

**Vierunddreißigster Tätigkeitsbericht
des
Hessischen Datenschutzbeauftragten
Professor Dr. Michael Ronellenfitsch**

**vorgelegt zum 31. Dezember 2005
gemäß § 30 des Hessischen Datenschutzgesetzes
vom 7. Januar 1999**

Inhaltsverzeichnis

Abkürzungsverzeichnis

Register der Rechtsvorschriften

Kernpunkte

- 1. Einführung**
- 2. Datenschutzbeauftragte**
 - 2.1 Hessischer Datenschutzbeauftragter
 - 2.1.1 Allgemeines
 - 2.1.1.1 Rechtsstellung
 - 2.1.1.2 Aufgabenstellung
 - 2.1.2 Neue Aufgaben
 - 2.1.2.1 Hessisches Umweltinformationsgesetz
 - 2.1.2.2 Hessisches Informationsfreiheitsgesetz
 - 2.1.2.3 Privater Bereich
 - 2.1.3 Unabhängigkeit des Hessischen Datenschutzbeauftragten und Instrumente der Neuen Verwaltungssteuerung
 - 2.2 Behördliche Datenschutzbeauftragte
 - 2.2.1 Ergebnisse einer Untersuchung zu Rechtsstellung und Aufgaben behördlicher Datenschutzbeauftragter
- 3. Europa**
 - 3.1 Allgemeines
 - 3.2 14. Wiesbadener Forum Datenschutz
 - 3.3 Gemeinsame Kontrollinstanz für das Schengener Informationssystem
 - 3.3.1 Entwicklungen des Schengener Informationssystems
 - 3.3.2 Gemeinsame Überprüfungen der Ausschreibungen zu Drittausländern
 - 3.3.3 Auswirkungen der gemeinsamen Überprüfung in Hessen
 - 3.4 Gemeinsame Kontrollinstanz für EUROPOL
 - 3.4.1 Verbesserter Zugang zu Dokumenten
 - 3.4.2 Stellungnahme zu Analysedateien
 - 3.4.3 Prüfung der Rechtmäßigkeit einer etwaigen Speicherung
 - 3.4.4 Prüfung der Abkommen mit Drittstaaten
 - 3.4.5 Kontrolle von EUROPOL
- 4. Bund**
 - 4.1 Rechtsprechung des Bundesverfassungsgerichts zum Kernbereich privater Lebensgestaltung

- 4.1.1 Konsequenzen für das Land Hessen
- 4.2 Einführung des E-Passes
- 4.3 Fußball-Weltmeisterschaft 2006
 - 4.3.1 Allgemeine Sicherheitsfragen
 - 4.3.2 Eintrittstickets
 - 4.3.3 Akkreditierung
- 5. Land**
 - 5.1 Hessischer Landtag**
 - 5.1.1 Datenschutzbeauftragte für Fraktionen im Hessischen Landtag
 - 5.2 Justiz**
 - 5.2.1 Moderne Justiz, Datenschutz und richterliche Unabhängigkeit
 - 5.2.2 Verwechslungsgefahr bei Insolvenzbekanntmachungen im Internet
 - 5.3 Polizei und Strafverfolgung**
 - 5.3.1 Erfahrungen mit der Videoüberwachung, insbesondere in Frankfurt am Main
 - 5.3.2 Gelöscht und doch nicht gelöscht – Prüfung von Polizeidatenbeständen
 - 5.3.3 Mangelndes Auskunftsverhalten der Staatsanwaltschaft bei dem Landgericht Frankfurt
 - 5.3.4 Mangelnder Informationsaustausch zwischen Polizei und Justiz
 - 5.4 Verfassungsschutz**
 - 5.4.1 Novellierung des Verfassungsschutzgesetzes
 - 5.4.2 Gemeinsames Informations- und Analysezentrum für die Polizei und das Landesamt für Verfassungsschutz
 - 5.5 Verkehrswesen**
 - 5.5.1 Inhalt von Führerscheinakten – Speicherung im örtlichen Fahrerlaubnisregister
 - 5.5.2 Nutzung von Bankverbindungsdaten aus der Kfz-Zulassung
 - 5.6 Schulverwaltung**

- 5.6.1 Neuerungen im Schulgesetz
- 5.6.2 Folgerungen der IT-Sicherheitsleitlinie für die Schulen

- 5.7 Bibliotheken**
- 5.7.1 Speicherung von Lesernamen bei Bibliotheken

- 5.8 Gesundheitswesen**
- 5.8.1 Elektronische Speicherung und Langzeitarchivierung von Krankenakten im Krankenhaus
- 5.8.2 Aktuelle Entwicklung des Neugeborenen-Screenings
- 5.8.3 Rahmenbedingungen für den Aufbau von Biobanken
- 5.8.4 Unzulässige Verarbeitung von Versichertendaten in Vietnam
- 5.8.5 Schuleingangsuntersuchungen – Informationsbedarf der hessischen Gesundheitsämter kommt einem Wildwuchs gleich
- 5.8.6 Neue Datenverarbeitungsprojekte des Medizinischen Dienstes der Krankenversicherung Hessen
- 5.8.7 Datenschutzrechtliche Probleme der Auftragsdatenverarbeitung für die Erfassung von ärztlichen Gutachten des Medizinischen Dienstes der Krankenversicherung Hessen

- 5.9 Sozialwesen**
- 5.9.1 Hartz IV – Vorlage von Kontoauszügen
- 5.9.2 Unzulässiger Inhalt von Wohngeld-Antragsformularen
- 5.9.3 Datenschutzrechtliche Rahmenbedingungen im Bereich der Jugendgerichtshilfe

- 5.10 Personalwesen**
- 5.10.1 E-Beihilfe
- 5.10.2 Datenschutzrechtliche Begleitung der Einführung der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung

- 5.10.3 Bekanntgabe von Bediensteten, die Altersteilzeit beantragt haben, an den Personalrat
- 5.10.4 Datenübermittlung durch den polizeiärztlichen Dienst an die Polizeiverwaltung
- 5.11 Finanzwesen**
- 5.11.1 Darf das Finanzamt Geschäftspost an die Privatanschrift des Einzelunternehmers versenden?
- 6. Kommunen**
- 6.1 Forderungsmanagement von Kommunen
- 6.2 Prüfung des Online-Abrufs von Privaten aus dem Liegenschaftskataster
- 6.3 Wahlstatistik
- 7. Sonstige Selbstverwaltungskörperschaften**
- 7.1 Hochschulen**
- 7.1.1 Datenschutzrechtliche Fragen bei der Privatisierung des Universitätsklinikums Gießen und Marburg
- 7.1.2 Anwendung der IT-Sicherheitsleitlinie des Landes auf die Hochschulen
- 7.2 Sparkassen**
- 7.2.1 Prüfung der Netzwerksicherheit bei Sparkassen
- 8. Entwicklungen und Empfehlungen im Bereich der Technik und Organisation**
- 8.1 Sachstand zur Zentralisierung der IT
 - 8.1.1 Übergreifende Aspekte
 - 8.1.2 Verschlüsselung
 - 8.1.3 Signatur
 - 8.1.4 Dokumentenmanagementsystem
 - 8.1.5 Stand Ende des Jahres
- 8.2 Sachstand zur Einführung eines Dokumentenmanagementsystems in der hessischen Landesverwaltung
 - 8.2.1 Allgemeines
 - 8.2.2 Einführungsstrategie in Stufen
 - 8.2.3 Vorabkontrolle

- 8.2.4 Sachstand
- 8.3 Probleme der Passwortverwaltung in Rechenzentren
 - 8.3.1 Der Fall
 - 8.3.2 Ausgangslage
 - 8.3.3 Lösungsansätze
 - 8.3.4 Fazit
- 8.4 Telearbeitsplätze in der Hessischen Landesverwaltung
 - 8.4.1 Technische Ausstattung/Konfiguration
 - 8.4.2 Zusätzliche Ergebnisse der Prüfungen vor Ort
 - 8.4.3 Fazit
- 8.5 Orientierungshilfe „Mobile Netze“
 - 8.5.1 Technische Aspekte
 - 8.5.2 Rechtliche Aspekte
- 8.6 Voice over IP (VoIP) – weit mehr als Internet-Telefonie
 - 8.6.1 Was ist VoIP?
 - 8.6.2 Gefährdungen
 - 8.6.3 Fazit
- 8.7 Kein Kopierschutz bei Internetveröffentlichungen
 - 8.7.1 Ausgangslage
 - 8.7.2 Technischer Kopierschutz
 - 8.7.3 Fazit
- 9. Bilanz**
- 9.1 Vorratsdatenspeicherung durch Telekommunikations-, Tele- und Mediendienstanbieter
(33. Tätigkeitsbericht, Ziff. 4.2.1)
- 9.2 Datenübermittlungen an Parteien zu Wahlwerbezwecken aus dem Einwohnermelderegister
(32. Tätigkeitsbericht, Ziff. 8.3)
- 9.3 Videoüberwachung in öffentlichen Verkehrsmitteln
(31. Tätigkeitsbericht, Ziff. 3.1.3)
- 9.4 Datenbankprotokolle im Einwohnerwesen
(33. Tätigkeitsbericht, Ziff. 6.4)
- 9.5 Neue Rechtsgrundlagen zur DNA-Analyse im Strafverfahren
(32. Tätigkeitsbericht, Ziff. 5.2; 5.3; 20.10)
- 10. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder**

- 10.1 Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck
- 10.2 Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006
- 10.3 Einführung der elektronischen Gesundheitskarte
- 10.4 Einführung biometrischer Ausweisdokumente
- 10.5 Appell der Datenschutzbeauftragten des Bundes und der Länder:
Eine moderne Informationsgesellschaft braucht mehr Datenschutz
- 10.6 Keine Vorratsdatenspeicherung in der Telekommunikation
- 10.7 Gravierende Datenschutzängel beim Arbeitslosengeld II endlich beseitigen
- 10.8 Telefonbefragungen von Leistungsbeziehern von Arbeitslosengeld II datenschutzgerecht gestalten
- 10.9 Telefonieren mit Internet-Technologie (Voice over IP – VoIP)
- 10.10 Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden
- 10.11 Unabhängige Datenschutzkontrolle in Deutschland gewährleisten
- 10.12 Sicherheit bei E-Government durch Nutzung des Standards OSCI

Organisationsplan des Hessischen Datenschutzbeauftragten

Sachwortverzeichnis

Abkürzungsverzeichnis

ABl. des HKM	Amtsblatt des Hessischen Kultusministeriums
Abs.	Absatz
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaften
BA	Bundesagentur für Arbeit
bDSB	behördlicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfGE	Entscheidungssammlung der Bundesverfassungsgerichtsurteile
bzw.	beziehungsweise
CSIS	Zentrales Schengener Informationssystem
d. J.	dieses Jahres
DFB	Deutscher Fußball-Bund
DMP	Disease-Management-Programm
DMS	Dokumentenmanagementsystem
DNA	Desoxyribonucleinacid (Desoxyribonucleinsäure)
DoS	Denial of Service
DRM	Digital Rights Management
DSB	Datenschutzbeauftragter
DSL	Digital Subscriber Line
DV	Datenverarbeitung
DVO	Zweite Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens
EG	Europäische Gemeinschaft
etc.	et cetera
EU	Europäische Union
EURODAC	Europäisches Fingerabdrucksystem (Européen und Dactyloscopie)
EUROJUST	Europäische Stelle zur justiziellen Zusammenarbeit
EUROPOL	Europäisches Polizeiamt

E-Pass	elektronischer Pass
ff.	fortfolgende/r/s
FIFA	Fédération Internationale de Football Association (Internationaler Fußballverband)
GG	Grundgesetz
ggf.	gegebenenfalls
HArchivG	Hessisches Archivgesetz
HBG	Hessisches Beamtenengesetz
HDSG	Hessisches Datenschutzgesetz
HKG	Hessisches Krankenhausgesetz
HMdI	Hessisches Ministerium des Innern und für Sport
HMG	Hessisches Meldegesetz
HPVG	Hessisches Personalvertretungsgesetz
HSchulG	Hessisches Schulgesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HUIG-E	Entwurf des Hessischen Umweltinformationsgesetzes
HVwVG	Hessisches Verwaltungsvollstreckungsgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
ICAO	International Civil Aviation Organisation
ICMP	Internet Communication Message Protocol
IfSG	Infektionsschutzgesetz
inkl.	inklusive
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IT	Informationstechnik
JGG	Jugendgerichtsgesetz
Kfz	Kraftfahrzeug
KGRZ	Kommunales Gebietsrechenzentrum
KoopA ADV	Koordinierungsausschuss Automatisierte Datenverarbeitung
KWG	Kommunalwahlgesetz
LTDrucks.	Landtagsdrucksache
LWO	Landeswahlordnung

MESTA	Mehrländer-Staatsanwaltschafts-Automation
MRZ	Machine Readable Zone
NJW	Neue Juristische Wochenschrift
NSIS	Nationales Schengener Informationssystem
NVS	Neue Verwaltungssteuerung
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OSCI	Online Services Computer Interface
PDA	Personal Digital Assistant
pdf	Portable Document Format (Dateiformat)
PDV 300	Ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit
PIN	Personal Identification Number
POLAS-HE	Polizeiliches Auskunftssystem Hessen
PTLV	Präsidium für Technik, Logistik und Verwaltung
RFID	Radio Frequency Identification
SAP R/3	In der Hessischen Landesverwaltung eingesetzte Standardsoftware zur Unterstützung betriebswirtschaftlicher Funktionen wie z. B. internes und externes Rechnungswesen, Materialwirtschaft und Personalverwaltung
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SIP	Session Initiation Protocol
SMS	System Management Server
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSO	Single-Sign-On
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
SUS	System Update Server
TC	Trusted Computing
TCP/IP	Transmission Control Protocol/Internet Protocol
TDDSG	Teledienstedatenschutzgesetz

