaren.

§ 4 Nr. 16e Umsatzsteuergesetz ist eine bundesgesetzliche Vorschrift. Ich habe deshalb den Bundesbeauftragten für den Datenschutz gebeten, in diesem Sinne tätig zu werden, was dieser auch getan hat. Da es sich beim Petenten um ein hessisches Unternehmen handelt, habe ich mich gleichzeitig mit dem Hessischen Minister der Finanzen in Verbindung gesetzt und meine Ansicht vorgetragen. Mir wurde zugesagt, die Angelegenheit zu prüfen und über den Bundesrat einen entsprechenden Vorstoß einzubringen.

Ich werde in der Angelegenheit weiter berichten.

8.2
Das Finanzamt im Firmennetz

Der neue § 147 Abs. 6 Abgabenordnung lässt ab Januar 2002 im Rahmen der Außenprüfung einen unmittelbaren Zugriff des Betriebsprüfers auf die gesamte EDV-Buchhaltung eines Unternehmens und damit deren systematische Auswertung zu. Es ist verfassungsrechtlich dringend erforderlich, dass dieser Befugnisausweitung datenschutzrechtliche Grenzen gesetzt werden.

Mit Art. 7 des Gesetzes zur Senkung der Steuersätze und der Reform der Unternehmensbesteuerung (Steuersenkungsgesetz − StSenkG) hat der Bundesgesetzgeber eine gewichtige Änderung der Abgabenordnung verabschiedet. Durch die Neufassung des § 147 Abs. 6 Abgabenordnung (AO) werden nunmehr die Befugnisse der Finanzämter im Rahmen der Außenprüfung durch einen EDV-Zugriff auf die elektronische Buchführung von Wirtschaftsunternehmen erheblich erweitert.

§ 147 Abs. 6 AO

Sind die Unterlagen nach Absatz 1 mit Hilfe eines Datenverarbeitungssystems erstellt worden, hat die Finanzbehörde im Rahmen einer Außenprüfung das Recht, Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen. Sie kann im Rahmen einer Außenprüfung auch verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet oder ihr die gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden. Die Kosten trägt der Steuerpflichtige.

Der neue § 147 Abs. 6 AO lässt einen unmittelbaren Zugriff auf das gesamte Datenmaterial zu, der die systematische Auswertung der gesamten Buchhaltung ermöglicht. Die Finanzämter erhalten nicht nur das Recht, Einsicht in die gespeicherten Daten zu nehmen und das DV-System zur Prüfung der Unterlagen zu nutzen, sondern auch die Befugnis, dass die EDV-Buchhaltung nach den Vorgaben des Betriebsprüfers auszuwerten ist. Am weitesten reicht die Befugnis, die gesamte Buchhaltung auf einen maschinell verwertbaren Datenträger zur Verfügung gestellt zu bekommen. Die Kosten dieses Verfahrens hat der Betroffene zu tragen.

Während das Recht auf Einsichtnahme datenschutzrechtlich eher unproblematisch ist, weil auch schon bisher im Rahmen der finanzamtlichen Ermittlungen auf alle erheblichen Daten des Steuerpflichtigen Zugriff genommen werden kann, sind die weiterreichenden Nutzungen zweifelhaft. Obwohl die Finanzverwaltung während des Gesetzgebungsverfahrens immer wieder betonte, dass mit der neuen Vorschrift nur die bisherigen Prüfungsrechte dem technischen Fortschritt angepasst werden, ist qualitativ ein erheblicher Schritt in Richtung „Gläserner Betrieb“ erfolgt. Wo früher der Betriebsprüfer Kontakt mit einer Auskunftsperson suchen musste, vorhandene Unterlagen durcharbeiten und Unklarheiten in einem Abschlussgespräch klären musste, kann jetzt ein Duplikat der gesamten Buchführung mit ins Finanzamt genommen und ohne

Einvernehmen mit der Betriebsleitung systematisch ausgewertet, dauerhaft gespeichert und für eine wiederholte Prüfung von Einzelfragen permanent herangezogen werden. Letztlich wird die gesamte Betriebsbuchhaltung einschließlich der Leitungsbeschlüsse durch die Mitnahme und nachfolgende Einsichtnahme verfügbar.

In der Regel sind Finanzbuchhaltung und sonstige EDV bislang nicht in der Weise getrennt, dass technische Sperren eine Einsichtnahme verhindern. Da Auswertungen für alle Zwecke der Außenprüfung nach § 194 AO oder § 42f Einkommensteuergesetz verwendet werden können, wird es in Zukunft möglich sein, besondere Auswertungen der EDV-Buchhaltung allein zu Zwecken von Kontrollmitteilungen laufen zu lassen (§ 194 Abs. 3 i.V.m. § 147 Abs. 6 Satz 2 AO). Bei flächendeckendem Einsatz derartiger Kopien können EDV-Abgleiche mit anderen Betrieben vorgenommen werden, die ihre EDV dem Finanzamt in gleicher Weise haben zur Verfügung stellen müssen.

Die neue Vorschrift trifft − ebenso wie die Abgabenordnung insgesamt − keine gesetzlichen Vorkehrungen, um die Erforderlichkeit der Erhebung der Daten und deren weitere Verarbeitung, die Grenzen der Übermittlung, die Verwertbarkeit, Zweckbindung oder Löschung der Daten zu regeln. Die Einschränkung, dass die Befugnisse ausschließlich im Rahmen der Außenprüfung wahrgenommen werden dürfen, enthält keine ins Gewicht fallende Zuständigkeitsbegrenzung. Die immense Ansammlung von Firmendaten kann für Dritte von unbezahlbarem Wert sein und entsprechende Begehrlichkeiten wecken.

Die Unternehmen sind gezwungen, mit entsprechenden Investitionskosten eine Zugangssoftware zu installieren, die die für das Finanzamt bestimmten Daten von sonstigen Daten (Kundendaten, Entwicklungsdaten, Lohnkontendaten, Kalkulationsdaten, Arbeitnehmerdaten) trennt. Eine solche Abschottung wird notwendig, um unberechtigte Einblicke zu verwehren. Die Unternehmen haben nur extrem kurze Zeit, diese Umrüstung vorzunehmen oder gänzlich auf EDV-Buchhaltung zu verzichten.

Inwieweit eine Einschränkung dieser weitgehenden Vorschrift durch den Einführungserlass des Bundesministeriums der Finanzen erfolgen wird, ist noch nicht absehbar. Der Bundesminister der Finanzen hat seinen Entwurf der Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU; Stand bei Redaktionsschluss 6. Oktober 2000) im Internet veröffentlicht (http://www.bundesfinanzministerium.de/fach/index.htm). Darin ist zwar geregelt, dass Daten, die bereits vor dem 1. Januar 2002 archiviert sind, nicht wieder in das DV-System eingespeist werden müssen, wenn dies mit unverhältnismäßigem Aufwand für den Steuerpflichtigen verbunden wäre. Weitere datenschutzrechtliche Vorgaben sieht das Papier jedoch nicht vor. Insbesondere fehlt eine Ermessensbindung für die Finanzverwaltung. Auch eine Protokollierung der Aktivitäten des Betriebsprüfers (welche Kontrollen wann durchgeführt wurden) und eine Zuständigkeitsbegrenzung (nur der zuständige Betriebsprüfer darf die Daten auswerten) ist nicht vorgeschrieben worden. Aufbewahrungsfristen und Löschungsmodalitäten fehlen völlig.

Ein Anwendungserlass könnte − wenn er mit datenschutzrechtlichen Maßnahmen ausgestaltet wird − die weite Ermächtigung in § 147 Abs. 6 AO eingrenzen, obwohl es eigentlich nicht Aufgabe von Erlassen ist, datenschutzrechtliche Belange eines zu weit formulierten Gesetzes durch jederzeit abänderbare untergesetzliche Verwaltungsanweisungen nachzuschieben. Das Recht auf informationelle Selbstbestimmung ist Grundrechtsschutz. Ein Eingriff in dieses Recht bedarf nicht erst seit dem Volkszählungsurteil einer tragfähigen gesetzlichen Grundlage.

Ich habe meine zu diesem Thema veröffentlichte Presseerklärung dem Hessischen Minister der Finanzen vorgelegt und hatte auch Gelegenheit, meine Bedenken in einem persönlichen Gespräch zu erläutern. Der Staatsminister hat die verfassungsrechtliche Problematik anerkannt und teilt die grundsätzlichen Bedenken. Er hat zugesagt, sich über den Bundesrat (die Ländervertretung) für eine verfassungsmäßige Lösung stark zu machen.

9. Gesundheit

9.1
Verarbeitung personenbezogener Patientendaten im Rahmen des neuen Hausarztmodells (§ 73 SGB V) und in Praxisnetzen (u. a. §§ 140a ff. SGB V)

Bei der Verarbeitung personenbezogener Patientendaten im Rahmen des Hausarztmodells und innerhalb von Praxisnetzen muss die ärztliche Schweigepflicht eingehalten werden.

Seit einigen Jahren findet bundesweit in zunehmendem Umfang ein Aufbau von sog. Praxisnetzen statt, d. h. von Vernetzungen von niedergelassenen Ärzten bzw. von niedergelassenen Ärzten und Krankenhäusern. Mittels derartiger Praxisnetze wird − mit Unterschieden im Einzelnen − insbesondere eine Optimierung der Qualität und Wirtschaftlichkeit der Behandlung angestrebt.

Auch das am 22. Dezember1999 verabschiedete Gesetz zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreformgesetz 2000) sieht eine verstärkte Kooperation und Kommunikation zwischen den Leistungserbringern vor. Zum einen ist in § 73 Abs. 1b SGB V eine zentrale Datenhaltung beim Hausarzt gesetzlich vorgesehen. Dieser Regelung zufolge darf ein Hausarzt mit schriftlicher (widerruflicher) Einwilligung des Versicherten bei Leistungserbringern, die einen seiner Patienten behandeln, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben. Die behandelnden Leistungserbringer sind verpflichtet, den Versicherten nach dem von ihm gewählten Hausarzt zu fragen und diesem mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, die in Satz 1 genannten Daten zum Zwecke der bei diesem durchzuführenden Dokumentation und der weiteren Behandlung zu übermitteln; die behandelnden Leistungserbringer sind berechtigt, mit schriftlicher Einwilligung des Versicherten, die für die Behandlung erforderlichen Behandlungsdaten und Befunde bei dem Hausarzt und anderen Leistungserbringern zu beschaffen und für die Zwecke der von ihnen zu erbringenden Leistungen zu verarbeiten und zu nutzen.

Zum anderen sind in den §§ 140a ff. SGB V Regelungen zu sog. integrierten Versorgungsformen enthalten. Die Teilnahme der Versicherten an den integrierten Versorgungsformen ist freiwillig (§ 140a Abs. 2 SGB V). Die Vertragspartner müssen u. a. die Gewähr dafür übernehmen, dass sie eine an dem Versorgungsbedarf orientierte Zusammenarbeit zwischen allen an der Versorgung Beteiligten sicherstellen, einschließlich der Koordination zwischen den verschiedenen Versorgungsbereichen und einer ausreichenden Dokumentation, die allen an der integrierten Versorgung Beteiligten im jeweils erforderlichen Umfang zugänglich sein muss (§ 140b Abs. 3 Satz 3). Der Leistungserbringer darf aus der gemeinsamen Dokumentation die den Versicherten betreffenden Behandlungsdaten und Befunde nur dann abrufen, wenn der Versicherte ihm gegenüber seine Einwilligung erteilt hat, die Information für den konkret anstehenden Behandlungsfall genutzt werden soll und der Leistungserbringer zu dem Personenkreis gehört, der nach § 203 StGB zur Geheimhaltung verpflichtet ist (§ 140a Abs. 2 Satz 2 SGB V).

Im Rahmen von Beratungen habe ich darauf hingewiesen, dass das vom Gesetzgeber angestrebte Ziel einer verstärkten Koordination und Kommunikation zwischen den jeweils behandelnden Leistungserbringern grundsätzlich nachvollziehbar ist. Aus datenschutzrechtlicher Sicht ist es jedoch von zentraler Bedeutung, dass die verstärkte Koordination und Kommunikation zwischen den behandelnden Leistungserbringern am konkreten Behandlungsbezug orientiert bleibt. Insbesondere darf es nicht dazu kommen, dass ein Patient, der sich einer Behandlung durch einen am Praxisnetz teilnehmenden Arzt unterzieht, seine medizinischen Daten pauschal gegenüber allen an dem Netz beteiligten Leistungserbringern offenbaren muss.

Darüber hinaus habe ich das Hessische Sozialministerium, die Landesärztekammer Hessen, die Landeszahnärztekammer, die Kassenärztliche Vereinigung Hessen, die Kassenzahnärztliche Vereinigung, die Landesapothekerkammer, die hessische Krankenhausgesellschaft und die meiner Zuständigkeit unterliegenden gesetzlichen Krankenkassen eingehend darüber informiert, dass bei der Einführung des Hausarztmodells und bei dem Aufbau von Praxisnetzen die Beachtung der datenschutzrechtlichen Vorgaben von zentraler Bedeutung sind und die ärztliche Schweigepflicht in jedem Fall auch im Rahmen des Hausarztmodells und innerhalb von Praxisnetzen eingehalten werden muss.

Nach dem gegenwärtigen Sachstand sehe ich − u. a. nach einem intensiven Meinungsaustausch unter den Datenschutzbeauftragten des Bundes und der Länder − derzeit insbesondere die folgenden datenschutzrechtlichen Aspekte als besonders wesentlich an:

1. Auch bei der Kommunikation zwischen Ärzten gilt nach wie vor, insbesondere auch innerhalb von Praxisnetzen, die Schweigepflicht i.S.v. § 203 StGB und die Schweigepflicht der ärztlichen Berufsordnung. Sie darf erst nach Einwilligung des Patienten durchbrochen werden, soweit keine weitergehende Befugnisse zur Offenbarung der Daten (z. B. spezialgesetzliche Regelungen) vorliegen.

2. Soweit für die Kommunikation innerhalb eines Praxisnetzes eine Verarbeitung pseudonymisierter oder anonymisierter Daten ausreichend ist − z. B. für Zwecke der Qualitätssicherung − dürfen keine personenbezogenen Patientendaten ausgetauscht werden. Die Pseudonymisierung sollte durch den behandelnden Arzt erfolgen, um den Kreis derer klein zu halten, die Kenntnis von den sensitiven Daten haben.

3. Eine generelle und vorab für alle Behandlungen erklärte Einwilligung der Patienten in die künftige Verarbeitung ihrer medizinischen Daten, deren Umfang und Tragweite sie zum Zeitpunkt der Erklärung nicht übersehen können, ist nicht rechtswirksam. Die allgemeinen rechtlichen Anforderungen an Einwilligungserklärungen müssen beachtet werden. Insbesondere müssen die Betroffenen über Umfang und Zweck der vorgesehenen Verarbeitung ihrer Daten konkret informiert werden. Die Einwilligung ist in der Regel schriftlich zu erteilen. Ferner ist ein vorausgehender Hinweis durch den behandelnden Arzt bzw. andere Leistungserbringer erforderlich, dass die Einwilligung freiwillig ist und ein Widerruf der Einwilligung möglich ist.

4. Die Verpflichtung der Leistungserbringer, im Rahmen der integrierten Versorgung eine ausreichende Dokumentation der Behandlung sicherzustellen, die allen an der integrierten Versorgung Beteiligten im jeweils erforderlichen Umfang zugänglich sein muss, erfordert grundsätzlich keine zusätzliche gesonderte (Teil-) Dokumentation der an der integrierten Versorgungsform Beteiligten neben der Befunderfassung durch den Hausarzt gemäß § 73 Abs. 1b Satz 1 und 2 SGB V. Soweit im Rahmen eines solchen Praxisnetzes eine zusätzliche gesonderte (Teil-) Dokumentation der Behandlung der Patienten geplant wird, bedarf Umfang und Funktion dieser gemeinsamen Dokumentation (z. B. Notfalldatensatz, Kerndatensatz etc.) präziser Klärung.

5. Für die Datenspeicherung in einer gesonderten (Teil-) Dokumentation ist eine Einzeleinwilligung des Patienten für den konkreten Behandlungsfall erforderlich. Dies schließt eine Entscheidung über die Zugriffsberechtigung auf diese Daten ein.

6. Bei der Speicherung von Patientendaten beim Hausarzt oder in einer gesonderten (Teil-) Dokumentation der am Netz beteiligten Leistungserbringer ist die eindeutige Verantwortlichkeit für die Richtigkeit und Rechtmäßigkeit der Datenspeicherung sicherzustellen.

7. Für den Abruf von Patientendaten aus der gesonderten (Teil-) Dokumentation der am Praxisnetz beteiligten Leistungserbringer ist eine auf den konkreten Behandlungsfall bezogene Einwilligung des Patienten erforderlich. Es muss technisch sichergestellt werden, dass ein nicht an dem konkreten Behandlungsfall des Patienten beteiligter Arzt keinen Zugriff auf die in der gesonderten Dokumentation gespeicherten Daten dieses Patienten hat. Je nach Umfang der gesonderten (Teil-) Dokumentation müssen darüber hinausgehende technische Vorkehrungen getroffen werden, die einen sektoralen Zugriff auf den Datenbestand ermöglichen. Dem Patienten muss das Recht zugestanden werden, die Einwilligung auf Teile des Datenbestandes zu beschränken. Verfahrensmäßig ist sicherzustellen, dass die einmal gewährte Zugriffsmöglichkeit auf die Patientendaten nach Abschluss der Behandlung dieses Patienten nicht fortbesteht.

Gegen die Sicherstellung einer Notfallzugriffsberechtigung auf die jeweils erforderlichen Daten mit besonderer Protokollierung und Information des Hausarztes bestehen keine datenschutzrechtlichen Bedenken.

8. Durch ein effektives Verfahren ist sicherzustellen, dass der Patient sein Recht auf Auskunft und Einsicht in dem gesetzlich festgelegten Umfang bei seinem Hausarzt bzw. bei jedem an dem Praxisnetz beteiligten Leistungserbringer, der Zugriff auf die in der gemeinsamen (Teil-) Dokumentation gespeicherten Daten dieses Patienten hat, geltend machen kann.

9. Es bestehen datenschutzrechtliche Bedenken dagegen, dass ein Praxisnetz seine gesonderte (Teil-) Dokumentation im Rahmen einer Auftragsdatenverarbeitung bei einer externen nicht-öffentlichen Stelle verarbeiten lässt. Insbesondere ist zu berücksichtigen, dass der Beschlagnahmeschutz und das Zeugnisverweigerungsrecht des Arztes bei einer Datenweitergabe an einen externen Dritten nicht mehr gewährleistet sind. Soweit sich im Einzelfall die Notwendigkeit einer zentralen medizinischen Datei außerhalb des ärztlichen Bereichs begründen lassen sollte, müssten zum Ausgleich angemessene technische und organisatorische Sicherungsmaßnahmen vorgesehen werden.

10. Je nach Nutzung und Sicherheitsstandard eines konkreten Netzes (Intranet oder Internet) ist von der Erforderlichkeit einer kryptografischen Verschlüsselung personenbezogener Daten auszugehen. Dies gilt insbesondere, falls personenbezogene Patientendaten über das Internet versandt werden sollen. Darüber hinaus ist eine Sicherheitsinfrastruktur wichtig, die eine vertrauenswürdige Schlüsselerzeugung und Schlüsselverwaltung gewährleistet, um die automatisierte Überprüfung der Zugriffsberechtigung eines Leistungserbringers auf verschlüsselte Daten vornehmen zu können.

Da hinsichtlich der datenschutzrechtlichen Fragen der Vernetzung im Gesundheitsbereich sowohl die Zuständigkeit meiner Dienststelle für den öffentlichen Bereich (u. a. Kassenärztliche Vereinigung Hessen, Landesärztekammer, Krankenkassen, öffentlich-rechtliche Krankenhäuser) als auch die Zuständigkeit der Regierungspräsidien als Aufsichtsbehörde für den nicht-öffentlichen Bereich (u. a. niedergelassene Ärzte, nicht-öffentliche Krankenhäuser) gegeben ist, stehen beide Stellen für Beratungen zur Verfügung.

9.2
Datenschutzrechtliche Anforderungen an den Aufbau von medizinischen Forschungsnetzen

Beim Aufbau bundesweiter Forschungsnetze sind die Rechte der Patienten zu beachten. Personenbezogene Patientendaten dürfen vom behandelnden Arzt ohne Einwilligung des Patienten nicht an Dritte übermittelt werden. Soweit eine Übermittlung reidentifizierbarer Patientendaten an das Forschungsnetz zur Erreichung des Forschungszwecks notwendig ist, sollte die Übermittlung der personenbezogenen Daten nicht direkt an das Forschungsnetz, sondern an einen rechtlich selbständigen, unabhängigen Treuhänder erfolgen. Die Übermittlung personenbezogener oder pseudonymisierter Patientendaten bedarf einer schriftlichen Vereinbarung zwischen behandelndem Arzt und Forschungsnetz über die weitere Verarbeitung der Daten.

In diesem Jahr habe ich als federführender Landesbeauftragter den Verein Medizinisches Kompetenznetzwerk Parkinson-Syndrom e.V. beraten, welche datenschutzrechtlichen Anforderungen bei dem Aufbau des bundesweiten Forschungsnetzes Kompetenznetz Parkinson (KNP) zu beachten sind. Das Kompetenznetz Parkinson ist in der Vorbereitung am weitesten fortgeschritten und hat teilweise exemplarische Funktion für die folgenden Kompetenznetze.

9.2.1
Zweck der Forschungsnetze

Zweck des Vereins ist die Vernetzung naturwissenschaftlicher und theoretisch-medizinischer Grundlagendisziplinen sowie klinischer Arbeitsgruppen. Die Vernetzung soll die Diagnostik und Therapie von Parkinson-Syndromen fördern. Sitz des Vereins ist Marburg. Das Kompetenznetz besteht derzeit aus einem Verbund von 13 Universitätskliniken, Städtischen Kliniken, Parkinson-Fachkliniken, niedergelassenen Ärzten sowie Regionalgruppen der Deutschen Parkinson Vereinigung aus dem gesamten Bundesgebiet. Das KNP ist eines von neun derzeit vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen differenzierter Forschungsprogramme geförderter Kompetenznetze, die insbesondere auch die Durchführung von interdisziplinären Forschungsprojekten zu einem speziellen Krankheitsbild intensivieren sollen. Die weiteren Krankheitsbilder sind chronisch entzündliche Darmerkrankungen, Depression und Suizidalität, Krebs im Kindesalter, Leukämie, maligne Lymphome, Schlaganfall, Schizophrenie und Rheuma. Das KNP ist das größte der neun Kompetenznetze.

Die Kompetenznetze gehören der Telematikplattform (TMF) an. Der Zusammenschluss im Rahmen der TMF und die Einrichtung des Koordinierungsbüros der TMF am Fraunhofer Institut Software- und Systemschutz (ISST) hat u. a. zum Ziel, die Kompetenzen der Forschungsnetze auf dem Gebiet der Telematik zu bündeln und den Transfer von Know-how innerhalb der Forschungsnetze und der Forschungsnetze untereinander zu systematisieren und zu koordinieren. Der Aufbau der Infrastruktur der neun Kompetenznetze wird die Rahmenbedingungen auch für sonstige Verbundforschungen im Gesundheitsbereich langfristig wesentlich prägen. Die Art und Weise der Nutzung der Infrastruktur der Kompetenznetze nach Ablauf des Förderungszeitraums des Bundesministeriums für Bildung und Forschung (fünf Jahre) ist noch offen.

Parallel zu meinen Gesprächen mit dem Kompetenznetz Parkinson hat sich der Arbeitkreis Wissenschaft der Datenschutzbeauftragten des Bundes und der Länder unter meinem Vorsitz intensiv mit den generellen datenschutzrechtlichen Anforderungen an den Aufbau von Forschungsnetzen befasst. Es hat im Berichtszeitraum zwei Arbeitstreffen des Arbeitskreises Wissenschaft mit dem Koordinierungsbüro der TMF am Fraunhofer ISST und mit Vertretern verschiedener Forschungsnetze gegeben, bei denen die datenschutzrechtlichen Anforderungen an die Ausgestaltung verschiedener Konzepte für Forschungsnetze diskutiert wurden. Diese Diskussion wird fortgesetzt.

9.2.2
Einzelheiten zur Struktur der Kompetenznetzes

Die Einbeziehung eines Patienten kommt durch den persönlichen Kontakt mit dem behandelnden Arztes (Prüfarzt) zustande. Der Prüfarzt bittet den Patienten um seine Einwilligung in die Teilnahme an dem Forschungsprojekt. Beim Prüfarzt werden die Stammdaten erhoben und als sog. Minimal Daten (Minimal Data Set), erweiterte Daten (Extended Data Set) und projektspezifische Daten (Project specific Data Set) gespeichert. Der Prüfarzt pseudonymisiert die Minimal Daten, die erweiterten Daten und die projektspezifischen Daten und gibt sie in pseudonymisierter Form an einen Teilprojektserver des KNP weiter. Von dem Teilprojektserver werden die Minimal Daten und die erweiterten Daten in pseudonymisierter Form einmal täglich an den zentralen Datenbankserver des KNP weitergeleitet. Zugleich übermittelt der Prüfarzt die Stammdaten des Patienten und das Pseudonym an einen Treuhänder.

Eine Speicherung anonymisierter Patientendaten im Kompetenznetz ist für die Forschungszwecke nicht ausreichend. Eine Pseudonymisierung wird von den Forschern als notwendig angesehen, damit in bestimmten Fällen eine Reidentifizierung der Patienten möglich ist, z. B. um die Behandlung zu optimieren, um geeignete Patienten für Folgestudien oder neue Teilprojekte zu finden.

Zugriff auf die pseudonymisierten Patientendaten des Teilprojektservers sollen alle von dem Teilprojektleiter zugelassenen Prüfärzte haben. Zugriff auf die pseudonymisierten Patientendaten des zentralen Datenbankservers haben nur diejenigen Personen, denen auf Antrag Zugriff durch das oberste Gremium des Kompetenznetzes Parkinson, die Zentrale Konsensuskonferenz, gestattet wird.

9.2.3
Datenschutzrechtliche Anforderungen

9.2.3.1
Einwilligungserklärung des Patienten

Der Einwilligung des Patienten muss eine schriftlich konkrete Information des Patienten über den Umfang und Zweck der vorgesehenen Verarbeitung seiner Daten im Kompetenznetz Parkinson vorausgehen. Die Information muss insbesondere darstellen, ob und ggf. welche Stellen personenbezogene, pseudonymisierte und/oder anonymisierte Daten erhalten und welchen Personen oder Stellen die Daten im Rahmen von Forschungsprojekten oder Studien möglicherweise zu einem späteren Zeitpunkt verfügbar gemacht werden. In der Einwilligungserklärung muss darauf hingewiesen werden, dass die Einwilligung freiwillig ist, dem Patienten aus der Verweigerung der Einwilligung keine Nachteile entstehen und ein Widerruf der Einwilligung mit Wirkung für die Zukunft jederzeit möglich ist. Widerruft ein Patient seine Einwilligung, so muss sichergestellt sein, dass die personenbezogenen Patientendaten umgehend gelöscht werden.

Eine Einwilligung des Patienten ist nur dann rechtswirksam, wenn er vorher über den Verwendungszweck seiner Daten konkret informiert wurde und die Folgen seiner Einwilligung absehen kann. Eine generelle Einwilligung des Patienten in die Verwendung seiner Daten für künftige Forschungsvorhaben kommt daher nur hinsichtlich anonymisierter oder pseudonymisierter Daten in Betracht.

Ein mit mir abgestimmter Entwurf für eine Einwilligungserklärung des Patienten liegt inzwischen vor.

9.2.3.2
Vertrag Prüfarzt − Kompetenznetz

Die Übermittlung der Patientendaten durch den Prüfarzt an das Kompetenznetz bedarf − parallel zur Einwilligung des Patienten − einer schriftlichen Vereinbarung zwischen Arzt und Kompetenznetz, in der auch die Verwendung der Daten festgelegt wird. Der Prüfarzt, der seine Patientendaten übermittelt, muss sicherstellen, dass die Daten nur im Rahmen der Einwilligung des Patienten verwendet werden. Das Kompetenznetz muss sich insbesondere verpflichten, dass die Patientendaten nur für den vorgesehenen Zweck verarbeitet werden. Es muss gewährleistet werden, dass vor einer Weitergabe pseudonymisierter Daten aus der zentralen Datenbank des Kompetenznetzes an Forscher geprüft wird, ob durch die Herausgabe der Datensätze an diese Empfänger ein Reidentifizierungsrisiko entsteht. In diesem Fall dürfen die Datensätze nicht an Drittempfänger in der beantragten Form herausgegeben werden, sondern müssen Maßnahmen getroffen werden, die das Reidentifizierungsrisiko vermindern (z. B. eine Reduktion der Datenfelder etc.).

Ein Entwurf für einen Vertragstext, der die datenschutzrechtlichen Aspekte angemessen berücksichtigt, liegt inzwischen vor.

9.2.3.3
Einsatz eines Treuhänders

Die Verwaltung der Stammdaten und der Pseudonyme der Patienten sollte nicht durch das Kompetenznetz selbst, sondern durch einen Treuhänder erfolgen, damit der Kreis derjenigen Personen, die personenbezogene Patientendaten zur Kenntnis erhalten, eng begrenzt bleibt und das Risiko einer Kenntnisnahme der Daten durch Unbefugte minimiert wird.

Als Treuhänder sollte eine außenstehende Person oder rechtlich selbstständige Stelle gewählt werden, die einer besonderen Schweigepflicht unterliegt und bei der die Daten gegen eine Kenntnisnahme durch Dritte − auch gegen Beschlagnahme durch die Staatsanwaltschaft − gesetzlich geschützt sind.

Das Kompetenznetz Parkinson hat einen Rechtsanwalt als Treuhänder eingesetzt. Ein mit mir abgestimmter Vertragstext liegt vor. Aufgabe des Treuhänders ist es insbesondere, die Stammdaten und die Pseudonyme der Patienten sicher aufzubewahren und eine Reidentifizierung nur in den Fällen zu gestatten, die in der Satzung des Kompetenznetzes, der Einwilligungserklärung des Patienten und den Verträgen zwischen Prüfarzt und Kompetenznetz vorgesehen sind. Eine Reidentifizierung ist z. B. für den Fall vorgesehen, dass bestimmte Patientengruppen um ihre Einwilligung in die Teilnahme an einem weiteren Forschungsprojekt gebeten werden sollen.

9.2.3.4
Rechte der Patienten auf Einsicht und Auskunft

Der Patient hat ein Recht auf Einsicht und Auskunft bezüglich seiner personenbezogenen oder auf seine Person wiederbeziehbaren Daten. Hierüber und über die zuständige Stelle ist er im Formblatt zu informieren.

9.2.3.5
Pseudonymisierungsverfahren

Vor dem Einsatz des Pseudonymisierungsverfahren ist insbesondere zu klären,

- ob die identifizierenden Daten durch eine nicht sprechende Nummer ersetzt werden können oder ob sie verschlüsselt werden sollen,
- wer über die Zuordnungstabellen bzw. das Verschlüsselungsverfahren verfügen soll und wo es abgelegt wird,
- wer das Pseudonym generieren soll und
- wer unter welchen rechtlichen Voraussetzungen Pseudonym und Identifikationsdaten zusammenführen darf.

Darüber hinaus ist vor dem Einsatz von Pseudonymisierungsverfahren sicherzustellen, dass sich durch

- die Art der Generierung der Pseudonyme
- den Umfang der Verbreitung der Pseudonyme und
- den Umfang der zum Pseudonym gespeicherten Daten

keine unverhältnismäßigen Reidentifizierungsrisiken für die betroffenen Patienten ergeben. Dabei ist insbesondere zu berücksichtigen, über welches Zusatzwissen der Empfänger der Daten in der Regel verfügt.

Das im Rahmen des Kompetenznetzes Parkinson für einen Patienten generierte Pseudonym darf nicht in allen Forschungsbereichen dauerhaft weiter verwendet werden, weil das Reidentifizierungsrisiko zu groß würde. Es darf daher z. B. nicht in allen Forschungsnetzen für einen bestimmten Patienten dasselbe Pseudonym gespeichert werden. Eine derartige Verfahrensweise könnte auch vielfältige vom Patienten nicht vorhersehbare Forderungen nach Auswertungsmöglichkeiten für andere Zwecke durch andere Stellen nach sich ziehen.

Die Weitergabe von Pseudonymen innerhalb des Kompetenznetzes ist auf die Fälle zu beschränken, in denen die Kenntnisnahme ein und desselben Pseudonyms zur Erreichung des Forschungszwecks unerlässlich ist. Nur so können die Reidentifizierungsrisiken für die Patienten hinreichend begrenzt bleiben. Ansonsten sind anonyme Daten weiterzuleiten.

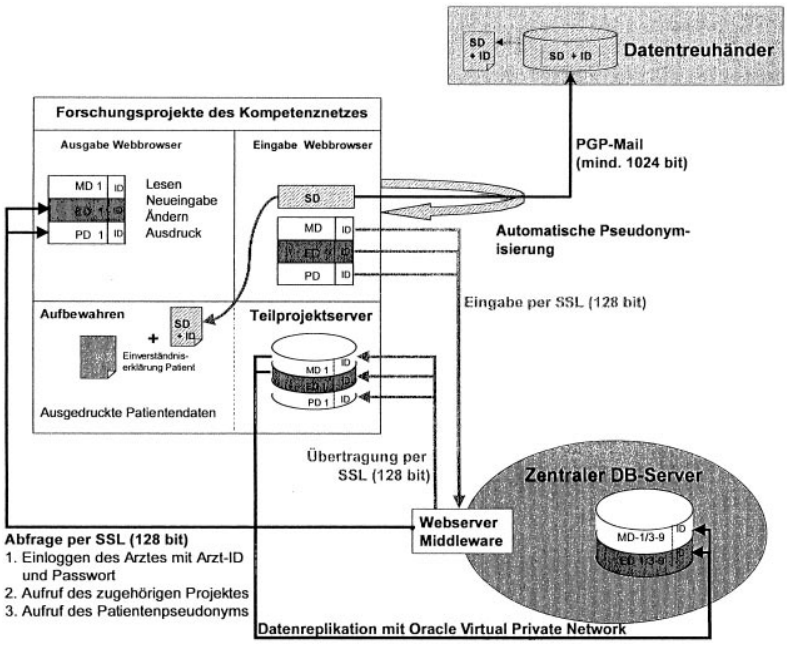
Das KNP wird zur Erzeugung des Pseudonyms Daten aus dem Personalausweis entnehmen. Dadurch wird eine einheitliche Schreibweise erreicht. Diese identifizierenden Daten werden dann mit einem asymmetrischen Verschlüsselungsverfahren (s. 22. Tätigkeitsbericht, Ziff. 21.1) zu einem Pseudonym verschlüsselt. Die datenschutzrechtliche Bewertung hängt entscheidend davon ab, dass die Pseudonyme so formuliert werden, dass sie nicht auf Personen rückführbar sind. Um eine Reidentifikation durch Außenstehende wesentlich zu erschweren, werden die Pseudonyme nur als Index innerhalb der Datenbank genutzt, um sie beim Prüfarzt oder Treuhänder mit den Daten eines Patienten zusammenführen zu können. Forschern und anderen Personen, die auf die Daten zugreifen können, sollen das Pseudonym nicht sehen können, sondern nur eine interne „laufende“ Nummer der Datenbank. Dadurch wird verhindert, dass Außenstehende eine Liste von Pseudonymen erhalten. Die im Konzept dargestellten Verfahren erfüllen insgesamt die datenschutzrechtlichen Anforderungen.

9.2.3.6
Technisch-organisatorische Maßnahmen zur Datensicherheit

Die vorgesehenen Datensicherheitsmaßnahmen wurden insbesondere unter dem Gesichtspunkt ausgewählt, dass technische Lösungen zur Umsetzung verfügbar sind. Sie werden, soweit erforderlich, dem Stand der Technik angepasst. Dies gilt auch für den Fall, dass im Bereich des TMF andere Standards oder Lösungen vorgesehen sind.

Nach dem Konzept des KNP sollen die Daten bei der Übertragung verschlüsselt werden. E-Mails sollen mit PGP verschlüsselt und signiert werden (zur Sicherheit bei E-Mails: s. 28. Tätigkeitsbericht, Ziff. 10.1), während zwischen den Servern ein symmetrisches Verschlüsselungsverfahren (s. 22. Tätigkeitsbericht, Ziff. 21.1 und 23. Tätigkeitsbericht, Ziff. 27.1) mit Schlüssellängen von 128 Bit vorgesehen ist.

Durch die Verschlüsselung und Signatur wäre die Kommunikation gesichert. Es müssen aber auch für die regionalen und zentralen Server ausreichende Sicherheitsmaßnahmen ergriffen werden, die ein Verfälschen der Daten verhindern. Diese Maßnahmen bedürfen noch der Klärung.



Patientenerfassung: Ein Prüfarzt eines Teilprojektes erfasst Patienten im Rahmen einer Studie. Der Arzt hat nur Zugriff auf die von ihm selbst eingegebenen Daten.
Ein Aufruf der Daten ist für den Prüfarzt möglich zum Eingeben, Ändern, Drucken, für Teilprojektleiter zum Lesen, Kommentieren, Drucken.

9.3
Hessisches Krebsregistergesetz: Umsetzung des Widerspruchsrechts der Patientinnen und Patienten

Das Hessische Sozialministerium muss sicherstellen, dass das den Patientinnen und Patienten nach dem Hessischen Krebsregistergesetz zustehende Widerspruchsrecht beachtet und korrekt umgesetzt wird.

Durch das Krebsregistergesetz vom 4. November (BGBl. I S. 3351) wurden die Länder verpflichtet, bis zum 31. Januar 1999 eigene Krebsregistergesetze zu erlassen. In Hessen wurde zunächst ein Ausführungsgesetz, befristet bis zum 31. Dezember 1999, erlassen. Damit ergab sich 1999 die Notwendigkeit einer Neuregelung der rechtlichen Grundlagen für die Verarbeitung personenbezogener Daten im Hessischen Krebsregister. Der Hessische Landtag hat zunächst ein Gesetz zur Änderung des Ausführungsgesetzes zum Krebsregistergesetz (AGKRG; GVBl. II S. 25) beschlossen, in dem eine Übergangsregelung bis zum 31. Dezember 2001 festgelegt ist. Bis dahin sollen die ersten Auswertungen bezüglich der Verfahrensweise und der inhaltlichen Ergebnisse der bereits gespeicherten Daten sowie die langfristigen rechtlichen Rahmenbedingungen der Verarbeitung personenbezogener Daten im Hessischen Krebsregister diskutiert und entschieden werden.

Die Übergangsregelung enthält in § 2 Abs. 2 Neuformulierungen zum Recht des Patienten, einer personenbezogenen Meldung seiner Erkrankung an das Hessische Krebsregister zu widersprechen. Im Gesetz ist jetzt auch festgelegt, dass die Information des Patienten über das Widerspruchsrecht zu dokumentieren ist.

§ 2 Abs. 2 AGKRG

Soweit die Patientinnen oder Patienten über ihre Erkrankung aufgeklärt sind, sind sie vor der Meldung zu informieren. Dabei sind sie in einem Informationsblatt über den Zweck der Meldung und darüber aufzuklären, dass sie einer Meldung mit voller Anschrift (namentliche Meldung) widersprechen können. Die Information ist zu dokumentieren. Widerspricht die Patientin oder der Patient oder konnte sie oder er vor der Meldung nicht informiert werden, darf die Meldung nur in kodierter Form erfolgen.

Im Interesse des Patienten und auch der behandelnden Ärzte sollten in Hessen einheitliche klare Vorgaben für die Umsetzung des Widerspruchsrechts der Patienten vorliegen. Unter Berücksichtigung der Diskussion mit den Landesbeauftragten für den Datenschutz, in deren Zuständigkeitsbereich ebenfalls ein Widerspruchsrecht des Patienten gegen eine personenbezogene Meldung ihrer Erkrankung an das Krebsregister gesetzlich festgelegt ist, habe ich dem Hessischen Sozialministerium folgendes Verfahren vorgeschlagen:

- Der behandelnde Arzt händigt dem Patienten ein Merkblatt aus, in dem über die rechtlichen Regelungen des Hessischen Krebsregistergesetzes, insbesondere über die vorgesehenen Meldungen und über das Widerspruchsrecht informiert wird.
- Der behandelnde Arzt vermerkt in der Krankenakte die Aushändigung des Merkblatts an den Patienten.

Durch diese Verfahrensweise ist gewährleistet, dass bei einem evtl. Streit über eine vorgenommene Meldung an das Krebsregister nachträglich festgestellt werden kann, ob und ggf. durch wen und zu welchem Zeitpunkt ein Patient über das Widerspruchsrecht informiert wurde. Eine schriftliche Erklärung des Patienten zu der Frage, ob er sein Widerspruchsrecht ausüben will, sehe ich nicht als erforderlich an. Sie würde dazu führen, dass der Patient gezwungen ist, sich zu einem bestimmten Zeitpunkt mit der Frage der Wahrnehmung seines Widerspruchsrechts zu befassen, in dem für ihn möglicherweise existentielle Fragen seiner Erkrankung im Vordergrund stehen. Die von mir vorgeschlagene Verfahrens-

weise überlässt es dem Patienten, wann und in welchem Umfang er sich mit der Frage seines Widerspruchsrechts auseinandersetzen will.

Die o. a. rechtlichen Vorgaben müssen selbstverständlich auch für evtl. Meldungen durch Ärzte gelten, die keinen direkten Kontakt mit dem Patienten haben (Pathologen etc.).

9.4
Recall-System des Medizinischen Zentrums für Augenheilkunde der Phillips-Universität Marburg

Die Übermittlung personenbezogener Patientendaten von niedergelassenen Augenärzten an die Augenklinik der Universität Marburg zur Speicherung der Daten im Recall-System bedarf einer Einwilligung der Patienten, die die Vorgaben des § 7 Hessisches Datenschutzgesetz berücksichtigt.

9.4.1
Fallbeschreibung

Durch die Eingabe eines Patienten bin ich auf eine problematische Verfahrensweise des Medizinischen Zentrums für Augenheilkunde der Phillips Universität Marburg aufmerksam geworden. Dieser beklagte sich darüber, von der Augenklinik angeschrieben und darauf aufmerksam gemacht worden zu sein, dass in nächster Zeit ein erneuter Termin bei seinem Augenarzt anstünde und er diesen doch bitte wahrnehmen möge. Der Betroffene war − nicht zuletzt wegen einer Diabetes-Erkrankung − in fortlaufender Behandlung bei einem niedergelassenen Arzt. Wie die Augenklinik zu seiner Anschrift gekommen war und zudem über seine Erkrankung Bescheid wusste, konnte er sich nicht erklären. Der Patient schrieb daher die Klinik an und forderte sie auf, seine Daten zu löschen und ihn nicht mehr anzuschreiben. Das wurde ihm von der Klinik auch zugesagt. Aufgrund einer organisatorischen Panne wurde die Löschung aber nicht vorgenommen und er bei einer anderen Gelegenheit erneut angeschrieben. Daraufhin wandte sich der Betroffene an mich.

9.4.2
Das Recall-System

Das angewandte Verfahren dient nach den mir gegebenen Erläuterungen der Augenklinik dem Zweck, Gesundheitsschäden zu vermindern. Obwohl exakte epidemiologische Erfassungen über Patienten mit Diabetes mellitus fehlen, schätzt man die jährliche Anzahl der Erblindungen in der Bundesrepublik Deutschland auf ca. 1500−2000. Aus Sicht der Ärzte ist diese Zahl für ein hochindustrialisiertes Land mit seinen medizinischen Möglichkeiten viel zu hoch. Aus diesem Grund wurde in Zusammenarbeit mit der WHO (World Health Organisation) und der IDF (International Diabetic Federation) Ende der achtziger Jahre eine Deklaration verfasst. Diese ist an die Augenärzte gerichtet mit dem Zweck, die Erblindungsquote in Europa um ein Drittel zu senken. Im Jahre 1990 wurde in Deutschland die „Initiativgruppe zur Früherkennung diabetischer Augenerkrankungen“ gegründet. Das vorgegebene Ziel soll dadurch erreicht werden, dass die vom Diabetes mellitus betroffenen Patienten über ihr Krankheitsbild aufgeklärt werden; außerdem soll die Zusammenarbeit zwischen den Ärzten gefördert werden, um diabetische Augenerkrankungen frühzeitig zu erfassen und zu behandeln.

Dazu wurde ein Untersuchungsbogen entwickelt, der den Augenärzten bundesweit zur Verfügung gestellt wird und von diesen ausgefüllt an eine zentrale Stelle, das medizinische Zentrum für Augenheilkunde in Marburg, zurückgeschickt werden soll. Der Bogen besteht aus einem Durchschreibesatz mit einem Original und drei Durchschriften. Der Originalbogen mit dem Stempel des untersuchenden Augenarztes soll dem überweisenden Hausarzt, Internist, Kinderarzt bzw. Diabetologen zugesandt werden. Die erste Durchschrift verbleibt bei dem untersuchenden Augenarzt, die zweite bekommt der Patient ausgehändigt. Die dritte Durchschrift wird an die Universitäts-Augenklinik geschickt. Dort werden Name und Anschrift des Patienten sowie dessen medizinische Daten gespeichert. Zu einem bestimmten Zeitpunkt erhält der Betroffene dann ein Schreiben der Klinik, mit dem er daran erinnert wird, erneut einen Augenarzt aufzusuchen.

9.4.3
Datenschutzrechtliche Problematik und rechtliche Bewertung

Die Weitergabe der Patientendaten an die Augenklinik erfolgt an eine externe Stelle, die mit der Behandlung des Patienten nicht befasst ist. Das bedarf einer Rechtsgrundlage. Als solche kommt nur die Einwilligung des Patienten in Betracht, da wissenschaftliche Ziele i. S. der Forschungsregelung des § 33 HDSG nicht verfolgt werden. Die datenschutzrechtlichen Probleme liegen darin, dass der Patient nicht ausreichend über das Recall-System informiert wird. Deswegen fehlt es an einer zweifelsfreien Einwilligung zur Übermittlung der Daten vom Augenarzt an die Universitäts-Augenklinik. Zwar ist auf dem Durchschreibebogen, der an die Augenklinik geht, eine Unterschrift des Patienten vorgesehen, der sich dadurch „mit einem Recall einverstanden“ erklärt. Es wird allerdings nichts darüber ausgesagt, ob und in welcher Form der Patient über das System inhaltlich informiert worden ist. Zudem ist die Einwilligungserklärung nur fragmentarisch abgefasst. Nähere Angaben zum Inhalt und Zweck der Datenübermittlung sowie zur Speicherung, Verarbeitung und Löschung der Daten in der Augenklinik sind nicht aufgeführt.

Diese Verfahrensweise entspricht nicht den Vorgaben des § 7 HDSG. Danach ist die Rechtswirksamkeit der Einwilligung an bestimmte Voraussetzungen geknüpft. Vor der Einwilligung ist der Betroffene über die Einzelheiten der geplanten Verarbeitung seiner Daten zu informieren und auf die Freiwilligkeit der Einwilligung und die Möglichkeit des Widerrufs der Einwilligung hinzuweisen (§ 7 Abs. 2 HDSG). Primär verantwortlich für das Vorliegen einer rechtswirksamen Einwilligung ist der niedergelassene Arzt, der seine Patientendaten an die Augenklinik offenbart. Parallel dazu ist aber auch die Augenklinik als speichernde Stelle für die Behandlungsdaten von Patienten der Augenärzte aus der gesamten Bundes-

republik dafür verantwortlich, dass in dieser Datei nur Daten gespeichert werden, die die Klinik rechtmäßig erhalten hat und weiterverarbeiten darf.

9.4.4
Weitere Verfahrensweise

Die Beschwerde hat dazu geführt, über den Datenschutzbeauftragten der Phillips-Universität Kontakt mit dem ärztlichen Direktor der Augenklinik aufzunehmen. Dabei zeigte sich, dass sich die Klinik nicht darüber im Klaren gewesen ist, dass es Defizite im Hinblick auf Patienteninformation und Einwilligungserklärung gibt. Da der Erhebungsbogen in Kürze neu gedruckt wird, wurde der Klinikleitung nachdrücklich empfohlen, den Bogen zu ergänzen, damit die Patienten eine rechtlich einwandfreie Einwilligungserklärung unterschreiben können. Hierzu habe ich einen Formulierungsvorschlag gemacht, der von der Klinik umgesetzt wird. Die Informationen zum „Recall“ sollen künftig auf einem gesonderten Informationsschreiben platziert werden, das dem Patienten ausgehändigt wird. Erwogen wird auch, ob die Information auf das Durchschreibeexemplar gedruckt werden soll, das der Betroffene ausgehändigt bekommt. Den Fehler, nach Aufforderung die Daten des Beschwerdeführers nicht gelöscht zu haben, räumte die Klinik als Missgriff ein.

9.5
Outsourcing des Pfortendienstes im Bürgerhospital Friedberg

Das Bürgerhospital Friedberg lässt den Pfortendienst von einem privaten Unternehmen organisieren. Bei einer Prüfung habe ich festgestellt, dass dem Pfortendienst weit mehr personenbezogene Daten von Patienten zur Verfügung stehen als er für die konkrete Aufgabenerfüllung benötigt.

Im Rahmen meiner Prüfung der Verarbeitung personenbezogener Daten im Auftrag hessischer Krankenhäuser (s. 28. Tätigkeitsbericht, Ziff. 8.3) erhielt ich u. a. Kenntnis davon, dass von Krankenhäusern teilweise auch der Pfortendienst auf private Dritte verlagert wird. Ich habe daraufhin beim Bürgerhospital Friedberg überprüft, welche Patientendaten für die Wahrnehmung des Pfortendienstes an Externe weitergegeben werden.

9.5.1
Rechtliche Vorgaben für eine Auftragsdatenverarbeitung

Maßstab für die rechtliche Beurteilung ist § 4 Hessisches Datenschutzgesetz (HDSG). Danach dürfen personenbezogene Daten unter bestimmten Voraussetzungen durch öffentliche oder private Stellen im Auftrag verarbeitet werden. Da § 12 Abs. 1 des Hessischen Krankenhausgesetzes ausdrücklich auf die Anwendung des Hessischen Datenschutzgesetzes verweist, gilt § 4 HDSG auch für die hessischen Krankenhäuser. Bei einer Auftragsvergabe ist von den Krankenhäusern zu beachten, dass sie für die Einhaltung der datenschutzrechtlichen Vorschriften weiter verantwortlich bleiben. Gegenstand und Umfang der Datenverarbeitung sowie die vom Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen (§ 10 HDSG) sind im Einzelnen vom Auftraggeber festzulegen und zu dokumentieren. Zudem muss sich das Krankenhaus Einsichts- und Kontrollrechte vorbehalten, den Auftragnehmer auf die Einhaltung der Vorschriften des Hessischen Datenschutzgesetzes verpflichten und dem Hessischen Datenschutzbeauftragten ein Kontrollrecht sichern. Weitere ausführliche Informationen zur Auftragsvergabe sind im 28. Tätigkeitsbericht, Ziff. 8.3 enthalten.

9.5.2
Vergabe der Aufgaben des Pfortendienstes an ein privates Unternehmen

Die Geschäftsleitung des Bürgerhospitals in Friedberg, einer Einrichtung mit etwa 250 Betten, hat im Zuge von Maßnahmen zur Kostensenkung den Pfortendienst des Krankenhauses einem privaten Unternehmen übergeben. An der Pforte, die am Haupteingang der Klinik platziert ist, werden Besuchern oder Anrufern u. a. Auskünfte darüber gegeben, ob eine bestimmte Person als Patient aufgenommen worden ist und auf welcher Station bzw. welchem Zimmer der Patient sich befindet. Das Pfortenpersonal verfügt über einen Bildschirm und hat Zugang zur Patientendatenbank des Krankenhauses. Damit ist es jederzeit und unmittelbar möglich, den Patienten ausfindig zu machen, z. B. über die Eingabe seines Nachnamens.

9.5.3
Ergebnis meiner Überprüfung

Bei meiner Überprüfung musste ich feststellen, dass das Pfortenpersonal auf eine Vielzahl von Patientendaten zugreifen kann, die für Auskünfte gegenüber Dritten gar nicht erforderlich sind. Das verstößt gegen § 11 Abs. 1 HDSG, wonach eine Verarbeitung personenbezogener Daten nur dann erfolgen darf, wenn sich diese im Rahmen der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben bewegt und für den jeweils damit verbundenen Zweck erforderlich ist.

So war neben dem Namen und Vornamen des Patienten sowie der Station, Zimmer- und Telefonnummer auch der Zugriff auf die Anschrift und den Beruf des Betroffenen möglich. Außerdem waren in dem alphabetisch sortierten Datensatz, auf den der Pfortendienst lesenden Zugriff hatte, das Aufnahme- und das Entlassungsdatum sowie der Pflegesatz und die Wahlleistungen enthalten.

Der Beruf des Patienten wie auch der Pflegesatz oder in Anspruch genommene Wahlleistungen sind für Auskünfte an Dritte ebenso wenig erforderlich wie die Anschrift des Betroffenen. Noch klärungsbedürftig ist, ob das Aufnahme- und Entlassungsdatum vom Pfortendienst benötigt wird.

Nicht nur der Umfang der zur Verfügung stehenden Daten war problematisch. Hinzu kam, dass die Speicherdauer sich nicht in dem Rahmen hielt, der als angemessen zu erachten ist. Eine systematische Löschroutine gab es nicht. So befanden sich im System noch Datensätze von Patienten, die seit mehr als einem halben Jahr aus dem Krankenhaus entlassen waren.

9.5.4
Vereinbarungen mit der Verwaltungsleitung des Krankenhauses

Mit dem Verwaltungsleiter des Bürgerhospitals wurde vereinbart, dass der dem Pfortendienst zur Verfügung stehende Datensatz deutlich und auf das erforderliche Maß reduziert wird. Ohne die Arbeit und Effizienz der Pforte zu beeinträchtigen, ist eine Reduktion auf die Merkmale Name, Vorname, Station, Zimmer- und Telefonnummer möglich. Außerdem wurde zugesichert, die Datensätze entlassener Patienten künftig zeitnah zu löschen.

9.6
Einführung eines Krankenhauskommunikationssystems im Universitätsklinikum Marburg

Im Universitätsklinikum Marburg wird ein neues Krankenhauskommunikationssystem eingeführt. Die Einführung wird von mir hinsichtlich der Umsetzung der datenschutzrechtlichen Vorgaben beratend begleitet. Das Universitätsklinikum entwickelt eine datenschutzgerechte Konzeption, die das Recht der Patienten auf eine klare Eingrenzung des Personenkreises, der ihre Krankheitsdaten zur Kenntnis erhält, angemessen berücksichtigt.

9.6.1
Rechtliche Vorgaben

Ein Patient, der sich zur Behandlung in ein Universitätsklinikum begibt, möchte selbstverständlich nicht, dass einige tausend Mitarbeiter seine sensitiven Krankheitsdaten zur Kenntnis erhalten. Er erwartet vielmehr zu Recht, dass die Kenntnis seiner Daten auf die mit seiner Behandlung betrauten Mitarbeiter beschränkt bleibt. Ein Krankenhaus ist keine datenschutzrechtliche Einheit, innerhalb derer personenbezogene Daten beliebig ausgetauscht werden dürfen. Der im Hessischen Datenschutzgesetz festgelegte Grundsatz der Zweckbindung personenbezogener Daten (§ 13 Abs. 1 und 2 HDSG) ist in Krankenhäusern besonders streng zu beachten. Darüber hinaus gilt grundsätzlich auch innerhalb des Krankenhauses die ärztliche Schweigepflicht i.S.v. § 203 Strafgesetzbuch (StGB). Im Krankenhaus darf daher jeder Arzt bzw. Mitarbeiter nur diejenigen Patientendaten zur Kenntnis erhalten, die er für seine eigene konkrete Aufgabenerfüllung benötigt. Im Hessischen Krankenhausgesetz (HKG) ist hierzu eine Regelung enthalten, die eine Abschottung der Datenbestände der Fachabteilungen innerhalb des Krankenhauses vorschreibt. In § 12 Abs. 2 HKG ist konkret festgelegt, in welchen Fällen personenbezogene Daten an Dritte außerhalb des Krankenhauses weitergegeben werden dürfen (z. B. zur Mit- oder Weiterbehandlung des Patienten). In Abs. 3 ist ergänzend geregelt, dass diese Regelungen auch innerhalb der Krankenhäuser mit Behandlungseinrichtungen verschiedener Fachrichtungen gelten. Eine Fachabteilung, die einen Patienten nicht behandelt, darf dessen medizinische Daten daher grundsätzlich nicht zur Kenntnis erhalten.

§ 12 Abs. 3 HKG

Abs. 2 und § 33 Abs. 1 bis 4 des Hessischen Datenschutzgesetzes gelten in Krankenhäusern mit Behandlungseinrichtungen verschiedener Fachrichtungen (Fachabteilungen) auch zwischen diesen.

Bei der Ausgestaltung der Zugriffsberechtigungen für ein Krankenhauskommunikationssystem müssen diese rechtlichen Vorgaben auf jeden Fall berücksichtigt werden. Angesichts der Komplexität der Kommunikationsvorgänge im Krankenhaus, der Vielzahl und auch der Fluktuation von Mitarbeitern mit verschiedenen Aufgabenbereichen und der zu berücksichtigenden besonderen Schichtdienst- und Notfallsituationen ist dies keine einfache Aufgabe. Es bedarf eines detaillierten Datenschutzkonzepts. Ein solches Konzept dient gleichzeitig der klaren klinikumsinternen Zuweisung von Aufgaben- bzw. Verantwortungsbereichen.

9.6.2
Aktueller Sachstand im Universitätsklinikum Marburg

In den vergangenen Jahren habe ich bei Prüfungen und Gesprächen vielfach festgestellt, dass die Ausgestaltung der Zugriffsberechtigungen in den Krankenhäusern nicht hinreichend differenziert erfolgte, z. B. Pförtner auf die gesamten medizinischen Daten aller Patienten zugreifen konnten, die Datenbestände der Fachabteilungen nicht voneinander abgeschottet waren etc. (s. auch Ziff. 9.4). Das Universitätsklinikum Marburg entwickelt nunmehr ein datenschutzgerechtes Konzept, das für die Einführung eines Kommunikationssystems in anderen Kliniken wesentliche Anregungen beitragen kann. Das Krankenhausinformationssystem (KIS) kann noch nicht die Patientenakte in Papierform ersetzen, weil derzeit eine digitale Signatur im Sinne des Signaturgesetzes noch nicht eingeführt werden kann. Eine elektronische Behandlungsdokumentation ohne digitale Signatur kann nicht in hinreichender Weise die Richtigkeit der Daten sicherstellen und hat nicht den für ein Klinikum notwendigen Beweiswert im Prozess. Das KIS soll aber im gesamten Klinikum alle Arbeiten rund um den Patienten unterstützen. Für das KIS wurde ein detailliertes Datenschutzkonzept erarbeitet, das ständig weiterentwickelt wird. Insgesamt arbeiten im Universitätsklinikum etwa 5.000 Mitarbeiterinnen und Mitarbeiter. Die neuen Programme laufen seit dem 13. Dezember 1999 an den drei Standorten des Klinikums, Lahnberge, Lahntal und Ortenberg, parallel zu noch vorhandenen älteren Verfahren in anderen Bereichen. Eine bedingte Abnahme des Systems ist im März 2000 erfolgt. Mit einer weiteren Ausbaustufe soll nach umfassendem Testbetrieb im Frühjahr 2001 begonnen werden.

9.6.2.1
Bereich der Verwaltung

Für die Aufnahme der Patientinnen und Patienten im Universitätsklinikum sind zu den normalen Dienstzeiten die insgesamt etwa 60 Mitarbeiterinnen und Mitarbeiter (einschließlich Halbtagskräfte) der entsprechenden Verwaltungsabteilung zuständig. Die für die Aufnahme der Patienten zuständigen Mitarbeiterinnen und Mitarbeiter an den Leitstellen haben grundsätzlich keinen Zugriff auf medizinische Daten der Patienten. Eine Ausnahme sind die medizinischen Daten, die gem. § 301 Sozialgesetzbuch V (SGB V) zur Abrechnung an die Krankenversicherung übermittelt werden müssen (z. B. Aufnahmegrund, Diagnosen, Prozeduren), da die Leitstellen zugleich für die Leistungserfassung zuständig sind.

Hinsichtlich des Umfangs des Datensatzes, auf den sie Zugriff haben, ist zwischen dezentralen und zentralen Aufnahmebereichen sowie zwischen der Aufnahme zu normalen Dienstzeiten und außerhalb der normalen Dienstzeiten zu unterscheiden.

Die reguläre Aufnahme während der normalen Dienstzeiten erfolgt entweder stationär oder ambulant nur durch Verwaltungspersonal. Außerhalb der normalen Dienstzeiten erfolgt auf einigen Stationen eine Kurzaufnahme mit einem eingeschränkten Datensatz durch dafür speziell geschultes medizinisch-pflegerisches Personal. Die Kurzaufnahmen werden bei Dienstbeginn von Verwaltungspersonal in reguläre Aufnahmen überführt und ergänzt.

Bei der Aufnahme eines neuen Patienten wird eine Patienten-Identifikations-Nummer (PID) vergeben. Diese Nummer behält der Patient dauerhaft für seine Behandlungen im Universitätsklinikum. Die Fallnummer wird im Bereich der stationären Aufnahme pro Aufenthalt vergeben, im Bereich der ambulanten Aufnahme wird pro Mandant (Fachabteilung/Poliklinik) und Abrechnungsart eine Fallnummer vergeben. Die Fallnummer wird im Bereich der stationären Aufnahme pro Aufenthalt vergeben, im Bereich der ambulanten Aufnahme wird für jeden Patienten (Fachabteilung/Poliklinik) und jede Abrechnungsart eine Fallnummer vergeben.