TKG	Telekommunikationsgesetz
u. a.	unter anderem
UK-Gesetz	Gesetz über die Errichtung des Universitätsklinikums Gießen und Marburg
URL	Uniform Resource Locator
vgl.	vergleiche
VoIP	Voice over IP (Internet Protocol)
VPN	Virtual Private Network
WLAN	Wireless Local Area Networks
WM	Weltmeisterschaft
WoGG	Wohngeldgesetz
WStatG	Wahlstatistikgesetz
WSUS	Windows Server Update Services
z. B.	zum Beispiel
Ziff.	Ziffer
ZPO	Zivilprozessordnung

Register der Rechtsvorschriften

AO	Abgabenordnung 1977 vom 16. März 1976 (BGBl. I S. 613, berichtigt BGBl. 1977 I S. 269) in der seit dem 1. September 2002 geltenden Neufassung vom 1. Oktober 2002 (BGBl. I S. 3866)
BDSG	Bundesdatenschutzgesetz in der Fassung vom 14. Januar 2003 (BGBl. I S. 66)
BGB	Bürgerliches Gesetzbuch in der Fassung vom 2. Januar 2002 (BGBl. I S. 42), zuletzt geändert durch Gesetz vom 7. Juli 2005 (BGBl. I S. 1970)
DSO-HLT	Datenschutzordnung des Hessischen Landtags vom 5. April 1995 (Anlage 3 zur GO-HLT)
DVO	Zweite Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens vom 22. Februar 1935 (RGBl. I S. 215), zuletzt geändert durch Verordnung vom 23. Mai 1986 (GVBl. I S. 197)
EUROPOL-Übereinkommen	Übereinkommen auf Grund von Art. K.3 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts (EUROPOL-Übereinkommen) vom 26. Juli 1995 (ABl. der EG Nr. C 316/25), ergänzt durch Beschluss des Rates vom 3. Dezember 1998 (ABl. der EG 1999 Nr. C 26, S. 21)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. I S. 1), zuletzt geändert durch Art. 96 Gesetz zur Änderung des Grundgesetzes vom 26. Juli 2002 (BGBl. I S. 2863)
GO-HLT	Geschäftsordnung des Hessischen Landtags vom 16. Dezember 1993 (GVBl. I S. 628), zuletzt geändert durch Beschluss des Landtags vom 16. Juni 2004 (GVBl. I S. 223)
HArchivG	Hessisches Archivgesetz vom 18. Oktober 1989 (GVBl. I S. 270), zuletzt geändert durch Art. 1 ÄndG vom 10. März 2002 (GVBl. I S. 34)
HBeihVO	Hessische Beihilfenverordnung in der Fassung vom 5. Dezember 2001 (GVBl. I S. 491, ber. S. 564), zuletzt geändert durch Zehnte ÄndVO vom 15. September 2005 (GVBl. I S. 642)
HBG	Hessisches Beamtengesetz in der Fassung vom 11. Januar 1989 (GVBl. I S. 25), zuletzt geändert durch Art. 26a KommunalisierungsG vom 21. März 2005 (GVBl. I S. 229)
HDSG	Hessisches Datenschutzgesetz in der Fassung vom 7. Januar 1999 (GVBl. I S. 98)

HFraktG	Gesetz über die Rechtsstellung und Finanzierung der Fraktionen im Hessischen Landtag (Hessisches Fraktionsgesetz) vom 5. April 1993 (GVBl. I S. 106)
HessVwVG	Hessisches Verwaltungsvollstreckungsgesetz vom 4. Juli 1966 (GVBl. I S. 151) in der Fassung vom 27. Juli 2005 (GVBl. I S. 574)
HKHG	Hessisches Krankenhausgesetz 2002 in der Fassung vom 6. November 2002 (GVBl. I S. 662), zuletzt geändert durch Art. 4 FinanzausgleichsÄndG 2005 vom 20. Dezember 2004 (GVBl. I S. 462)
HMG	Hessisches Meldegesetz in der Fassung vom 19. März 1999 (GVBl. I S. 274)
HPVG	Hessisches Personalvertretungsgesetz vom 24. März 1988 (GVBl. I S. 103), zuletzt geändert durch Art. 16 Zweites Verwaltungsstrukturreformgesetz vom 20. Dezember 2004 (GVBl. I S. 506)
HSchG	Hessisches Schulgesetz in der Fassung vom 29. November 2004 (GVBl. I S. 330)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung in der Fassung vom 14. Januar 2005 (GVBl. I S. 14), zuletzt geändert durch Gesetz vom 17. Oktober 2005 (GVBl. I S. 674, 676)
HVG	Hessisches Gesetz über das Liegenschaftskataster und die Landesvermessung vom 2. Oktober 1992 (GVBl. I S. 453) in der Fassung vom 20. Dezember 2004 (GVBl. I S. 506)
HVwVG	Hessisches Verwaltungsvollstreckungsgesetz in der Fassung vom 27. Juli 2005 (GVBl. I S. 574)
IFG	Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz) vom 5. September 2005 (BGBl. I S. 2722)
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz) in der Fassung vom 20. Juli 2000 (BGBl. I 2000, S. 1045), zuletzt geändert durch Gesetz vom 5. November 2001 (BGBl. I S. 2960)
IT-Sicherheitsleitlinie	StAnz. 2004, S. 3829
JGG	Jugendgerichtsgesetz in der Fassung der Bekanntmachung vom 11. Dezember 1974 (BGBl. I S. 3427), zuletzt geändert durch Vereinfachung und Vereinheitlichung der Verfahrensvorschriften zur Wahl und Beurteilung ehrenamtlicher Richter vom 21. Dezember 2004 (BGBl. I S. 3599)
Kriterienkatalog	Katalog zur Einführung von alternierender Telearbeit

	im Bereich der hessischen Landesverwaltung (StAnz. 2003 S. 2748)
KWG	Hessisches Kommunalwahlgesetz in der Fassung vom 1. April 2005 (GVBl. I S. 197)
LfV-Gesetz	Gesetz über das Landesamt für Verfassungsschutz vom 19. Dezember 1990 (GVBl. I S. 753), zuletzt geändert durch Gesetz vom 30. April 2002 (GVBl. I S. 82)
LWO	Landeswahlordnung in der Fassung vom 26. Februar 1998 (GVBl. I S. 101, 167), zuletzt geändert durch Verordnung vom 25. April 2002 (GVBl. I S. 110)
PassG	Passgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert durch Art. 13 des Gesetzes zur Umbenennung des Bundesgrenzschutzes in Bundespolizei vom 21. Juni 2005 (BGBl. I S. 1818)
PDV 300	Ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit (StAnz. 2003 S. 4235)
Planungshandbuch zum Produkthaushalt	Produktorientierte Haushaltsaufstellung Planungshandbuch für Produkthaushalt 2007, Version 1.0, Stand 2. Dezember 2005
PrüffristVO	Verordnung über Prüffristen bei gefahrenabwehrbehördlicher und polizeilicher Datenspeicherung (Prüffristenverordnung) vom 26. Juni 1996 (GVBl. I S. 322), zuletzt geändert durch die Verordnung zur Änderung polizeirechtlicher Vorschriften vom 1. Dezember 2004 (GVBl. I S. 393)
SDÜ	Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juli 1985 zwischen den Regierungen der Staaten der Benelux- Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen vom 19. Juli 1990 – Schengener Durchführungsübereinkommen (BGBl. II 1993 S. 1013)
SGB I	Erstes Buch Sozialgesetzbuch - Allgemeiner Teil - vom 11. Dezember 1975 (BGBl. I S. 3015), zuletzt geändert durch Art. 2 Gesetz zur Vereinbarung der Verwaltungsverfahren im Sozialrecht (Verwaltungsvereinfachungsgesetz vom 21. März 2005 (BGBl. I S. 818)
SGB II	Zweites Buch Sozialgesetzbuch - Grundsicherung für Arbeitsuchende - vom 24. Dezember 2003 (BGBl. I S. 2954, 2955), zuletzt geändert durch Art. 4 Abs. 35 Gesetz zur Neuorganisation der Bundesfinanzverwaltung und zur

	Schaffung eines Refinanzierungsregisters vom 22. September 2005 (BGBl. I S. 2809)
SGB VIII	Achtes Buch Sozialgesetzbuch - Kinder und Jugendhilfe - in der Fassung der Bekanntmachung vom 8. Dezember 1998 (BGBl. I S. 3546), zuletzt geändert durch Gesetz zur Weiterentwicklung der Kinder- und Jugendhilfe (Kinder- und Jugendhilfeweiterentwicklungsgesetz - KICK) vom 8. September 2005 (BGBl. I S. 2729)
SGB X	Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - in der Fassung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Art. 9 Gesetz zur Organisationsreform in der gesetzlichen Rentenversicherung vom 9. Dezember 2004 (BGBl. I S. 3242)
SGB XII	Zwölftes Buch Sozialgesetzbuch - Sozialhilfe - vom 27. Dezember 2003 (BGBl. I S. 3022), zuletzt geändert durch Art. 1, 2 Gesetz zur Änderung des Gesetzes zur Einordnung des Sozialhilferechts in das Sozialgesetzbuch vom 9. Dezember 2004 (BGBl. I S. 3305)
StPO	Strafprozessordnung in der Fassung vom 7. April 1987 (BGBl. I S. 1074, ber. S. 1319), zuletzt geändert durch das Gesetz zur Novellierung der forensischen DNA-Analyse vom 12. August 2005 (BGBl. I S. 2360)
StVG	Straßenverkehrsgesetz vom 19. Dezember 1952 (BGBl. I S. 837), zuletzt geändert durch das Dritte Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer straßenverkehrsrechtlicher Vorschriften vom 14. August 2005 (BGBl. I S. 2412)
TDDSG	Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz) vom 22. Juli 1997 (BGBl. I S. 1870) zuletzt geändert durch Art. 3 des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 14. Dezember 2001 (BGBl. I S. 3721)
TerrorBekämpfG	Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 9. Januar 2002 (BGBl. I S. 361)
TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190)
UK-Gesetz	Gesetz über die Errichtung des Universitätsklinikums Gießen und Marburg vom 16. Juni 2005 (GVBl. I S. 432)

UIG	Umweltinformationsgesetz in der Fassung vom 8. Juli 1994 (BGBl. I S. 1490), zuletzt geändert durch das Gesetz zur Neugestaltung des Umweltinformationsgesetzes und zur Änderung der Rechtsgrundlagen zum Emissionshandel vom 22. Dezember 2004 (BGBl. I S. 3704)
Umweltinformationsrichtlinie des Europäischen Parlaments und des Rates	Richtlinie 2003/4/EG des Europäischen Parlaments und Rates vom 28. Januar 2003 über den Zugang der Öffentlichkeit zu Umweltinformationen und zur Aufhebung der Richtlinie 90/313/EWG des Rates
Verordnung EG Nr. 2252/2004 des Rates	Verordnung über Normen und Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten vom 13. Dezember 2004 (Amtsblatt der Europäischen Union vom 29. Dezember 2004 L 385/1)
WoGG	Wohngeldgesetz in der Fassung vom 7. Juli 2005 (BGBl. I S. 2029), zuletzt geändert durch Art. 4 Abs. 16 des Gesetzes vom 22. September 2005 (BGBl. I S. 2809)
WStatG	Wahlstatistikgesetz in der Fassung vom 21. Mai 1999 (BGBl. I S. 1023), zuletzt geändert durch Erstes Gesetz zur Änderung des Wahlstatistikgesetzes vom 17. Januar 2002 (BGBl. I S. 412)
ZPO	Zivilprozessordnung in der Fassung vom 5. Dezember 2005 (BGBl. I S. 3202)

Kernpunkte

1. Der Hessische Datenschutzbeauftragte steht durch den technischen Fortschritt ermöglichten Effektivitätssteigerungen auf dem Verwaltungssektor positiv gegenüber. Die Einführung der Neuen Verwaltungssteuerung darf aber nicht dazu führen, dass in die Unabhängigkeit oder das originäre Aufgabenspektrum des Hessischen Datenschutzbeauftragten eingegriffen wird (Ziff. 2.1.3).
2. Auch ist es der Landesregierung verwehrt, ihre öffentlichen Aufgaben so zu organisieren, dass sie der vorgesehenen unabhängigen Kontrolle durch den Hessischen Datenschutzbeauftragten entzogen sind. Das Hessische Datenschutzgesetz ist so konzipiert, dass eine „Flucht ins Privatrecht“ nichts an der Kontrollkompetenz des Hessischen Datenschutzbeauftragten ändert (Ziff. 2.1.2.3).
3. In der modernen Informationsgesellschaft, die die Hessische Landesregierung nachdrücklich fördern will, muss das Grundrecht auf informationelle Selbstbestimmung durch ein Verständnis der grundrechtlich ebenfalls verbürgten Informationsfreiheit ergänzt werden, das den freien Zugang zu behördlichen Informationen sichert. Dieses Kommunikationsgrundrecht ist das notwendige Gegengewicht zum staatlichen Informationsmonopol. Dadurch entstehen Kollisionen zwischen der informationellen Selbstbestimmung und der Informationsfreiheit. Die Aufgabe der Sicherstellung des informationellen Gleichgewichts und des Ausgleichs bei Grundrechtskollisionen sollte wegen des Sachzusammenhangs dem Hessischen Datenschutzbeauftragten zuwachsen (Ziff. 2.1.2).
4. Das Bundesverfassungsgericht hat seine Rechtsprechung zum Schutz des Kernbereichs privater Lebensgestaltung vor staatlichen Eingriffen bekräftigt. Diese erfordert – wie ich bereits im 33. Tätigkeitsbericht moniert habe – eine Novellierung des HSOG (Ziff. 4.1).
5. Die Fußball-Weltmeisterschaft 2006 wirft nicht nur organisatorisch und sicherheitspolitisch, sondern auch datenschutzrechtlich vielfältige Fragen auf, an deren Lösung ich mitgewirkt habe (Ziff. 4.3).
6. Die Nutzung neuer Medien für die Bekanntmachung von Informationen, die bislang in Registern zur Einsicht vorgehalten wurden, erfordert viel Fingerspitzengefühl im Hinblick auf

die erforderlichen Datenschutzabwägungen. Dies gilt sowohl bei der Auswahl der Informationen, die bei der Internetveröffentlichung des Insolvenzregisters eingestellt werden (Ziff. 5.2.2), als auch bei der Kontrolle der Einhaltung von Auflagen, die für einen Online-Abruf aus dem Liegenschaftskataster zur Konkretisierung der Berechtigung für einzelne Abrufe gemacht wurden (Ziff. 6.2). Die Konzeption von Internetveröffentlichungen muss berücksichtigen, dass es einen wirksamen Kopierschutz für dieses Medium derzeit nicht gibt (Ziff. 8.7).