Die etwa 30 Mitarbeiterinnen und Mitarbeiter, die dezentral in den Kliniken im Lahntal und am Ortenberg für die Aufnahme von Patienten in ihre eigene Abteilung zuständig sind, sollen Zugriff jeweils nur auf die Administrationsdaten der Patienten ihrer Abteilung haben. Dies konnte zwar bisher noch nicht vollständig umgesetzt werden. Das Klinikum hat dies jedoch für 2001 zugesagt. Die Mitarbeiterinnen, die im zentralen Aufnahmebereich des Klinikums Lahnberge in den stationären Pflegeleitstellen, in der Notfall-Leitstelle oder in der Vertretungsfunktion arbeiten, haben Zugriff auf die Verwaltungsdaten aller im Universitätsklinikum aufgenommenen Patienten. In den Aufnahme- und Leitstellen werden Patienten für verschiedene Kliniken bzw. Abteilungen aufgenommen.

9.6.2.1.1
Ambulante Aufnahme

Das elektronische Aufnahmeformular enthält die Datenfelder für Name, Vorname, Geburtsdatum, Adresse, PID-Nummer, Fallnummer, Fachabteilung, Poliklinik bzw. Ambulanz, Aufnahmeart (stationär oder ambulant), Abrechnungsart, Beruf/Arbeitgeber, überweisender Arzt, Kostenträger Leistungen (nach Hauskatalog bzw. EBM, DKG-NT), Chefarztwahl, Daten nach § 301 SGB V (Behandlungsdiagnose nach ICD beim ambulanten Operieren).

9.6.2.1.2
Stationäre Aufnahme

Bei der stationären Aufnahme sind zusätzlich die Datenfelder Station, einweisender Arzt oder einweisendes Krankenhaus, Einweisungs- und Aufnahmediagnose, Daten nach § 301 SGB V (Diagnosen, Prozeduren nach ICD bzw. OPS-301), sonstige Wahlleistungen (Zimmerzuschläge, Telefon etc.) im Datensatz aufgeführt.

Wenn im Rahmen einer Aufnahme eine Fallnummer vergeben wurde, kann der jeweilige Mitarbeiter, der die Aufnahme vorgenommen hat, den gesamten Datensatz dieses Patienten nicht mehr löschen. Ohne Vergabe einer Fallnummer ist eine Einsichtnahme in die bereits gespeicherten medizinischen Patientendaten für keinen Mitarbeiter möglich. Wurde eine Fallnummer vergeben, so ist ab diesem Zeitpunkt nur noch eine vom System protokollierte Stornierung durch bestimmte Verwaltungsmitarbeiter der Sachgebiete ambulante und stationäre Abrechnung möglich. Auf diese Weise ist sichergestellt, dass in keinem Fall von einem Mitarbeiter die bereits gespeicherten medizinischen Patientendaten eingesehen werden können, ohne dass ein von ihm zu bearbeitender Aufnahmeantrag vorliegt.

9.6.2.1.3
Datensatz der Pfortenauskunft

Auf das Modul Pfortenauskunft können neben der Pforte auch Leitstellen, Sekretariate des klinischen Bereichs, Sachbearbeiter sowie das Archiv zugreifen. Diese letzteren, die ohnehin weitergehende Befugnisse als die Pforte haben, können im Rahmen einer „Fallübersicht“ noch zusätzliche Daten einsehen, die über die im folgenden genannten hinausgehen. Für die Pforte sind sichtbar:

- Name
- Vorname
- Geburtsname
- Geburtsdatum
- Bettnummer, Fallnummer, PID-Nummer
- Fachabteilung

- Station
- Raum
- Telefon
- Aufnahmedatum
- Entlassungsdatum

Damit ist der Datensatz im Wesentlichen auf die zur Wahrnehmung des Pfortendienstes erforderlichen Daten beschränkt. Die Notwendigkeit des Aufnahme- und Entlassungsdatums für den Pfortendienst wird noch diskutiert.

9.6.2.2
Medizinischer Bereich

9.6.2.2.1
Pflegebereich

Nach erfolgter Aufnahme des Patienten in einer medizinischen Fachabteilung und seiner Zuweisung zu einer Station steht der Name des Patienten im System in der für die Pflegekräfte zugänglichen Bettenübersicht der jeweiligen Station auf der Warteliste. Es ist Aufgabe der Pflegekräfte, dem Patienten im System ein Bett innerhalb der Station zuzuweisen. Die Pflegedirektion hat Zugriff auf die Bettenübersichten aller Fachabteilungen. Die Pflegekräfte (ca. 1.600) haben Zugriff jeweils nur auf die Bettenübersichten ihrer eigenen Stationen.

Insgesamt können die Pflegekräfte auf die die Fachabteilungen übergreifenden Daten der sog. Pfortenauskunft zugreifen (z. B. für den Fall, dass sich ein verwirrter Patient auf einer falschen Station befindet). Weitere Zugriffe sind auf die Bettenübersicht und die medizinische Dokumentation der eigenen Station eröffnet. Wenn ein Patient verlegt werden soll, veranlasst die zuständige Pflegekraft, dass der Patient aus der Bettenübersicht der eigenen Station gelöscht und in die Warteliste der weiterbehandelnden Station aufgenommen wird. Ein Zugriff auf die Bettenübersicht der weiterbehandelnden Station ist der Pflegekraft im Rahmen der Verlegung nicht möglich.

9.6.2.2.2
Ärztlicher Bereich

Die behandelnden Ärzte einer Fachabteilung haben Zugriff auf die folgenden Daten:

- Pfortenauskunft
- Verwaltungsdaten ihrer eigenen Fachabteilung
- Sog. zentrale Krankengeschichte des in der eigenen Fachabteilung in Behandlung befindlichen Patienten, d. h. die Daten von Behandlungen aller Fachabteilungen dieses Patienten, die zu einem früheren Zeitpunkt stattgefunden haben und von der betreffenden Abteilung der (zentralen) Krankengeschichte hinzugefügt wurden. Es ist vorgesehen, dass ein Patient bei seiner Aufnahme gefragt wird, ob er einem Zugriff der behandelnden Fachabteilung auf die früheren Behandlungsdaten widersprechen möchte. Für diesen Fall soll die technische Möglichkeit einer Sperre der entsprechenden Falldaten im System eingerichtet werden.
- Probleme (Allergien etc.); sofern diese als notfallrelevant klassifiziert sind, können sie jedoch von allen Ärzten des Klinikums eingesehen werden.
- Diagnosen, Operationen etc. (im Wesentlichen Daten i.S.v. § 301 SGB V)
- Krankengeschichte der eigenen Abteilung.

Der Umfang der Möglichkeiten, die o. a. Daten im System zu lesen, ist für den Chefarzt, Oberarzt, Arzt und das Pflegepersonal der jeweiligen Fachabteilung identisch. Die Möglichkeiten des schreibenden bzw. ändernden Zugriffs auf die Daten sind differenziert.

Generell ist jedoch ein schreibender Zugriff nur auf Daten der eigenen Fachabteilung möglich. Wenn eine Vidierung − d. h. eine systemeigene Vorstufe der digitalen Signatur − der abteilungseigenen Daten erfolgt ist und in die sog. „Zentrale Krankengeschichte“ überstellt wurde, so sind für alle aufgrund des Behandlungszusammenhanges berechtigten Abteilungen nur noch lesende Zugriffe möglich.

9.6.2.2.3
Verfahren bei Leistungsanforderungen einer Funktionsabteilung, hier: Radiologie

Derzeit erfolgt die Anforderung einer Leistung noch in Papierform. Wenn eine solche Anforderung bei der Leitstelle der Radiologie eingeht, wird der Patient in der Leitstelle im System identifiziert und die Anforderung wird dann aufgenommen. Die Mitarbeiterinnen und Mitarbeiter der Leitstelle haben Zugriff auf die folgenden Daten:

- Pfortenauskunft
- Aufnahmedaten des Patienten
- Fachabteilungskrankengeschichte der Radiologie.

Darüber hinaus ist es derzeit für die Leitstelle der Radiologie technisch möglich, alle ihr namentlich bekannten Patienten des Universitätsklinikums aufzurufen und die medizinische Dokumentation dieser Patienten einzusehen, soweit sie in der sog. „zentralen Krankenakte“ enthalten ist. Diese Einsichtsrechte werden vom Klinikum im Einzelfall für erforderlich gehalten, z. B. wenn auf der Leistungsanforderung die Diagnose fehlt oder Angaben in der Problemliste für die Radiologie wichtig sind. Solche Zugriffe werden aber dem Klinikum zufolge aus zeitlichen Gründen selten genutzt und vom System

protokolliert. Die Einsichtsrechte gehen über den für die Aufgabenerfüllung dieser Mitarbeiterinnen und Mitarbeiter erforderlichen Umfang hinaus. Auch die vom Klinikum genannten Zwecke können diese umfangreichen Zugriffsmöglichkeiten nicht dauerhaft rechtfertigen. Ich habe daher eine Abänderung des Verfahrens gefordert.

Es besteht jetzt Konsens zwischen dem Klinikum und mir, dass diese umfassenden Zugriffsmöglichkeiten beschränkt werden müssen. Das Klinikum hat zugesagt, dass sie entfallen, sobald die nächste Ausbauphase in Produktion geht.

Im Bereich der Radiologie können die Mitarbeiterinnen und Mitarbeiter der Leitstelle, die MTA und die Ärzte auf denselben Umfang von Daten lesend zugreifen.

Der Patient, für den eine Leistungsanforderung in der Radiologie vorliegt, wird von einer MTA in die Terminliste der Radiologie aufgenommen. Ein Arzt der Radiologie führt die Befundung und die Vidierung des Befundes durch. Das Ergebnis der Untersuchung wird elektronisch und in Papierform an die anfordernde Fachabteilung übersandt.

Ein entsprechendes Verfahren wie bei der Radiologie findet auch bei anderen Funktionsabteilungen (Endoskopie, Nuklearmedizin, Pathologie) statt.

9.6.2.2.4
Konsiliarische Beratung

Soweit eine Fachabteilung einen Arzt einer anderen Fachabteilung um konsiliarische Beratung bittet, kann der konsiliarisch tätige Arzt nicht von selbst einen Zugriff auf die Daten des betreffenden Patienten initiieren. Die behandelnde Fachabteilung muss dem konsiliarisch zugezogenen Arzt die Krankenakte zur Verfügung stellen oder den Zugriff auf die Daten des Patienten eröffnen. Derzeit besteht noch die technische Schwierigkeit, dass ein Zugriff auf die Daten der Patienten einer anderen Fachabteilung erfolgt, ohne dass im System nach Einzelpersonen differenziert wird. Dies habe ich als problematisch angesehen. Als Lösung ist vorgesehen, eine klinikumsweite Fall-Liste im Rahmen einer speziellen Rolle zugänglich zu machen. Eine ansonsten zur Patientenaufnahme berechtigte Verwaltungskraft an der Leitstelle kann dann aufgrund einer schriftlichen Anforderung einer anderen behandelnden Abteilung den betreffenden Patienten aus dieser klinikumsweiten Fall-Liste in die eigene Konsil-Liste oder auch Ambulanz-Liste umbuchen. Damit erhält der Arzt, nicht aber die Verwaltungskraft für die konsiliarische Beratung Zugriff auf die Daten des entsprechenden Patienten. Die Umbuchung soll systemseitig protokolliert werden und die Einträge in den Konsil-Listen etc. sollen Löschfristen unterliegen, nach deren Ablauf die Zugriffsmöglichkeit auch für den Arzt entfällt.

9.6.2.2.5
Verfahren bei Wechsel der Fachabteilung

Die Verlegung stationärer Patienten in eine andere Fachabteilung erfolgt über den Pflegearbeitsplatz (siehe Ziff. 9.6.1.2.1). Damit gehen auch die Zugriffsrechte an die neue behandelnde Abteilung über.

10. Telekommunikation

Telekommunikations-Datenschutzverordnung

Die neue Telekommunikations-Datenschutzverordnung lässt einige Forderungen der Datenschutzbeauftragten des Bundes und der Länder unberücksichtigt.

Der Bundesrat hat am 29. September 2000 der von der Bundesregierung vorgelegten Telekommunikations-Datenschutzverordnung (TDSV) − BR-Drucks. 300/00 − mit Änderungen zugestimmt (Stenografischer Bericht 754. Sitzung, S. 377). Die Verordnung, über die wegen der vom Bundesrat verlangten Änderungen die Bundesregierung noch einmal beschließen muss, wird an die Stelle der bisherigen Telekommunikationsdienstunternehmen-Datenschutzverordnung vom 12. Juli 1996 treten (BGBl. I S. 982). Sie regelt den Schutz personenbezogener Daten der an der Telekommunikation Beteiligten, soweit Anbieter von Telekommunikationsdiensten die Daten verarbeiten. Die vom Bundesrat geforderten Änderungen beruhen im Wesentlichen auf Vorschlägen der Datenschutzbeauftragten des Bundes und der Länder. Die Datenschutzbeauftragten waren bereits in die Ausarbeitung der Verordnung einbezogen. Auch ich habe mehrmals gegenüber dem Hessischen Ministerium für Wirtschaft, Verkehr und Landesentwicklung zu Entwürfen Stellung genommen. Trotz Unterstützung durch das Ministerium konnten einige meiner Forderungen jedoch nicht durchgesetzt werden. Zu den wichtigsten zählen:

10.1
Recht des Kunden zur Bestimmung des Umfangs der Datenspeicherung

Diensteanbieter dürfen Verbindungsdaten gemäß § 7 Abs. 3 TDSV (neu) unter Kürzung der Zielnummer um die letzten drei Ziffern bis zu sechs Monate nach Versendung der Rechnung speichern. Nach § 7 Abs. 4 TDSV (neu) können die Kunden vom rechnungsstellenden Diensteanbieter verlangen, dass die Verbindungsdaten vollständig gespeichert oder mit Versendung der Rechnung vollständig gelöscht werden. Dieses Wahlrecht der Kunden bestand bislang gegenüber allen Diensteanbietern. Die Beschränkung auf den rechnungsstellenden Diensteanbieter hat zur Folge, dass die Verbindungsdaten bei allen übrigen Diensteanbietern, die beispielsweise Daten von Call-by-Call-Verbindungen speichern, unabhängig von der ausgeübten Wahl des Kunden bis sechs Monate nach Versendung der Rechnung gespeichert bleiben dürfen.

Verbindungsdaten unterliegen nach der Rechtsprechung des Bundesverfassungsgerichts dem grundrechtlich geschützten Telekommunikationsgeheimnis (Art. 10 GG) und gemäß § 85 Abs. 1 Telekommunikationsgesetz dem einfachgesetzlichen Fernmeldegeheimnis und sind daher genauso schützenswert wie der Inhalt der Kommunikation. Damit ist unvereinbar,

dass die an der Bereitstellung der Kommunikationsverbindung beteiligten Diensteanbieter, die keine Rechnung stellen, die Daten weiterhin speichern dürfen. Die Regelung widerspricht dem in § 3 Abs. 4 TDSV (neu) aufgenommenen Gebot der Datensparsamkeit bei der Auswahl und Gestaltung von Datenverarbeitungsverfahren. Wie bisher hätte deshalb die neue TDSV alle Anbieter von Telekommunikationsdiensten verpflichten müssen, die Wahl der Kunden zu respektieren. Die rechnungsstellenden Anbieter hätten zudem verpflichtet werden müssen, die anderen Anbieter über den Zeitpunkt des Rechnungsversandes und die damit verbundene Löschungspflicht zu informieren. Ungeachtet der unvollständigen Fassung des § 7 Abs. 4 TDSV können Benutzer aufgrund des Art. 10 GG und § 85 TKG eine vollständige Löschung beantragen und notfalls einklagen.

10.2
Einzelverbindungsnachweis

Art. 7 Abs. 2 EG-Telekommunikationsrichtlinie (ABl. L 24 vom 30.1.1998) verpflichtet die Mitgliedstaaten, das Recht der Teilnehmer, Einzelgebührennachweise zu erhalten, und das Recht anrufender Benutzer und angerufener Teilnehmer auf Vertraulichkeit miteinander in Einklang zu bringen.

Art. 7 Abs. 2 EG-Telekommunikationsrichtlinie

Die Mitgliedstaaten wenden innerstaatliche Vorschriften an, um das Recht der Teilnehmer, Einzelgebührennachweise zu erhalten, und das Recht anrufender Benutzer und angerufener Teilnehmer auf Vertraulichkeit miteinander in Einklang zu bringen, …

Dazu finden sich in der TDSV (neu) keine Regelungen. Es hängt nach wie vor allein von der Wahl des anrufenden Anschlussinhabers ab, ob er eine aufgeschlüsselte Rechnung erhält, in der sämtliche Einzelverbindungen mit vollständiger Zielnummer der Angerufenen aufgelistet sind. Über die Einführung eines Modells, bei dem der Angerufene über die Preisgabe seiner Rufnummer entscheidet, sollte ernsthaft nachgedacht werden. Um die Streitfrage nicht auf dem Rücken der Anbieter auszutragen, könnte für diesen Fall vorgesehen werden, dass der Angerufene anstelle des Anrufenden die Kosten übernimmt. Ein solches Modell würde außerdem die komplizierte Regelung in § 8 Abs. 2 TDSV (neu), mit der sichergestellt werden soll, dass Beratungseinrichtungen nicht in Einzelverbindungsnachweisen erwähnt werden, erübrigen und damit zu einer nicht unerheblichen Verwaltungsvereinfachung beitragen.

10.3
Missbrauchsbekämpfung

Eine Verschlechterung für den Datenschutz der Kunden bringt die Regelung zur Missbrauchsbekämpfung in § 9 TDSV (neu). Der Diensteanbieter darf den Gesamtbestand aller Verbindungsdaten, die nicht älter als sechs Monate sind, rastern, um Verbindungen aufzuspüren, bei denen der Verdacht einer rechtswidrigen Nutzung von TK-Netzen und -diensten besteht. Bislang war der Zeitraum auf einen Monat begrenzt. Durch die Neuregelung wird vor allem das Wahlrecht des Kunden nach § 7 Abs. 4 TDSV unterlaufen. Die Begründung zu § 9 TDSV (neu) stellt zwar klar, dass die Diensteanbieter nicht verpflichtet sind, die Daten sechs Monate zu speichern. Es besteht jedoch die Gefahr, dass Diensteanbieter die Befugnis voll ausnutzen.

Diese Gefahr hat offensichtlich auch der Wirtschaftsausschuss des Bundesrates gesehen und deshalb empfohlen, den Zeitraum für eine zulässige Rasterung des Gesamtbestandes der Verbindungsdaten auf vier Monate festzusetzen (BR-Drucks. 300/2/00, Nr. 7). Dem hat jedoch der Ausschuss für Innere Angelegenheiten widersprochen, da eine kürzere Frist als sechs Monate die Arbeit der Strafverfolgungsbehörden unangemessen beeinträchtige (BR-Drucks. a.a.O.). Der Bundesrat ist dem Argument des Innenausschusses gefolgt.

Positiv zu vermerken ist der in § 9 Abs. 2 TDSV (neu) enthaltene Hinweis auf die Möglichkeit einer pseudonymisierten Auswertung des Gesamtbestandes der Verbindungsdaten. Dies entspricht einer alten Forderung der Datenschutzbeauftragten, denn mit einer solchen Recherchemethode werden die Eingriffe in das Telekommunikationsgeheimnis und das Recht auf informationelle Selbstbestimmung der Kunden erheblich verringert.

11. Entwicklungen im Bereich der Technik

11.1
Schwachstellensuche bei Firewalls und in Rechnernetzen

Firewalls sind unverzichtbar, um Netzwerke gegen Angriffe von außen zu schützen. Eine Kontrolle, ob sie ihre Funktion erfüllen, gehört zu den Bestandteilen eines Sicherheitskonzepts. Als Hilfsmittel bei derartigen Kontrollen bieten sich Port-Scanner an, die auch in Rechnernetzen die Suche nach Schwachstellen unterstützen können.

11.1.1
Ausgangslage

Das Hessische Landesverwaltungsnetz (HCN 2000) ist durch Firewalls gegen das Internet abgeschottet. Im letzten Jahr hat die Hessische Zentrale für Datenverarbeitung (HZD) als Betreiberin eine Schwachstellenanalyse der Firewalls und der vorgelagerten Webserver vornehmen lassen. Die Analyse wurde durch einen Port-Scanner unterstützt. Diese Schwachstellenanalyse habe ich beratend begleitet.

Ein Port-Scanner ist ein Programm, das testet, wie ein Rechner auf Verbindungswünsche reagiert. Dabei werden die Ports (Nummern, mit denen im Internetprotokoll TCP/IP verschiedene Dienste gekennzeichnet werden) abgefragt. Die Reaktionen auf diese Verbindungswünsche können Informationen über die eingesetzte Software liefern. Im Prinzip greift der Port-Scanner die untersuchten Rechner wie ein Hacker an.

Einen großen Teil der Ergebnisse hätte man auch durch genaue Kontrolle der Dokumentation und der Konfiguration der Firewalls und der Server erhalten können. Dies ist aber je nach Komplexität des Netzes sehr zeitaufwändig und erfordert speziell ausgebildetes Personal. Im Übrigen sind mit dem Port-Scanner weitere Aspekte kontrolliert worden. Der Port-Scanner hat zudem getestet, ob die Rechner entsprechend der Konfiguration reagieren. Das eingesetzte Programm bot auch noch weitere Funktionen. So wurden beispielsweise automatisch einfache Passwörter getestet. Im Prinzip ist das Programm nicht nur geeignet, Firewalls zu scannen, sondern auch, andere Rechner auf Angriffspunkte zu testen. Das ist umso wichtiger, als derartige Produkte auch im Internet und damit weltweit kostenlos abrufbar sind und somit auch potentiellen Hackern zur Verfügung stehen.

11.1.2
Ergebnisse des Tests

Die Schwachstellenanalyse mit Hilfe des Port-Scanners führte zu Ergebnissen, die aus Sicherheitsgründen an dieser Stelle nicht im Detail wiedergegeben werden können. Einige allgemeine Ergebnisse und Schlussfolgerungen können jedoch hier aufgezeigt werden.

11.1.2.1
Ergebnisse der Schwachstellenanalyse

Die Analyse zeigte, dass der Scanner zum Zeitpunkt der Prüfung bei den Firewalls keine Schwachstellen aufdecken konnte. Die Informationsserver besaßen teilweise unerkannte Schwachstellen, die ein hohes Risiko bedeuten konnten. Sie sind mittlerweile beseitigt. Hierfür war der Scanner sehr hilfreich, weil er eine ausführliche Schwachstellenbeschreibung und Anleitung zur Fehlerbehebung erstellte. Die Beschreibungen waren aber in der Regel nur für technisch versiertes Personal verständlich. Bei den Tests haben die NETBIOS-Ports (137, 138, 139; spezifisch für Windows), wenn sie nicht abgeblockt waren, zu den größten Lücken geführt. Darüber konnten zum Beispiel aufschlussreiche Informationen zu Benutzern und Dateisystemen gewonnen werden.

11.1.2.2
Allgemeine Anforderungen an den Einsatz von Port-Scannern

Aus dem von der HZD durchgeführten Test ergeben sich für mich die nachfolgend aufgeführten Anforderungen an den Einsatz von Port-Scannern.

- Bevor ein Port-Scanner eingesetzt wird, muss klar sein, von wem er zu welchem Zweck genutzt werden soll. Dabei ist zu prüfen, ob der Einsatz rechtlich zulässig ist. So ist es einer datenverarbeitenden Stelle natürlich möglich, das eigene Netz zu untersuchen. Ein Zugriff auf fremde Rechner, z. B. wenn eine Firewall durch einen Dienstleister betrieben wird, kann aber nur erfolgen, wenn es der Vertrag zulässt.
- Port-Scanner liefern Hinweise bei einer Schwachstellenanalyse. Diese kann durch die Systemverantwortlichen, den behördlichen Datenschutzbeauftragten oder durch externe Stellen vorgenommen werden. Bei Dienststellen des Landes Hessen oder hessischen Kommunen könnte die Schwachstellenanalyse im Rahmen einer Prüfung durch den Hessischen Datenschutzbeauftragten erfolgen.
- Die Ergebnisse müssen durch qualifiziertes Personal interpretiert werden.
- Der Scanner liefert eine Momentaufnahme. Er sollte daher wiederkehrend eingesetzt werden, um die korrekte Umsetzung der Sicherheitsrichtlinien und die Suche nach neuen oder neu erkennbaren Schwachstellen vorzunehmen.
- Es sollte immer die aktuelle Version eingesetzt werden.
- Die Ergebnisse müssen mit den für die geprüften Rechner Verantwortlichen diskutiert werden, damit relevante Teilergebnisse bestimmt werden und das Vorgehen zur Beseitigung der Schwachstellen festgelegt wird.
- Ein Suchlauf stellt sich für das gescannte System wie ein Angriff durch einen Hacker dar. Vor einem Suchlauf sollte daher in der Regel die Leitung der Dienststelle informiert sein.
- Wenn es nicht darum geht festzustellen, ob das Personal Angriffe erkennt und wie es darauf reagiert, sollten die DV-Verantwortlichen ebenfalls informiert werden.

Neben Scannern von kommerziellen Anbietern gibt es auch Programme im Internet, die genutzt werden können. In Büchern werden als bekannteste Produkte SATAN, Nessus, Cerberus oder SAINT genannt. Ob und welche den Ansprüchen am ehesten genügen, muss jede Stelle selbst entscheiden. Sie kann sich dabei von den Informatikern meiner Dienststelle beraten lassen.

11.2
Sicherheitslücken bei IT-Produkten

Um eine dem Datenschutzgesetz genügende Sicherheit zu erreichen, müssen relevante Sicherheitslücken in IT-Systemen geschlossen werden. Die Verantwortlichen werden immer wieder mit neuen Bedrohungen der Datensicherheit konfrontiert. Das Internet bietet vielfältige Informationen zu diesen Fragestellungen.

Auch im letzten Jahr ist es immer wieder vorgekommen, dass Anwender aus der Presse über Angriffe auf Rechnersysteme erfahren mussten. Diese Berichte haben auch zu zahlreichen Anfragen bei meiner Dienststelle geführt. Ein Beispiel, das

für viel Aufsehen gesorgt hat, weil man es nicht erwartet hatte, war das erfolgreiche Eindringen von Hackern in das Netzwerk der Firma Microsoft. Auch in anderen Bereichen besteht die Gefahr der Ausforschung von Verwaltungs- oder Betriebsgeheimnissen. Hinzu traten Hinweise auf Sicherheitsprobleme, die für die breite Öffentlichkeit nicht augenfällig wurden, weil sie nur der Fachöffentlichkeit und im Internet offengelegt wurden. Beispielsweise haben sich in der letzten Zeit Hinweise gehäuft, dass aktive Elemente auf Internetseiten (vgl. 27. Tätigkeitsbericht, Anhang 2: Orientierungshilfe Internet) zu einem erheblichen Sicherheitsrisiko werden können. So wurde mit dem Programm „Brown-Orifice“ gezeigt, wie man einen Rechner ausspionieren kann. Voraussetzung ist, dass Java-Script zugelassen und eine bestimmte Browser-Software eingesetzt wird. Diese und weitere Sicherheitslücken haben dazu geführt, dass das BSI (Bundesamt für Sicherheit in der Informationstechnik) wie auch das DFN-CERT (Deutsches Forschungsnetz, Computer Emergence Response Team; Anlaufstelle bei Sicherheitsproblemen) raten, aktive Inhalte in den Browsern zu deaktivieren.

Informationen zu Fragen der IT-Sicherheit, aber auch Hilfestellungen, wie Sicherheitslücken beseitigt werden können, sind im Internet verfügbar. Jeder Bürger, jedes Unternehmen und jede Verwaltung muss sich die Frage stellen, ob die genutzten IT-Systeme ausreichend gegen Missbrauch gesichert sind.

Es ist nicht möglich, eine 100 %-Sicherheit zu erreichen. Über die für Behörden vorgeschlagene Vorgehensweise hat mein Amtsvorgänger bereits im 23. Tätigkeitsbericht, Ziff. 25.1 berichtet. Damit die Datensicherheit eines IT-Systems auf einem adäquaten Niveau ist, reicht es nicht aus, ein Konzept zu erstellen und den dort vorgesehenen Stand einzurichten. IT-Systeme wie auch die Angriffe auf sie entwickeln sich. Es wird neue Software eingespielt, bestehende Anwendungen werden geändert, es werden neue Kommunikationsmöglichkeiten eröffnet und es werden weitere Rechner in das System genommen. Jede Änderung kann Sicherheitslücken mit sich bringen. Auch zu unveränderten Systemen können weitere Sicherheitslücken bekannt werden. Im Ergebnis kann eine ausreichende IT-Sicherheit nur in einem kontinuierlichen Anpassungsprozess erreicht werden, bei dem eine Reihe von Voraussetzungen zu beachten sind:

- Es muss festgelegt sein, wessen Aufgabe es ist, das Thema der IT-Sicherheit zu bearbeiten.
- Die verantwortliche Person muss über ein Zeitbudget verfügen, sich aus dem verfügbaren System zu informieren.
- Es muss geklärt sein, wie über Vorschläge zur Verbesserung der IT-Sicherheit entschieden wird.

Im Internet gibt es eine Reihe von Anbietern, die kostenlos zu diesem Thema informieren. Die folgende Übersicht soll einen ersten Einblick geben. Die Anbieter vermitteln weitere Informationen. Bei Fragen zu einem bestimmten Produkt sollte zuerst im Informationsangebot des Anbieters gesucht werden.

- Herstellerunabhängige Informationen über Schwachstellen bieten das DFN-CERT (http://www.cert.dfn.de oder http://www.cert.org), das BSI (http://www.bsi.bund.de), die Initiative der Bundesregierung „Sicherheit im Internet“ (http://www.sicherheit-im-internet.de) und verschiedene Zeitschriften. Praktisch alle Zeitschriften bringen mehrmals jährlich Berichte mit dem Schwerpunkt IT-Sicherheit. Je nach Wissenstand des Lesers kann der eine oder der andere Bericht das Thema besser darstellen. U. a. finden sich in den Internetangeboten der Zeitschriften c’t, chip, pc-professional oder Computerbild Hinweise auf Sicherheitslücken und deren Lösung.
- Anwender sollten sich in Mailinglisten aufnehmen lassen, die aktuell über Sicherheitslücken informieren.

Die Informationen müssen darauf geprüft werden, ob und inwieweit sie für die technische Ausstattung der Dienststelle relevant sind. Sofern es Lösungen für die beschriebene Schwachstelle gibt, muss geklärt werden, ob sie eingesetzt werden sollen. In vielen Fällen wird es zu aufgetretenen Sicherheitslücken keine oder nur sehr aufwändige Lösungsmöglichkeiten geben. Hier müssen dann organisatorische Anpassungen oder verstärkte Kontrollen erfolgen, um das Risiko begrenzen.

11.3
Mustervereinbarung Hardwarewartung

Für eine Auftragsdatenverarbeitung nach § 4 HDSG hatte ich im letzten Tätigkeitsbericht einen detaillierten Mustervertrag vorgestellt. Eine Vereinbarung zur Hardwarewartung kann sich auf wenige Punkte beschränken. Hierzu habe ich ein Muster vorbereitet, das unter http.//www.datenschutz.hessen.de abgerufen werden kann.