7. Im Bereich von Polizei und Strafverfolgung führte das mangelnde Auskunftsverhalten der Staatsanwaltschaft bei dem Landgericht Frankfurt zu einer förmlichen Beanstandung (Ziff. 5.3.3). Bei der Prüfung von Polizeidatenbeständen wurde offenbar, dass das Konzept der Hessischen Polizei zur Löschung von personenbezogenen Daten nach Abschluss eines Verfahrens und Ablauf der verfügbaren Aufbewahrungsfrist wegen technischer Mängel in der Praxis nicht funktioniert (Ziff. 5.3.2).
8. In Schulen wird eine Vielfalt personenbezogener Daten verarbeitet, was sowohl rechtliche als technische Regelungen erfordert, um Datenschutzanforderungen gerecht zu werden. Die Novelle des Hessischen Schulgesetzes habe ich zum Anlass genommen, über die aus datenschutzrechtlicher Sicht wichtigsten Änderungen zu informieren (Ziff. 5.6.1). Zur Umsetzung der IT-Sicherheitsleitlinie in den Schulen wird das Hessische Kultusministerium auf meinen Vorschlag hin Muster für die Schulen entwickeln (Ziff. 5.6.2).
9. Im Gesundheitswesen gibt es eine breite Palette datenschutzrechtlicher Probleme: Einen besonders eklatanten Datenschutzverstoß stellt die Verarbeitung von Versichertendaten im Rahmen eines sog. Disease-Management-Programmes in Vietnam dar (Ziff. 5.8.4). Das Neugeborenen-Screening in Hessen ist noch immer nicht datenschutzgerecht umgesetzt (Ziff. 5.8.2). Bei der elektronischen Speicherung und Archivierung von Krankenakten in Krankenhäusern sind vielfältige Probleme zu lösen, um die Unterlagen beweiskräftig auch über lange Zeiträume verfügbar zu halten (Ziff. 5.8.1).
10. Dem E-Government-Konzept des Landes mit seinen Zentralisierungs- und Standardisierungsansätzen musste ich einen Großteil meiner Arbeitskapazität widmen. Die Beiträge zur Zentralisierung der IT (Ziff. 8.1) und zu den einzelnen Teil-Projekten E-Beihilfe, das die elektronische Bearbeitung von Beihilfeanträgen von Landesbediensteten einführt

(Ziff. 5.10.1), zum Einsatz von SAP R/3 HR für die Personalverwaltung der Landesbediensteten (Ziff. 5.10.2) und zur Einführung des Dokumentenmanagementsystem DOMEA (Ziff. 8.2) nehmen deshalb einen breiten Raum in diesem Tätigkeitsbericht ein. Das E-Government-Konzept des Landes steht und fällt generell mit der datenschutzgerechten Gestaltung der eingesetzten Schlüsseltechnologien. Hieran arbeiten die Landesregierung und ich weiterhin intensiv zusammen.

1. Einführung

Der Datenschutz ringt noch um seine sachadäquate Positionierung in der modernen Informations- und Kommunikationsgesellschaft. Einerseits gilt es, die ständig wachsenden Gefahren für die informationelle Selbstbestimmung und die sonstigen Persönlichkeitsrechte der Betroffenen abzuwehren und zu bewältigen und den viel beschworenen „gläsernen Menschen“ zu verhindern. Andererseits hat die grundrechtlich gewährleistete Informationsfreiheit durch die technischen Zugriffsmöglichkeiten der breiten Bevölkerung auf ein nahezu unerschöpfliches Reservoir an Informationen eine Dimension erlangt, die noch vor wenigen Jahren unvorstellbar war. Aufgabe des Datenschutzes ist es auch, aktiv dazu beizutragen, dass niemand an der Informationsbeschaffung gehindert wird, weil er zugleich einen Eingriff in die informationelle Selbstbestimmung befürchten oder sich um die Datensicherheit Sorgen machen muss. Zwischen dem Recht, vor rechtswidrigen Datenzugriffen verschont zu werden und dem Recht auf ungehinderten Zugang zu allgemein zugänglichen Informationen wächst der Datenschutz in eine Rolle hinein, die über die bisherige abwehrgeprägte Funktion hinausgeht. Kompetenzrechtlich ist dem erst in Ansätzen Rechnung getragen. Diese Ansätze werden unter Ziff. 2 skizziert.

Schwerpunktmäßig betrifft dieser Tätigkeitsbericht aber naturgemäß die Wahrnehmung meiner abwehrrechtlichen Befugnisse im öffentlichen Bereich. Hier ist es um den Datenschutz nach wie vor nicht schlecht bestellt, obwohl auch hier der Neigung entgegengetreten werden muss, das technische „Machbare“ auch zu machen und sich dann an die Verschiebung der Toleranzschwelle zu gewöhnen. Maßnahmen zur Terrorismusbekämpfung dürfen nicht zu Freiheitseinbußen werden, die Wasser auf die Mühlen derjenigen ist, die uns die Freiheitlichkeit unserer Rechts- und Gesellschaftsordnung gerade übel nehmen.

Der vorliegende Tätigkeitsbericht beginnt dementsprechend mit einigen allgemeinen Bemerkungen zur Rechts- und Aufgabenstellung und Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten. Daran schließt ein Überblick über die europäische Entwicklung des Datenschutzes an. Auf Bundesebene ist vor allem über die Rechtsprechung des Bundesverfassungsgerichts zum Kernbereich privater Lebensgestaltung mit Ausstrahlungen auf das Land Hessen zu berichten. Einen Schwerpunkt dieses Tätigkeitsberichts machen wieder datenschutzrechtlich relevante Fragestellungen in Hessen im Bereich des Landtags, der Justiz, der Polizei und des Verfassungsschutzes, des Verkehrswesens, der Schulen, des Gesundheitswesens, des Sozialwesens, der Kommunen und Selbstverwaltungskörperschaften sowie auf den Gebieten

des Personal- und Finanzwesens aus. Ein weiterer Schwerpunkt liegt auf der Darstellung der Entwicklungen und den Empfehlungen im Bereich der Technik und Organisation und insbesondere dem E-Government-Konzept des Landes. Den Abschluss bilden wieder der Bilanzbericht und die Entschlüsse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die vom Hessischen Datenschutzbeauftragten mitverantwortet werden.

2. Datenschutzbeauftragte

2.1

Hessischer Datenschutzbeauftragter

2.1.1

Allgemeines

Die Entwicklung der Rahmenbedingungen des Datenschutzes gab schon in meinem 33. Tätigkeitsbericht Anlass für klarstellende Bemerkungen zur Aufgabenstellung und Kontrollzuständigkeit des Hessischen Datenschutzbeauftragten. Die neuesten Entwicklungen machen es wiederum erforderlich, die Grundlagen der Rechts- und Aufgabenstellung des Hessischen Datenschutzbeauftragten in Erinnerung zu rufen.

2.1.1.1

Rechtsstellung

Der auf Vorschlag der Landesregierung vom Landtag für die Dauer der jeweiligen Wahrperiode gewählte Hessische Datenschutzbeauftragte steht in einem öffentlich-rechtlichen Amtsverhältnis. Er ist verpflichtet, sein Amt gerecht zu verwalten und die Verfassung des Landes Hessen und das Grundgesetz für die Bundesrepublik Deutschland getreulich zu wahren. (§ 21 Abs. 1, 2, 3 Satz 1, Abs. 4 Satz 1 HDSG). Als oberste Landesbehörde ist der Hessische Datenschutzbeauftragte in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen (§ 22 HDSG). Dem Hessischen Datenschutzbeauftragten ist vom Präsidenten des Landtags die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen, die im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen ist. Die Beamten und sonstigen Beschäftigten werden auf Vorschlag des Hessischen Datenschutzbeauftragten ernannt, deren Dienstvorgesetzter er ist und an dessen Weisungen sie ausschließlich gebunden sind (§ 31 HDSG).

Diese rechtlichen Vorgaben sind auch bei der Umsetzung der Neuen Verwaltungssteuerung und der Neugestaltung des behördlichen Haushaltswesens verbindlich (vgl. Ziff. 2.1.3), wobei ich keineswegs beabsichtigte, unter Berufung auf meine Unabhängigkeit für mein Haus sinnvolle organisatorische und haushaltmäßige Neuerungen zu blockieren.

2.1.1.2

Aufgabenstellung

Der Hessische Datenschutzbeauftragte hat in Konkretisierung der allgemeinen Aufgabe nach § 1 Abs. 2 HDSG, die Ausführung des Hessischen Datenschutzgesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen, zahlreiche spezielle Aufgaben eigen- oder fremdinitiiert wahrzunehmen:

- Gemäß § 24 Abs. 1 Satz 1 HDSG überwacht er, dem gesetzlichen **Schutzzweck** des § 1 Abs. 1 Nr. 1 HDSG Rechnung tragend, die Einhaltung der datenschutzrechtlichen Vorschriften bei den Daten verarbeitenden Stellen. Wer der Überwachung des Hessischen Datenschutzbeauftragten im Einzelnen unterliegt, wurde im 33. Tätigkeitsbericht unter Ziff. 2.2 dargestellt.
- Im Zusammenhang mit der vorstehenden Überwachungsfunktion kann der Hessische Datenschutzbeauftragte Empfehlungen zur Verbesserung des Datenschutzes geben, insbesondere kann er die Landesregierung und einzelne Minister sowie die übrigen Daten verarbeitenden Stellen in Fragen des Datenschutzes **beraten** (§ 24 Abs. 1 Satz 2 HDSG). Die Beratungsfunktion beinhaltet die Beratung von Behörden und Institutionen z. B. bei der datenschutzgerechten Einführung oder Änderung von IT-Verfahren und in organisatorischen Fragen, durch die Bereitstellung von Orientierungshilfen und Mustern oder in Form der Durchführung von Schulungen; sie besteht aber auch in Stellungnahmen und Anregungen in Normsetzungsverfahren.
- Die Beratungsfunktion erstreckt sich auch auf die **Bürgerinnen und Bürger**, die über die Entwicklungen im Bereich der automatisierten Datenverarbeitung und ihre Auswirkungen auf die informationelle Selbstbestimmung informiert werden müssen, damit sie die Rechte aus den §§ 18 bis 20 und 28 HDSG effektiv wahrnehmen können.
- Aus der in § 25 Abs. 1 HDSG normierten Berechtigung des Landtags und der Landesregierung, den Hessischen Datenschutzbeauftragten mit der Erstattung von **Gutachten** und der Durchführung von **Untersuchungen** in Datenschutzfragen und Fragen des freien

Zugangs zu Informationen zu betrauen, ergibt sich dessen korrespondierende Aufgabenstellung.

- Über die Koordinierungsaufgabe nach § 24 Abs. 4 Satz 1 HDSG hinaus zählen zu den Aufgaben des Hessischen Datenschutzbeauftragten **Koordinierungsleistungen** wie die Arbeit in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und in deren Arbeitskreisen sowie in europäischen und internationalen Gremien.
- Gemäß § 24 Abs. 2 Satz 1 HDSG beobachtet der Hessische Datenschutzbeauftragte die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der Daten verarbeitenden Stellen. Hierbei hat er insbesondere darauf zu achten, dass die automatisierte Datenverarbeitung nicht zu einer Verschiebung in der **Gewaltenteilung** zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und kommunalen Selbstverwaltung führen (§ 24 Abs. 2 Satz 2 i. V. m. § 1 Abs. 2 Nr. 2 HDSG).
- Weitere Aufgaben des Hessischen Datenschutzbeauftragten ergeben sich im Zusammenhang mit der **Berichtspflicht** gegenüber Landtag und Landesregierung nach § 30 Abs. 1 HDSG.