In den letzten Jahren sind immer wieder Anfragen eingegangenen, in denen nach Handreichungen für datenschutzrechtliche Standardlösungen gesucht wurden. Neben den „Orientierungshilfen“, die von den Datenschutzbeauftragten des Bundes und der Länder erarbeitet werden, und „Arbeitshilfen“ hatte ich einen Mustervertrag zur Auftragsdatenverarbeitung nach § 4 HDSG vorgestellt (28. Tätigkeitsbericht, Ziff. 25.2).

Nachdem mehrfach datenverarbeitende Stellen um Hinweise über Verträge für den Fall einer Geräte- bzw. Hardwarewartung gebeten hatten, habe ich eine Mustervereinbarung für Wartungsarbeiten erstellt. Die Mustervereinbarung kann auch als Zusatzvereinbarung zu einem langfristigen Wartungsvertrag oder Einzelauftrag geschlossen werden. Soweit die Wartung im Rahmen eines BVB-Wartungs-, BVB-Kauf- oder BVB-Mietvertrages (StAnz. 1994, S. 2050 ff.) erbracht wird, wird empfohlen, diese Vereinbarung als Zusatz zu § 14 BVB-Wartung, § 22 BVB-Kauf bzw. § 23 BVB-Miete abzuschließen. Für die Software-Pflege, d.h. für die programm- und datenbestandsbezogene Wartung und für Fernwartung vgl. die Mustervereinbarung Fernwartung (Ziff. 22.1).

Mustervereinbarung zur Regelung datenschutzrelevanter Sachverhalte bei Reparaturen, technischen Wartungsarbeiten und Austausch von Komponenten an PC und Servern ohne Software-Pflege

§ 1
Geheimhaltung von Daten

1. Der Auftragnehmer verpflichtet sich, bei technischen Reparaturen, technischen Wartungsarbeiten oder Austausch von Komponenten auf gespeicherte Daten nur insoweit zuzugreifen, wie es die nachfolgenden Bestimmungen gestatten.
2. Sollten dem Auftragnehmer Inhalte von Datenbeständen bekannt werden, verpflichtet er sich, diese geheim zu halten.

3. Der Auftragnehmer verpflichtet sich, das bei Reparaturen, technischen Wartungsarbeiten oder beim Austausch von Komponenten eingesetzte Personal in der gleichen Weise zu verpflichten und die so begründeten Geheimhaltungspflichten zu überwachen.
4. Die Vergabe von Unteraufträgen ist nur mit Zustimmung des Auftraggebers zulässig. Bei Unteraufträgen, die der Auftraggeber genehmigt hat, hat der Auftragnehmer den Unterauftragnehmer in gleicher Weise zu verpflichten. Für den Unterauftragnehmer gilt Ziff. 1 entsprechend.
5. Der Auftragnehmer sichert dem Auftraggeber zu, dass er nach Abschluss der Arbeiten alle Daten des Auftraggebers, die er während der Arbeiten kopiert oder ausgedruckt hat, unverzüglich löschen oder vernichten wird. Datenträger, die der Auftraggeber für die Arbeiten zur Verfügung gestellt hat, sind dem Auftraggeber unmittelbar nach Abschluss der Arbeiten wieder auszuhändigen.

§ 2
Sparsame Datenverwendung

1. Ist der Zugriff auf Daten wegen der Art der vereinbarten Reparaturen, der technischen Wartungsarbeiten oder wegen des Austauschs von Komponenten unvermeidbar, so verpflichtet sich der Auftragnehmer, den Datenzugriff auf das unverzichtbare Mindestmaß zu beschränken.
2. Setzen die Arbeiten einen Zugriff auf personenbezogene Daten zwingend voraus, informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber entscheidet, wie in derartigen Fällen vorzugehen ist.
3. Gestattet der Auftraggeber den Zugriff auf ausgewählte personenbezogene Datenbestände, so dürfen die vereinbarten Arbeiten ausschließlich mit diesen Datenbeständen ausgeführt werden.
4. Soweit wegen der Art der vereinbarten Reparaturen, technischen Wartungsarbeiten oder beim Austausch von Komponenten ein Zugriff auf personenbezogene Daten erfolgt, dürfen keine Veränderungen vorgenommen werden. Versehentlich vorgenommene Veränderungen sind dem Auftraggeber bekannt zu geben.
5. Änderungen an Systemdateien, die im Zuge der Arbeiten erforderlich geworden sind, müssen vom Auftragnehmer dokumentiert werden. Auf Verlangen des Auftraggebers sind solche Veränderungen nach Abschluss der Arbeiten rückgängig zu machen.

§ 3
Austausch von Komponenten

1. Beim Austausch von Komponenten, mit denen Daten dauerhaft gespeichert werden können, insbesondere Festplattenlaufwerken und ähnlichen Speichermedien, stellt der Auftragnehmer sicher, dass entnommene Komponenten nach Abschluss der Arbeiten in einer Weise zerstört werden, die den Zugriff oder eine Wiederherstellung von Daten technisch ausschließt.
2. Wünscht der Auftraggeber die Aushändigung von ausgetauschten Komponenten, sind diese bis zur Übergabe unter Verschluss zu halten.

§ 4
Übertragung von Speicherinhalten

1. Umfasst der Auftrag ein Kopieren gespeicherter Daten, die sich auf ersetzten Komponenten oder beschädigten Speichermedien befunden haben, so ist ein Kopierverfahren zu verwenden, das die Anzeige des Inhalts von Datenbeständen so weit wie möglich vermeidet. § 1 Ziff. 2 und § 2 Ziff. 4 gelten entsprechend.
2. Nach der Übertragung sind die entnommenen Komponenten oder die überlassenen Speichermedien vollständig zu löschen oder zu vernichten. Wenn der Auftraggeber das wünscht, sind sie ihm unverändert und ungelöscht auszuhändigen.

§ 5
Schadensersatz

1. Wird der Inhalt von Datenbeständen entgegen der Geheimhaltungspflichten Dritten bekannt, hat der Auftragnehmer den dadurch entstehenden Schaden zu ersetzen. Zum ersatzpflichtigen Schaden gehören auch Zahlungen, die der Auftraggeber Dritten zu leisten hat.
2. Den Nachweis für fehlendes Verschulden hat der Auftragnehmer zu erbringen.
3. Für ein Verschulden ihres Personals haften Auftragnehmer und Unterauftragnehmer in gleicher Weise wie für eigenes Verschulden.

Datum	Unterschrift Auftraggeber	Unterschrift Wartungsfirma

11.4
Anonymes Surfen im Internet

Wer im Internet surft oder E-Mails verschickt, hinterlässt Spuren, die auf seine Person zurückgeführt werden können. Es gibt Dienstleistungen im Internet, die bis zu einem gewissen Grad einen Schutz dagegen bieten sollen.

Grundsätzlich kann jede Internet-Nutzung nachvollzogen werden. Es kann festgestellt werden, bei welcher Stelle (Internet-Nutzer, Internet-Provider, Betreiber eines Servers) welche Daten abgerufen worden sind. Im Zentrum der aktuellen Dis-

kussionen stehen die Risiken der Datenspeicherung bei den Betreibern von Servern. Bei Beratungen und Schulungen wird mir immer wieder die Frage gestellt, was es mit dem „gläsernen Surfer“ auf sich hat und wie man sich gegen solche Ausforschungen schützen kann. Die möglichen Lösungen hängen von der eingesetzten Technik ab, so dass im Detail Unterschiede bei den Abhilfeformen bestehen.

11.4.1
Problemaufriss

Wer im Internet surft, greift auf Webserver zu. Die Server erhalten bei einem Zugriff immer die IP-Adresse des anfragenden Rechners, damit sie überhaupt die abgerufenen Daten an den richtigen Rechner zurückschicken können. Viele Webanbieter wollen das Benutzerverhalten detailliert analysieren. Zu diesem Zweck werden Informationen über die abgerufenen Seiten des Anbieters mit den IP-Adressen der jeweiligen Nutzer verknüpft. Die Server können auch ohne Zutun des Surfers weitere Informationen abfragen, indem sie diese von dem Browser durch verdeckte Befehle gezielt anfordern. Ferner kann ein Server auch sog. Cookies auf dem anfragenden Rechner hinterlegen; sie übermitteln, wann was auf dem anfragenden Rechner oder auf dem Server geschah. Andere technische Mittel sind sog. Web-Bugs. Sie ergänzen die technische Palette, um das Verhalten der Surfer nachvollziehbar zu machen. Alle Techniken werden in besonderem Maße durch die Werbewirtschaft eingesetzt, die sich dadurch eine zielgenaue Werbung erhofft. Im Ergebnis wird dadurch aber das Verhalten der Surfer, meist ohne ihr Wissen, ausgeforscht.

Cookies (engl. cookie = Keks) sind kleine Dateien, die zusammen mit den eigentlich angeforderten Daten aus dem Internet verschleiert an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers auf dem Computer, den er verwendet) auf das Internet-Angebot erkennbar.

Web-Bugs sind winzige, auf den Seiten des Anbieters versteckte Bilder mit hinterlegten Programmbefehlen, die vom Benutzer beim Abruf der Seiten nicht oder kaum wahrgenommen werden. Wenn sie mit einem Browser angesehen werden, könnten sie die IP-Adresse, die www-Adresse der besuchten Webseite, den Zeitpunkt des Ansehens und Informationen eines zuvor gesetzten Cookies an die www-Adresse eines vorgegebenen Servers senden. Sie können auch in E-Mails untergebracht werden.

Informationen, die während des Surfens über den Browser in Erfahrung gebracht werden können, sind z. B.:

- das Betriebssystem des Rechners;
- der benutzte Browser;
- ob aktive Elemente erlaubt sind;
  Die ersten drei Informationen geben potentiellen Hackern Anhaltspunkte für Schwachstellen, die bei einem Angriff genutzt werden könnten.
- die E-Mail-Adresse, soweit sie im Browser gespeichert ist;
  Durch die E-Mail-Adresse ist es natürlich besonders einfach, auf die Person zu schließen.
- die zuletzt aufgerufenen Webseiten;
  Aus den zuletzt aufgerufenen Webseiten lassen sich Schlüsse über Interessen des Surfers ziehen. Wenn es dann noch gelingt, diese Informationen nicht nur für die laufende Sitzung, sondern auch für zurückliegende Sitzungen zu erhalten, ergibt sich ein aussagekräftiges Nutzerprofil.
- die IP-Adresse;
  Wenn die IP-Adresse fest vergeben ist oder sich nicht ändert (z. B. wenn man bei Nutzung einer Flatrate den Rechner am Internet nicht abmeldet), steht damit das Herkunftsland fest, mitunter auch die Institution, der der Anfragende angehört. Die IP-Adresse ist das gemeinsame Merkmal, über das die Daten zusammengeführt werden können. So speichern z. B. über 90% der Top-100-Anbieter im Internet die Daten ihrer Nutzer. Eine Auswertung, wer sich für welche Angebote interessiert, kann dann mit der IP-Adresse geschehen. Auch wenn die IP-Adresse von dem Internet-Provider bei jedem neuen Zugang zum Internet aus einem Pool freier Adressen zufällig ausgewählt wird, ist damit nicht automatisch die Anonymität gegeben.

  Durch die in die politische Diskussion gebrachte Forderung der Innenminister des Bundes und der Länder, Internet-Provider und Betreiber von Servern zur Protokollierung der Verbindungsdaten einschließlich der IP-Adressen und des Nutzungszeitraums sowie zu einer bestimmten Dauer der Aufbewahrung dieser Daten zu verpflichten, wäre es Strafverfolgungsbehörden in jedem Fall möglich, auf den Nutzer zu schließen (vgl. Entschließung „Für eine freie Telekommunikation in einer freien Gesellschaft“, Ziff. 21.1).

  Die Zuordnung einer IP-Adresse zu einer Person kann beim Internet-Provider unschwer erfolgen, da er zu Abrechnungszwecken weitere personenbezogene Daten des Benutzers hat. Darüber hinaus kann aber u.U. auch eine solche Zuordnung beim Betreiber eines Servers erfolgen, z. B. wenn sich die Person über eine Bestellung oder die Eingabe einer E-Mail-Adresse zu erkennen gibt.

Neben den Informationen, die ein Server durch quasi lesenden Zugriff beschafft, gibt es auch die technische Möglichkeit, Daten auf dem Rechner des Surfers zu hinterlassen. Mit solchen Cookies oder mit Web-Bugs stehen Anbietern schon jetzt Mittel zur Verfügung, um Nutzerprofile zu erstellen. Durch das Auswerten von Cookies erkennen sie, welche Angebote jemand mit diesem Rechner bereits früher einmal abgerufen hat. Web-Bugs erlauben es dann − technisch − auch die Verbindung zu E-Mail-Adressen und zu Personen herzustellen.

Eine detaillierte Beschreibung, wie Nutzerprofile zu Werbezwecken erstellt werden, ist im Internetangebot des Heise Verlags (http://www.heise.de) und der onlinezeitung telepolis (http://www.heise.de/tp) zu finden.

11.4.2
Abhilfe

Um im Internet anonym zu surfen, müsste vor allem die IP-Adresse des eigenen Rechners verschleiert werden. Außerdem dürften möglichst keine Daten über die Nutzung, also keine Cookies oder Verlaufsdaten akzeptiert und gespeichert werden. Zumindest am Ende einer Sitzung sollten die auf dem PC des Nutzers entstandenen Daten, was er wo im Internet getan hat, gelöscht werden.

Anbieter im Internet − sog. Anonymizer, die allerdings oft kommerzielle Interessen haben −, kann man als Startpunkt für das Surfen wählen, sie verschleiern die eigene IP-Adresse. Alle Anfragen laufen dann im Internet unter der IP-Adresse des Anonymizers, der die Ergebnisse an den Ursprungsrechner weitergibt.

Der Internet-Nutzer kann im Browser durch bewusst gesetzte Parameter unterbinden, dass Cookies gespeichert werden oder dass vor einer Speicherung nachgefragt wird. In vielen Fällen muss der Nutzer jedoch ein Cookie akzeptieren, damit er überhaupt ein Internetangebot nutzen kann. Deshalb sollte er Cookies, Verlaufdaten u. ä. am Ende einer Sitzung löschen. Im Internet werden Programme angeboten, die dies automatisch auf dem PC des Nutzers erledigen sollen. Unter den Internetz-Adressen http://www.zdnet.de/download/magazine/pcpro/tt-wc.html (Name des Programms: „one-klick-privacy“) und unter http://www.setsystems.com (Name des Programms: „Complete Cleanup“) werden beispielsweise derartige Programme angeboten.

Auch über eine E-Mail gibt der Nutzer sich als Absender in aller Regel eindeutig zu erkennen. In den meisten Fällen soll der Empfänger auch wissen, von wem eine E-Mail stammt. Durch das gezielte Sammeln von E-Mails, was durch Geheimdienste oder im Zusammenhang mit Industriespionage zum Teil exzessiv geschieht, ergeben sich dann Profile von Nutzern. Zwar kann der Inhalt einer E-Mail verschlüsselt werden, damit ihn nur der Empfänger zur Kenntnis nehmen kann, aber von wem an wen eine E-Mail verschickt wurde, ist trotzdem bekannt. Die Verschleierung des Absenders, und über den Rückweg auch des Empfängers, bieten sog. Remailer an. Diese ersetzen die Absenderadresse durch eine eigene Adresse, deren Zuordnung zu dem richtigen Absender nur ihnen bekannt ist. Dadurch wird zwar die Anonymität gegenüber potentiellen Sammlern und evtl. dem Empfänger erreicht, es entsteht aber beim Remailer ein zentraler detaillierter Datenbestand, der eine Zuordnung zulässt. Es muss daher zumindest eine klare Zweckbindung der beim Remailer entstehenden Daten sichergestellt werden, damit hier keine neuen Gefährdungspotentiale entstehen. Außerdem wird ein Empfänger in vielen Fällen keine anonyme E-Mail akzeptieren.

In jedem Fall sollte der Nutzer sich hinreichend informieren, wie für die eigenen Rahmenbedingungen die Lösung aussehen kann. Dann erhöhen Anonymizer und Remailer den Datenschutz. Wichtig ist vor allem eine Kontrolle der eigenen Speicherungstechnik, um hinterlassene Cookies nicht dauerhaft im eigenen Rechner oder Netz vorzuhalten.

12. Ausländerrecht

12.1
Personenausschreibungen im Schengener Informationssystem

Aus unterschiedlichem Anlass habe ich die Rechtmäßigkeit von Datenspeicherungen im Schengener Informationssystem überprüft. Dabei wurde festgestellt, dass die Ausschreibung zum Wiedereinreiseverbot in das Schengengebiet durch hessische Ausländerbehörden oft unzulässig oder falsch ist.

Nach der Abschaffung der Personenkontrollen an den Binnengrenzen der sog. Schengen-Vertragsstaaten wurde als Kompensationsmaßnahme das Schengener Informationssystem (SIS) eingeführt. Es hat u. a. zum Ziel, die öffentliche Sicherheit und Ordnung und die Sicherheit des Staates in den Vertragsstaaten zu gewährleisten. So werden zum Beispiel Personen, die mit Auslieferungshaftbefehl einer Vertragspartei gesucht werden, mit dem Ziel der Festnahme zur Personenfahndung ausgeschrieben. Ein anderer Grund für die Personenfahndung ist eine Einreiseverweigerung. Drittausländer − also Ausländer, die keinem der Schengen-Vertragsstaaten angehören −, die wegen einer Straftat verurteilt worden sind oder gegen die der begründete Verdacht besteht, dass sie schwere Straftaten begangen haben, werden zur Einreiseverweigerung ausgeschrieben. Auch die Ausweisung oder Abschiebung eines Ausländers kann einer Ausschreibung zur Einreiseverweigerung zugrunde gelegt werden.

Art. 96 Abs. 3 SDÜ

Die Entscheidungen können ebenso darauf beruhen, dass der Drittausländer ausgewiesen, zurückgewiesen oder abgeschoben worden ist, wobei die Maßnahme nicht aufgeschoben oder aufgehoben worden sein darf, ein Verbot der Einreise oder des Aufenthalts enthalten oder davon begleitet sein muss und auf der Nichtbeachtung des nationalen Rechts über die Einreise oder den Aufenthalt von Ausländern beruhen muss.

Jeder hat das Recht, über die zu seiner Person im Schengener Informationssystem gespeicherten Daten Auskunft zu erhalten (Art. 109 Abs. 1 SDÜ). Weiterhin hat jeder das Recht auf Prüfung der zu seiner Person gespeicherten Daten (Art. 114 Abs. 2 SDÜ).

Art. 114 Abs. 2 SDÜ

Jeder hat das Recht, die Kontrollinstanzen zu ersuchen, die zu seiner Person im Schengener Informationssystem gespeicherten Daten sowie deren Nutzung zu überprüfen. Dieses Recht wird nach Maßgabe des nationalen Rechts der Vertragspartei, an die das Ersuchen gerichtet wird, ausgeübt. Wurden die Daten durch eine andere Vertragspartei eingegeben, so erfolgt die Kontrolle in enger Abstimmung mit der Kontrollinstanz dieser Vertragspartei.

Die Prüfung, wie Auskunfts- und Löschungsanträge der Betroffenen nach Art. 109 Abs. 1 und 114 Abs. 2 SDÜ bearbeitet werden, zeigte häufig, dass nach abgelehntem Asylantrag die Anschrift des Betroffenen nicht mehr stimmte und auch

nicht festgestellt werden konnte. Die Betroffenen waren entweder längst außer Landes oder „untergetaucht“. In diesen Fällen war die Ausschreibung im SIS nicht zulässig, denn sie waren nicht ausgewiesen, abgeschoben oder zurückgewiesen, wie es in Art. 96 Abs. 3 SDÜ vorgesehen ist.

Ich stieß weiterhin auf das Problem, dass die deutschen Ausländerbehörden eine Vorschrift im SDÜ zur Löschung teilweise falsch auslegen.

Art. 112 Abs. 1 SDÜ

Die zur Personenfahndung in dem Schengener Informationssystem aufgenommenen personenbezogenen Daten werden nicht länger als für den verfolgten Zweck erforderlich gespeichert. Spätestens drei Jahre nach Ihrer Einspeicherung ist die Erforderlichkeit der weiteren Speicherung von der ausschreibenden Vertragspartei zu prüfen. Für die Ausschreibung gemäß Artikel 99 beträgt diese Frist ein Jahr.

Das Bundeskriminalamt (BKA) wertet regelmäßig den nationalen Datenbestand des SIS aus und weist gegebenenfalls die Ausländerbehörden darauf hin, dass in Kürze seit der Einspeicherung drei Jahre verstrichen sein werden. Es gibt den Ausländerbehörden in jedem Einzelfall einen Vordruck zur Hand, mit dem sie die Löschung in dem Informationssystem veranlassen können. Das in Deutschland praktizierte Verfahren sieht vor, dass − falls die Löschung nicht veranlasst wird − die Aufbewahrungsdauer um weitere drei Jahre verlängert wird. Bleibt der Vordruck also unbearbeitet, wird die Aufbewahrungsdauer automatisch verlängert. Erst nach Ablauf von weiteren drei Jahren erfolgt die Löschung. Dieses Verfahren führt dazu, dass in zahlreichen Fällen keine hinreichende Sachentscheidung über die Notwendigkeit einer Verlängerung auf sechs Jahre getroffen wird.

12.1.1
Auskunftsanträge von Betroffenen

Über den Bundesbeauftragten für den Datenschutz und die nationale Kontrollinstanzen anderer Schengen-Vertragsstaaten erreichten mich im Berichtszeitraum ca. 20 Anträge nach Art. 114 Abs. 2 SDÜ.

Bei meinen Überprüfungen habe ich die verschiedensten Fallkonstellationen angetroffen.

Bei einigen Personen waren die Ausschreibungsvoraussetzungen nicht erfüllt. Die Betroffenen waren weder ausgewiesen, zurückgewiesen noch abgeschoben, wie Art. 96 Abs. 3 SDÜ verlangt. In einem Fall räumte die Ausländerbehörde ein, die Ausschreibung sei versehentlich erfolgt. In einem anderen Fall − in dem die Ausschreibung offensichtlich rechtswidrig war − musste das Innenministerium eingeschaltet werden, bis die Ausländerbehörde des Landkreises Bergstraße zugestand, sie habe im Interesse einer bundeseinheitlichen Handhabung die Ausschreibung der Ausländerin gelöscht. In einer Reihe weiterer Fälle konnte aufgrund von Erklärungen und vorgelegten Unterlagen davon ausgegangen werden, dass die Personen sich mittlerweile rechtmäßig in einem anderen Schengen-Staat aufhielten. Daraufhin löschten die Ausländerbehörden ihre Ausschreibung. In zwei Fällen hatten Straftäter die Personalien anderer Personen benutzt. Als die Unbescholtenen eine Schengen-Außengrenze übertreten wollten, wurden sie für die gesuchte Person gehalten und durften die Grenze nicht übertreten. Nur bei weniger als der Hälfte aller geprüften Fälle war die Datenspeicherung nicht zu beanstanden.

12.1.2
Prüfserie bei weiteren acht Ausländerbehörden

Im Rahmen eines Informationsaustausches mit anderen Datenschutzbeauftragten wurde von der Erfahrung berichtet, dass einige Ausländerbehörden ihrer Prüfpflicht nach dreijähriger Speicherdauer nicht nachkommen. Die Hinweise, die das BKA nach Auswertung des nationalen Datenbestandes des SIS den Ausländerbehörden erteilt, blieben unbearbeitet.

Ich bin diesem Vorwurf nachgegangen und erhielt vom BKA eine Aufstellung aller Datensätze, über die in einem bestimmten Zeitraum hessische Ausländerbehörden auf den Ablauf der Dreijahresfrist aufmerksam gemacht worden sind. Zu diesem Zweck wurden die Ausländerbehörden in Frankfurt, Gießen, Groß-Gerau, Hanau, Hofheim, Kassel, Limburg und Wetzlar geprüft.

Aus Sicht des Datenschutzes ging die Ausländerbehörde des Landkreises Kassel am sorgfältigsten vor. In allen Fällen befand sich die Mitteilung des BKA mit Bearbeitungsvermerken versehen in den Ausländerakten. Weitgehend handelte es sich um Kopien, denn mit den Originalen war, nachdem nach dreijähriger Speicherdauer im SIS keine weiteren Informationen zu den abgeschobenen oder ausgewiesenen Personen mehr angefallen sind, die Löschung der Daten veranlasst worden.

Ähnlich sorgfältig wurde im Main-Taunus-Kreis vorgegangen. Ebenfalls mit Bearbeitungsvermerken versehen, fanden sich fast alle Hinweise des BKA in den Akten. Allerdings mit gegenteiligem Prüfergebnis: Weil sich nach der Ausweisung oder Abschiebung der Betroffenen in den verstrichenen drei Jahren keine neueren Informationen zu den Ausländern ergaben und die Ausweisungen oder Abschiebungen mit einem unbefristeten Wiedereinreiseverbot in die Bundesrepublik verbunden sind, müsse die Ausschreibung im SIS − so die Ausländerbehörde des Main-Taunus-Kreises − erhalten bleiben. Es wurde also die Löschung nicht veranlasst.

Im Main-Kinzig-Kreis waren zwar alle Hinweise des BKA in den Akten abgeheftet, allerdings war nicht ersichtlich, dass sie auch bearbeitet waren. Die Angabe der Ausländerbehörde, wenn die Mitteilungen abgeheftet sind, seien sie auch bearbeitet worden, überzeugte nicht. Die genaue Nachschau ergab in mehreren Fällen Zweifel an der Rechtmäßigkeit der Ausschreibung im SIS, die die Ausländerbehörde nicht ausräumen konnte.

Einer Ausländerbehörde war das Verfahren überhaupt nicht bekannt. In den anderen Landkreisen waren die Mitteilungen des BKA zu einem geringen Teil nicht auffindbar, zum Teil mit und ohne Bearbeitungsvermerk in den Akten zu finden.

In Einzelfällen führte die Prüfung zu der Feststellung, dass schon die Ausschreibung unzulässig war; die Löschung wurde veranlasst. Weitgehend wurde aber die Feststellung getroffen, dass sich an der Aktenlage seit der Abschiebung nichts geändert habe, daraufhin blieb die Ausschreibung erhalten. Bei dem selben Sachverhalt, nämlich, dass sich z. B. nach der Ausweisung der betroffenen Person keine neuen Informationen ergeben haben, wird bei der einen Ausländerbehörde die Löschung veranlasst, bei der anderen − aus exakt dem selben Grund − die Verlängerung der Speicherdauer hingenommen. Das Prüfungsergebnis ist nicht akzeptabel.

12.1.3
Ausschreibungen der Ausländerbehörde des Rheingau-Taunus-Kreises

Zweck des Kontrollbesuchs war es, einen umfassenden Eindruck über die Ausschreibungspraxis im SIS bei der Ausländerbehörde zu gewinnen.

Zu diesem Zweck hatte das Hessische Landeskriminalamt eine Auswertung aus HEPOLIS, dem Hessischen Polizei-Informations-System erstellt, in der alle vom Rheingau-Taunus-Kreis im Informationssystem der Polizei (INPOL) ausgeschriebenen Personen aufgelistet waren. Von den 74 betroffenen Ausländern konnten zu 25 Personen die Ausländerakten vorgelegt werden. Bei dem größten Teil der 49 fehlenden Akten war die Zuständigkeit an eine andere Ausländerbehörde übergegangen, sodass die Akte nicht mehr beim Rheingau-Taunus-Kreis geführt wurde. In neun Fällen konnte aber weder die dazugehörige Akte gefunden werden noch konnte dargelegt werden, aus welchen Gründen die Ausschreibung erfolgt war. Die Ausländerbehörde hätte also im Falle einer Verhaftung der betroffenen Personen nicht sagen können, weshalb sie diese überhaupt veranlasst hatte. Ich habe von der Ausländerbehörde verlangt, dass sie, wenn sie den Verbleib der Akten nicht feststellen kann, die Löschung der entsprechenden Ausschreibungen veranlassen muss.

Bei der Durchsicht der 25 vorgelegten Akten fiel Folgendes auf:

In sieben Fällen gab es ausschließlich Ausschreibungen im INPOL, nicht im SIS. Diese Ausschreibungen gehörten zu sog. Altfällen, deren Speicherung im SIS automatisch nach sechs Jahren gelöscht wurde. Diese Frist ist abgelaufen. Dies gilt nicht für die Inpol-Speicherung, deren Frist zehn Jahre beträgt.

In weiteren elf Fällen ergaben sich Zweifel an der Rechtmäßigkeit der Ausschreibung. Es handelte sich zum Teil um Personen, deren Asylantrag abgelehnt worden war und deren Aufenthalt nicht feststand. Die Ausländerbehörde sagte zu, in allen elf Fällen die Ausschreibung zur Einreiseverweigerung im Schengen-Gebiet zu löschen.

In den verbleibenden sieben Fällen war die Behörde der in Art. 112 Abs. 1 SDÜ festgelegten Verpflichtung, die Erforderlichkeit der Ausschreibung nach drei Jahren zu überprüfen, nicht nachgekommen. Es mangelte schon daran, dass die vom BKA erstellten Hinweisschreiben (s. 12.1.2) nicht in der Akte abgeheftet waren.

Die Ausländerbehörde sagte zu, die Erinnerungsschreiben des BKA künftig korrekt zu bearbeiten.

12.1.4
Erlass des Hessischen Ministeriums des Innern

Ich habe das Hessische Innenministerium über meine Feststellungen informiert und darum gebeten sicherzustellen, dass die Ausländerbehörden nicht bei gleichem Sachverhalt gegenteilige Entscheidungen treffen. Die Prüfpflicht nach Art. 112 SDÜ kann sich nicht darin erschöpfen, den Hinweis auf den Ablauf der Dreijahresfrist unbearbeitet zur Akte zu nehmen, oder lediglich festzustellen, dass sich an der Informationslage von vor drei Jahren nichts geändert hat. In einem Erlass vom 05.10.2000 hat das Hessische Ministerium des Innern und für Sport unter anderem festgelegt:

Auszug aus dem Erlass des HMdI vom 5. Dezember 2000

2.2. Ausschreibungen im SIS nach Art. 96 Abs. 3 SDÜ

Wenn die Ausländerbehörde vor dem Ablauf der Ausschreibungsfrist nach spätestens drei Jahren die Mitteilung über den Fristablauf erhält, hat sie im Einzelfall zu überprüfen, ob die Verlängerung der Ausschreibung erforderlich ist (Art. 112 Abs. 4 SDÜ). Die Gründe für eine Verlängerung der Ausschreibung sind in der Akte zu vermerken.

Meine Anforderungen wurden mit diesem Erlass erfüllt. Nach dem Verstreichen einer Übergangsfrist werde ich erneut die Praxis prüfen.

12.2
Kontrolle der Ausländerbehörde des Rheingau-Taunus-Kreises

Bei Kontrollen wurden ein rechtlich fehlerhaftes Verhalten bei der Ermittlung von sogenannten Scheinehen und schwere Mängel bei den räumlichen Datensicherungsmaßnahmen festgestellt.

12.2.1
Verfahren bei der Ermittlung von sog. Scheinehen

Ehen zwischen deutschen und ausländischen Staatsangehörigen, aber auch solche zwischen Ausländern, die nur zu dem Zweck eingegangen werden, dem Ausländer aufenthaltsrechtliche Vorteile zu schaffen, werden als sog. Scheinehen qualifiziert.

Bei unserer Prüfung (Ziff. 12.1.3) wurden fünf Akten untersucht, in denen sich Unterlagen über Ermittlungen wegen des Verdachts einer sog. Scheinehe befanden. In zwei Fällen wurde die Scheinehenermittlung durch eine andere als die

geprüfte Ausländerbehörde durchgeführt. Nur in einem Fall waren die Ermittlungen aus datenschutzrechtlicher Sicht berechtigt und das Verfahren nicht zu beanstanden. Im vierten Fall war die Art und Weise der durchgeführten Ermittlungen rechtswidrig. Aus der Akte ergab sich, dass Anlass für die Ermittlungen ein anonymer Anruf des Inhalts war, dass die betroffene ausländische Staatsangehörige zwar mit einem älteren deutschen Mann verheiratet sei, die Ehe aber nie vollzogen werde. Aus dem nach behördlichen Ermittlungen angefertigten Vermerk war zu ersehen, dass die Behörden im Funktionsbereich des Krankenhauses, in dem die Betroffene tätig war, eine Befragung durchgeführt hatten. Die dort zufällig anwesenden Personen waren gefragt worden, wer bei der entsprechenden Kollegin wohne und ob es sich um einen deutschen oder einen ausländischen Mann handele. Außerdem wurde ein Lichtbild des ausländischen Ex-Ehemanns vorgelegt. Erst anschließend unternahm man den Versuch die Betroffene aufzusuchen, um sich erstmals mit ihr zu unterhalten. Dieses Verfahren ist rechtlich zu beanstanden. Es wurde gegen den Grundsatz verstoßen, dass personenbezogene Daten grundsätzlich bei dem Betroffenen zu erheben sind.

§ 75 Abs. 2 AuslG

Die Daten sind beim Betroffenen zu erheben. Sie dürfen auch ohne Mitwirkung des Betroffenen bei anderen öffentlichen Stellen, ausländischen Behörden und nicht-öffentlichen Stellen erhoben werden, wenn
1. dieses Gesetz oder eine andere Rechtsvorschrift es vorsieht oder zwingend voraussetzt,
2. es im Interesse des Betroffenen liegt und davon ausgegangen werden kann, dass dieser in Kenntnis des Verwendungszwecks seine Einwilligung erteilt hätte,
3. die Mitwirkung des Betroffenen nicht ausreicht oder einen unverhältnismäßigen Aufwand erfordern würde,
4. die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
5. es zur Überprüfung der Angaben des Betroffenen erforderlich ist.

Die Voraussetzungen für eine Durchbrechung nach § 75 Abs. 2 Satz 2 Ausländergesetz (AuslG) liegen nicht vor. Die Ermittlungsbeamten hätten zuerst versuchen müssen, ein Gespräch mit der Betroffenen zu führen und nur bei verbleibenden Zweifeln zu dem Mittel greifen dürfen, völlig Unbekannte zu fragen.

Im fünften Fall stießen wir auf ein uns bereits bekanntes datenschutzrechtliches Problem (s. hierzu auch 25. Tätigkeitsbericht, Ziff. 13.2.2.2). Zum Beweis dafür, dass der Betroffene mit einer deutschen Frau nicht mehr in einer Ehe, sondern getrennt lebt, übermittelte die für die Lohnsteuerkartenerteilung zuständige Stelle einer anderen Stadt eine Bescheinigung, in der mitgeteilt wurde, dass die Ehepartner getrennt leben. Die Angabe zum Ehestand in der Steuererklärung ist ein Datum, das für Steuerverfahren erforderlich ist und unterliegt deshalb dem Steuergeheimnis nach § 30 Abgabenordnung (AO). Die Voraussetzungen für eine Durchbrechung des Steuergeheimnisses nach § 77 Abs. 3 AuslG liegen nicht vor.

§ 77 Abs. 3 AuslG

Personenbezogene Daten, die nach § 30 AO dem Steuergeheimnis unterliegen, dürfen übermittelt werden, wenn der Ausländer gegen eine Vorschrift des Steuerrechts einschließlich des Zollrechts und des Monopolrechts oder des Außenwirtschaftsrecht oder gegen Einfuhr-, Ausfuhr-, Durchfuhr- oder Verbringungsverbote oder -beschränkungen verstoßen hat und wegen dieses Verstoßes ein strafrechtliches Ermittlungsverfahren eingeleitet oder eine Geldbuße … verhängt worden ist.

Die Übermittlung dieser Angabe durch die Lohnsteuerkartenstelle ist demnach unzulässig. Das führt zu einem Verwertungsverbot für die Ausländerbehörde. Die Schwalbacher Ausländerbehörde hat zugesichert, dass künftig derartige Verlangen auf Auskunft an die Lohnsteuerkarten nicht mehr gestellt werden und dass − falls es zu einer Spontanübermittlung durch andere Stellen kommt − das Verwertungsverbot beobachtet wird.

Diese Fälle zeigen, dass es beim Verfahren der Ermittlung von Scheinehen immer wieder zu datenschutzrechtlichen Verstößen kommt (s. hierzu auch 25. Tätigkeitsbericht, Ziff. 13.2). Ich habe deshalb schon im Jahr 1996 beim Hessischen Ministerium des Innern angeregt, den Ausländerbehörden durch Erlass die wesentlichen Rechtmäßigkeitsvoraussetzungen für diese Ermittlungen an die Hand zu geben. Die Stadt Frankfurt besitzt eine mit mir abgestimmte eigene Dienstanweisung. Leider hat das Ministerium im Sommer 2000 mitgeteilt, dass es nicht beabsichtige, in dieser Sache einen Erlass zu fertigen.

12.2.2
Räumliche Datensicherungsmaßnahmen

Bei derselben Ausländerbehörde wurde festgestellt, dass der Publikumsverkehr in einer aus datenschutzrechtlicher Sicht nicht akzeptablen Art und Weise in der Ausländerbehörde stattfindet. An den Tagen mit Publikumsverkehr wird ein Teil des Flurs in der Ausländerbehörde, von dem die einzelnen Räume der Mitarbeiter abgehen, durch eine sog. Theke abgetrennt, die keinerlei Trennwände aufweist. Die Besucher müssen sich in drei verschiedene Listen eintragen, werden später per Namen aufgerufen und ihre Anliegen werden offen an der Theke behandelt. Der grundsätzlich zur Verfügung stehende Warteraum wird nach den gewonnenen Erkenntnissen nicht benutzt. Grund dafür ist wohl, dass die ausländischen Bürger nicht genau wissen, wann sie zu erscheinen haben und sich jederzeit bereit halten wollen. Die Besucher stehen deshalb in drei Schlangen bis dicht vor der Theke. Jeder kann bei seinem Nachbarn und auch bei seinem Vordermann alles verfolgen und mithören. Hinzu kommt, dass die Sachbearbeiter teilweise lauter als gewöhnlich sprechen, damit die ausländischen Bürger sie besser verstehen.

Bereits während der Prüfung wurde beanstandet, dass dies eine aus datenschutzrechtlicher Sicht nicht akzeptable Organisation des Besucherverkehrs ist. Der Behörde wurde nahegelegt, die ausländischen Bürger in den jeweiligen Arbeitszimmern zu empfangen und − falls dies aus Sicherheitsgründen erforderlich erscheinen sollte − die Türen offen stehen zu lassen. Mit den Mitarbeitern und Mitarbeiterinnen des Ausländeramts wurden ferner Maßnahmen besprochen, die zwar nicht optimal sind, aber die datenschutzrechtlichen Belange der Betroffenen besser als bisher berücksichtigen und als Provisorium zeitnah umzusetzen sind. Ich werde mich demnächst über die Umsetzung der Maßnahmen informieren.

13. Melderecht

13.1
Anforderung einer erweiterten Melderegisterauskunft per Vordruck

Eine erweiterte Melderegisterauskunft kann auch an Rechtsanwälte nur dann erteilt werden, wenn das berechtigte Interesse eindeutig nachgewiesen wird.

Die Anfrage einer Kommune machte mich darauf aufmerksam, dass Rechtsanwaltskanzleien erweiterte Melderegisterauskünfte mit Hilfe eines Vordrucks anfordern, in dem nur mit allgemeinen Floskeln ohne Fallbezug versichert wird, dass ein berechtigtes Interesse an der Auskunft vorliege. Mit der erweiterten Auskunft soll die Meldebehörde über eine bestimmte Person nicht nur deren Anschrift, sondern ebenso Geburtsdaten, Staatsangehörigkeit oder andere Informationen bekannt geben.

Grundsätzlich kann jeder Bürger nach § 34 Abs. 1 Hessisches Meldegesetz (HMG) eine Grundauskunft über Name und Adresse für jede namentlich genannte Person erhalten, ein besonderer Nachweis über den Grund der Anfrage ist nicht erforderlich. Die Meldeämter müssen allerdings prüfen, ob schutzwürdige Interessen der gemeldeten Personen entgegenstehen (§ 7 S. 1 und 2 HMG); ohne eine solche Prüfung ist die Ermessensentscheidung, die sie zu treffen haben, rechtlich unvollständig. Noch strengere Maßstäbe legt § 34 Abs. 2 HMG an, wenn zusätzliche Daten abgefragt werden. Diese dürfen nur bekannt gegeben werden, wenn ein „berechtigtes“ Interesse an diesen Daten gegenüber der Meldebehörde glaubhaft gemacht werden kann.

§ 34 HMG

(1) Personen, die nicht Betroffene sind, und anderen als den in § 31 Abs. 1 bezeichneten Stellen darf die Meldebehörde nur Auskunft über
1. Vor- und Familiennamen,
2. Doktorgrad und
3. Anschriften einzelner bestimmter Einwohnerinnen und Einwohner

übermitteln (einfache Melderegisterauskunft). Dies gilt auch, wenn jemand Auskunft über Daten einer Vielzahl namentlich bezeichneter Einwohnerinnen und Einwohner begehrt.

(2) Soweit jemand ein berechtigtes Interesse glaubhaft macht, darf ihm zusätzlich zu den in Abs. 1 Satz 1 genannten Daten einer einzelnen bestimmten Person eine erweiterte Melderegisterauskunft erteilt werden über
1. Tag und Ort der Geburt,
2. frühere Vor- und Familiennamen,
3. Familienstand, beschränkt auf die Angabe, ob verheiratet oder nicht,
4. Staatsangehörigkeiten,
5. frühere Anschriften,
6. Tag des Ein- und Auszugs,
7. gesetzliche Vertreterin/gesetzlicher Vertreter oder Betreuerin oder Betreuer und
8. Sterbetag und -ort.

Die mir von der Kommune vorgelegte allgemeine Versicherung des Anwaltbüros, dass ein berechtigtes Interesse vorliege, reicht für die erforderliche Prüfung, ob eine Auskunft überhaupt gegeben werden darf, nicht aus. Die Kommune darf dem Auskunftsverlangen nur stattgeben, wenn eine hinreichend klare und substanzhaltige Schilderung des Sachverhalts gegeben wird. Zur Glaubhaftmachung müssen Unterlagen (z. B. Verträge etc.) vorgelegt werden, die die zweckändernde Datennutzung rechtfertigen. Nach der Bearbeitung des Auskunftsersuchens sind die vorgelegten Unterlagen von der Meldebehörde im Regelfall zurückzusenden. Wird Auskunft erteilt, ist in der Akte zu vermerken, aufgrund welcher Unterlagen das berechtigte Interesse des Antragstellers bejaht wurde.

Ich habe die Kommune über die Rechtslage informiert, insbesondere darüber, dass Melderegisterauskünfte nur erteilt werden dürfen, wenn das berechtigte Interesse sauber dargestellt und mit detaillierten Unterlagen wirklich nachgewiesen wird.

13.2
Datenübermittlungen der Einwohnermeldeämter an die Gebühreneinzugszentrale

Datenübermittlungen an die GEZ finden manchmal schneller statt, als sich dies der Meldesachbearbeiter vorstellen kann.

Häufig erreichen mich telefonische Anfragen von Bürgern, die nach einem Umzug einen Brief der Gebühreneinzugszentrale (GEZ) im Briefkasten vorfinden.

Nach § 18 Meldedatenübermittlungsverordnung (MeldDÜVO) informiert die Meldebehörde rechtmäßig die GEZ über jeden Zu-, Um- und Wegzug einer Person über 18 Jahre. Dies geschieht im Zusammenhang mit der automatisierten Führung des Melderegisters so unauffällig, dass sogar Meldesachbearbeitern diese Datenübermittlung nicht mehr bewusst ist.

§ 18 Abs. 1 MeldDÜVO

Die Meldebehörde darf dem Hessischen Rundfunk oder der von ihm auf Grund des Art. 8 Abs. 4 Satz 2 des Rundfunkgebührenstaatsvertrages vom 5. Dezember 1974 (GVBl. 1975 I S. 136), geändert durch Staatsvertrag vom 3. April 1987 (GVBl. I S. 166), beauftragten Stelle zum Zwecke des Einzugs der Rundfunkgebühren nach Art. 8 des Rundfunkgebührenstaatsvertrages im Falle der Anmeldung, Abmeldung oder des Todes folgende Daten volljähriger Einwohner übermitteln:
1. Familiennamen (jetziger und früherer Name mit Namensbestandteilen),
2. Vornamen,
3. Tag der Geburt,

4. Anschriften (gegenwärtige und frühere Anschriften, Haupt- und Nebenwohnung),
5. Tag des Ein- und Auszugs,
6. Sterbetag.

Der Pflegevater eines zehnjährigen Kindes beschwerte sich darüber, dass dieses Kind, nachdem es in seine Familie aufgenommen worden war, einen Brief der GEZ erhalten hat, obwohl die Daten aufgrund des laufenden Adoptionsverfahrens an sich besonders geschützt sein sollten.

Da Daten von Personen unter 18 Jahren grundsätzlich nicht an die GEZ übermittelt werden, konnte zunächst weder die GEZ noch die Kommune sich diese Datenübermittlung erklären. Durch Recherchen beim zuständigen Rechenzentrum konnte ich folgenden Sachverhalt ermitteln: Das melderechtliche Verfahren sieht grundsätzlich keine gesonderte Erfassung des Zuzugs alleinstehender Minderjähriger vor. Die Kommune konnte daher einen einfachen Zuzug des alleinstehenden Pflegekindes DV-technisch nicht darstellen. Mit Hilfe einer „Überlistung“ des Programms wollte die Kommune das Problem ohne großen Aufwand lösen. Sie veränderte für den Zuzug das Geburtsdatum des Kindes, sodass dieses kurzfristig „volljährig“ wurde. In einem sofort folgenden weiteren Schritt wurde das Geburtsdatum berichtigt, das Melderegister enthielt umgehend wieder die richtigen Daten des Kindes. Der kurze Moment des Zuzugs einer vermeintlich volljährigen Person genügte aber, um die GEZ automatisch über den Zuzug des Kindes zu informieren. Hiermit hatte auch der Meldesachbearbeiter nicht gerechnet.

Die GEZ hat nach Aufklärung des Sachverhalts die Daten des Kindes sofort gelöscht. Die Kommune wird künftig nicht mehr versuchen, das Programm zur Führung des Einwohnermelderegisters zu „überlisten“.

13.3
Automatisierter Zugriff auf Einwohnermeldedateien durch Vollstreckungsbehörden

Ein automatisierter Abruf der Einwohnermeldedaten durch Vollstreckungsstellen ist nicht zulässig. Die Gemeinde muss ausnahmslos die Schutzwürdigkeit der Personendaten prüfen.

Eine Kommune übersandte mir das Anschreiben und ein Formular zur Erteilung einer Einverständniserklärung des Kreisausschusses zur datenschutzrechtlichen Prüfung. Der Kreisausschuss wollte zur zeitnahen Durchsetzung von Forderungen und im Hinblick auf die knappe personelle Besetzung der Vollstreckungsstelle Anfragen bei den Meldebehörden umgehen, indem den Mitarbeiterinnen und Mitarbeitern der Vollstreckungsstelle ein Zugriff auf die Einwohnermeldedateien der Kommunen eröffnet wird.

Nach § 31 Abs. 4 Hessisches Meldegesetz (HMG) sind regelmäßige Datenübermittlungen an andere Behörden nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist. Die Hessische Meldedatenübermittlungsverordnung (MeldDÜVO) schreibt in § 1 Abs. 4 i.V.m. mit §§ 13 und 15 vor, dass Meldedaten automatisiert nur von Polizeidienststellen bzw. Kraftfahrzeugzulassungs- und Führerscheinstellen abgefragt werden dürfen.

§ 31 Abs. 4 HMG

Regelmäßige Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen sind zulässig, soweit dies durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zwecks der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten bestimmt ist.

§ 1 Abs. 4 MeldDÜVO

Automatisierte Verfahren, die den Abruf personenbezogener Daten aus dem Melderegister ermöglichen, sind in den Fällen der §§ 13 und 15 zulässig

Für den vom Kreisausschuss angestrebten automatisierten Abruf der Einwohnermeldedaten durch die Vollstreckungsstelle gibt es keine Rechtsgrundlage, er ist daher unzulässig. Die Einwilligung von Kommunen, die das Einwohnermelderegister führen, kann eine Rechtsgrundlage nicht ersetzen. Die Meldeämter müssen in jedem Einzelfall prüfen, ob einer Übermittlung schutzwürdige Interessen der Betroffenen entgegenstehen (§ 7 Satz 1 und 2 HMG).

§ 7 HMG

Schutzwürdige Belange Betroffener dürfen durch die Verarbeitung personenbezogener Daten nicht beeinträchtigt werden. Schutzwürdige Belange werden insbesondere beeinträchtigt, wenn die Verarbeitung, gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehenen Zweck, Betroffene unverhältnismäßig belastet.

Da ich davon ausgehen muss, dass nicht nur die anfragende Kommune, sondern alle kreisangehörigen Städte und Gemeinden ein entsprechendes Schreiben erhalten haben, habe ich nicht nur die anfragende Kommune, sondern auch den Kreisausschuss über die Rechtslage informiert.

14. Gewerberecht

Löschung von Daten aus der Gewerbeanzeige nach Abmeldung des Gewerbes

Die Gewerbeordnung enthält keine Regelung, wie lange Daten aus der Gewerbeanzeige aufzubewahren sind, nachdem das Gewerbe abgemeldet wurde. Mit dem Hessischen Minister für Wirtschaft, Verkehr und Landesentwicklung halte ich eine Aufbewahrungsdauer der Daten aus der Gewerbeanzeige von fünf Jahren nach Abmeldung des Gewerbes für die Aufgabenerfüllung der Gewerbebehörden für angemessen.

Durch die Stadt Kassel und das Regierungspräsidium Kassel bin ich auf das Problem aufmerksam gemacht worden, dass die Gewerbeordnung (GewO) keine Regelung enthält, wie lange die Daten aus der Gewerbeanzeige aufzubewahren sind,

nachdem das Gewerbe abgemeldet wurde. Die Gewerbeordnung verweist in diesem Punkt vielmehr auf die Datenschutzgesetze der Länder.

§ 14 Abs. 11 GewO

Für das Ändern, Sperren oder Löschen der nach den Abs. 1−4 erhobenen Daten gelten die Datenschutzgesetze der Länder.

Gem. § 19 Abs. 3 HDSG sind Daten unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist. Es war daher zu prüfen, ob die für die Überwachung der Gewerbetreibenden gespeicherten Daten nach Abmeldung des Gewerbes zeitnah zu löschen sind. Dies ist jedoch für die Aufgabenerfüllung der Gewerbebehörden insgesamt nicht sachgerecht.

Das Regierungspräsidium Kassel hatte eine Aufbewahrungsdauer von zehn Jahren vorgeschlagen und den Minister für Wirtschaft, Verkehr und Landesentwicklung gebeten, diese Aufbewahrungsdauer per Erlass verbindlich für alle Gewerbebehörden festzuschreiben. Der Wirtschaftsminister bat mich dazu um datenschutzrechtliche Stellungnahme. Zur Begründung trug das Regierungspräsidium vor, dass die Daten aus der Gewerbeanzeige auch anderen Zwecken dienten als lediglich der Überwachung der Tätigkeit der Gewerbetreibenden. Die Gewerbeanzeigen dienten auch arbeitsschutzrechtlichen, berufsrechtlichen, statistischen und steuerrechtlichen Zwecken. Im Übrigen gebe es Ermittlungsbedarf innerhalb von Behörden nach der Gewerbeausübung eines Gewerbetreibenden in den letzten Jahren. Diese Ermittlungen dienten letztlich der Überwachung der Gewerbetreibenden. Im Gewerbeuntersagungsverfahren sei zur Beurteilung der gewerberechtlichen Zuverlässigkeit von Bedeutung, wie und wo sich ein Gewerbetreibender in den letzten Jahren gewerblich betätigt habe.

Da es sich bei dieser Fragestellung nicht um eine besondere hessische Frage handelt, habe ich bei den Datenschutzbeauftragten der anderen Bundesländer nachgefragt, wann dort die Daten aus der Gewerbeanzeige gelöscht werden, wenn ein Gewerbebetrieb abgemeldet wird. Die Verwaltungspraxis stellte sich höchst unterschiedlich dar. Der Datenschutzbeauftragte eines Bundeslandes vertrat die Auffassung, dass die allgemeine Löschungsvorschrift des Landesdatenschutzgesetzes − bei Normengleichheit mit der hessischen Regelung − die sofortige Löschung der Daten nach Abmeldung des Gewerbebetriebes gebietet. Einige wenige Datenschutzbeauftragte hielten eine zehnjährige Aufbewahrungsdauer für die Aufgabenerfüllung der Gewerbebehörden bei ebenfalls gleicher Rechtslage für angemessen.

Ich teile die Auffassung des Regierungspräsidiums Kassel, wonach die Vorschrift des § 14 GewO neben der Überwachung der Tätigkeit der Gewerbetreibenden auch anderen Zwecken dient, nämlich arbeitsschutzrechtlichen, berufsrechtlichen, statistischen und steuerrechtlichen. Eine unverzügliche Löschung der Daten der Gewerbeanzeige bei Abmeldung des Gewerbes halte ich deshalb für nicht sachgerecht. Allerdings teile ich nicht die Auffassung des Regierungspräsidiums Kassel, wonach Daten aus abgemeldeten Gewerben für zukünftige mögliche Untersagungsverfahren herangezogen werden können. Entweder hat ein Betroffener früher sein Gewerbe zuverlässig ausgeübt, dann ist der Rückgriff nicht erforderlich; oder der Gewerbetreibende war unzuverlässig oder ungeeignet. Dann hätte ihm das Gewerbe nach § 35 GewO untersagt werden müssen, was nach § 149 Abs. 2 GewO einen entsprechenden Eintrag in das Gewerbezentralregister nach sich gezogen hätte. Eine Auskunft aus dem Gewerbezentralregister kann die Gewerbebehörde in einem Untersagungsverfahren jederzeit erhalten. Deswegen halte ich die Zehnjahresfrist im Einklang mit den meisten anderen Datenschutzbeauftragten für zu lang. Eine Aufbewahrung von fünf Jahren ist angemessen und verhältnismäßig. Die Frist entspricht im Übrigen auch den allgemeinen Aufbewahrungsbestimmungen für das Schriftgut des Landes Hessen, wonach Akten, für die keine besondere Aufbewahrungsfrist festgesetzt worden ist, fünf Jahre aufzubewahren sind.

Das Hessische Ministerium für Wirtschaft, Verkehr und Landesentwicklung hat diese Frist mit Erlass vom 11.12.2000 für die Gewerbebehörden verbindlich festgelegt.

15. Kommunen

15.1
Präsentation ehrenamtlicher Funktionsträger im Internetangebot von Kommunen

Die Veröffentlichung von personenbezogenen Daten im Internet hat eine andere Dimension als in herkömmlichen Broschüren. Besonderheiten ergeben sich schon daraus, dass weltweit abgerufen und deshalb ein angemessenes Datenschutzniveau bei der Übermittlung nicht gewährleistet werden kann. An die Einwilligung zur Veröffentlichung sind besondere Anforderungen zu stellen.

Nach Mitteilung des behördlichen Datenschutzbeauftragten hat eine Stadt beabsichtigt, ein bisher in Papierform für ihre Bürger dieser Stadt vorgehaltenes Verzeichnis der städtischen Dienststellen, Ansprechpartner, Stadtverordneten, Ortsbeiräte, Stadtbezirksvorsteher, Schiedsmänner mit Angaben wie Namen, Rufnummern und Anschriften ins Internet einzustellen. Bei dem Kreis der aufgeführten Personen handelt es sich um Bedienstete der Stadt, Mandatsträger und Ehrenbeamte. Die Besonderheit ist, dass Mandatsträger und Ehrenbeamte im Unterschied zu den städtischen Bediensteten nicht stets über die dienstlichen Adressen und Telefonnummern innerhalb der üblichen Dienstzeiten unmittelbar erreichbar sind. Deshalb hatten die meisten Amtsträger eine berufliche Anschrift und Telefonnummer, manche auch eine private Adresse angegeben und ihre Einwilligung zur Bekanntgabe der Daten in der Broschüre gegeben. Es war zunächst daran gedacht, alle in der Broschüre zusammengestellten Daten gleichzeitig ins Internet zu übernehmen. Dagegen hatte der Datenschutzbeauftragte Bedenken, weil die Veröffentlichung der Daten im Internet eine andere Qualität und einen wesentlich erweiterten Verbreitungsgrad hat. Er war zu Recht der Ansicht, dass die ursprüngliche Einwilligung dies nicht umfasste und wandte sich unter anderem mit der Frage an mich, ob die Bereitstellung als Internet-Seite nicht eine Übermittlung an Empfänger außerhalb des Geltungsbereich des Grundgesetzes und der EG-Datenschutzrichtlinie sei und deshalb nur unter den Voraussetzungen des § 17 Abs. 2 HDSG zugelassen werden dürfe.

Mit dieser Ansicht hatte der Datenschutzbeauftragte Recht. Wie bereits in meinem 28. Tätigkeitsbericht unter Ziff. 9.2 dargestellt, ist die Veröffentlichung der Namen und der dienstlichen Adresse von Stadtverordneten und anderen Amtsträgern zulässig, weil sie sich für diese Funktion nicht auf den grundrechtlichen Datenschutz berufen können. Sie sind nicht als Privatpersonen, sondern als Funktionsträger betroffen. Darüber hinausgehende Daten − vor allem Privatadressen und private Telefonnummern (dazu zählen bei ehrenamtlich Tätigen auch die beruflichen Anschriften und Telefonnummern) − dürfen nur mit Einwilligung in Broschüren wie auch im Internet veröffentlicht werden. Die Einwilligung genügt in diesen Fällen nur dann den Voraussetzungen des § 7 Abs. 2 HDSG, wenn der Betroffene über Art und Zweck der Datenverwendung, die Risiken, die Folgen und den Empfängerkreis informiert ist.

§ 7 Abs. 2 HDSG

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Sie muss sich im Falle einer Datenverarbeitung nach Abs. 4 ausdrücklich auch auf die dort genannten Daten beziehen. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen. 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.

Gegenüber der Bekanntgabe in einer Broschüre in Papierform stellt das Internet eine völlig andere Qualität dar und zwar schon deshalb, weil es vielfältige Auswertungs- und Verknüpfungsmöglichkeiten eröffnet. Da wesentliche Unterschiede bestehen, weil die Datenübermittlung einen anderen und größeren Kreis erreicht, genügt die Einwilligung in die Veröffentlichung der Daten in einer Broschüre nicht als Grundlage für die Zulässigkeit der Veröffentlichung im Internet. Die Einwilligung muss sich speziell auch auf das Medium beziehen. Das ist schon deshalb von Bedeutung, weil die Freigabe für die Veröffentlichung im Internet auch die Einwilligung in eine Übermittlung der Daten in Länder außerhalb des Geltungsbereichs des Grundgesetzes und der EG-Datenschutzrichtlinie einschließen muss, in denen ein angemessener Datenschutz nicht gewährleistet ist.

§ 17 Abs. 2 HDSG

Eine Übermittlung an Empfänger außerhalb des in Abs. 1 genannten Bereichs ist auf Grund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt oder beim Empfänger ein angemessener Datenschutz gewährleistet ist. Vor der Entscheidung über die Angemessenheit ist der Hessische Datenschutzbeauftragte zu hören. Sofern beim Empfänger kein angemessener Datenschutz gewährleistet ist, dürfen personenbezogene Daten nur übermittelt werden wenn,

1. der Betroffene seine Einwilligung gegeben hat,
2. die Übermittlung für die Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung, oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
3. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
4. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Der Empfänger, an den die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu Zwecken verarbeitet werden dürfen, die mit den Zwecken zu vereinbaren sind, zu deren Erfüllung sie ihm übermittelt werden.

Die nach § 17 Abs. 2 vorgeschriebene Anhörung des Hessischen Datenschutzbeauftragten kann bei einer Bereitstellung von personenbezogenen Daten im Internet unterbleiben, weil sie kein anderes Ergebnis haben kann, als dass ein angemessenes Datenschutzniveau nicht gewährleistet ist. Die Einstellung von nicht ausschließlich amtsbezogenen, sondern personenbezogenen Daten in das Internet ist deshalb nur unter den Voraussetzungen von § 17 Abs. 2 Satz 3, insbesondere also bei Einwilligung zulässig. Da die Bereitstellung der Daten im Internet eine Veröffentlichung im Sinne von § 3 Abs. 4 HDSG darstellt, hat sie für den Betroffenen auch die Folge, dass die veröffentlichten Daten nicht mehr in den Schutzbereich des Hessischen Datenschutzgesetzes fallen.

§ 3 Abs. 4 HDSG

Dieses Gesetz gilt nicht für personenbezogene Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind sowie für Daten des Betroffenen, die von ihm zur Veröffentlichung bestimmt sind.

Bei der Einholung der Einwilligung sollte auf diese Folge besonders hingewiesen werden. Zwar kann die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden, worauf der Betroffene auch nach § 7 Abs. 2 Satz 6 HDSG hinzuweisen ist. Bei einer Veröffentlichung im Internet hat das gegenüber konventionellen Medien zwar den Vorteil, dass das Berichtigen und Löschen der Daten tatsächlich rasch erfolgen kann und deshalb für die Zukunft Vorsorge getroffen ist, dass neue „Besucher“ des Internet-Angebotes diese Daten nicht mehr präsentiert bekommen. Die aus dem ursprünglichen Datenbestand abgerufenen Daten können aber vom Empfänger noch weiter verwendet werden, sofern er sie gespeichert hatte. Derartige Daten sind praktisch nicht mehr rückrufbar. Sie sind veröffentlicht und daher datenschutzrechtlich ungeschützt.

15.2
Zuverlässigkeitsprüfung von Hundehaltern

Die vom Bundesrat geforderte Erweiterung der Auskünfte aus dem Bundeszentralregister für die Zuverlässigkeitsprüfung von Hundehaltern ist im beabsichtigten Umfang nicht mit dem Recht auf informationelle Selbstbestimmung vereinbar.