2.1.2

Neue Aufgaben

In Ihrer Stellungnahme zu meinem 33. Tätigkeitsbericht betont die Landesregierung die Segnungen der Informations- und Kommunikationstechnik, die den Bürgerinnen und Bürgern einen schnellen und unkomplizierten Zugang zu Informationen aller Art und zur Kommunikation ohne räumliche Grenzen ermögliche. Auch ich sehe die Vorteile des freien Informationszugangs, der im Übrigen die bislang getrennten Grundrechte der Meinungsäußerungsfreiheit und Informationsfreiheit in Art. 5 Abs. 1 Satz 1 GG zu einem einheitlichen Kommunikationsgrundrecht verknüpft. Die informationelle Selbstbestimmung ist daher ambivalent und darf nicht nur aus der Schrankenperspektive gesehen werden. Daraus wachsen dem Hessischen Datenschutzbeauftragten die in der Einleitung skizzierten neuen Aufgaben im Hinblick auf die freie Informationsbeschaffung zu. Wenn Hessen seiner Vorreiterrolle im Datenschutzbereich weiterhin gerecht werden will, muss es bei der Definition der

Aufgabenstellung des Hessischen Datenschutzbeauftragten diese neuen Entwicklungen berücksichtigen.

2.1.2.1

Hessisches Umweltinformationsgesetz

Die Umweltinformationsrichtlinie des Europäischen Parlaments und des Rates vom 28. Januar 2003 (2003/4/EG) erfordert eine Umsetzung durch den hessischen Landesgesetzgeber, weil das Umweltinformationsgesetz des Bundes ausschließlich den Zugang zu Umweltinformationen gegenüber informationspflichtigen Stellen des Bundes, nicht jedoch des Landes regelt.

Der Referentenentwurf eines Hessischen Umweltinformationsgesetzes (HUIG-E) vom 14. Februar 2005 enthielt folgende Regelung:

§ 11 HUIG-E

(1) Zur Wahrung des Rechts auf Zugang zu Umweltinformationen nimmt der oder die Landesbeauftragte für den Datenschutz die Aufgabe des oder der Landesbeauftragten für den Informationszugang wahr.

(2) Jeder hat das Recht, die oder den Landesbeauftragten anzurufen.

(3) Die Regelungen des Hessischen Datenschutzgesetzes über die Aufgaben und Befugnisse des oder der Landesbeauftragten für den Datenschutz finden entsprechende Anwendung.

(4) Die Vorschriften über den gerichtlichen Rechtsschutz bleiben unberührt.

Die mit mir abgestimmte Begründung hierzu lautete:

„Diese Vorschrift setzt den Gedanken der bürgernahen Verwaltung um. Informationssuchende, die der Auffassung sind, dass ihr Informationersuchen zu Unrecht abgelehnt, nicht oder nur unzureichend beantwortet wurde, sollen nicht allein auf die Beschreitung des formalen Verwaltungsrechtswegs verwiesen werden. Der oder die Informationsbeauftragte für Umweltinformationen soll ähnlich wie ein Ombudsmann agieren können und die Möglichkeit

haben, Akten und sonstige Umweltinformationen einzusehen und zu beurteilen, ob die Stelle, bei der die Umweltinformation angefordert wurde, die richtige Ermessenentscheidung gefällt hat. Als neutrale Stelle kann er sich einerseits bei den angefragten Stellen für die Durchsetzung von berechtigten Umweltinformationsansprüchen einsetzen, andererseits aber auch die Gründe für eine berechnigte Ablehnung dem Informationssuchenden wegen seiner Neutralität glaubwürdiger darlegen als die betroffene Stelle selbst. Es steht zu erwarten, dass die Einschaltung des Informationszugangsbeauftragten hilft, die Zahl der Verwaltungsstreitverfahren zu verringern.

Das Amt des Umweltinformationszugangsbeauftragten dem Hessischen Datenschutzbeauftragten zu übertragen, bietet sich schon deshalb an, weil es in vielen Fällen um den Widerstreit zwischen dem Recht auf Informationszugang und dem Recht auf Geheimhaltung von schutzwürdigen Daten geht, also eine Güterabwägung mit Datenschutzinteressen oder ähnlichen schützenswerten Geheimhaltungsinteressen erfolgen muss. Hier könnte das vorhandene Wissen einer bereits bestehenden Institution genutzt werden. Die Erfahrungen der Länder, die eine solche Institution für das allgemeine Recht auf Informationszugang geschaffen und diese bei den jeweiligen Landesdatenschutzbeauftragten angesiedelt haben, sind durchweg positiv. Überträgt man diese – allerdings außerhalb des Umweltbereichs – gesammelten Erfahrungen, kann die Aufgabe mit dem derzeit beim Hessischen Datenschutzbeauftragten vorhandenen Personalbestand mit bewältigt werden.“

In meiner Stellungnahme zum Gesetzentwurf vom 21. März 2005 habe ich nur eventualiter die Aussage im letzten Absatz des vorstehenden Zitats dahingehend relativiert, dass keine Aussagen zu dem zu erwartenden Aufwand getroffen werden könnten und hinzugefügt:

„Sollte die Praxis zeigen, dass der derzeitige Personalbestand meines Hauses nicht ausreicht, um die mit der neuen Aufgabe verbundene zusätzliche Arbeit zu erledigen, erwarte ich die Unterstützung der Landesregierung für eine entsprechende Anpassung.“ Diese Aussagen dürfte von der Landesregierung als Forderung um Personalaufstockung missverstanden worden sein. Durch meinen Vorschlag sollte gerade nicht die Bürokratisierung (in meinem Hause) vorangetrieben und der Verwaltungsapparat aufgebläht werden, sondern ein Beitrag zur Entbürokratisierung im Land Hessen geleistet werden. Die Kabinettsvorlage zum Entwurf für ein Hessisches Umweltinformationsgesetz vom Dezember 2005 sieht gleichwohl die Institution eines oder einer Umweltinformationsbeauftragten nicht mehr vor. Dies ist schon mit Rücksicht auf Art. 6 Abs. 1 der Umweltinformationsrichtlinie ein untauglicher ein Schlag gegen das „Beauftragtenunwesen“ am untauglichen Objekt. Im sensiblen Umweltinformationsbereich soll

lediglich die gebotene Befriedungsaufgabe einem institutionalisierten Beauftragten übertragen werden. Die Wahrnehmung dieser Befriedungsaufgabe ist nach dem Wegfall des Widerspruchsverfahrens in der Kabinettsvorlage umso wichtiger, will man die vermeintliche Entbürokratisierung nicht mit einer gesteigerten Beanspruchung der Verwaltungsgerichtsbarkeit erkaufen.

Ich rege daher an, meinen ursprünglichen Vorschlag weiterzuverfolgen.

2.1.2.2

Hessisches Informationsfreiheitsgesetz

Das in der Stellungnahme der Landesregierung zu meinem 33. Tätigkeitsbericht zum Ausdruck gebrachte Bekenntnis zur modernen Informations- und Kommunikationsgesellschaft lässt es nur folgerichtig erscheinen, dass das Land Hessen wieder Anschluss an die Spitzengruppe der Länder findet, die den freien Informationszugang gewährleisten und ähnlich wie auch der Bund ein Informationsfreiheitsgesetz erlässt. Im Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz – IFG) vom 5. September 2005 (BGBl. I S. 2722) ist geregelt, dass jeder den Bundesbeauftragten für die Informationsfreiheit anrufen kann, wenn er sein Recht auf Informationszugang als verletzt ansieht (§ 12 Abs. 1). Die Aufgabe des Bundesbeauftragten für die Informationsfreiheit wird nach § 13 Abs. 2 IFG vom Bundesbeauftragten für den Datenschutz wahrgenommen. Eine vergleichbare Regelung drängt sich aus den unter Ziff. 2.1.2.1 aufgeführten Gründen für des Land Hessen auf. Auch insoweit ist davon auszugehen, dass der Hessische Datenschutzbeauftragte diese neue Aufgabe im Rahmen seiner Kapazitäten effektiv und sachgerecht wahrnehmen könnte.

2.1.2.3

Privater Bereich

Ob die Aufgabenstellung und Zuständigkeit des Hessischen Datenschutzbeauftragten auf den privaten Bereich erstreckt werden sollte, kann hier dahinstehen, da gegenwärtig eine derartige Übertragung in Hessen nicht ansteht. Zumindest erscheint es jedoch geboten, den öffentlichen

Bereich weiterhin funktional zu bestimmen und nicht durch lediglich formale Privatisierungen die Aufgabenstellung des Hessischen Datenschutzbeauftragten auszuhöhlen. Folglich darf der Anwendungsbereich des Hessischen Datenschutzgesetzes nicht zu eng gezogen werden. Das Gesetz gilt nicht nur für Behörden und sonstige öffentliche Stellen des Landes, der kommunalen Gebietskörperschaften sowie für die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren – auch privatrechtliche – Vereinigungen (§ 3 Abs. 1 Satz 1 HDSG). Vielmehr gilt nach § 3 Abs. 1 Satz 2 HDSG dieses Gesetz auch für nichtöffentliche Stellen, soweit sie „hoheitliche“ Aufgaben unter Aufsicht der vorgenannten Stellen wahrnehmen. Zweck des Gesetzes war es, wie aus der Begründung der Vorschrift eindeutig hervorgeht, die „Flucht ins Privatrecht“ zu verhindern. Die „hoheitlichen“ Aufgaben sind demzufolge nicht nur die obrigkeitlich durch Befehl und Zwang wahrzunehmenden Aufgaben, sondern die originär staatlichen Aufgaben, derer sich die öffentliche Hand durch eine materielle Privatisierung nicht entledigen kann. Originäre Staatsaufgaben sind Aufgaben, die der Staat nach seinem Verfassungsverständnis erfüllen muss. Hier wäre es anachronistisch, allein die Aufgaben als originäre Staatsaufgaben einzuordnen, die nur durch hoheitliche Eingriffe erfüllt werden können. Dem modernen Staat obliegen auch Leistungsaufgaben. Angesprochen sind insbesondere die Aufgaben der öffentlichen Daseinsvorsorge. Der Staat bzw. die kommunalen Selbstverwaltungskörperschaften müssen kraft Verfassungsauftrags Träger der Daseinsvorsorge sein. Welche Aufgaben das im Einzelnen sind, lässt sich nicht ein für allemal festlegen, weil es keinen abschließenden Katalog der öffentlichen Aufgaben gibt. Das schließt jedoch eine Bestandsaufnahme nicht aus. In diesem Sinn kann man sich auf die Bereiche einigen, die mit Sicherheit zur Daseinsvorsorge zählen und die damit auch dann weiterhin der Kontrolle der unabhängigen Datenschutzbeauftragten des Bundes und der Länder nach den Vorschriften für öffentliche Stellen unterliegen, wenn die Wahrnehmung der Daseinsvorsorgeaufgabe unter Fortbestand der staatlichen Gewährleistungsverantwortung auf Private übertragen wird. Wie bei der Daseinsvorsorge die Privatautonomie hinter dem öffentlichen Interesse an der Aufgabenerfüllung zurücktritt, so dass die „Flucht in das Privatrecht“ zwecklos ist, ändert die Funktionsübertragung in den nichtöffentlichen Bereich nichts an bestehenden datenschutzrechtlichen Zuständigkeiten. Insoweit ist die von der Hessischen Landesregierung in ihrer Stellungnahme zum 33. Tätigkeitsbericht vertretene Ansicht, dass der Betrieb eines Verkehrsflughafens, mit dem unstrittig öffentliche Zwecke erfüllt werden, nicht auch die Folge hat, dass die Erfüllung dieser öffentlichen Zwecke einer öffentlich-rechtlichen Kontrolle unterliegt, nicht zutreffend. Die teleologische Extension des Begriffs der „hoheitlichen Aufgaben“ in § 3 Abs. 1 Satz 2 HDSG verortet die öffentliche Aufgabenerfüllung nichtöffentlicher Stellen

lediglich dort, wo sie hingehört, nämlich im öffentlichen Bereich. Keineswegs wird unzulässigerweise auf den privaten Bereich zugegriffen.

Dies gilt auch für die Privatisierung des Universitätsklinikums Gießen und Marburg. Unverändert bleibt selbstverständlich meine Zuständigkeit für die Erhebung und Weiterverarbeitung von Patientendaten des Universitätsklinikums durch öffentliche (Forschungs-)stellen. Es bleibt auch eindeutig unverändert bei meiner Zuständigkeit, soweit das Universitätsklinikum künftig nach den neuen Vorschriften des Gesetzes für die hessischen Universitätskliniken (§§ 5, 15, 22, 25a UniKlinG) insbesondere mit der Aufgabe der Unterstützung des Fachbereichs Medizin, bei dessen Aufgabenerfüllung in Forschung und Lehre beliehen wird. Das Universitätsklinikum untersteht insoweit auch der Rechtsaufsicht des Ministeriums für Wissenschaft und Kunst. Aber auch darüber hinausgehend verbleibt es insgesamt dabei, dass das Universitätsklinikum ausschließlich meiner Kontrollzuständigkeit unterliegt, denn insgesamt dominiert die öffentliche Aufgabenstellung des Universitätsklinikums. Die Privatisierung ist im Kernbereich lediglich formeller Natur. Es bleibt öffentliche Aufgabe, eine ordnungsgemäße Krankenversorgung der Bevölkerung in einem Krankenhaus der Maximalversorgung sicherzustellen, und die Krankenversorgung muss auf die Erfordernisse von Forschung und Lehre ausgerichtet sein.