Im Rahmen des Vollzugs der am 15. August 2000 in Kraft getretenen Gefahrenabwehrverordnung über das Halten und Führen von gefährlichen Hunden (Gesetz- und Verordnungsblatt für das Land Hessen Teil I − 2000, S. 411) müssen die Ordnungsbehörden die Zuverlässigkeit der Hundehalter überprüfen. Für diese Prüfung können sie beim Bundeszentral-

register ein sog. Behördenführungszeugnis anfordern (§ 32 Abs. 3 Bundeszentralregistergesetz (BZRG)). Von den Ordnungsbehörden wurde kritisiert, dass das Behördenführungszeugnis für die Beurteilung der Zuverlässigkeit der Hundehalter nicht ausreiche. Vielmehr seien für die Beurteilung der Zuverlässigkeit der Halter gefährlicher Hunde auch Informationen unerlässlich, die sich aus Entscheidungen von Verwaltungsbehörden gegen den Hundehalter ergeben. Dazu gehört z. B. auch die Entziehung der Fahrerlaubnis. Auch aus derartigen Entscheidungen könne sich eine eventuelle Unzuverlässigkeit ergeben. Diese Entscheidungen sind nicht in einem Führungszeugnis für Behörden enthalten, sondern nur in den unbeschränkten Auskünften i.S.v. § 41 BZRG.

Auf einen daraufhin gestellten Antrag des Landes Hessen hat der Bundesrat in einer Entschließung zum Schutz vor Kampfhunden (BR-Drucks. 417/00 − Beschluss −) die Änderung des Bundeszentralregistergesetzes verlangt. Darin wird die Bundesregierung aufgefordert, ein Änderungsgesetz mit dem Ziel vorzulegen, dass unbeschränkte Auskünfte an diejenigen Behörden erteilt werden dürfen, welche die Zuverlässigkeit von Hundehaltern zu prüfen haben. Gleichzeitig soll die Tilgung der Eintragungen im Register für diese Fälle kein Verwertungsverbot nach sich ziehen.

Eine unbeschränkte Auskunft nach § 41 BZRG ist sonst nur für die wenigen ausgewählten Stellen zulässig, die in § 41 BZRG aufgezählt sind; außerdem unterliegen die Auskünfte einer engen Zweckbindung.

§ 32 Abs. 3 BZRG

In ein Führungszeugnis für Behörden (§ 30 Abs. 5, § 31) sind entgegen Absatz 2 auch aufzunehmen
1. Verurteilungen, durch die eine freiheitsentziehende Maßregel der Besserung und Sicherung angeordnet worden ist,
2. Eintragungen nach § 10, wenn die Entscheidung nicht länger als zehn Jahre zurückliegt,
3. Eintragungen nach § 11.

§ 41 BZRG

(1) Von Eintragungen, die in ein Führungszeugnis nicht aufgenommen werden, … darf … nur Kenntnis gegeben werden
1. den Gerichten …
2. den obersten Bundes- und Landesbehörden,

…

(4) Die Auskunft nach den Absätzen 1 bis 3 wird nur auf ausdrückliches Ersuchen erteilt. Die in Absatz 1 genannten Stellen haben den Zweck anzugeben, für den die Auskunft benötigt wird; sie darf nur für diesen Zweck verwertet werden.

Die vom Bundesrat geforderte Änderung des Bundeszentralregistergesetzes würde zu einer starken Ausweitung der Mitteilungspflichten führen.

Das begegnet insofern Bedenken, als alle im Bundeszentralregister gespeicherten Straftaten im Rahmen der Zuverlässigkeitsprüfung übermittelt werden sollen. Sachgerechter wäre eine Lösung, die − wie § 32 Abs. 4 BZRG − den sachlichen Zusammenhang mit der Zuverlässigkeitsprüfung hervorhebt. Folgerichtig würden nur Straftaten mitgeteilt, die mit Körperverletzung und Gewaltanwendung sowie Nötigung in Verbindung stehen.

Bei der weiteren Ausgestaltung des Verfahrens ist darauf zu achten, dass die Zuverlässigkeitsprüfungen nicht ins Uferlose ausgeweitet werden. Für jeden einzelnen Sachbereich ist eine konkrete Abwägung zwischen dem mit der Zuverlässigkeitsprüfung angestrebten Schutz der Allgemeinheit und dem Interesse der zu überprüfenden Bürgerinnen und Bürger an der Wahrung ihres Rechtes auf informationelle Selbstbestimmung erforderlich. Weit zurückliegende Straftaten sollten aus Resozialisierungsgründen nicht in Verwaltungsverfahren verwertet werden, die die Hundehaltung betreffen, soweit kein sachlicher Bezug dazu erkennbar ist.

Das Aussetzen des Verwertungsverbotes trotz Tilgung einer Strafe aus dem Register ist nach meiner Einschätzung nicht mehr verhältnismäßig, um die routinemäßige Überprüfung von Hundehaltern durchzuführen.

§ 52 Abs. 1 Ziff. 4 BZRG

Die frühere Tat darf abweichend von § 51 Abs. 1 nur berücksichtigt werden, wenn

…

4. der Betroffene die Zulassung zu einem Beruf oder einem Gewerbe, die Einstellung in den öffentlichen Dienst oder die Erteilung einer Waffenbesitzkarte, eines Munitionserwerbscheins, Waffenscheins, Jagdscheins oder einer Erlaubnis nach § 27 des Sprengstoffgesetzes beantragt, falls die Zulassung, Einstellung oder Erteilung der Erlaubnis sonst zu einer erheblichen Gefährdung der Allgemeinheit führen würde; das gleiche gilt, wenn der Betroffene die Aufhebung einer die Ausübung einer Berufes oder Gewerbes untersagenden Entscheidung beantragt.

Die unbeschränkte Auskunft nach § 52 Abs. 1 BZRG ist sonst nur für Sonderfälle schwerwiegender Rechtsbeeinträchtigungen vorgesehen. Auch hinsichtlich der Hundehaltung sollten daher nur Delikte vom Verwertungsverbot des § 51 Abs. 1 BZRG ausgenommen werden, die auf Vorkommnisse zurück gehen, die mit der Hundehaltung in Zusammenhang stehen. Das Überschreiten der Erforderlichkeitsgrenze habe ich gegenüber dem Hessischen Ministerium des Innern gerügt.

15.3
Kommunale Archivsatzung

Wenn Gemeinden ein eigenes öffentliches Archiv führen, müssen sie eine den Regelungen des Hessischen Archivgesetzes entsprechende Satzung beschließen und umsetzen.

Im Rahmen der Anfrage des Archivleiters einer hessischen Gemeinde zur Zulässigkeit der Herausgabe von Unterlagen aus der NS-Zeit für Forschungszwecke war von mir zu prüfen, aufgrund welcher Vorschriften personenbezogene Unterlagen Forschern durch das kommunale Archiv zur Verfügung gestellt werden können. Dabei wurde erneut deutlich, dass das Hessische Archivgesetz von den Kommunen unzureichend umgesetzt wird (s. bereits 26. Tätigkeitsbericht Ziff. 10.6).

Die Schaffung eines öffentlichen Archivs als öffentlich-rechtliche Einrichtung liegt zunächst im freien Ermessen der Gemeinde, das durch § 4 Archivgesetz (HArchivG) allerdings in einen bestimmten Rechtsrahmen eingebunden ist.

§ 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.

Bei zahlreichen hessischen Gemeinden, die tatsächlich ein öffentliches Archiv führen, liegt ein gravierendes Defizit darin, dass die konkreten Rechtsverhältnisse zwischen Nutzer und Archiv nicht in einer Kommunalsatzung geregelt sind wie das Gesetz eindeutig fordert. Aus § 6 HArchivG letzter Satz lässt sich dabei herleiten, dass die Kernaussagen des Archivgesetzes von einer solchen Satzung übernommen werden müssen.

§ 6 letzter Satz HArchivG

Die Anwendung des Gesetzes auf die Archive der Gemeinden, Landkreise und kommunalen Verbände bestimmt sich nach § 4 Abs. 1.

Datenschutzrechtlich relevant sind diese Feststellungen vor allem für die häufig vorkommenden Fälle, dass archivierte Unterlagen, in die Forscher einsehen möchten, personenbezogene Daten von noch lebenden Personen enthalten. Ein solches Einsichtsrecht kann sich nur aus § 15 Abs. 4 HArchivG oder, soweit diese Vorschrift für kommunale Archive nicht direkt gilt, aus einer gleichlautenden Satzungsregelung ergeben.

§ 15 Abs. 4 HArchivG

Die festgelegten Schutzfristen können im Einzelfall verkürzt werden, wenn es im öffentlichen Interesse liegt; bei personenbezogenem Archivgut ist eine Verkürzung nur zulässig, wenn die Benutzung für ein bestimmtes Forschungsvorhaben erfolgt und schutzwürdige Belange der betroffenen Personen oder Dritter nicht beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange erheblich überwiegen; soweit der Forschungszweck es zulässt, sind die Forschungsergebnisse ohne personenbezogene Angaben aus dem Archivgut zu veröffentlichen. Eine Benutzung personenbezogener Akten ist unabhängig von den in Abs. 1 genannten Schutzfristen auch zulässig, wenn die Person, auf die sich das Archivgut bezieht, oder im Fall ihres Todes ihre Angehörigen zugestimmt haben; die Einwilligung ist von dem überlebenden Ehegatten, nach dessen Tod von seinen Kindern und wenn weder ein Ehegatte noch Kinder vorhanden sind, von den Eltern der betroffenen Person einzuholen.

Soweit die personenbezogenen Unterlagen ohne wesentlichen Aufwand anonymisiert werden können, sollten die Gemeindearchive keine Unterlagen mit Personenbezug zur Einsicht bereitstellen. Durch Einwilligung der Betroffenen oder ihrer Nachfahren entfallen die meisten datenschutzrechtlichen Probleme.

Die von der oben erwähnten Anfrage betroffene Gemeinde habe ich daher gebeten, umgehend eine solche Archivsatzung zu erlassen. Ergänzend sollten Regelungen aufgenommen werden, wie sie in der „Benutzungsordnung für die hessischen Staatsarchive“ (StA 1997, S. 1300) enthalten sind. Hilfreich für die Erstellung einer solchen Satzung ist die „Mustersatzung für Kommunalarchive“, wie sie beim Hessischen Städtetag zu erhalten ist.

15.4
Sogar das Versenden von Müllwertmarken kann zu Beschwerden beim Datenschutzbeauftragten führen

Müllwertmarken dürfen nicht mit Briefumschlägen versandt werden, die Angaben über die Liegenschaften des Empfängers enthalten.

Drei Bürger einer hessischen Kommune beschwerten sich darüber, dass Müllwertmarken in Briefumschlägen verschickt wurden, deren Aufkleber nicht nur die Adresse des Empfängers zeigten. Der Aufkleber enthielt außerdem genaue Angaben darüber, für welche Liegenschaft der Briefinhalt bestimmt sein sollte. Die mir übersandten Briefumschläge ließen keinen Zweifel daran, dass die Kommune − wie schon vor einigen Jahren − wieder Informationen auf Briefumschlägen angebracht hatte, die Rückschlüsse auf persönliche Verhältnisse des Empfängers zulassen und deshalb datenschutzrechtlich zu beanstanden sind (§ 16 HDSG).

Recherchen bei der Gemeindeverwaltung ergaben, dass sie die unzulässige Versendeform auf Wunsch einzelner Liegenschaftseigentümer wählte, die diese Briefumschläge ungeöffnet an ihre Mieter weiterleiten wollten.

Ich habe die Kommune erneut darauf hingewiesen, dass Briefumschläge außer den nötigen Adressdaten grundsätzlich keine Rückschlüsse auf Daten oder persönliche Verhältnisse des Empfängers enthalten dürfen. Die Kommune hat das entsprechende Fachamt angewiesen, unabhängig von einzelnen gegenteiligen Bürgerwünschen künftig Müllwertmarken nur noch in neutralen Umschlägen zu versenden.

15.5
Netzzugriffsrechte für Bürgermeister und Amtsleiter

Für den Bürgermeister einer Kommune oder den Amtsleiter einer Verwaltungsbehörde darf ein Zugriff auf Verwaltungsdaten nur dann eingeräumt werden, wenn diese zu dessen Aufgabenerfüllung erforderlich sind. Maßgebend sind die fachaufsichtlichen und dienstrechtlichen Befugnisse, die der Bürgermeister oder Amtsleiter hat.

Eine Gemeinde bat um datenschutzrechtliche Prüfung, ob dem Wunsch des Bürgermeisters, innerhalb des Netzwerkes volles Zugriffsrecht auf alle Arbeitsplätze und den Server zu erhalten, entsprochen werden darf.

Die Zweckbindung nach § 13 Hessisches Datenschutzgesetz (HDSG) gebietet, dass Bedienstete und ihre organisationsrechtlichen Vertreter in öffentlichen Verwaltungen einen Zugriff nur auf die Daten haben, die sie zur Erfüllung ihrer

Aufgaben benötigen. Ein Zugriff durch Weisungsberechtigte und Vorgesetzte ist zulässig, soweit dies zur Erfüllung ihrer fachaufsichtlichen Aufgaben und der dienstrechtlichen Befugnisse gegenüber nachgeordneten Bediensteten erforderlich ist. Die Zugriffsbefugnis ist auf fachaufsichtliche Weisungsstränge zu begrenzen, die im Organisationsplan der jeweiligen Verwaltung vorgesehen sind.

§ 13 HDSG

(1) Personenbezogene Daten dürfen grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, dann ist dies nur aus den in § 12 Abs. 2 und 3 genannten Gründen zulässig. Besondere Amts- oder Berufsgeheimnisse bleiben unberührt.
...

(4) Personenbezogene Daten, die für andere Zwecke erhoben worden sind, dürfen auch zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zu Ausbildungs- und Prüfungszwecken in dem dafür erforderlichen Umfang verwendet werden.

Für Kommunalverwaltungen bedeutet das: Als höchste weisungsbefugte Stelle ist jeweils das Mitglied des Gemeindevorstandes anzusehen, dem die Ressortzuständigkeit obliegt.

Auch wenn der Bürgermeister nach § 70 Abs. 1 und § 71 Abs. 1 Hessische Gemeindeordnung (HGO) ein mit besonderen Rechten ausgestattetes Verwaltungsorgan der Gemeinde ist, steht ihm keine allgemeine fachaufsichtliche Zuständigkeit über alle Ressorts zu. Deswegen ist ein generelles Zugriffsrecht im Rahmen eines Netzwerkes durch den Bürgermeister nicht zulässig. Seine fachaufsichtlichen Befugnisse reichen nur so weit wie seine Ressortzuständigkeit. Diese wird − von Einzelfällen abgesehen − nach § 70 Abs. 2 HGO durch die Ressortzuständigkeit anderer Mitglieder des Gemeindevorstandes beschränkt.

§ 70 HGO

(1) Der Bürgermeister bereitet die Beschlüsse des Gemeindevorstands vor und führt sie aus, soweit nicht Beigeordnete mit der Ausführung beauftragt sind. Er leitet und beaufsichtigt den Geschäftsgang der gesamten Verwaltung und sorgt für den geregelten Ablauf der Verwaltungsgeschäfte. Er verteilt die Geschäfte unter die Mitglieder des Gemeindevorstands.

(2) Soweit nicht auf Grund gesetzlicher Vorschrift oder Weisung des Bürgermeisters oder wegen der Bedeutung der Sache der Gemeindevorstand im ganzen zur Entscheidung berufen ist, werden die laufenden Verwaltungsangelegenheiten von dem Bürgermeister und den zuständige Beigeordneten selbständig erledigt.

Auch die in § 70 Abs. 1 Satz 2 HGO vorgesehenen Überwachungsbefugnisse des Bürgermeisters können ein generelles Zugriffsrecht auf das Netzwerk nicht begründen; sie betreffen nur den allgemeinen Geschäftsgang, aber keine Einzelentscheidungen.

Soweit der Bürgermeister gemäß § 73 Abs. 2 Satz 1 HGO Dienstvorgesetzter aller Mitarbeiter der Gemeinde ist, obliegen ihm nur die beamtenrechtlichen Entscheidungen, die die persönlichen Angelegenheiten betreffen. Hierzu gehört die dienstliche Weisungsbefugnis nach § 70 Satz 2 HBG bzw. die entsprechenden Regelungen im BAT nicht. Weisungsberechtigt ist nur der Vorgesetzte im Sinne von § 4 Abs. 2 Satz 2 HBG. Erst wenn das Verhalten eines Mitarbeiters Anlass gibt, an der rechtmäßigen Ausführung seines Dienstes zu zweifeln, kann im Einzelfall ein weitergehendes Untersuchungsrecht aus den allgemeinen dienstrechtlichen Befugnissen des Dienstvorgesetzten hergeleitet werden. Auf § 70 HBG i.V.m. § 73 Abs. 2 Satz 1 HGO kann daher ebenfalls kein allgemeines Netzzugriffsrecht des Bürgermeisters gestützt werden.

§ 73 Abs. 2 HGO

Der Bürgermeister ist Dienstvorgesetzter aller Beamten, Angestellten und Arbeiter der Gemeinde mit Ausnahme der Beigeordneten. Durch Verordnung der Landesregierung wird bestimmt, wer die Obliegenheiten des Dienstvorgesetzten gegenüber dem Bürgermeister und den Beigeordneten wahrnimmt, wer oberste Dienstbehörde und wer Einleitungsbehörde im Sinne des Disziplinarrechts für Gemeindebedienstete ist.

§ 4 Abs. 2 HBG

Dienstvorgesetzter ist, wer für beamtenrechtliche Entscheidungen über die persönlichen Angelegenheiten der ihm nachgeordneten Beamten zuständig ist. Vorgesetzter ist, wer einen Beamten für seine dienstliche Tätigkeit Anordnungen erteilen kann.
...

§ 70 HBG

Der Beamte hat seine Vorgesetzten zu beraten und zu unterstützen. Er ist verpflichtet, die von ihnen erlassenen Anordnungen auszuführen und ihre allgemeinen Richtlinien zu befolgen. Dies gilt nicht für Beamte, die nach besonderer gesetzlicher Vorschrift an Weisungen nicht gebunden und nur dem Gesetz unterworfen sind.

Ich habe die Gemeinde aufgefordert, diese Rechtslage bei der Einrichtung von Zugriffsrechten auf das Netzwerk für den Bürgermeister zu berücksichtigen.

Auch die Anfrage eines Staatlichen Amtes für Lebensmittelüberwachung, Tierschutz und Veterinärwesen, dessen Amtsleiter einen Netzwerkszugriff auf alle Arbeitsplätze anstrebte, musste nach den gleichen Grundsätzen geprüft werden. Das bedeutet, dass eine Zugriffsbefugnis immer dann zu eröffnen ist, wenn dies zur Erfüllung fachlicher Weisungsaufgaben erforderlich ist. Für monokratisch geführte Behörden folgt aus der Vorgesetztenstellung und aus den fachlichen Weisungsbefugnissen, dass dem Amtsleiter, der im Streitfall mit dem alleinigen Entscheidungsrecht ausgestattet ist, ein Zugriff auf alle Verwaltungsdaten einzuräumen ist. Der Unterschied zur Gemeinde ergibt sich aus der fehlenden Ressortgliederung.

15.6
Volkshochschule ist und bleibt Privatsache

Die Auslage einer Liste der Teilnehmer eines Volkshochschulkurses mit Namen, Adressen und Telefonnummern ist nicht zulässig.

Wer einen Volkshochschulkurs belegt, muss in ausgelegten Teilnehmerlisten Adresse und Telefonnummer nicht allgemein bekannt geben.

Nachdem eine Leiterin von Volkshochschulkursen vergeblich versucht hatte, das Auslegen von Teilnehmerlisten mit Namen, Adressen und Telefonnummern der Teilnehmer abzuschaffen schickte sie mir den Briefwechsel mit der Volkshochschule zur datenschutzrechtlichen Überprüfung. Die Auffassung der betroffenen Volkshochschule, dass die meisten Menschen im Telefonbuch stehen und deshalb die Offenlegung von Adresse und Telefonnummer aller Kursteilnehmer kein Datenschutzproblem darstellen könne, vermag ich nicht zu teilen. Den Hinweis, dass Besucher solcher Kurse, die Probleme mit der Kursliste haben, an das Büro der Volkshochschule verwiesen werden können, halte ich für keine befriedigende Lösung.

Nach § 11 HDSG ist das Verarbeiten personenbezogener Daten zulässig, wenn es zur rechtmäßigen Erfüllung von Aufgaben und dem damit verbundenen Zweck erforderlich ist. Das Erheben von Daten durch die Volkshochschule und ihre Weitergabe an Kursleiter/Kursleiterinnen ist zur ordnungsgemäßen Durchführung von Kursen erforderlich und daher unter datenschutzrechtlichen Gesichtspunkten zulässig. Eine Weitergabe dieser Daten an alle Teilnehmer − auch mit ausgelegten Listen − kann jedoch schutzwürdige Belange der Betroffenen beeinträchtigen (§ 16 Abs. 1 HDSG). Sie ist daher nur mit schriftlicher Einwilligung aller Kursteilnehmer zulässig. Soweit Kursteilnehmer über Änderungen des Kursverlaufs informiert werden müssen, ist dies durch den Kursleiter vorzunehmen.

Ich habe deshalb die betreffende Volkshochschule aufgefordert, sicherzustellen, dass künftig keine Teilnehmerlisten mit Adressen und Telefonnummern mehr ausgelegt werden. Zur Lösung des Problems sind unterschiedliche Listen für den Kursleiter und die Auslage zu erstellen. Eine Dokumentation der Anwesenheit ist ohne großen Zeitaufwand auch durch den Kursleiter selbst möglich.

Inzwischen hat mir die Volkshochschule mitgeteilt, dass die Listen zur Auslage in den Kursen nur noch die Namen der Kursteilnehmer enthalten.

16. Personalwesen

16.1
Mitarbeiterinnen-/Mitarbeitergespräche

Die Dokumentation von kooperativen Mitarbeiter-/Mitarbeiterinnengesprächen braucht nach dem geltenden Personalaktenrecht nicht in die jeweilige Personalakte aufgenommen zu werden. Gemeinden können daher vorsehen, dass Aufzeichnungen regelmäßig nicht zu den Personalakten kommen.

Eine Kommune hat angefragt, ob die Dokumentation von Beurteilungsgesprächen, die Vorgesetzte mit Bediensteten führen, in die Personalakte aufgenommen werden muss.

In die Personalakte aufzunehmen sind in erster Linie statusbeeinflussende Personalmaßnahmen. Personenbezogene Vorgänge, die auf den Dienstbetrieb als solchen abzielen, müssen hingegen nicht dort dokumentiert werden.

§ 107 Abs. 1 Satz 2 Hessisches Beamtengesetz (HBG) bestimmt, dass zur Personalakte eines Bediensteten alle Unterlagen gehören, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Das legt nahe, Dokumentationen von Mitarbeiter- oder Mitarbeiterinnengesprächen in die Personalakte aufzunehmen. Eine allein am Normtext orientierte Betrachtung greift allerdings etwas kurz.

Vorrangiges Ziel des Personalaktenrechts ist, das Persönlichkeitsrecht der Bediensteten im Rahmen einer effektiven Verwaltung zu stärken (BRDrucks. 223/90 S. 23).

Dieser Intention würde es zuwiderlaufen, wenn informelle Mitarbeitergespräche in die Personalakte aufgenommen werden müssten; es ist ja gerade der Sinn solcher Gespräche, ein Kommunikationsforum außerhalb der dienstlichen Formalien zur Verfügung zu stellen. So heißt es denn auch in der Konzeptbeschreibung der Kommune, dass es Ziel der Mitarbeiter- und Mitarbeiterinnengespräche sei, die Qualität der Kommunikation zu verbessern.

Weiter heißt es in dem Konzept: Das kommunale Mitarbeiter- und Mitarbeiterinnengespräch und dort gemachte Aufzeichnungen seien strikt vertraulich zu behandeln; Aufzeichnungen fänden nicht Eingang in die Personalakte. Die Dokumentation verbleibe bei den jeweiligen Gesprächspartnern. Der nächst höheren Ebene sei nur mitzuteilen, ob und wann das Gespräch geführt worden sei. Weitergehende Informationen seien nur im Einvernehmen an andere Stellen weiterzugeben. Bei einem Stellenwechsel der Mitarbeiter würden die Gesprächsunterlagen vernichtet. Bei einem Wechsel der Vorgesetzen haben Vorgesetzter und Mitarbeiter zu vereinbaren, welche Bestandteile des Mitarbeiterinnen- und Mitarbeitergesprächs an den neuen Vorgesetzten weitergegeben würden. Auf dieser Grundlage werde dann ein neues Mitarbeiter- und Mitarbeiterinnengespräch geführt. Ergänzend heißt es, das Mitarbeitergespräch schaffe keine rechtserheblichen Fakten und Dokumente. Das Gespräch sei etwas anderes und daher kein Ersatz für eine formelle dienstliche Personalbeurteilung.

Damit ist prägnant ein Vorgang angesprochen, der in die Personalakte aufgenommen werden muss, nämlich formelle dienstliche Beurteilungen (BRDrucks. 223/90 S. 40). Das Mitarbeiter- und Mitarbeiterinnengespräch soll aber gerade

unterhalb dieser formalen Schwelle stattfinden. Die Vertraulichkeit dient der informationellen Selbstbestimmung. Daher ist das Konzept personalakten- und datenschutzrechtlich nicht zu beanstanden.

Dies habe ich der anfragenden Kommune mitgeteilt.

16.2
Evaluation der Lehre

Professoren von (Fach-)Hochschulen, die Vorlesungen halten, werden als öffentlich-rechtliche Funktionsträger tätig. In dieser Eigenschaft können sie sich nur auf Artikel 5 Absatz 3 Grundgesetz berufen. Evaluationsverfahren verstoßen nicht gegen das Datenschutzrecht.

Eine Fachhochschule hat mir mitgeteilt, dass Professorinnen und Professoren der Fachhochschule die Durchführung von Evaluationsverfahren als Eingriff in ihr Recht auf informationelle Selbstbestimmung und als Verstoß gegen geltendes Datenschutzrecht ansähen, und mich um Überprüfung gebeten.

Das angewandte Evaluationsverfahren basiert auf Fragebogen, die von den Studierenden zu einzelnen Veranstaltungen ausgefüllt und anschließend zentral ausgewertet wird. Gegen das Verfahren wird von Professorinnen und Professoren vorgebracht, dass die Erhebung und Verarbeitung der Daten nur zulässig sei, wenn sie individuell zugestimmt hätten. Es gebe ein aus dem Recht auf informationelle Selbstbestimmung abgeleitetes Zustimmungsverweigerungsrecht, dessen Ausübung zur Folge habe, eine Evaluation dieser Personen zu unterlassen.

Die Evaluation ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Das Lehrpersonal nimmt bei Vorlesungen amtliche Funktionen wahr. Hochschullehrer werden als öffentlich-rechtliche Amtswalter tätig. Deswegen besteht kein Ansatzpunkt, das Grundrecht auf informationelle Selbstbestimmung ins Feld zu führen. Amtswalter können sich in ihrer Eigenschaft als öffentlich-rechtliche Funktionsträger regelmäßig nicht auf Grundrechte berufen. Das gilt für das Grundrecht auf informationelle Selbstbestimmung auch im Hochschulbereich.

Soweit unter dem Gesichtspunkt verfassungsrechtlich gewollter Staatsferne Grundrechtsschutz bei Forschung und Lehre durch Art. 5 Abs. 3 Grundgesetz (GG) gewährleistet wird, sind bestimmte Formen der Evaluation möglicherweise fragwürdig. Dies zu beurteilen, fällt jedoch nicht in die Kompetenz des Datenschutzbeauftragten.

Ich habe die Fachhochschule entsprechend unterrichtet.

16.3
Zweckbindung von erhobenen Personaldaten

Wenn Anhaltspunkte für eine Straftat vorliegen, können ausnahmsweise Erkenntnisse aus dem Personalbereich in Wohngeldangelegenheiten verwertet werden.

Eine Kommune hat angefragt, ob Daten aus dem Personalbereich ausnahmsweise in einer Wohngeldangelegenheit verwertet werden dürften. Im Personalbereich lagen Anhaltspunkte für einen Betrug vor.

Ich teilte nicht die Rechtsauffassung der Kommune, dass alle Verwaltungszweige der Stadtverwaltung als eine Einheit begriffen werden können, innerhalb derer erhobene und gespeicherte Daten hin und her wandern dürfen. Jeder Verwaltungszweig darf nur die Informationen verwerten, die er für seine Zwecke erhoben und gespeichert hat. Dieser Einsicht schien die Kommune aber selbst zuzuneigen, da im Schreiben betont wurde, eine datenschutzrechtlich einwandfreie Vorgehensweise sei anzustreben.

Datenschutzrechtlich geht es um die Zweckbindung personenbezogener Daten. Grundsätzlich gilt, dass personenbezogene Daten nur für den Zweck weiterverarbeitet werden dürfen, für den sie erhoben worden sind, § 13 Abs. 1 Hessisches Datenschutzgesetz (HDSG). Erhobene Daten sind grundsätzlich auf das Verwaltungsverfahren zu beschränken, für dessen Durchführung sie erlangt worden sind. Nur ausnahmsweise darf die Zweckbindung durchbrochen werden (§ 13 Abs. 2 Satz 1 i.V.m. § 12 Abs. 2 und 3 HDSG). Eine solche Ausnahme lag hier aber vor, da Anhaltspunkte für einen Betrug gegeben waren (§ 12 Abs. 2 Nr. 4).

§ 13 Abs. 2 Satz 1 HDSG

Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, dann ist dies nur aus den in § 12 Abs. 2 und 3 genannten Gründen zulässig.

§12 Abs. 2 HDSG

Bei öffentlichen Stellen dürfen Daten im Einzelfall ohne seine Kenntnis nur erhoben werden, wenn

...

4. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben.

Die Kommune ist also datenschutzrechtlich nicht gehindert gewesen, ihren Verdacht, den sie im Personalbereich gewonnen hatte, an die Mitarbeiterinnen und Mitarbeiter der Wohngeldstelle weiterzuleiten, damit diese wegen Betrugs ermitteln konnten. Dies habe ich der Kommune mitgeteilt.

16.4
Einsichtsrecht der kommunalen Revision in Personalakten

Trotz des besonderen Schutzes von Personalaktendaten ist die kommunale Revision befugt, in Personalakten einzusehen.

Eine Kommune hatte angefragt, ob im Rahmen einer kommunalen Revision in Personalakten eingesehen werden darf.

§ 107 Abs. 3 Hessisches Beamtengesetz, der gem. § 34 Abs. 1 Satz 2 Hessisches Datenschutzgesetz (HDSG) auch für die Angestellten und Arbeiter im öffentlichen Dienst gilt, bestimmt, dass Zugang zur Personalakte nur Beschäftigte haben

dürfen, die im Rahmen der Personalverwaltung mit der Verarbeitung für Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung und Personalwirtschaft erforderlich ist. Diese Regelung ist aber nicht abschließend. Im Gesetzgebungsverfahren zu dieser Vorschrift ist besonders betont worden, dass Einsichtsrechte aufgrund anderer Rechtsvorschriften zulässig sind (BRDrucks. 223/90 S. 48). § 13 Abs. 4 HDSG regelt, dass personenbezogene Daten, die für andere Zwecke erhoben worden sind, zur Ausübung von Kontrollbefugnissen in dem dafür erforderlichen Umfang verwendet werden dürfen. Solche Kontrollrechte sind der kommunalen Revision im Rahmen der §§ 128 ff. − 132 der Hessischen Gemeindeordnung zugestanden worden.