2.1.3

Unabhängigkeit des Hessischen Datenschutzbeauftragten und Instrumente der Neuen Verwaltungssteuerung

Bei der Umsetzung der Neuen Verwaltungssteuerung muss die Rechtsstellung des Hessischen Datenschutzbeauftragten als unabhängige oberste Landesbehörde außerhalb der Landesregierung und frei von deren Einfluss berücksichtigt werden. Auch bei der Einführung der kaufmännischen Buchführung und des Produkthaushaltes ist dieser Stellung Rechnung zu tragen.

Der Hessische Datenschutzbeauftragte ist nicht Teil der Landesverwaltung, sondern eine unabhängige oberste Landesbehörde, deren zentrale Aufgabe die Beratung und Kontrolle der Landesverwaltung auf dem Gebiet des Datenschutzes, der Aufrechterhaltung des Informationsgleichgewichtes und des Informationszugangs ist (vgl. §§ 22, 24 und 25 HDSG, und Ziff. 2.11.2). Deshalb können Beschlüsse des Kabinetts und der Landesregierung den Hessischen Datenschutzbeauftragten nicht unmittelbar binden. Gleichwohl habe ich weitgehend die

landeseinheitlichen Verfahrensweisen der Verwaltungssteuerung, der Einführung der kaufmännischen Buchführung und des Produkthaushalts übernommen, weil ich meinerseits einheitliche Haushalts-, Buchführungs- und Rechnungslegungsregeln für notwendig halte. So ist seit dem Jahr 2004 auch in meiner Dienststelle das Rechnungswesen auf SAP R/3 umgestellt und ich habe weitgehend in Anlehnung an die Vorgaben für die Landesverwaltung ein Zielsystem entwickelt sowie Produkte und die dazugehörigen Leistungen definiert, obwohl für meine Dienststelle durch die SAP R/3-Einführung und die flankierenden Maßnahmen keine Einsparung, sondern ein erheblicher Mehraufwand entstanden ist. Die besondere Stellung meiner Behörde und die Aufgabenstellung führen aber dazu, dass das für die Landesverwaltung entwickelte Modell nicht in vollem Umfang auf meine Dienststelle zugeschnitten ist und dementsprechend variiert werden muss. Das war freilich den mit der einheitlichen Umsetzung des Systems in der gesamten Landesverwaltung betrauten Mitarbeitern des Hessischen Ministeriums der Finanzen nicht immer bewusst.

Daher war ich gezwungen klarzustellen, dass ebenso wie bei den anderen außerhalb der Exekutive angesiedelten Dienststellen das Zielsystem des Hessischen Datenschutzbeauftragten nicht von der Landesregierung beschlossen werden kann, sondern dem Kabinett nur zur Kenntnis gebracht wird. Das Kabinett kann allerdings Anregungen und Wünsche zur Formulierung geben, die ich dann in meine Erwägungen einbeziehe. Die Fassung der Ziele obliegt gleichwohl nicht dem Kabinett; das gilt auch für Änderungen an diesem System.

Die Konzepte für die Hessische Landesverwaltung sehen vor, dass künftig Produkthaushalte zu erstellen sind, die der Landtag – wie bisher den Haushaltsplan – beschließt (Methodenkonzept Budgetierung und betriebswirtschaftliche Steuerungselemente für die Landesverwaltung Hessen, Ziff. 2.4; Planungshandbuch zum Produkthaushalt 2007, Ziff. 2.2). Bei der Einführung des Produkthaushalts ergeben sich spezifische Probleme für unabhängige außerhalb der Landesverwaltung stehende Behörden, da das System der Neuen Verwaltungssteuerung für die hierarchische Landesverwaltung entwickelt wurde. Das Verfahren sieht vor, dass die Ressorts innerhalb des ihnen mit dem Eckwertebeschluss der Landesregierung zugewiesenen Rahmens einen Vorschlag erstellen, welche Produkte in welcher Menge sie zu welchen Kosten im Haushaltsjahr erstellen werden. Dieser Vorschlag ist Basis der Haushaltsverhandlungen und für die Beschlussfassung im Haushaltsverfahren. Entsprechend den Verhandlungen bei der kameralen Haushaltsführung können beim Produkthaushalt in den Haushaltsverhandlungen und durch das Parlament Verschiebungen der Schwerpunkte, also der Budgets für die Produkterbringung ebenso

wie Kürzungen und Aufstockungen der Budgets und des Gesamtbudgets beschlossen werden. Bei der Ausführung dieses verabschiedeten Produkthaushalts sind Verschiebungen zwischen den Produkten (also „Deckungsfähigkeit“) nur in sehr begrenzten Umfang ohne förmliches Zustimmungsverfahren durch den Finanzminister zugelassen.

Der Hessische Datenschutzbeauftragte hat in Anlehnung an die Konzepte der Landesverwaltung und auf Basis der bisherigen Aufgabenwahrnehmung zwei Produkte entwickelt.

Produkt Nr. 1 „Normsetzung einschließlich Anfragen aus Parlament/Regierung“ enthält

- alle Arbeiten, die im Zusammenhang mit der Beratung bei Gesetzgebungsverfahren anfallen,
- Koordinierungsleistungen wie die Arbeit in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und in deren Arbeitskreisen sowie in europäischen und internationalen Gremien und
- die Erfüllung der Berichtspflicht gegenüber Parlament und Regierung, z. B. durch Abgabe des jährlichen Tätigkeitsberichtes.

Produkt Nr. 2 „Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften“ fasst Leistungen wie

- Beratung und Prüfung von Behörden und Institutionen,
- Behandlung von Bürger- und Behördenanfragen und
- Durchführung von Schulungen

zusammen.

Die Verteilung des für die effektive Erfüllung der mir übertragenen Aufgaben zu verwendenden Aufwands auf diese beiden Produkte ist nur begrenzt kalkulierbar, weil insgesamt mehr als die Hälfte der beim Hessischen Datenschutzbeauftragten durchgeführten Tätigkeiten nicht planbar, sondern fremdinitiiert sind. Das wird auf Anhieb deutlich, wenn man z. B. an die großen E-Government-Projekte des Landes denkt, die mir keineswegs immer bereits in den für die Haushaltsplanung erforderlichen Vorlaufzeiten angekündigt werden und schon gar nicht in ihrem datenschutzrechtlichen Beratungs- und Prüfungsaufwand abschätzbar sind. Gleiches gilt auch für einschneidende Pannen beim Umgang mit personenbezogenen Daten (wie z. B. kürzlich die unzulässige Übermittlung von Gesundheitsdaten nach Vietnam, vgl. Ziff. 5.8.4), auf die mit einer Prüf- und Beratungsserie unmittelbar reagiert werden muss. Innerhalb der Produktes Nr. 2 ist ein Ausgleich dann möglich, wenn z. B. eine geplante Prüfung verschoben werden kann und der

fremdinitiierte Anteil den planbaren Teil in diesem Produkt nicht übersteigt. Produkt Nr. 1 setzt sich dagegen überwiegend aus fremdinitiierten Leistungen (Beteiligungen im Gesetzgebungsverfahren und damit verbundene Koordinierungen) und nicht disponiblen Pflichtbestandteilen (Tätigkeitsbericht) zusammen. Deshalb verändern unvorhersehbare große Gesetzgebungsaktivitäten (z. B. nach den Terroranschlägen) unmittelbar das Verhältnis der Anteile der beiden Produkte gravierend. Beim bisherigen Haushaltsverfahren, bei dem das Gesamtbudget festgelegt und die Einnahmen und Ausgaben nach bestimmten Zweckbestimmungen aufgliedert wurden (z. B. Personalausgaben, sächliche Verwaltungsausgaben, Baumaßnahmen), konnte eine Beeinflussung der Aufgabenwahrnehmung und damit eine Beeinträchtigung meiner Unabhängigkeit nicht auftreten. Das ist bei der Budgetierung im Haushalt auf Produktebene anders, weil sie prinzipiell dazu führen könnte, dass ich z. B. den Schwerpunkt meiner Aufgabenwahrnehmung nicht mehr selbst bestimmen kann. Ich habe Verständnis dafür, dass eine Zusammenführung der Veranschlagung aller Aufgaben in nur einem Produktbudget sich haushaltsrechtlich verbietet, weil dies einem Globalhaushalt gleichkäme. Allerdings kann es nicht von einer Genehmigung des Finanzministeriums abhängen, auf welche meiner Aufgaben ich den Schwerpunkt lege und ob ich eine Aufgabe im erforderlichen Umfang ausüben kann. Eine solche Abhängigkeit von einer meiner Kontrolle unterliegenden Stelle würde die Unabhängigkeit massiv beeinträchtigen.

Angesichts dieses Sachverhaltes habe ich Gespräche mit dem Finanzministerium geführt und eine von den für die Ressorts festgelegten Vorgaben abweichende Regelung vereinbart. Diese beinhaltet insbesondere eine höhere Deckungsfähigkeitsmarge zwischen den Produkten meines Hauses. Ich werde beobachten, ob die getroffenen Regelungen mir genügend Spielraum für eine unabhängige Aufgabenwahrnehmung gewähren. Sollte das nicht der Fall sein, hat das Finanzministerium mir eine entsprechende Anpassung der getroffenen Vereinbarungen avisiert.

Die Anwendung der für die Landesverwaltung vorgesehen Steuerungsinstrumente für ein externes Controlling auch auf mein Haus würde die Unabhängigkeit noch weiter beeinträchtigen. Sie würde eine Steuerung meiner Aufgabenwahrnehmung durch die Landesregierung und das Parlament bedeuten. Meine Aufgabe verpflichtet mich ohnehin, so effektiv wie möglich zur Sicherstellung der informationellen Selbstbestimmung und der informationellen Gewaltenteilung in Hessen beizutragen. Sie verpflichtet mich besonders, diese unabhängig und damit weisungsfrei bei der Aufgabenausführung und frei von externer Steuerung durchzuführen. Das heißt keineswegs, dass ich meine Aufgaben ungeplant ausführe und keinerlei Rechenschaft ablegen

muss. Für die planbaren Teile praktiziere ich zur internen Steuerung schon seit langem eine Jahresplanung mit Ausführungskontrolle. Gegenüber Parlament und Regierung lege ich jährlich mit meinem Tätigkeitsbericht Rechenschaft. Die Ansätze der Landesregierung für ein internes Controlling greife ich dort gerne auf, wo sie wirtschaftlich sind und zur Effektivitätssteigerung auch in meinem Haus eingesetzt werden können. Schon die Einführung der kaufmännischen Buchführung hat in meinem Haus jedoch zu einem zusätzlichen Verwaltungsaufwand geführt und Personalkapazität von den originären Aufgaben abgezogen, ohne dass dem für meine kleine und auch ohne aufwändige IT-Unterstützung überschaubare Dienststelle ein adäquater Nutzen gegenübersteht. Die Konzepte der Neuen Verwaltungssteuerung der Landesverwaltung werde ich auf meine Dienststelle daher nur insoweit übertragen, wie die damit verfolgten Ziele ohne Einbeziehung meiner Dienststelle nicht realisiert werden können, meine Unabhängigkeit nicht beeinträchtigt wird und nicht weitere Personalkapazität meinen originären Aufgaben entzogen wird.

2.2

Behördliche Datenschutzbeauftragte

2.2.1

Ergebnisse einer Untersuchung zu Rechtsstellung und Aufgaben behördlicher Datenschutzbeauftragter

Im Rahmen einer Diplomarbeit beim Hessischen Datenschutzbeauftragten wurde erneut und aktuell die Situation behördlicher Datenschutzbeauftragter untersucht. Zur Unterstützung kleinerer Dienststellen wurde ein Merkblatt zu Aufgaben und Stellung behördlicher Datenschutzbeauftragter entwickelt und in mein Internetangebot eingestellt.

Eine Studentin der Verwaltungsfachhochschule, die bei mir ihre praktische Studienzeit ableistete und hat unter meiner Betreuung eine Diplomarbeit zum Thema Aufgaben und Stellung des behördlichen Datenschutzbeauftragten angefertigt und in diesem Rahmen mit wissenschaftlichen Methoden einen Fragebogen entwickelt. Auf dieser Grundlage führte sie eine Umfrage als Stichprobe bei den Dienststellen durch, die bereits im Jahre 1997 zur gleichen Thematik befragt wurden (vgl. 26. Tätigkeitsbericht, Ziff. 4.1), wertete die Ergebnisse aus und bewertete diese.

Ferner hat sie einen Vorschlag für ein Merkblatt zu Aufgaben und Stellung behördlicher Datenschutzbeauftragter entwickelt.

Befragt wurden 30 Dienststellen, die aus dem Kreis der bereits 1997 befragten Dienststellen ausgewählt wurden und repräsentativ Landes- und Kommunalbehörden aller Stufen enthielten. Die gegenüber der seinerzeitigen Befragung deutliche Reduzierung der Stichprobe (10 % der 1997 befragten Stellen) war wegen des engen zeitlichen Rahmens einer Diplomarbeit notwendig. Der Fragebogen wurde nach empirischen Gesichtspunkten und unter Berücksichtigung der seinerzeit bei der ersten Befragung gewonnenen Erkenntnisse neu gestaltet und inhaltlich überarbeitet (s. Abb. 1). Er wurde mit einem offiziellen Schreiben von mir und dem Hinweis auf die mir gegenüber nach § 29 HDSG bestehende Auskunftspflicht versandt.