Vor diesem Hintergrund habe ich die Kommune dahingehend informiert, dass ein Einsichtsrecht − soweit für die Aufgabenerfüllung erforderlich − für die Mitarbeiterinnen und Mitarbeiter der kommunalen Revision in Personalakten besteht.

16.5
Einsichtsrecht der Frauenbeauftragten in Beurteilungen von Stellenbewerberinnen und -bewerbern

Die Frauenbeauftragten haben ein Einsichtsrecht in Beurteilungen von Stellenbewerberinnen und Stellenbewerbern.

Eine Kommune hat angefragt, ob die Frauenbeauftragte in Beurteilungen von Stellenbewerberinnen und -bewerbern ein Einsichtsrecht hat.

Hintergrund dieser Frage war, dass Bewerber- bzw. Bewerberinnendaten oftmals Personalaktendaten i.S.d. Hessischen Beamtengesetzes sind. Diese Daten dürfen grundsätzlich nur Beschäftigte zur Kenntnis erhalten, 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 (§ 107 Abs. 3 Hessisches Beamtengesetz). Diese Vorschrift gilt gem. § 34 Abs. 1 Satz 2 HDSG für alle Bewerberinnen und Bewerber, auch für diejenigen Beschäftigten, die keine Beamten sind.

Das Personalaktenrecht ist jedoch keine abschließende Regelung. Ergänzend ist § 18 Abs. 2 Hessisches Gleichberechtigungsgesetz (HGlG) anwendbar.

§ 18 Abs. 2 HGlG

Die Frauenbeauftragte erhält auf Verlangen Einsicht in alle Akten, die Maßnahmen, an denen sie zu beteiligen ist, betreffen. Bei Personalentscheidungen erhält sie auf Verlangen auch Einsicht in Bewerbungsunterlagen einschließlich derer von Bewerberinnen und Bewerbern, die nicht in die engere Auswahl einbezogen wurden.

Aufgrund dieser Vorschrift sind die Frauenbeauftragten gesetzlich ermächtigt, in Bewerbungsunterlagen Einsicht zu nehmen. Sie sind nicht auf die Einwilligung der betreffenden Bewerberinnen und Bewerber in die Einsichtnahme in ihre Bewerbungsunterlagen angewiesen. Kopien der Unterlagen dürfen allerdings nicht erstellt werden, da sonst die Einhaltung der Löschungspflicht aus § 34 Abs. 4 HDSG kaum zu überwachen ist.

Diese Rechtslage habe ich der Kommune mitgeteilt.

17. Schulen

Prüfung des Staatlichen Schulamtes Heppenheim

Die Prüfung des Staatlichen Schulamtes Heppenheim festigte den Eindruck, dass die Umsetzung des neuen Hessischen Datenschutzgesetzes teilweise nur schleppend erfolgt.

Im Rahmen meiner Prüftätigkeit stattete ich im Berichtsjahr dem Staatlichen Schulamt Heppenheim einen Besuch ab. Inzwischen haben die hessischen Schulämter die grundlegenden Änderungen ihrer Zuständigkeitsstrukturen und des neuen Hessischen Datenschutzgesetzes weitgehend umgesetzt. Insgesamt fand ich eine Reihe von Mängeln vor, deren gravierendste ich darstellen möchte:

17.1
Verfahrensverzeichnis

Nach dem seit 1. Juni 1999 geltenden § 6 Abs. 1 Hessisches Datenschutzgesetz (HDSG) muss jede Behörde für Anwendungsprogramme, über deren Einsatz sie selbst bestimmt, ein sog. Verfahrensverzeichnis anfertigen.

§ 6 Abs. 1 HDSG

Wer für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten zuständig ist, hat in einem für den behördlichen Datenschutzbeauftragten bestimmten Verzeichnis festzulegen:

1. Name und Anschrift der datenverarbeitenden Stelle,
2. die Zweckbestimmung und die Rechtsgrundlage der Datenverarbeitung,
3. die Art der gespeicherten Daten,
4. den Kreis der Betroffenen,
5. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Art und Herkunft regelmäßig empfangener Daten,
6. die zugriffsberechtigten Personen oder Personengruppen,
7. die technischen und organisatorischen Maßnahmen nach § 10,
8. die Technik des Verfahrens,
9. Fristen für die Löschung nach § 19 Abs. 3,
10. eine beabsichtigte Datenübermittlung an Drittstaaten nach § 17 Abs. 2,
11. das begründete Ergebnis der Untersuchung nach § 7 Abs. 6 Satz 3.

Die näheren Einzelheiten hat der Hessische Innenminister in seinem Erlass vom 14. April 1999 (StAnz. 1999 S. 1226ff.) festgesetzt. Als ein solches Anwendungsprogramm muss auch die automatisierte amtliche Zeiterfassung angesehen werden. Da für keines der vom Schulamt eigenständig eingesetzten Programme ein solches Verfahrensverzeichnis vorlag, habe ich die nachträgliche Erstellung gefordert.

17.2
Vorabkontrolle

Eine weitere Neuerung brachte das Hessische Datenschutzgesetz mit § 7 Abs. 6, in dem die sog. Vorabkontrolle oder auch Technikfolgenabschätzung geregelt ist.

§ 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.

Über Einzelheiten der Durchführung der Vorabkontrolle hatte mein Amtsvorgänger schon in seinem 27. Tätigkeitsbericht unter Ziff. 2.2.3.2 berichtet. Die praktische Umsetzung bringt naturgemäß zahlreiche Detailfragen, die aus dem Gesetz heraus nicht unmittelbar beantwortet werden können, aber grundsätzliche Bedeutung haben. In Abstimmung mit dem Hessischen Innenministerium hatte ich daher ein Papier erstellt, das eine Checkliste zur Erstellung der Vorabkontrolle enthält (s. 28. Tätigkeitsbericht, Ziff. 25.1). Das Schulamt verfügt über eine Reihe von DV-Programmen, die erst nach dem Tage des Inkrafttretens des neuen Hessischen Datenschutzgesetzes eingeführt wurden. Auch hier fordere ich eine nachträgliche Durchführung dieser Vorabkontrolle. Nicht betroffen davon waren die Programme, deren Einsatz vom Hessischen Kultusministerium zentral für alle hessischen Schulämter vorgesehen waren, wie etwa das vorgefundene Programm Planpers.Kost. Für die Erstellung der dazu notwendigen Vorabkontrolle ist das Hessische Kultusministerium sachlich zuständig.

17.3
Zugang zu Personalakten

Im Rahmen der Prüfung der vom Schulamt getroffenen organisatorischen und technischen Maßnahmen zur Gewährleistung der Datensicherheit war bedeutsam, welche Mitarbeiter zu welchem Raum Zutritt haben (Verteilung der Türschlüssel). Ein System bzw. eine Übersicht war nicht verfügbar. Grundsätzlich muss sich die Zuteilung der Raumzutrittsrechte an der dienstlichen Notwendigkeit der Raumnutzung orientieren. Problematisch werden Unklarheiten in diesem Punkt vor allem bei der Verwahrung von Personalakten. Die Personalhauptakten für alle im Schulamtsbezirk tätigen Lehrkräfte sind im Archivraum des Schulamtes Heppenheim untergebracht. Wer einen Schlüssel zu diesem Raum besitzt, war nicht aufzuklären. Damit war es möglich, dass auch Mitarbeiter, die nicht mit der Personalsachbearbeitung befasst sind, Zutritt hatten. Dies verstößt jedoch gegen § 107 Abs. 3 Hessisches Beamtengesetz (HBG).

§ 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; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

Ich habe daher gefordert, eine neue Schlüsselverteilung vorzunehmen und dabei die dienstliche Notwendigkeit des Raumzutritts zu prüfen.

17.4
Schulpsychologischer Dienst

Das beim Prüftermin geführte Gespräch mit Schulpsychologen des Amtes brachte ein banal erscheinendes Problem zutage, das aber Gefahrenpotentiale enthält. Mit der edv-technischen Aufrüstung der Schulämter hat auch der Schulpsychologe die Möglichkeit, Gutachten aus seiner Tätigkeit als Psychologe automatisiert zu speichern. Dabei ist er wegen der hohen Sensibilität der Daten durch einen Erlass des Hessischen Kultusministeriums gehalten, diese Daten entweder bei der Speicherung zu verschlüsseln oder auf einer Diskette abzulegen, die wegzuschließen ist. Je nach Anwendungsprogramm ist es jedoch möglich, dass der Rechner die Texte − etwa zur zwischenzeitlichen Datensicherung − auf einer temporären Datei unverschlüsselt speichert. Dort ist der Text zunächst jedem PC-Nutzer zugänglich. Der Schulpsychologe hat daher nach der endgültigen Speicherung zu prüfen, ob die betroffenen Texte tatsächlich auch endgültig in den temporären Dateien gelöscht worden sind. Ich habe das Hessische Kultusministerium gebeten, auf diese Gefahr in einem nachfolgenden Erlass hinzuweisen.

18. Statistik

Die Gemeinden dürfen statistische Umfragen ohne Auskunftspflicht durchführen, soweit dies für Zwecke der Vorbereitung und Begründung politischer Entscheidungen erforderlich ist.

Die Gemeinde Groß-Krotzenburg hatte im Zusammenhang mit der Ausweisung neuer Baugebiete ein Umlegungsverfahren in Gang gesetzt und dazu die Grundstückseigentümer mit einem Fragebogen konfrontiert. Der Fragebogen entsprach nicht den statistikrechtlichen Anforderungen.

18.1
Statistische Umfragen

Seit über zehn Jahren ist das Hessische Landesstatistikgesetz (HessLStatG) vom 19. Mai 1987 (GVBl. I, S. 67) in Kraft. Dennoch sind immer wieder bei statistischen Umfragen Verstöße gegen die gesetzlichen Anforderungen zu verzeichnen.

Kommunen können statistische Umfragen durchführen, sofern der Magistrat oder Gemeindevorstand die Notwendigkeit für eine kommunale statistische Umfrage festgestellt hat und die statistische Geheimhaltung gewährleistet ist (§ 12 Abs. 3 bis 5 HessLStatG). Die Aufgaben der Kommunalstatistik muss einer Stelle innerhalb der Gemeindeverwaltung übertragen werden, die organisatorisch von anderen Verwaltungsstellen getrennt und räumlich sowie personell abgeschottet ist.

Während größere Städte wie Frankfurt, Wiesbaden oder Darmstadt sich eigene kommunale Statistikstellen leisten, sind derartige Organisationseinheiten in kleineren Kommunen weder personell noch organisatorisch realisierbar. Deshalb bedienen sich diese Gemeinden in der Regel externer Dienstleister, die im Auftrag der Kommune tätig werden und ein abschließendes Ergebnis präsentieren.

18.2
Probleme bei der Durchführung kommunaler Umfragen

Rechtsprobleme gibt es immer wieder im Zusammenhang mit der konkreten Durchführung eines solchen Projekts. Das beginnt in der Regel damit, dass eine Vermischung einzelner Erhebungs- und Aufbereitungsphasen zwischen Auftraggeber und Auftragnehmer erfolgt. Zum anderen werden die in eine Befragung einbezogenen Bürgerinnen und Bürger oftmals nicht oder nur unvollständig über den Zweck der Erhebung, die Datenverarbeitung sowie den Zeitpunkt der Löschung der Daten informiert. Besonders wichtig ist, dass der Auftraggeber zunächst prüft, ob überhaupt eine Befragung mit personenbezogenen Angaben für das Erhebungsziel notwendig ist oder nicht auch eine anonyme Erhebung den gleichen Erfolg verspricht.

Unabhängig vom Charakter der Datenerhebung ist der Betroffene auf die Freiwilligkeit an der Teilnahme hinzuweisen. Häufig ist festzustellen, dass dieser wichtige Hinweis unterbleibt oder aber auf dem verwendeten Fragebogen „schlecht platziert“ ist und damit dem Befragten nicht sofort in den Blick gelangt. Ein anderer Schwachpunkt, den es zu bemängeln gibt, ist die ungenügende Information zum Erhebungszweck, zur Zweckbindung und zur Weiterverarbeitung. Zum Transparenzgebot, das im § 14 HessLStatG zum Ausdruck kommt, gehört u. a. die Nennung des Auftraggebers und das Ziel, das mit der Erhebung verfolgt wird. Will die Kommune zum Beispiel ein Meinungsbild zu einem bestimmten Bauprojekt oder zu einem baurechtlichen Umlegungsverfahren erfragen und bedient sie sich hierzu eines privaten Unternehmens, so hat sie deutlich zu machen, wer Initiator der Befragung und wer verantwortlich für die Durchführung einer solchen Erhebung ist. Immer wieder kommt es vor, dass für die Betroffenen nicht ohne weiteres erkennbar ist, wer für eine entsprechende Aktion verantwortlich ist.

18.3
Umfragen mit und ohne Personenbezug

Findet die Befragung ohne Personenbezug statt, ist die Angelegenheit unproblematisch. Ist ein Personenbezug vorhanden oder aber aufgrund der erfragten Merkmale ein Personenbezug herstellbar, sind an die Datenverarbeitung erhöhte Anforderungen zu stellen. Unter anderem hat der Auftragnehmer für ausreichende Datensicherheit zu sorgen (§ 10 Abs. 2 HDSG). Vertraglich hat die Kommune bei einer Datenverarbeitung im Auftrag sicherzustellen, dass der Auftragnehmer die Erfordernisse einer ordnungsgemäßen Datenverarbeitung beachtet. Das beinhaltet sowohl den korrekten Umgang mit den personenbezogenen Fragebögen, die automatisierte Erfassung und Aufbereitung, als auch deren Auswertung und die Speicherung der Daten. Es sind insbesondere die Löschungsvorschriften einzuhalten. Selbstverständlich gehört zu den Informationspflichten, die Betroffenen darüber zu unterrichten, was mit den Erhebungsunterlagen geschieht und wann die den Personenbezug herstellenden Merkmale (Hilfsmerkmale) gelöscht werden.

18.4
Datenverarbeitung für Planungszwecke

Das Hessische Datenschutzgesetz enthält im § 32 eine Regelung, in der die Erhebung und Verarbeitung personenbezogener Daten für Planungszwecke geregelt ist. Die Entscheidung, ob die Datenerhebung für Zwecke der Planung erfolgt und damit die rechtlichen Vorgaben des § 32 HDSG greifen oder aber die Vorschriften über die Kommunalstatistik nach dem Landesstatistikgesetz heranzuziehen sind, ist zuweilen schwierig. § 32 HDSG ist auch einschlägig, wenn es um konkrete Absichten zur Umsetzung eines Vorhabens geht. Plant die Gebietskörperschaft beispielsweise den Bau eines Kindergartens, einer Umgehungsstraße oder ähnliches und will sie die Erforderlichkeit der Maßnahme anhand von Analysen und Fallzahlen untermauern, so kommt die Sonderregelung für Planungen zum Zuge. Bei eher unbestimmten, auf die Zukunft ausgerichteten Erkundungen wäre eher an die statistische Umfrage zu denken.

Letztlich sind die Voraussetzungen, die an eine rechtmäßige Datenverarbeitung gestellt werden, nicht weit von einander entfernt. Freiwilligkeit, Transparenz des Verfahrens und umfassende Information gegenüber den Auskunftgebenden sind die rechtlichen Prämissen, an denen sich derartige Verfahren stets zu orientieren haben.

18.5
Rechtliche Bewertung des von der Gemeinde Groß-Krotzenburg verwendeten Fragebogens

Der zur Versendung gekommene Fragebogen der Gemeinde hatte einige Mängel. So waren die unter 18.2 und 18.4 beschriebenen erforderlichen Maßnahmen nicht oder nur unzureichend berücksichtigt. Darauf habe ich in einer Stellungnahme hingewiesen und die für die Erhebung verantwortlichen Stellen aufgefordert, künftig datenschutzrechtlichen Erfordernissen Rechnung zu tragen.

19. Europa

Schengener Durchführungsübereinkommen

Auch im vergangenen Jahr hat die Gemeinsame Kontrollinstanz für das Schengener Informationssystem ihre Arbeit fortgesetzt. Sie hat die verschiedenen Entwicklungen im Rahmen der Integration von Schengen in die Europäische Union kritisch verfolgt, insbesondere die Errichtung einer unabhängigen Geschäftsstelle für die Kontrollinstanzen von Schengen und EUROPOL. Darüber hinaus hat sie sich mit der Kontrolle des zentralen Schengener Informationssystems (CSIS) und verschiedenen Einzelproblemen beschäftigt.

Im Berichtszeitraum nahm der Hessische Datenschutzbeauftragte − vertreten durch eine Mitarbeiterin − zugleich für die anderen Landesdatenschutzbeauftragten an verschiedenen Sitzungen der Gemeinsamen Kontrollinstanz für das Schengener Informationssystem in Brüssel teil.

Die Gemeinsame Kontrollinstanz hat ihren 4. Tätigkeitsbericht für den Zeitraum März 1999 bis Februar 2000 erstellt und auf einer Pressekonferenz im Oktober d. J. vorgestellt. Der Bericht kann im Internet (http://www.datenschutz-berlin.de) abgerufen werden. Gedruckte Einzelstücke können bei mir angefordert werden.

19.1
Fortschritte bei der Integration in die Europäische Union

Der Antrag Großbritanniens auf partielle Anwendung des sog. Schengen-Besitzstands (s. 28. Tätigkeitsbericht, Ziff. 4.1), nämlich beschränkt auf solche Bestimmungen, die sich nicht auf die Freizügigkeit beziehen, wurde mittlerweile positiv beschieden.

Für Dänemark, Finnland, Schweden sowie Norwegen und Island als durch Assoziierungsabkommen mit der Europäischen Union verbundene Staaten soll der „Schengen-Besitzstand“ Anfang 2001 in Kraft gesetzt werden, so dass sich diese Länder dann am Schengener Informationssystem beteiligen können.

Darüber hinaus hat die Einbindung von „Schengen“ in die Europäische Union auf Grund des Inkrafttretens des Amsterdamer Vertrags am 1. Mai 1999 weitere Fortschritte gemacht. Dies gilt zum einen für die im Protokoll zum Vertrag vorgesehene Zuordnung des sog. Schengener Besitzstands, also die einschlägigen Rechtsakte und Beschlüsse zum Vertrag zur Gründung der Europäischen Gemeinschaft (EGV) oder zum Vertrag über die Europäische Union (EUV). Mit der Zuordnung wird darüber entschieden, ob der Bereich wirklich vergemeinschaftet wird. Daraus ist abzuleiten, ob eine Fortschreibung oder Änderung der Rechtsvorschriften in dem im EGV vorgesehenen Verfahren durch die Organe der Europäischen Union, insbesondere unter Beteiligung des Europäischen Parlaments erfolgt, ob die Zuständigkeit des Europäischen Gerichtshofs gegeben ist oder ob es bei einer bloßen exekutiven Zusammenarbeit (EUV) bleibt. Die vom Rat der Europäischen Union getroffene Zuordnung bewirkt, dass wesentliche Teile des Schengener Durchführungsübereinkommens (Art. 92 bis 119), also die Vorschriften über das Schengener Informationssystem, die verschiedenen Ausschreibungskategorien, über die Kontrollinstanz und den Datenschutz nicht vergemeinschaftet werden, sondern der intergouvernementalen Zusammenarbeit vorbehalten bleiben.

Auch in dem nicht vergemeinschafteten Bereich ist der Rat nur begrenzt weitergekommen. Zwar ist die Zusammenlegung der Kontrollinstanzen von Schengen und EUROPOL und der noch zu schaffenden Kontrollinstanz für das Zollinformationssystem (s. 28. Tätigkeitsbericht, Ziff. 4.1) weiter betrieben worden. Ein erster Schritt ist die Zusammenlegung der Geschäftsstellen der verschiedenen Kontrollinstanzen. Die Gemeinsame Kontrollinstanz hat mit Recht immer wieder gefordert, dass die Wahrung der Unabhängigkeit für deren Geschäftsstelle oberstes Gebot ist. Sie muss aus der Hierarchie des Generalsekretariats der Europäischen Union herausgenommen und weisungsfrei sein sowie eigene Haushaltsmittel haben. Wichtig ist zudem, dass die Geschäftsstelle über eine ausreichende Anzahl kompetenter Mitarbeiter und Mitarbeiterinnen verfügt, die eigenständig Initiativen ergreifen oder rechtliche Fragestellungen ausarbeiten können.

Mittlerweile ist ein dahingehender Beschluss des Rates der Europäischen Union in Kraft getreten. Die Gemeinsame Kontrollinstanz wird kritisch verfolgen, ob die genannten Anforderungen an die Geschäftsstelle eingehalten werden.

19.2
Kontrolle des zentralen Schengener Informationssystem (CSIS)

Die Gemeinsame Kontrollinstanz hat zum dritten Mal eine Kontrolle des CSIS in Straßburg vorgenommen (s. 28. Tätigkeitsbericht, Ziff. 4.3). Veröffentlicht werden können nur Auszüge des Prüfberichts, da weite Teile als geheim eingestuft werden.

Folgende Mängel konnten u. a. festgestellt werden:

- Das CSIS ist mit Abteilungen des französischen Innenministeriums in einem Gebäude untergebracht. Die physische Trennung zwischen den Räumlichkeiten des CSIS-Personals und denen des französischen Innenministeriums sind immer noch nicht zufriedenstellend. Dies gilt insbesondere für den Raum, in dem die Magnetbänder untergebracht sind, sowie für den Panzerschrank. Das Verzeichnis der zugangsberechtigten Personen oder das Ausweislesegerät für den CSIS-Betriebsraum werden nicht regelmäßig genutzt.
- Der Datenabgleich zwischen dem CSIS und den nationalen Teilen des Schengener Informationssystems (NSIS) dauert derzeit immer noch zu lange. Der gesamte Prozess muss deshalb beschleunigt werden, um sicherzustellen, dass Unterschiede rechtzeitig ermittelt und berichtigt werden.

- Gelöschte Daten dürfen nach Art. 113 Abs. 2 Schengener Durchführungsübereinkommen zu Kontrollzwecken noch ein Jahr gespeichert bleiben. Die Prüfung ergab, dass gleichwohl in einigen Fällen nach Abschluss dieses Jahres keine Löschung erfolgte.
- Es wurde festgestellt, dass nicht nur − wie in Art. 96 Schengener Durchführungsübereinkommen vorgesehen − Drittausländer, sondern auch Bürger der Europäischen Union im Schengener Informationssystem gespeichert wurden.
- Die Gemeinsame Kontrollinstanz hat überprüft, ob die zur Personenfahndung aufgenommenen personenbezogenen Daten, wie in Art. 112 Abs. 1 Schengener Durchführungsübereinkommen vorgesehen, nicht länger als erforderlich gespeichert werden.

Art. 112 Schengener Durchführungsübereinkommen

(1) Die zur Personenfahndung in dem Schengener Informationssystem aufgenommenen personenbezogenen Daten werden nicht länger als für den verfolgten Zweck erforderlich gespeichert. Spätestens drei Jahre nach ihrer Einspeicherung ist die Erforderlichkeit der weiteren Speicherung von der ausschreibenden Vertragspartei zu prüfen.

...

(3) Die technische Unterstützungseinheit des Schengener Informationssystems weist die ausschreibende Vertragspartei mit einem Vorlauf von einem Monat automatisch auf die im System programmierte Löschung hin.

Es wurde festgestellt, dass keine der Vertragsparteien eine kürzere Frist als drei Jahre für die Überprüfung der Daten festgelegt hat. Positiv konnte festgehalten werden, dass sichergestellt ist, dass die gespeicherten Daten − wie in Art. 112 Abs. 3 Schengener Durchführungsübereinkommen vorgesehen − nach Ablauf der in der Ausschreibung vorgegebenen Frist automatisch gelöscht werden.

Zu dem Problem, dass entgegen Art. 112 Abs. 1 Schengener Durchführungsübereinkommen in Hessen zum großen Teil keine Überprüfung der gespeicherten Daten nach drei Jahren stattfindet, s. Ziff. 12.1.

19.3
Weitere Probleme

19.3.1
Erweiterung der zugriffsberechtigten Stellen

Im 27. Tätigkeitsbericht, Ziff. 3.3 hatte ich berichtet, dass in Deutschland verschiedene Verwaltungsbehörden, u. a. die für das Kraftfahrzeugregister zuständigen Stellen, Interesse geäußert haben, auf den Datenbestand des Schengener Informationssystems zugreifen zu können. Diese Entwicklung hat sich fortgesetzt; nunmehr hat Deutschland beantragt, für das Bundesamt für die Anerkennung ausländischer Flüchtlinge einen Zugriff auf die Daten nach Art. 96 des Schengener Durchführungsübereinkommens einzurichten. Das Bundesministerium des Innern hat dargelegt, dass das Bundesamt für die Anerkennung ausländischer Flüchtlinge in Deutschland für die Erteilung von Aufenthaltstiteln nach § 43a Asylverfahrensgesetz zuständig ist und damit die Voraussetzungen nach Art. 101 Abs. 2 Schengener Durchführungsübereinkommen erfüllt.

Art. 101 Abs. 2 Schengener Durchführungsübereinkommen

Zugriff auf die nach Art. 96 gespeicherten Daten mit dem Recht diese unmittelbar abzurufen, erhalten außerdem die für die Sichtvermerkserteilung zuständigen Stellen …

Dieser Auffassung ist nichts entgegen zu setzen, sodass die Liste der zugriffsberechtigten Stellen um das Bundesamt für die Anerkennung ausländischer Flüchtlinge erweitert werden wird.

19.3.2
Geltendmachung des Auskunftsrechts

Die Gemeinsame Kontrollinstanz hat festgestellt, dass die Anzahl der Anträge auf Auskunft über die zu einer Person im Schengener Informationssystem gespeicherten Daten in den einzelnen Schengen-Staaten sehr unterschiedlich ist. Deutschland und Frankreich stehen mit jeweils 400 Anträgen im letzten Jahr an der Spitze bis hin zu Ländern, in denen überhaupt keine Auskunftsanträge gestellt wurden. Für diese großen Unterschiede sind eine Reihe von Faktoren verantwortlich, insbesondere auch die Information der Betroffenen über die bestehende Rechtslage. Die Gemeinsame Kontrollinstanz hat deshalb eine Umfrage in den einzelnen Ländern gestartet mit dem Ziel zu erfahren, inwieweit die im 27. Tätigkeitsbericht unter Ziff. 3.1 beschriebene Informationskampagne „Schengen“ durchgeführt wurde. Es geht dabei insbesondere um die in allen Sprachen der Europäischen Gemeinschaft vorliegende Broschüre über die den Betroffenen zustehenden Rechte. Festgestellt werden soll, ob und an welchen Orten diese Dokumente verteilt werden und auf welche Weise dieses Verfahren verbessert werden kann.

20. Bilanz

20.1
Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (28. Tätigkeitsbericht, Ziff. 5.1)

Der im letzten Jahr dargestellte Entwurf zur Neuregelung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) hat im Mai diesen Jahres zu einer Neufassung dieses Gesetzes geführt. Zur Umsetzung dieser Novelle hat der Hessische Innenminister die zuständigen Behörden mit mehreren Einführungserlassen unterrichtet.

Neben den Rahmenbedingungen für die neu eingeführte Videoüberwachung (s. dazu Ziff. 4.1) beschäftigen sich die Erlasse mit dem neu geschaffenen Instrumentarium der Schleierfahndung und weiteren Detailänderungen.

Voraussetzung für den Einsatz von verdachts- und ereignisunabhängigen Kontrollen (Schleierfahndung) ist u. a., dass die Kontrollstellen in ein Verzeichnis aufgenommen werden. Damit soll sichergestellt werden, dass die gesetzlichen Anforderungen, vor allen über die Lageerkenntnisse dokumentiert sind (s.a. meine Forderungen im 28. Tätigkeitsbericht, Ziff. 5.1.2).

Durch die Streichung des § 20 Abs. 9 HSOG ist die Benachrichtigung über die länger als drei Jahre andauernde Speicherung in Dateien entfallen. Diese Streichung ist sehr misslich, da das Polizeirecht häufiger als in anderen Bereichen zu Eingriffen in das Recht auf informationelle Selbstbestimmung führt. Dass es bei der Benachrichtigungspflicht hinter das Niveau des allgemeinen Datenschutzrechtes zurückfällt, ist unverständlich, vor allem weil dort aufgrund der EU-Richtlinie − endlich − im Interesse der Bürgerinnen und Bürger mit der umfassenden Benachrichtigung hinreichende Transparenz geschaffen worden war.

In den Einführungserlassen ist außerdem eine Pflicht zur Berichterstattung über eingesetzte Videoüberwachungsanlagen festgelegt. Damit knüpft der Innenminister an die Debatten im Gesetzgebungsverfahren an, in denen gefordert wurde, eine Evaluierung durch die Parlamente zu ermöglichen. Für eine Evaluierung sind selbstverständlich nicht nur Informationen über die Anlässe und die Prüfung der rechtlichen Voraussetzungen für die Installation der Anlagen notwendig, sondern auch Informationen über die am Überwachungsort und im weiteren Umfeld gewonnenen Erkenntnisse. Dazu gehört auch die Frage, ob mehr als eine Verlagerung der Kriminalitätsschwerpunkte an andere Orte erreicht werden kann.

20.2
Projekt Elektronische Fußfessel
(28. Tätigkeitsbericht, Ziff. 6)

Das im letzten Jahr beschriebene Projekt ist nunmehr als Modell im Bereich des Amtsgerichtsbezirkes Frankfurt am Main angelaufen. Im Mai hat der Justizminister in einem Erlass die Rahmenbedingungen für die Teilnahme am Projekt und die notwendigen Begleitinformationen dargestellt.

Bis Ende Oktober gab es zwölf Straftäter, die zum Tragen der Fußfessel verpflichtet worden sind. Aufgrund der zunächst geringen Zahlen der Probanden ist das Forschungsprojekt teilweise neu konzipiert worden. Voraussichtlich werden mehr qualitative Einzelinterviews geführt werden als Studien über Vergleichsgruppen. Grundlage der Gespräche mit Probanden oder Familienmitgliedern ist jeweils eine Einwilligungserklärung. Die Auswertung der Akten von Vergleichsgruppen erfolgt im Rahmen der neu eingeführten Forschungsklausel des § 476 Strafprozessordnung (StPO).

§ 476 StPO

(1) Die Übermittlung personenbezogener Informationen in Akten an Hochschulen, andere Einrichtungen, die wissenschaftliche Forschung betreiben, und öffentliche Stellen ist zulässig, soweit
1. dies für die Durchführung bestimmter wissenschaftlicher Forschungsarbeiten erforderlich ist,
2. eine Nutzung anonymisierter Informationen zu diesem Zweck nicht möglich oder die Anonymisierung mit einem unverhältnismäßigem Aufwand verbunden ist und
3. das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung erheblich überwiegt.

Bei der Abwägung nach Satz 1 Nr. 3 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(2) Die Übermittlung der Informationen erfolgt durch Erteilung von Auskünften, wenn hierdurch der Zweck der Forschungsarbeit erreicht werden kann und die Erteilung keinen unverhältnismäßigen Aufwand erfordert. Andernfalls kann auch Akteneinsicht gewährt werden. Die Akten können zur Einsichtnahme übersandt werden.

Die technische Durchführung und Betreuung des Projektes liegt bei der Hessischen Zentrale für Datenverarbeitung (HZD). Sie erfasst alle telefonisch übermittelten Daten, die die Fußfessel an einen mit dem Telefon verbundenen Datenspeicher gemeldet hat. Die in der HZD auflaufenden Daten aus der Überwachung durch die elektronischen Erfassungssysteme werden dort gespeichert und derzeit bis zum Ende des jeweiligen Überwachungszeitraumes aufbewahrt. In Papierform werden die sog. Alarmmeldungen aufbewahrt, die den Projektmitarbeitern zugeleitet werden. Diese werden auch Teil der Bewährungsakte.

Eine Erörterung mit dem Ministerium, ob wirklich − wie von der Richterschaft gefordert − alle Einzelmeldungen, die über die Telefonleitung abgefragt werden, bis zum Ende der Überwachung aufbewahrt werden müssen, ist noch nicht abgeschlossen.

Eine Bewertung der Frage, ob und inwieweit durch das Tragen der elektronischen Fußfessel die erreichten Vollzugserleichterungen den Eingriff in das Recht auf informationelle Selbstbestimmung aufwiegen, kann erst nach Abschluss des Projektes bzw. Vorliegen der Forschungsergebnisse erfolgen.

20.3
Internetpräsentation von Kommunen
(28. Tätigkeitsbericht, Ziff. 9.3)

Verschlüsselung und verlässliche Authentizitätsprüfung gehören zu den wichtigsten Dauerthemen für eine moderne Verwaltung, die das Internet als Kommunikationsmedium benutzt.

Im vergangenen Jahr (28. Tätigkeitsbericht, Ziff. 9.3) hatte ich über die Internetauftritte einiger Kommunen berichtet. Dabei galt mein Augenmerk vor allem den Formularservern der Kommunen, die es den Bürgerinnen und Bürgern ermög-

lichen sollten, direkt per E-Mail mit den Kommunen Kontakt aufzunehmen. Ich hatte in diesem Zusammenhang vor allem bemängelt, dass die Kommunen den Bürgerinnen und Bürgern keine Möglichkeit zur Verfügung gestellt hatten, ihre Daten zu verschlüsseln, damit die personenbezogenen Daten nicht schutzlos übers Netz gehen. Vielfach fand nicht einmal ein Hinweis für die Nutzerinnen und Nutzer statt, dass die Daten unverschlüsselt über das Netz gehen. Damit war regelmäßig die Vertraulichkeit der Kommunikation zwischen Bürger und Verwaltung nicht gewährleistet. Im Berichtsjahr habe ich zahlreiche Homepages der Gemeinden auf diese Frage hin überprüft und festgestellt, dass sich die wenigsten Kommunen an diese Vorgaben halten. Nach der Überprüfung des Internetangebots einer mittelhessischen Kommune hat mein Einschreiten dazu geführt, dass der gesamte Formularserver vom Netz genommen wurde. Hier wurden Formulare aus dem Sozialbereich zum Ausfüllen angeboten, ohne dass es ein Verschlüsselungsangebot oder den Hinweis auf Nichtverschlüsselung gegeben hätte. Ohne einsichtigen Grund entsprachen die online angebotenen Formulare nicht einmal den amtlichen Vordrucken.

Nicht minder wichtig ist die Sicherheit, mit der Authentizitätsprüfungen verwirklicht werden. Die Verwaltung muss – da nahezu alle Verwaltungsbezeichnungen personenbezogen angelegt sind – Identität, Authentizität und die Integrität der übermittelten Daten von Antragstellern in jedem Einzelfall untersuchen. Das Signaturgesetz und die erforderlichen Änderungen in den Verwaltungsvorschriften werden es in der Zukunft voraussichtlich ermöglichen, Verwaltungsvorgänge komplett über das Internet abzuwickeln. Wenn entsprechend diesen Regelungen die technischen Möglichkeiten geschaffen werden, sind damit insgesamt die heutigen Probleme Identitätsprüfung, Authentizität des Absenders und Integrität der übermittelten Daten lösbar. Es bleibt daher zu hoffen, dass bisher bestehende Mängel angegangen und beseitigt werden, indem das Signaturgesetz oder verwandte Normierungen in der Verwaltung umgesetzt werden. Neben den strengen Vorschriften des Signaturgesetzes wird auch an vereinfachte Legitimations- und Authentizitätsfeststellungen gedacht werden müssen, die nach dem Vorbild von EC-Karten aufbereitet werden, wo die Anforderungen des Signaturgesetzes aus Kostengründen weiterhin ohne Breitenwirkung bleiben.

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

21.1
Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Für eine freie Telekommunikation in einer freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

- **Erhebliche Zunahme der Telekommunikationsvorgänge**
  Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, E-Mail und Mailboxen sowie das Internet genutzt.
- **Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten**
  - Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.
  - Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch E-Mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.
  - Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.
  - Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.
  - Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.
- **Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten**
  Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.
- **Entwicklung des Internets zum Massenkommunikationsmittel**
  Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.
- **Schwer durchschaubare Rechtslage**
  Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht macht diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: *1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802*

- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100a der Strafprozessordnung (StPO) einbezogen − der Katalog wurde seit Einführung 11-mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.
- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.
- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen „ENFOPOL“ befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation:

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urteil vom 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.
- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.
- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.
- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.
- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.
- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.
- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungsverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o.g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.
- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.
- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.
- Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

21.2

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o. Ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen haben, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.
- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind − es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann − zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden − nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollten bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.
  Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o.g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum − ausschließlich zum Zweck der Sicherung des Rechtsschutzes − aufzubewahren.
- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung).
  Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.

  Damit sind Regelungen z. B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann.

  Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.
- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.
- Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.
- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung − bei Datenübermittlungen auch bei den Datenempfängern − erstrecken.
- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.
- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.
- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

21.3

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Data Warehouse, Data Mining und Datenschutz

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im „Data Warehouse“ werden

alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. „Data Mining“ bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem „Daten-Lagerhaus“ gesammelt werden.
- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden sind. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.
- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.
- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern“ rechtswidrig.
- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). „Data Mining“ ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von „Data Warehouse“- und „Data Mining“-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

21.4
Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,
- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,
- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,
- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse“ Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

21.5
Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000

Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung „INPOL-neu“ eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur so weit eingegriffen wird, wie dies im Rahmen der Erforderlichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die „gesamte kriminelle Karriere“ jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereit gehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf „Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung“. Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die „Straftaten“, nicht die einzelne Person und auch nicht das „Gesamtbild einer Person“. Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

21.6
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26. Juni 2000

Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten „Großen Lauschangriffe“ zu unterrichten. § 100e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufende parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahmen zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen erfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem „großen Lauschangriff“ ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z. B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn − wie in den „Wire-tap-Reports“ der USA − die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten

vorzulegenden jährlichen Berichte über die nach § 100c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten „Großen Lauschangriffe“.

21.7
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 2000

Auftragsdatenverarbeitung

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises II und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern dazu auf, die für die Datenverarbeitung beim Bundeskriminalamt gesetzlich gezogenen Grenzen strikt zu beachten. Sie appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

21.8
Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Datensparsamkeit bei der Rundfunkfinanzierung

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das „Bereithalten eines Rundfunkempfangsgerätes“ anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.

21.9
Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Vom Bürgerbüro zum Internet
− Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung −

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

21.10
Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Risiken und Grenzen der Videoüberwachung

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zu einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen
- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen,
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch videotechnisch gewonnener − insbesondere biometrischer − Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.

- Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. *Dafür kommen − **soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen** − unter Anderem in Betracht*[1]*:*
  - *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden,*
  - *für die Verkehrslenkung nur Übersichtsaufnahmen,*
  - *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.*
- Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
- Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.
- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

  Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

21.11
Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Entschließung zur Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz − § 3a E-BDSG) und die Einführung des Datenschutzaudit (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

21.12
Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000

Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

[1] Die kursiv gedruckte Passage wurde bei Stimmenthaltung der Datenschutzbeauftragten der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern und Nordrhein-Westfalen angenommen.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung“ bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestimmung“ vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.
2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnnen Informationen zu löschen oder an den Betroffenen herauszugeben.
3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.
4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.
5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.
6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.
7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.
8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.

Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur − wie bisher − Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

22. Materialien

22.1
Mustervertrag zur Fernwartung zwischen öffentlichen Stellen und öffentlichen oder nicht-öffentlichen Auftragnehmern

(Stand 26. Januar 2001)

Der Mustervertrag für die Fernwartung gemäß § 4 HDSG ist im Einzelfall aufgabenspezifisch anzupassen. An nichtöffentliche Stellen darf ein Auftrag nicht vergeben werden, wenn gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse überwiegende schutzwürdige Belange entgegenstehen. Soweit spezialgesetzliche Regelungen für die Daten, die im Auftrag verarbeitet werden sollen, Anwendung finden, ist zunächst zu prüfen, ob eine Auftragsdatenverarbeitung überhaupt zulässig ist. 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, insbesondere BVB-Wartung oder BVB-Pflege, datenschutzrechtlich ergänzt werden. Die jeweiligen Vertragsbestimmungen sind dem Mustervertrag zu entnehmen. Gem. § 4 Abs. 3 Satz 2 hat der Auftraggeber den Hessischen Datenschutzbeauftragten vorab über die Beauftragung zu unterrichten.

Vereinbarung

zwischen dem/der

……

– nachstehend Auftragnehmer genannt –

und dem/der

……

– nachstehend Auftraggeber genannt –

§ 1 Gegenstand der Vereinbarung

Diese Vereinbarung umfasst folgende, vom Auftragnehmer durchzuführende Fernwartungsarbeiten:

1. Hardware-Diagnose: für folgende Hardwareprodukt(e)
2. Software-Wartung: für folgend(e) Softwareprodukt(e)

Hinweis:
Hier sind Art und Umfang der durchzuführenden Fernwartungsarbeiten, die davon betroffenen EDV-Systeme und Daten genau zu beschreiben. Beispielsweise könnte eine Hardware-Diagnose zur Vorbereitung einer Wartung erfolgen oder die Wartung einer Anwendungssoftware.

Beispiel:
2. Software-Wartung:
Behebung von Fehlerzuständen in der Anwendung xyz in der Abteilung N.

Damit verbunden sind folgende Zugriffe:
Schreibender Zugriff auf die Konfigurationsdateien …… der Anwendung xyz.
Lesender Zugriff auf die anderen Dateien im Programmverzeichnis …… der Anwendung xyz
Lesender Zugriff auf die Anwendungsdaten in den Verzeichnissen ……
Ein Zugriff auf die Datei …… wird soweit erforderlich nach Rücksprache ermöglicht.

§ 2 Verfahrensregelungen

(1) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind schriftlich zu vereinbaren.

(2) Mitteilungen der Vertragsparteien über E-Mail oder Internet werden nur akzeptiert, wenn das Schriftstück verschlüsselt übertragen wurde und mit einer digitalen Signatur versehen worden ist.

§ 3 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Fernwartung sowie für die Wahrung der Rechte der Betroffenen bleibt der Auftraggeber verantwortlich.

(2) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf der Fernwartung 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 wird dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitgeteilt.

(3) Im System des Auftraggebers werden alle Zugriffe, die für Wartungsarbeiten erfolgen, protokolliert. Die Protokollierung muss so erfolgen, dass sie in einer Revision nachvollzogen werden kann. Die Protokollierung darf vom Auftragnehmer nicht abgeschaltet werden.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten feststellt, die bei der Fernwartung aufgetreten sind oder die einen Zugriff durch Unbefugte möglich machen.

(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer führt die Fernwartung ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Er verwendet Daten, die ihm im Rahmen der Erfüllung dieses Vertrags bekannt geworden sind, nur für Zwecke der Fernwartung. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Soweit möglich, erfolgt die Fernwartung am Bildschirm ohne gleichzeitige Speicherung.

(2) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen.

(3) Der Auftragnehmer sichert die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

(4) Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen; Ausnahmen sind besonders zu begründen.

(5) Der Auftragnehmer teilt dem Auftraggeber vor Beginn der Fernwartung schriftlich oder in der Form des Abs. 2 mit, welche Mitarbeiter er dafür einsetzen wird und wie diese Mitarbeiter sich identifizieren werden. Die Mitarbeiter des Auftragnehmers verwenden hinreichend sichere Identifizierungsverfahren.

(6) Der Beginn der Fernwartung ist telefonisch anzukündigen, um den Beauftragten des Auftraggebers die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen.

(7) Fernwartungen dürfen nur von der Wartungszentrale aus vorgenommen werden, deren Sicherheitsmaßnahmen in § 7 Abs. 1 vereinbart worden sind.

(8) Der Auftragnehmer erkennt an, 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. Ergeben sich Zweifel, so gestattet der Auftragnehmer die Begehung der Räume, von denen aus die Fernwartung durchgeführt wird.

(9) Die Fernwartung von Privatwohnungen aus ist nicht gestattet. Soll im Einzelfall davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers. In diesem Fall ist der Zugang zur Wohnung durch den Auftraggeber vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(10) 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.

(11) Nicht mehr benötigte Unterlagen und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

Hinweis: Für Beweissicherung, Auskunftsansprüche oder die Revision relevant

(12) Die Einschaltung von Subauftragnehmern ist ausgeschlossen. Soll im Einzelfall davon abgewichen werden, bedarf dies der gesonderten schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer hat in diesem Falle vertraglich sicher zu stellen, 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 § 5 erfüllt hat.

(13) 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.

(14) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

(15) Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, insbesondere wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird. Die Unterbrechung kann erfolgen, wenn eine Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten festgestellt wird.

§ 5 Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, 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; im Fall des § 4 Abs. 12 S. 2 gilt das auch gegenüber dem Subunternehmer.

(3) Auskünfte an Dritte darf der Auftragnehmer nicht erteilen, Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen (§ 3 Abs. 2) erteilen.

(4) Der Auftragnehmer verpflichtet sich, bei der Fernwartung in sensiblen Bereichen, beispielsweise bei Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, nur festangestellte Mitarbeiter für Fernwartungsarbeiten einzusetzen, die nach dem Verpflichtungsgesetz verpflichtet sind.

§ 6 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. Er benachrichtigt den Auftraggeber, bevor eine angekündigte Kontrolle stattfindet.

(2) Soweit Daten in einer Privatwohnung verarbeitet werden, ist das Zugangsrecht für die Mitarbeiter 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.

§ 7 Datensicherungsmaßnahmen (Erläuterungen s. Anhang)

(1) Für die Zwecke der Vorabkontrolle des Auftragnehmers nach § 10 HDSG werden folgende technische und organisatorische Maßnahmen für die Fernwartungszentrale 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) Um die Übertragung der Daten abzusichern und unbefugte Zugriffe auf die Rechner des Auftraggebers im Rahmen der Fernwartung zu verhindern, legt der Auftraggeber folgende technische und organisatorische Maßnahmen für beide Seiten verbindlich fest:

a) Zutrittskontrolle
Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden:

……

……

……

Hinweis:
In den meisten Fällen werden im Zusammenhang mit der Fernwartung keine Maßnahmen zur Zutrittskontrolle getroffen. Es ist aber denkbar, dass der Auftragnehmer die Hardwarekomponenten (Router etc.) installiert und betreut. In diesem Fall sollten hier die Maßnahmen beschrieben werden, wann Wartungspersonal wie Zutritt zur Hardware erhält.

b) Benutzerkontrolle
Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -verfahren gehindert werden:

……

……

……

Hinweis:
Hier sind insbesondere die Maßnahmen festzulegen,
- *mit denen sichergestellt wird, dass die Fernwartung nur mit Wissen und Willen des Auftraggebers stattfindet und*
- *die Identität des Wartungspersonals festgestellt wird.*

Beispiele:
Vor einer Wartung wird das Modem durch einen berechtigten Mitarbeiter des Auftraggerbers aktiviert.

Es wird eine Benutzerkennung für das Wartungspersonal eingerichtet. Um die Wartung durchführen zu können, muss die Kennung mit dem Passwort eingegeben werden.

Es wird ein durch Chipkarten unterstütztes Challenge-Response-Verfahren zur Identifizierung des Wartungspersonals eingesetzt.

c) Zugriffskontrolle
Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

……

……

……

Hinweis:
Im § 1 des Vertrags ist der Umfang der Fernwartung festgelegt. Entsprechend dem Auftrag müssen die Zugriffsregeln für das Wartungspersonal definiert werden. Ein Zugriff auf andere Anwendungen oder Daten muss ausgeschlossen werden. Auch sind dem Wartungspersonal grundsätzlich keine Administratorrechte einzuräumen. Änderungen im Betriebssystem oder systemnaher Software sollten nur von Mitarbeitern des Auftraggebers vorgenommen werden, damit der Auftraggeber den Überblick über den Stand des Systems behält. Dies gilt umso mehr, wenn mehrere Anwendungen auf einem Rechner laufen und Änderungen im System während der Fernwartung die anderen Anwendungen beeinflussen würden.

Beispiel:
Entsprechend dem Auftragsumfang werden die Zugriffsrechte des Wartungspersonals vergeben.

d) Datenverarbeitungskontrolle
Maßnahmen, damit personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden:

……

……

……

Hinweis:
Die vorgesehen Maßnahmen müssen u. a. gewährleisten, dass die Verbindung nur zwischen der Wartungszentrale und den zu wartenden Rechnern aufgebaut werden kann. Außerdem dürfen Dritte die übertragenen Daten nicht zur Kenntnis nehmen können.

Beispiele:
Die Datenübertragung wird verschlüsselt. Es kommt das Verfahren xyz zum Einsatz.
Durch Call-Back-Verfahren wird die Verbindung zur Fernwartungszentrale aufgebaut.

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:

……

……

……

Hinweis:
Die Protokollierung ist hier vor allem als Maßnahmen zu nennen. Um die Daten mit einem vertretbaren Aufwand auswerten zu können, müssen in der Regel Tools vorhanden sein.

Beispiele:
Die Bildschirmanzeige des Wartungspersonals wird auf einer Konsole beim Auftraggeber gespiegelt.
Die übertragenen Daten werden protokolliert.

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:

……

……

……

Hinweis:
Hier können Schulungsmaßnahmen und die Revision des Verfahrens der Fernwartung festgelegt werden.

(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) Unvorhergesehene Abweichungen von Abs. 1 hat der Auftragnehmer unverzüglich mitzuteilen. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

(6) 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 Fernwartung. 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 ausdrücklich bestätigt wird.

§ 8 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.

§ 9 Vergütung

...

§ 10 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.

§ 11 Vertragsstrafe

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von …… DM vereinbart.

§ 12 Nichterfüllung der Leistung

...

§ 13 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 und von anderen Datenbeständen getrennt zu halten.

(2) Sollten Daten 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.

Hinweis:
Diese Klausel muss wegen § 11 Nr. 2 AGB gesondert vereinbart werden.

§ 14 Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Erläuterungen zu § 7 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 wird en. Im Auftrag sind insbesondere die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Auch hat der Auftraggeber zu prüfen, ob beim Auftragnehmer die nach § 10 HDSG erforderlichen Maßnahmen getroffen werden.

Werden personenbezogene Daten bei der Fernwartung zur Kenntnis genommen, 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 diesen Grundschutz-Maßnahmen und den Sicherheitszielen des HDSG dargestellt werden, sind im Internetangebot des Hessischen Datenschutzbeauftragten abrufbar; http://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, das § 10 Abs. 2 HDSG genügt, müssen die einzelnen Maßnahmen im Vertrag gemeinsam festgelegt werden. Dabei sind wiederum die in § 10 Abs. 2 HDSG genannten Sicherheitsziele zu erreichen. Entsprechend dem Katalog sind die einzelnen Maßnahmen in den Vertrag zu über-

nehmen. 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: Es müssen Maßnahmen ergriffen werden, die ein − unberechtigtes − Eindringen in zu wartende Rechner soweit möglich verhindern. Dabei kann die Lösung vom einfachen Ausschalten des Modems bis zu technisch hochwertigen Challenge-Response-Verfahren gehen, die auf Chipkarten die geheimen Schlüssel speichern. Fallweise kann es nötig werden zu erkennen, ob und wie unberechtigte Personen versuchen einzudringen. Technische Komponenten, die dies feststellen können, sind Firewalls oder Intrusion Detection Systeme.
- Abhören der Kommunikation: Zum Schutz gegen unberechtigtes Abhören sind die Daten, die bei der Fernwartung übertragen werden zu verschlüsseln.
- Anmeldeprozeduren: Die Anmeldung im System oder der zu wartenden Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.

22.2
Dienstliche und private Nutzung von E-Mail und www

Bei der Nutzung der Internetdienste E-Mail und www entstehen eine Reihe datenschutzrechtlicher Fragen, die in nachfolgendem Papier diskutiert sind. Die Zulassung privater Nutzung erfordert die Einwilligung jedes Bediensteten in die Verarbeitung seiner Daten.

Umfang und Inhalt des Regelungsbedarfs für die Nutzung der Internetdienste (E-Mail, www, etc.) hängen von folgenden Faktoren ab:

- ob nur eine dienstliche oder auch eine (eingeschränkte) private Nutzung zugelassen werden soll,
- ob und ggf. an welchen Orten, in welchem Umfang und zu welchem Zweck eine Protokollierung bei E-Mail (z. B. Absender und Empfänger, Zeitpunkt der Versendung, Größe des Objekts) und www (z. B. Zeitpunkt und Inhalt des Aufrufs von Internetseiten) erfolgen soll und wie lange die Protokolle aufbewahrt werden sollen und
- welche organisatorischen Vorgaben für die Abarbeitung und damit auch die Kenntnisnahme von ein- und ausgehender dienstlicher E-Mail gemacht werden sollen.

22.2.1
Dienstliche Nutzung von E-Mail −
Verarbeitung von Verbindungsdaten durch die Dienststelle

Bei E-Mail werden auf dem E-Mail-Server Verbindungsdaten zu jeder E-Mail aufgezeichnet, d. h. wer wohin wann und in welcher Größe eine E-Mail versendet. Diese Daten können mit dem Ende der Verbindung gelöscht oder auch längerfristig gespeichert werden (programmabhängig). Eine Speicherung der Verbindungsdaten der E-Mail-Verbindung kann z. B. zum Zwecke der Fehlersuche oder der Missbrauchskontrolle erforderlich sein oder werden. In diesem Fall bestehen gegen eine Speicherung keine grundsätzlichen Bedenken. Die Zwecke der Protokollierung richten sich nach den Bedürfnissen der Dienststelle (z. B. Missbrauchskontrolle, Fehlersuche, Nachweis von Postein- und -ausgängen). Jede Dienststelle hat aufgrund der konkret bei ihr gegebenen Situation über die Zwecke und die Erforderlichkeit der Protokollierung sowie über die Dauer der Speicherung der Protokolldaten zu entscheiden. Die Protokolle dürfen nur zu dem festgelegten Zweck ausgewertet werden und nur solange gespeichert bleiben, wie es für diesen Zweck notwendig ist (§§ 13 Abs. 5, 34 Abs. 6 HDSG).

Darüber hinaus werden beim Speichern von E-Mails auf dem Arbeitsplatzrechner zusammen mit dem Inhalt Verbindungsdaten gespeichert. Für Umfang, Zweck und Dauer der Speicherung dieser Daten gilt Entsprechendes.

22.2.2
Dienstliche und private Nutzung von E-Mail

22.2.2.1
Verarbeitung von Verbindungsdaten durch die Dienststelle

Ist auch die private Nutzung von E-Mail erlaubt, ergeben sich zahlreiche Rechtsprobleme, insbesondere sind das Fernmeldegeheimnis (§ 85 Telekommunikationsgesetz) und die Regelungen des Teledienste-Datenschutzgesetzes (§ 6 TDDSG) zu beachten. Der Arbeitgeber wird mit der Zulassung der privaten Nutzung Diensteanbieter im Sinne des TDDSG. Er darf Verbindungsdaten nicht dauerhaft speichern; das TDDSG erlaubt eine Speicherung, soweit sie erfolgt, um dem Nutzer die Inanspruchnahme des Dienstes zu ermöglichen, und zu Abrechnungszwecken. Ist für die Aufrechterhaltung des Dienstes, z. B. für die Fehlersuche und -behebung, eine Protokollierung erforderlich, so darf sie auch erfolgen (§ 6 Abs. 1 Nr. 1 TDDSG).

Sind bereits bei der Zulassung der privaten Nutzung Einschränkungen gemacht worden (z. B. im Umfang oder Empfängerkreis oder im Hinblick auf eine Vermeidung der Behinderung des Dienstbetriebes), so muss die Prüfung der Einhaltung

dieser Einschränkungen möglich sein. Hierfür ist aber die Einwilligung der Nutzer erforderlich. Die Einwilligung der Beschäftigten kann weder kollektivrechtlich (sprich: durch Vereinbarung mit dem Personalrat) noch durch die konkludente Anerkennung einer Nutzungsordnung erfolgen. Mit jedem Mitarbeiter und jeder Mitarbeiterin muss eine schriftliche Vereinbarung über die Bedingungen der Nutzung der E-Mail für private Zwecke geschlossen werden, in der aber auf die Bedingungen der Nutzungsordnung verwiesen werden kann. In der Nutzungsordnung muss die Dienststellenleitung insbesondere auch festlegen, welche Überprüfungen vom Administrator oder von der Dienststellenleitung wahrgenommen werden. Die Vereinbarung muss (ggf. durch Verweis auf die Nutzungsordnung) den Umfang des Verzichts auf die Rechte beschreiben − z. B. die mögliche Kenntnisnahme des Inhalts privater E-Mails durch den Administrator, soweit dies zur Missbrauchskontrolle, oder durch den Vertreter, soweit dies zur Wahrnehmung der Vertretungsaufgaben notwendig ist. Unabhängig davon dürfen diejenigen Mitarbeiter und Mitarbeiterinnen, die aus dienstlichen Gründen den Inhalt einer privaten E-Mail zur Kenntnis erhalten, den Inhalt nicht verwenden und vor allem keine Informationen darüber weitergeben. Die Speicherung von Protokolldaten im erforderlichen Umfang ist zu den genannten Zwecken zulässig.

Die Auswertung der Protokolldaten wird in der Regel ein Administrator für die Dienststelle vornehmen. Es ist zulässig, dass dieser beauftragt wird, auch die Beachtung der Einschränkungen für die private Nutzung zu überprüfen. Das Fernmeldegeheimnis wird durch die Information der Dienststellenleitung z. B. über einen Verstoß gegen die Einschränkungen der privaten Nutzung nicht verletzt. Der Diensteanbieter (sprich die Dienststelle und die von ihr beauftragten Mitarbeiter/innen) ist für die Beachtung des Fernmeldegeheimnisses verantwortlich. Zu empfehlen ist jedoch, dass ein Administrator, der einen einmaligen Verstoß gegen die Einschränkungen der privaten E-Mail-Nutzung feststellt, zunächst den Betroffenen selbst direkt anspricht. Inwieweit eine Information an die Dienststellenleitung erfolgen muss, ist in dem Auftrag festzulegen, den die Dienststellenleitung dem Administrator erteilt.

22.2.2.2
Kenntnisnahme der Inhalte privater E-Mails durch die Dienststelle

Die Dienststelle ist weder verpflichtet, private E-Mail zuzulassen, noch für jeden Mitarbeiter und jede Mitarbeiterin zwei Adressen einzurichten. Ist die private Nutzung von E-Mail erlaubt, dürfen **die Inhalte** privater E-Mails grundsätzlich von der Dienststelle nicht zur Kenntnis genommen werden. Sofern dienstliche und private E-Mails aus technischen Gründen nicht unterschiedlich behandelt werden können (z. B. weil sie an die gleiche dienstliche E-Mail-Adresse gerichtet sind), würde das bedeuten, dass ohne vorherige Nutzungsvereinbarung mit den Mitarbeitern und Mitarbeiterinnen sämtliche E-Mails rechtlich zwingend nach den für die private E-Mail geltenden Rechtsvorschriften zu verarbeiten sind. Dies würde allerdings eine erhebliche Erschwerung für die Verarbeitung dienstlicher E-Mails mit sich bringen, z. B. weil eine Weiterleitung der E-Mails an die Vertretung und Kontrollen nicht zulässig wären. Damit würden legitime Interessen der Dienststelle beeinträchtigt. Um dienstliche Mitteilungen zu bearbeiten, müssen die Vertreter und Vertreterinnen ermächtigt werden, alle eingehenden E-Mails zu öffnen. Sobald der persönliche Inhalt einer E-Mail erkannt wird, ist die Nachricht zu schließen.

Auch durch die Einrichtung einer dienstlichen und einer privaten E-Mail-Adresse kann eine Kenntnisnahme des Inhalts privater E-Mails durch Dritte nicht vollständig ausgeschlossen werden. Der Administrator ist in jedem Fall technisch in der Lage, den Inhalt privater E-Mails zur Kenntnis zu nehmen. Deshalb kann auch in dieser Konstruktion das Fernmeldegeheimnis nicht vollständig gewahrt werden.

Ist die private Nutzung zugelassen, eine Trennung von der dienstlichen Nutzung aber nicht möglich oder nicht vorgesehen, so erfordert der Dienstbetrieb die Einwilligung des privaten Nutzers in die Verarbeitung seiner Daten (siehe oben). Die Dienststelle muss dann jeden Mitarbeiter, der die Einwilligung verweigert, von der privaten Nutzung ausschließen. Ohne Einwilligung der Betroffenen ist die Aufrechterhaltung des Dienstbetriebes unmöglich, da die Öffnung privater E-Mails das Fernmeldegeheimnis verletzen und gegen die Verarbeitungsregeln des TDDSG verstoßen würde. Die Beschäftigten müssen daher ausdrücklich einwilligen (§ 3 Abs. 1 TDDSG). Das Teledienste-Datenschutzgesetz verbietet dem Dienstanbieter zwar, die Erbringung des Teledienstes von der Einwilligung des Nutzers in zusätzliche Datenverarbeitung abhängig zu machen, das gilt jedoch nur, soweit der Dienstanbieter eine Monopolstellung innehat (§ 3 Abs. 3 TDDSG). Letzteres trifft auf den Arbeitgeber nicht zu, denn er ist nicht verpflichtet, den Bediensteten die Nutzung des Internets überhaupt zu ermöglichen.

22.2.3
Dienstliche und private Nutzung des www:
Verarbeitung von Verbindungsdaten/Kenntnisnahme des Inhalts aufgerufener Internetseiten durch die Dienststelle

Für die Protokollierung des Aufrufs von Internet-Seiten gilt Entsprechendes. Eine Protokollierung des Aufrufs von Internet-Seiten kann in der Dienststelle u. U. an mehreren Orten erfolgen. Nicht nur auf Servern oder Firewalls, sondern auch am Arbeitsplatz werden Daten über aufgerufene Internetseiten − je nach Einstellung der Browser − gespeichert. Bei der Protokollierung ist eine Trennung nach dienstlicher und privater Nutzung des Internet technisch nicht möglich. Für jede Protokollierung müssen insbesondere der Zweck (Datensicherheit, Fehlersuche, Missbrauchskontrolle), der Umfang und die Dauer der Speicherung festgelegt werden.

Eine Vollprotokollierung aller Internetzugriffe der Mitarbeiter zur laufenden Verhaltens- und Leistungskontrolle ist unverhältnismäßig und daher unzulässig.

Sofern eine private Nutzung des Internet zugelassen wird, bedarf es hierfür individueller Nutzungsvereinbarungen. Insofern gelten die Ausführungen zu 22.2.2 und 22.2.3 entsprechend.