Abb. 1

Fragebogen zum behördlichen Datenschutzbeauftragten (bDSB)

Dienststelle:	Name des bDSB:	Telefon: (Vorwahl/Rufnummer)
----------------------	-----------------------	--

Bitte beantworten Sie die folgenden Fragen bzw. kreuzen Sie Zutreffendes an. Bitte nutzen Sie auch die Gelegenheit eigene Anmerkungen zu machen.

1. In welchem Jahr wurden Sie zum bDSB bestellt?

2. Sind Sie als bDSB der Behördenleitung unterstellt (bzw. einem hauptamtlichen Beigeordneten)?
Wenn nein, wem sind Sie unterstellt?

Ja Nein

3. In welchem Umfang werden Sie als bDSB von der Erfüllung anderer Aufgaben freigestellt?

4. Welche Funktion/Tätigkeit üben Sie ansonsten in Ihrer Verwaltung aus?

5. Wie hoch schätzen Sie den auf die Funktion des bDSB entfallenden Anteil Ihrer Arbeitszeit
(Angabe bitte in durchschnittlichen Arbeitsstunden pro Monat)?

6. Sind Sie mit den zur Erfüllung Ihrer Aufgaben als bDSB notwendigen räumlichen und sachlichen
Mitteln ausgestattet (z. B. verschließbares eigenes Büro, EDV-Ausstattung)?

Ja Nein

Anmerkungen:

7. Werden Sie in Ihrer Arbeit als bDSB durch Mitarbeiter unterstützt (z. B. Schreibdienst,
Hilfspersonal)?

Ja Nein

Anmerkungen:

8. Haben Sie an Datenschutz-Schulungen teilgenommen?

Ja Nein

Wenn ja, welche?

wann?

bei wem?

9. Wie bilden Sie sich sonst noch fort (z. B. im Bereich Datenschutzrecht, EDV-Kenntnisse)?

Fachliteratur Seminare Konferenzen Erfahrungsaustauschkreise

Sonstiges: _____

Anmerkungen:

10. Hatten Sie schon Kontakt zum Hessischen Datenschutzbeauftragten in Wiesbaden?

Ja Nein

Wenn ja, in welcher Angelegenheit?

11. Welche der in § 5 Absatz 2 HDSG genannten Aufgaben wurden von Ihnen bisher durchgeführt?
Welche Datenschutz-Aufgaben wurden von Ihnen außerdem konkret durchgeführt?

12. Sind Ihnen alle in Ihrer Dienststelle eingesetzten Verfahren, bei denen personenbezogene Daten verarbeitet werden, in der aktuellen Version bekannt?

Ja Nein Anmerkungen:

13. Wie ist die Öffentlichkeit über Ihre Bestellung als bDSB informiert worden? Sind Sie in dem Organisationsplan Ihrer Dienststelle als bDSB ausgewiesen?

14. Wenn Sie an Ihre Tätigkeit insgesamt als bDSB denken, gibt es noch Hinweise und Anmerkungen, die Sie erwähnen möchten?

Dem Einsatz der Diplomandin ist es zu verdanken, dass die Rücklaufquote nahezu 100 % betrug. Nur in einer Dienststelle, in der die Position des behördlichen Datenschutzbeauftragten gerade neu besetzt war, konnte der Fragebogen nicht sinnvoll ausgefüllt werden, sodass dieser außer Betracht blieb.

Gegenüber der 1997 durchgeführten Untersuchung war in allen Fällen ein behördlicher Datenschutzbeauftragter bestellt, 55 % der Bestellungen stammten noch aus der Zeit vor der Novellierung des Hessischen Datenschutzgesetzes 1998.

Bemerkenswert ist, dass in immerhin 6,9 % der Fälle Datenschutzbeauftragte entgegen dem Gesetzeswortlaut nicht unmittelbar der Dienststellenleitung bzw. einem hauptamtlichen Beigeordneten unterstellt waren. Diesen Fällen werde ich nachgehen.

Hinsichtlich der Freistellung von anderen Aufgaben ergibt sich ein differenziertes Bild, das auch mit der Größe der zu betreuenden Dienststelle zusammenhängt: In großen Dienststellen waren die behördlichen Datenschutzbeauftragten ganz oder zur Hälfte von anderen Aufgaben freigestellt (13,8 %); in kleineren Dienststellen wurden sie zum Teil in geringem Umfang und fallweise freigestellt (24,1 %); immerhin 62,1 % gaben an, dass sie keinerlei Entlastung von sonstigen Aufgaben erhielten. Bei der Bewertung dieser Zahl ist zu berücksichtigen, sich aus zusätzlichen Erläuterungen ergibt, dass oft lediglich die förmliche Freistellung fehlte. Meist wurden in durchaus nennenswerten Prozentsätzen Aufgaben eines Datenschutzbeauftragten ausgeübt und die sonstige Tätigkeit ließ den erforderlichen Zeitrahmen zu. Nur 6,9 % führten zusätzlich bei den Hinweisen und Anregungen Klage über das zu geringe bzw. fehlende Zeitbudget für ihre Aufgabe. In jedem Fall ergibt sich gegenüber der Umfrage von 1997, bei der noch 85,5 % angegeben hatten, sie würden nicht entlastet, ein deutlich verbessertes Bild. Allerdings ist den Dienststellen, bei denen eine Freistellung ihrer Datenschutzbeauftragten tatsächlich nicht stattfindet, ein Verstoß gegen das HDSG vorzuwerfen.

In die Bewertung dieser statistischen Zahlen ist auch die Befragung zu den wahrgenommenen Aufgaben einzubeziehen. Immerhin nahezu 80 % hatten bereits alle oder einige der in § 5 Abs. 2 HDSG aufgeführten Aufgaben wahrgenommen und 62 % gaben an, dass ihnen die in ihrer Dienststelle eingesetzten Verfahren bekannt seien. Die Aufgabenwahrnehmung war sehr unterschiedlich, was angesichts der unterschiedlichen Größe der Dienststellen nicht verwunderlich war. Bemerkenswert ist allerdings, dass nur 58,6 % der in § 5 Abs. 2 Nr. 2 HDSG genannten

Verpflichtung zur Datenschutzunterweisung der Bediensteten ihrer Dienststelle nachgekommen waren.

Mehr als ein Drittel der Befragten gab an, die in der Dienststelle eingesetzten Datenverarbeitungsverfahren seien ihnen nicht bekannt oder sie seien sich nicht sicher, ob sie vollständige Kenntnis darüber hätten. Das ist zwar etwas besser als bei der letzten Umfrage, wo dieser Prozentsatz noch bei knapp der Hälfte lag. Gleichwohl kann das Ergebnis angesichts der seitdem geänderten Rechtslage nicht befriedigen. Mit der Novellierung des HDSG 1998 ist nämlich den behördlichen Datenschutzbeauftragten die Aufgabe der Führung der Verzeichnisse auferlegt. Die Antworten lassen leider den Schluss zu, dass dies nicht bei allen Daten verarbeitenden Stellen praktiziert wird.

Zur eigenen Fortbildung gaben 72,4 % der Befragten an, an einer Datenschutzausbildung teilgenommen zu haben, meist in zeitlichem Zusammenhang mit ihrer Bestellung. Einige hätten gerne auch an einschlägigen Seminaren oder Konferenzen privater Anbieter teilgenommen, was aber im Hinblick auf die Preise und die Haushaltslage nicht möglich sei. Über die laufende Entwicklung der Datenschutzfragen informierten sich 86,2 % durch Fachliteratur, einige durch weitere Quellen, wie z. B. die Tätigkeitsberichte des Hessischen Datenschutzbeauftragten. Gerne werden auch die Facharbeitskreise für Datenschutzbeauftragte zur Koordinierung und einheitlichen Lösung von Fachfragen wahrgenommen, die ich z. B. für Kommunen oder Krankenhäuser anbiete.

79,3 % der Befragten hatten bereits Kontakt zu meinem Haus, sei es in Einzelfragen oder regelmäßig zur Klärung von datenschutzrechtlichen Problemfällen.

Erfreulich ist, dass bei allen Befragten die für die Erfüllung ihrer Aufgabe notwendige Ausstattung vorhanden war und Interessenkollisionen mit anderen dienstlichen Aufgaben nicht bestanden.

Nachbesserungsbedarf gibt es allerdings hinsichtlich der Information in der Dienststelle und außerhalb zur Position des behördlichen Datenschutzbeauftragten. Immerhin 37,9 % der Datenschutzbeauftragten waren im Organisationsplan nicht ausgewiesen. Auch wenn einige Datenschutzbeauftragte angaben, ihre Funktion sei im Haus aber bekannt, so bin ich doch der Meinung, dass die Funktion auch im Organisationsplan ausgewiesen werden muss. Dies besonders auch, weil immerhin 69 % der Befragten angaben, die Position sei Externen, also allen die in

Kontakt mit der Dienststelle sind, wie z. B. Bürgerinnen und Bürgern, nicht bekannt gegeben worden. Bei dieser Situation ist es umso wichtiger, dass aus zentralen Informationen wie einem Organisationsplan diese Ansprechstelle für Datenschutzfragen hervorgeht. Besteht ein Internetangebot oder eine Informationsbroschüre der Dienststelle, bietet es sich an, den behördlichen Datenschutzbeauftragten auch hierin zu nennen.

Fazit der Untersuchung war, dass die Lage der behördlichen Datenschutzbeauftragten sehr stark auch von der Größe ihrer Dienststelle abhängt. Gerade in kleineren Dienststellen bedarf es besonderer Unterstützung der Bediensteten, die diese Funktion übernommen haben, weil auch der Leitung oft die Aufgaben und Stellung eines behördlichen Datenschutzbeauftragten nicht klar sind. Hinzu kommt, dass auch in der Ausbildung der Bediensteten für öffentliche Stellen ist die Information über das Thema Datenschutz und behördlicher Datenschutzbeauftragter nicht oder kaum vorhanden ist. Der Ansicht der Diplomandin, die hier Verbesserungspotential sah, pflichte ich nachdrücklich bei. Die Anregung, besonders für die Praxis in kleinen Dienststellen die wichtigsten Punkte zu Stellung und Aufgaben der behördlichen Datenschutzbeauftragten in einem Merkblatt für Dienststellenleitung, Bedienstete und Datenschutzbeauftragte zu erläutern und damit eine Hilfestellung für die weitgehend unbekannte Materie geben, habe ich gerne aufgenommen. Das von der Diplomandin entwickelte Merkblatt habe ich überarbeitet und in mein Internetangebot eingestellt. Es ist nachfolgend abgedruckt.

Merkblatt

zu Stellung und Aufgaben der behördlichen Datenschutzbeauftragten nach § 5 des Hessischen Datenschutzgesetzes (HDSG)

Stellung der behördlichen Datenschutzbeauftragten

Behördliche Datenschutzbeauftragte sind unmittelbar der Leitung der Behörde zu unterstellen. In Gemeinden und Gemeindeverbänden können sie auch einem hauptamtlichen Beigeordneten unterstellt werden. Die Unterstellung unter die Behördenleitung trägt der besonderen Position des Datenschutzbeauftragten Rechnung und ermöglicht den direkten Kontakt zur Leitung ohne Einhaltung eines sonstigen Dienstweges. Der bzw. die behördliche Datenschutzbeauftragte hat das Recht, sich jederzeit schriftlich oder mündlich an diese zu wenden und die Aufgabe, sie bei der Sicherung der Datenschutzbelange zu unterstützen. Die Verantwortung für die Verwirklichung des Datenschutzes verbleibt bei der Behördenleitung.

Dem oder der behördlichen Datenschutzbeauftragten obliegt die unabhängige Überwachung der Einhaltung des Datenschutzes. Diese Unabhängigkeit beinhaltet, dass er oder sie bei der Aufgabenwahrnehmung frei von Weisungen ist und wegen dieser Tätigkeit nicht benachteiligt werden darf.

Bei der Auswahl der Person für diese Aufgabe ist darauf zu achten, dass sie die für die Wahrnehmung der Aufgaben erforderliche Sachkenntnis und Zuverlässigkeit hat. Sollte die Sachkenntnis noch nicht bei Amtsantritt vorliegen, so hat die Dienststelle dafür Sorge zu tragen, dass sie schnellstmöglich erworben werden kann.

Der oder die behördliche Datenschutzbeauftragte ist in dem für die ordnungsgemäße Wahrnehmung dieser Funktion erforderlichen Umfang von der Erfüllung anderer Aufgaben freizustellen. Er oder sie muss also nicht ausschließlich mit dieser Funktion betraut sein, sondern kann zusätzlich auch weitere Aufgaben haben. Es darf allerdings nicht so verfahren werden, die Aufgabe zusätzlich zu den bisherigen Aufgaben zuzuweisen, ohne für eine Entlastung zu sorgen. Der Zeitaufwand für die Wahrnehmung der Aufgaben als Datenschutzbeauftragter hängt von der jeweiligen Größe der Dienststelle sowie von der Art und Menge der dort verarbeiteten personenbezogenen Daten ab. Bei größeren Dienststellen kann es daher notwendig sein, die Aufgabe als ausschließliche Aufgabe zu übertragen; bei kleinen Gemeinden kann dagegen eine Freistellung für einige Stunden in der Woche ausreichen. Je nach Umfang der gerade anstehenden Aufgaben (z. B. Entwicklung oder Einführung eines datenschutzrechtlich anspruchsvollen Verfahrens) kann die benötigte Freistellung variieren, daher ist auch eine flexible Handhabung des Freistellungsumfangs möglich.

Dem oder der behördlichen Datenschutzbeauftragten sind im erforderlichen Umfang Hilfspersonal sowie Räume, Einrichtungen und Mittel zur Verfügung zu stellen. Um die Aufgabe angemessen zu erfüllen, sollten Weiterbildungsmöglichkeiten wie Schulungen und Fachliteratur zum Datenschutz (Kommentare, Lehrbücher, Zeitschriften u. a.), sowie auch Möglichkeiten des

Erfahrungsaustausches mit Datenschutzbeauftragten anderer Behörden, die gleiche Aufgaben wahrnehmen, eröffnet werden.

Dienststellen haben behördlichen Datenschutzbeauftragten alle Informationen zur Verfügung zu stellen, die sie für die Aufgabenwahrnehmung benötigen. Dazu gehört auch die Information über alle datenschutzrelevanten Verfahren und Themen in der Dienststelle sowie die Aushändigung der Verfahrensverzeichnisse für in der Dienststelle eingesetzte Verfahren.

Bei der Auswahl von Bediensteten, die neben der Datenschutzaufgabe auch andere Aufgaben ausüben, ist darauf zu achten, dass Interessenkonflikte zwischen den Aufgaben ausgeschlossen sind. Interessenkonflikte können insbesondere dann auftreten, wenn behördliche Datenschutzbeauftragte gleichzeitig über die Einführung, Anwendung, Änderung oder Erweiterung der automatisierten Datenverarbeitung zu entscheiden haben. Daher dürfen z. B. Leiter und Beschäftigte des Organisationsamtes oder der für die Datenverarbeitung innerhalb der Dienststelle zuständigen Organisationseinheit nicht als behördliche Datenschutzbeauftragte bestellt werden. Auch Leiter von großen Organisationseinheiten sollten nicht zu behördlichen Datenschutzbeauftragten bestellt werden, da sie ihren eigenen Aufgabenbereich kritisch beleuchten müssten. Ebenfalls nicht geeignet sind Bedienstete, die aufgrund ihrer hierarchischen Stellung nicht darin geübt sind, Anforderungen zu formulieren und gegenüber Vorgesetzten durchzusetzen.

Der oder die Datenschutzbeauftragte ist schriftlich zu bestellen. Um es Beschäftigten, aber auch externen Personen, die in Kontakt mit der Dienststelle stehen zu ermöglichen, Datenschutzfragen unmittelbar mit dem bzw. der behördlichen Datenschutzbeauftragten zu klären, sollte die Position im Organisationsplan der Behörde für alle Beschäftigten und zentralen Dienste (z. B. die Telefonzentrale) erkennbar dargestellt werden.

Für den oder die behördliche Datenschutzbeauftragte ist auch ein Stellvertreter oder eine Stellvertreterin zu bestellen. Für die Besetzung dieser Position gelten die gleichen Anforderungen wie für die behördlichen Datenschutzbeauftragten.

Aufgaben der behördlichen Datenschutzbeauftragten

Behördliche Datenschutzbeauftragte haben innerhalb der Behörde den Datenschutz zu koordinieren und sind umfassend für den Datenschutz zuständig. Dabei haben sie die Funktion sowohl die Behördenleitung als auch die Beschäftigten zu beraten und zu unterstützen. Ihnen obliegt die Pflicht auf bestehende Missstände und Gefahren hinzuweisen.

Das Hessische Datenschutzgesetz benennt als Aufgaben der behördlichen Datenschutzbeauftragten insbesondere

- das Hinwirken auf die Einhaltung der Datenschutzvorschriften,
- die Unterrichtung der Beschäftigten über Vorschriften für den Datenschutz, z. B. durch Schulungen,
- die Unterstützung der Behörde bei der Erstellung des Verfahrensverzeichnisses und den technischen und organisatorischen Maßnahmen zur Durchführung des Datenschutzes und bei Kontakten mit dem Hessischen Datenschutzbeauftragten,
- die Führung des Verfahrensverzeichnisses und Bereithaltung für die Einsicht,
- die Überprüfung der Vorabkontrolle bei Einsatz oder Änderung von Verfahren automatisierten Verarbeitung personenbezogener Daten.

3. Europa

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrnehmung der Interessen der Länderdatenschutzbeauftragten in den europäischen Kontrollinstanzen für Schengen und EUROPOL übertragen. Der Beitrag stellt die Arbeitsschwerpunkte der Sitzungen der Kontrollinstanzen im Berichtsjahr dar und informiert über den Sachstand beim europäischen Fingerabdrucksystem EURODAC. Das jährlich veranstaltete Wiesbadener Forum Datenschutz widmete sich dem Spannungsfeld zwischen Anforderungen im Sicherheitsbereich und dem Datenschutz auf europäischer Ebene.

3.1

Allgemeines

Seit dem 1. Januar 2005 hat der Hessische Datenschutzbeauftragte vom Datenschutzbeauftragten des Landes Sachsen-Anhalt die Vertretung der Landesdatenschutzbeauftragten in der Gemeinsamen Kontrollinstanz für EUROPOL übernommen. Da ich – vertreten durch eine Mitarbeiterin – bisher schon für die anderen Landesdatenschutzbeauftragten in der Gemeinsamen Kontrollinstanz für Schengen teilnahm, bot sich diese Zusammenführung an: Es gibt ähnlich gelagerte Probleme bis hin zu thematischen Überschneidungen wie beispielsweise den Zugriff von EUROPOL auf das Schengener Informationssystem (SIS). Dementsprechend finden auch vermehrt gemeinsame Sitzungen der beiden Kontrollinstanzen mit den Kontrollinstanzen von EUROJUST und dem Zollinformationssystem statt.

Bei der letzten gemeinsamen Sitzung der Kontrollinstanzen waren der damals neu gewählte Kommissar Franco Frattini und der Europäische Datenschutzbeauftragte Peter Hustinx anwesend.

Thema von Herrn Frattini war die Aufrechterhaltung eines angemessenen Datenschutzstandards angesichts der verstärkten Zusammenarbeit von Polizei- und Justizbehörden der EU-Mitgliedstaaten zur Abwehr von Terrorismus und Organisierter Kriminalität.

Damit wurden Fragestellungen berührt, die auch auf dem vom hessischen Landtagspräsidenten und mir organisierten 14. Wiesbadener Forum Datenschutz diskutiert wurden (s. Ziff. 3.2).

Im Anschluss an eine der regulären Sitzungen der Kontrollinstanzen hatte meine Mitarbeiterin Gelegenheit, an einer vom Europäischen Datenschutzbeauftragten organisierten Informationsveranstaltung zu EURODAC (der Begriff setzt sich zusammen aus Européen und Dactyloscopie) teilzunehmen.

In EURODAC werden die Fingerabdrücke von Asylbewerbern und jenen Ausländern, die bei der illegalen Grenzüberschreitung aufgegriffen werden, gespeichert, insbesondere um abzuklären, ob bereits früher ein Asylantrag gestellt wurde.

Die Zentraleinheit von EURODAC wird von der Europäischen Kommission betrieben und ist seit Anfang 2003 in Betrieb. Die Frage der datenschutzrechtlichen Kontrolle ist bei EURODAC vergleichsweise einfach, da die entsprechenden Verordnungen (Verordnung EG Nr. 2725/2000 des Rates vom 11. Dezember 2000, ABl. der EG vom 15. Dezember 2000 L 316/1; Verordnung EG Nr. 407/2002 des Rates vom 28. Februar 2002, ABl. der EG vom 5. März 2002 L 62/1) ihre Rechtsgrundlage in der ersten Säule des Vertrags über die Europäische Union haben und somit die Zuständigkeit des Europäischen Datenschutzbeauftragten seit dessen Wahl Ende 2003 gegeben ist.

Daneben bleiben die Mitgliedstaaten bzw. deren Datenschutzkontrollbehörden für das Sammeln, Speichern und die Anlieferung der digitalisierten Fingerabdrücke zur Zentraleinheit von EURODAC zuständig.

Der Europäische Datenschutzbeauftragte hat mit einer Prüfung von EURODAC begonnen, wünschenswert wäre eine ergänzende – evtl. abgestimmte – Prüfung in den Mitgliedstaaten. Die Kommission hat im Juni des Jahres den zweiten Tätigkeitsbericht über die Aktivitäten der Zentraleinheit von EURODAC veröffentlicht (SEC (2005) 839).

3.2

14. Wiesbadener Forum Datenschutz

Das diesjährige Forum Datenschutz widmete sich dem Datenschutz im europäischen Staatenverbund vor dem Hintergrund einer veränderten Sicherheitslage.

Zum einen wurde dargestellt, auf welche Weise im europäischen Staatenverbund mit Blick auf internationalen Terrorismus und organisierte Kriminalität immer weitere Maßnahmen zur Aufrechterhaltung der Sicherheit der Bürger erfolgen. Dies wurde am Beispiel verschiedener europäischer Sicherheitsbehörden, insbesondere EUROPOL aber auch EURODAC und EUROJUST und der verstärkten Zusammenarbeit der Sicherheitsbehörden in den EU-

Mitgliedstaaten bis hin zur Forderung nach Vernetzung nationaler Informationsbestände deutlich gemacht.

Tendenzielle Übereinstimmung bestand bei Referenten und in der Diskussion, dass der Datenschutz bei dieser Entwicklung Schritt halten muss. Der Europäische Datenschutzbeauftragte Peter Hustinx warb in seinem Vortrag für einheitliche Datenschutzbestimmungen mit bereichsspezifischen Regelungen. Diese sollten nicht nur – wie bisher – für den vergemeinschafteten Teil der Tätigkeiten der Europäischen Union gelten, sondern auch für die dritte Säule. Der Tagungsband befindet sich in Vorbereitung.

3.3

Gemeinsame Kontrollinstanz für das Schengener Informationssystem

Im Berichtszeitraum fanden sechs Sitzungen der Gemeinsamen Kontrollinstanz statt, an denen ich bzw. meine Mitarbeiterin als Ländervertreter teilnahmen.

Zu den aus 25 europäischen Staaten entsandten Delegationen wird demnächst eine Delegation aus der Schweiz hinzukommen, da das Assoziierungsabkommen der Schweiz mit der Europäischen Union durch Volksabstimmungen angenommen wurde.

Innerhalb der Schengen-Staaten haben Deutschland, Frankreich und die Beneluxstaaten durch ein multilaterales „Schengen-III-Abkommen“, so genannter Prümer Vertrag vom 27. Mai 2005, Maßnahmen zur Intensivierung der grenzüberschreitenden polizeilichen Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der illegalen Migration getroffen. Das Abkommen ist ratifizierungsbedürftig und daher noch nicht anwendbar. Zur Vertiefung des polizeilichen Informationsaustausches wurden u. a. der gegenseitige unmittelbare Zugriff auf anonymisierte DNA- und Fingerabdruckdatenbanken (Treffer/kein-Treffer-System) der gegenseitige lesende Onlinezugriff auf Fahrzeugregister und der Informationsaustausch über reisende Gewalttäter im Zusammenhang mit Großveranstaltungen vereinbart.

Für den Bereich der Terrorismusbekämpfung enthält das Abkommen Regelungen zur Intensivierung des Informationsaustauschs, über terroristische Gefährder und den Einsatz von Flugsicherheitsbegleitern.

Zur verstärkten Bekämpfung der illegalen Migration wird der Einsatz von Dokumentenberatern und die gegenseitige Unterstützung bei Rückführungen vereinbart.

Den anderen Schengen-Staaten steht der Vertrag zum Beitritt offen. Es ist außerdem geplant, das Abkommen nach einer Phase der Evaluierung in den Rechtsrahmen der EU zu überführen.

Die Gemeinsame Kontrollinstanz stellt bis Jahresende den Tätigkeitsbericht für die Jahre 2004 und 2005 fertig.

3.3.1

Entwicklungen des Schengener Informationssystems

Wichtigstes Thema in der Gemeinsamen Kontrollinstanz war wiederum die Diskussion von Plänen zur Erweiterung des Schengener Informationssystems, dem so genannten SIS II. Das SIS soll zum einen für einen erweiterten Teilnehmerkreis von mindestens 25 Staaten zuzüglich der Schweiz und weiteren Beitrittskandidaten ausgelegt werden, allerdings soll es auch neue Funktionen erhalten, um damit effizienter den Interessen der Nutzer angepasst werden zu können.

Im 33. Tätigkeitsbericht, Ziff. 3.1.2.1 hatte ich von Änderungen des Schengener Durchführungsübereinkommens (SDÜ) unter der spanischen Ratspräsidentschaft berichtet. Diese sind mittlerweile in Kraft getreten, werden aber – auch wegen der fehlenden technischen Vorkehrungen – noch nicht angewandt.

Ich hatte weiterhin auf Pläne der Europäischen Kommission zur Änderung des Schengener Durchführungsübereinkommens aufmerksam gemacht (Ziff. 3.1.2.2). Diese liegen mittlerweile als Entwürfe für – säulenbedingt getrennte – Rechtsakte vor [Vorschlag für einen Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), BRDrucks. 511/2005 vom 21. Juni 2005; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rats über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), BRDrucks. 512/2005 vom 21. Juni 2005; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rats über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II), BRDrucks. 527/2005 vom 21. Juni 2005]. Diese Vorschläge sollen die Rechtsgrundlage für das künftige SIS II bilden. Sie treten an die Stelle der bisherigen Art. 92 bis 119 Schengener Durchführungsübereinkommen und werden auch die o. g. unter spanischer Ratspräsidentschaft verabschiedeten Änderungen ersetzen. Die

Gemeinsame Kontrollinstanz hat zu diesen Entwürfen eine ausführliche Stellungnahme vom 10. Oktober 2005 abgegeben, an der die deutsche Delegation sich maßgeblich beteiligt hat.

Folgende Probleme waren besonders wichtig:

- Aus den vorliegenden Entwürfen geht nicht klar hervor, ob und welche Rechtsakte auf europäischer Ebene parallele Anwendung finden (beispielsweise die EG-Datenschutzrichtlinie 95/46 vom 24. Oktober 1995 oder die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr 45/2001 vom 18. Dezember 2000). Eine entsprechende Klarstellung liegt im Interesse der Bürger, da die verschiedenen Ausnahmen in den genannten Rechtsakten zu gravierenden Schlechterstellungen führen können. Die Gemeinsame Kontrollinstanz hat deshalb gefordert, dass ein umfassendes Regelwerk für SIS II geschaffen und dies auch in den Erwägungsgründen klargestellt wird.
- Feststehen muss weiterhin, welche Instanz für das Zentrale Schengener Informationssystem (CSIS) zuständig ist. Diese Frage ist nicht nur hinsichtlich der Verantwortlichkeit für die Datenverarbeitung, sondern auch für die datenschutzrechtliche Kontrolle wichtig. Das CSIS soll nach den Vorschlägen nunmehr bei der Kommission geführt werden; nach Art. 12 Nr. 1 des entsprechenden Entwurfs ist die Kommission aber nur für das Betriebsmanagement zuständig. Art. 12 Nr. 2 des Entwurfs der Verordnung lautet:

Das Betriebsmanagement umfasst alle Aufgaben, die durchgeführt werden müssen, damit das SIS II im Einklang mit dieser Verordnung 24 Stunden am Tag und sieben Tage in der Woche funktioniert; dazu gehören insbesondere die für den einwandfreien Betrieb des Systems erforderlichen Wartungsarbeiten und technischen Weiterentwicklungen.

Im Umkehrschluss liegt die Zuständigkeit für alle anderen Aufgaben bei den Mitgliedstaaten. Da der Europäische Datenschutzbeauftragte nur für die Tätigkeiten der Kommission zuständig ist, hätte dies zur Folge, dass ihm nur eine sehr eingeschränkte auf das Betriebsmanagement reduzierte Kontrollbefugnis zukäme.

In dem Entwurf ist vorgesehen, dass die Gemeinsame Kontrollinstanz als Kontrollgremium wegfällt, deshalb müssten die Datenschutzbeauftragten der Mitgliedstaaten den größten Teil der datenschutzrechtlichen Kontrolle übernehmen. Hier klafft nach Auffassung der

Gemeinsamen Kontrollinstanz eine Kontrolllücke – beispielsweise wäre eine konzertierte Prüfung der Ausschreibung nach Art. 96 Schengener Durchführungsübereinkommen, wie sie vorgenommen wurde (s. Ziff. 2.2), nicht mehr möglich.

Die Gemeinsame Kontrollinstanz fordert deshalb eine institutionalisierte Zusammenarbeit der nationalen Datenschutzbeauftragten, mit den in Art. 115 Schengener Durchführungsübereinkommen genannten Aufgaben.

Art. 115 SDÜ

...

(2) In Bezug auf die technische Unterstützungsarbeit hat die Gemeinsame Kontrollinstanz die Aufgabe, die richtige Anwendung der Bestimmungen dieses Übereinkommens zu überprüfen. Sie hat hierfür Zugriff auf den zentralen Bestand.

(3) Die Gemeinsame Kontrollinstanz ist auch zuständig für die Prüfung der Anwendungs- und Auslegungsfragen im Zusammenhang mit dem Funktionieren des Schengener Informationssystems, für die Prüfung von Fragen im Zusammenhang mit den von den nationalen Kontrollinstanzen unabhängig vorgenommenen Kontrollen oder mit der Ausübung des Auskunftsrechts sowie für die Erarbeitung harmonisierter Vorschläge im Hinblick auf eine gemeinsame Lösung für die bestehenden Fragen.

- Die Speicherfristen für verschiedene Ausschreibungen werden von drei auf fünf bzw. zehn Jahre erhöht. Diese Erhöhung ist für die Gemeinsame Kontrollinstanz nicht nachvollziehbar, insbesondere auch weil in den vorausgehenden Dokumenten von einer Änderung der Speicherungsfrist nicht die Rede war. Wichtig erscheint der Kontrollinstanz eine regelmäßige Überprüfung der Erforderlichkeit der weiteren Speicherung und – falls diese erforderlich sein sollte – die Dokumentation der sie tragenden Gründe.
- Die Entwürfe sehen neben anderen Rechten des Betroffenen sowohl ein Auskunftsrecht (Art. 51 des Entwurfs für einen Beschluss) als auch ein so genanntes Recht auf Informationen (Art. 50 des Entwurfs für einen Beschluss) vor.

Art. 50

Recht auf Informationen

1. Auf Antrag erhält eine Person, deren Daten gemäß diesem Beschluss im SIS II verarbeitet werden, folgende Auskünfte:
 - a) die Identität der für die Verarbeitung verantwortlichen Stelle
 - ...

Solange dieses Informationsrecht nur auf Antrag gewährt werden soll, macht es neben der Existenz des Auskunftsrechts keinen Sinn. Es scheint, dass in Art. 50 zwei verschiedene Prinzipien kombiniert wurden: Das Recht des Bürgers darüber benachrichtigt zu werden, dass Daten zu seiner Person gespeichert sind (z. B. Art. 10 und 11 der EG-Datenschutzrichtlinie 95/46 vom 24. Oktober 1995) und das Auskunftsrecht. Die Gemeinsame Kontrollinstanz plädiert deshalb dafür, das Erfordernis der Antragstellung in Art. 50 zu streichen und damit ein Benachrichtigungsrecht – mit evtl. erforderlichen Ausnahmen – einzuführen.

3.3.2

Gemeinsame Überprüfungen der Ausschreibungen zu Drittausländern

In den letzten Tätigkeitsberichten (33. Tätigkeitsbericht, Ziff. 3.1.3, 32. Tätigkeitsbericht, Ziff. 3.3) hatte ich von einer in allen Schengen-Staaten nach gleichen Kriterien vorgenommenen Prüfung von Ausschreibungen zu Drittausländern berichtet. Die Ergebnisse sind in den Abschlussbericht der Gemeinsamen Kontrollinstanz vom 20. Juni d. J. eingeflossen. In diesem Bericht werden folgende Feststellungen getroffen:

- Die Gründe im nationalen Recht für eine Ausschreibung differieren sehr, es besteht das Bedürfnis nach einer Harmonisierung.
- Das Gleiche gilt für die Speicherfristen. Da die nationalen Aufbewahrungsfristen sehr unterschiedlich sind, wirkt sich dies auch auf die Praxis der Speicherung im SIS aus.

- Es ist sicherzustellen, dass keine EU-Staatsbürger gespeichert werden. In Deutschland ist dies durch technische Vorkehrungen ausgeschlossen.
- In formalen Verfahrensanleitungen muss sichergestellt werden, dass die für die Einspeicherung zuständigen Behörden nur richtige, aktuelle und erforderliche Daten verarbeiten.

3.3.3

Auswirkungen der gemeinsamen Überprüfung in Hessen

Das hessische Ergebnis der im Jahre 2004 stattgefundenen gemeinsamen Überprüfung hatte ich in meinem letzten Tätigkeitsbericht (Ziff. 3.2) ausführlich dargestellt. Zusammengefasst stellte ich fest, dass in über 10 % der geprüften Fälle die Ausschreibungsvoraussetzungen nicht vorlagen. Ausschreibungen, die älter als drei Jahre waren, waren überwiegend unrechtmäßig gespeichert. Als erste Konsequenzen hatte ich ebenfalls berichtet, dass in allen Einzelfällen die Fehler korrigiert und dass interne Dienstanweisungen erlassen oder sonstige organisatorische Maßnahmen getroffen wurden. Das Hessische Innenministerium hatte ich über das Ergebnis informiert.

In der unter meinem Vorsitz tagenden Arbeitsgruppe der für das Ausländerrecht zuständigen Referenten des Bundes- und der Landesdatenschutzbeauftragten wurden die Prüfergebnisse aus den Bundesländern gegenübergestellt. Dabei ergaben sich sehr unterschiedliche Ergebnisse, Beurteilungen und Analysen. Deshalb kam man überein, dass die Landesdatenschutzbeauftragten jeweils in ihrem Bundesland versuchen sollten, die festgestellten Mängel soweit wie möglich zu beheben.

Kurz nach dieser Festlegung hatte ich im Zusammenhang mit der Bearbeitung einer Eingabe nach Art. 114 Abs. 2 des Schengener Durchführungsübereinkommens (SDÜ) dazu Gelegenheit.

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. ...

Ein marokkanischer Staatsangehöriger, der im Jahre 1998 nach abgelehntem Asylantrag die Bundesrepublik auf dem Landwege verlassen wollte, war nach dem Grenzübergang in Weil am Rhein in der Schweiz verhaftet, nach Frankfurt rücküberführt und nach einer Abschiebehaft von zwei Wochen (zur Beschaffung eines Flugtickets) nach Casablanca abgeschoben worden. Er stellte Ende des Jahres 2004 ein Ersuchen nach Art. 114 Abs. 2 SDÜ, für dessen Bearbeitung meine Zuständigkeit gegeben war, weil eine hessische Ausländerbehörde die Datenspeicherung im Schengener Informationssystem verfügt hatte. Meine Überprüfung hatte ergeben, dass die Ausschreibung rechtmäßig war, denn sie knüpft formal an die tatsächlich stattgefundenene zwangsweise Rückführung an. Doch nach drei Jahren hätte gemäß Artikel 112 Abs. 1 SDÜ die Erforderlichkeit der Fortdauer der Datenspeicherung überprüft werden müssen.

§ 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.

Das entsprechende Schreiben des Bundeskriminalamtes, welches rechtzeitig auf den Ablauf der Dreijahresfrist hinweist, war auch in der Akte abgeheftet. Allerdings war eine Prüfung oder sonstige Bearbeitung nicht ersichtlich. Der Betreffende hatte außer dem Verstoß gegen das Ausländerrecht keine Straftat begangen. Er war nie mit falscher Identität eingereist. Es war aktenkundig, dass er versucht hatte, dem Ausreiseverlangen nachzukommen. Er hatte auch – nach Aktenlage – nicht versucht, entgegen des Einreiseverbotes noch einmal ins Schengengebiet einzureisen. Nach alledem war nichts ersichtlich, was eine Verlängerung des Einreiseverbotes hätte begründen können. Die Speicherung war demnach seit dem Jahr 2001 nicht rechtmäßig.

Da zum Zeitpunkt meiner Prüfung erneut weitere drei Jahre verstrichen waren, war nichts zu veranlassen, denn die Datenspeicherung war gerade gelöscht. Denn beim zweiten Verstreichen der Dreijahresfrist muss nicht mehr das Löschen der Daten, sondern die Fortdauer der Datenspeicherung ausdrücklich veranlasst werden. Beim ersten Mal werden die Daten automatisch weiterspeichert, beim zweiten Mal werden sie automatisch gelöscht. Da die Ausländerbehörde auch die zweite Frist verstreichen ließ, waren die Daten gelöscht.

Ich hatte diesen Fall dem Hessischen Innenministerium mitgeteilt. Es war die typische Fallgestaltung, wie sie von mir bei der zuvor beschriebenen strukturell angelegten Prüfung in über der Hälfte aller Fälle oben beschrieben wurde: Die nach Art. 112 Abs. 1 SDÜ vorgeschriebene Prüfung nach drei Jahren unterbleibt einfach.

Das Hessische Innenministerium hat sich in einem Erlass an die Regierungspräsidien meiner Beurteilung angeschlossen, diese wiederum haben den Erlass an alle Ausländerbehörden zur künftig strikten Beachtung der notwendigen Differenzierungen weitergegeben. Im Berichtsjahr wurden mir Wiederholungsfälle nicht offenbar.

3.4

Gemeinsame Kontrollinstanz für EUROPOL

Der Vorsitz der Gemeinsamen Kontrollinstanz hat im Dezember 2004 von dem damaligen Landesdatenschutzbeauftragten von Sachsen-Anhalt, Herrn Rainer Kalk, zu dem Spanier Emilio Aced Feléz gewechselt.

Die Gemeinsame Kontrollinstanz hat ihren zweiten Tätigkeitsbericht für die Jahre 2003 und 2004 vorgelegt. Er ist im Februar 2005 auch in Deutsch erschienen.

Auch EUROPOL hat seit April 2005 einen neuen Direktor. Herr Jürgen Storberg wurde von Max Peter Ratzel abgelöst. Derzeit hat EUROPOL etwa 500 Mitarbeiter, bis 2007 sollen es 700 werden. Dazu kommen die aus den Mitgliedstaaten entsandten Verbindungsbeamten.

Im Berichtszeitraum fanden vier Sitzungen der Gemeinsamen Kontrollinstanz statt, an denen ich bzw. meine Mitarbeiterin teilnahm. Dabei wurden folgende Probleme behandelt:

3.4.1

Verbesserter Zugang zu Dokumenten

Um den Bürgern einen besseren Zugang zu den von der Gemeinsamen Kontrollinstanz für EUROPOL erstellten Dokumenten zu ermöglichen, hat diese eine Änderung ihrer

Geschäftsordnung vorgenommen. Sie hat das ehemals in Art. 6 Abs. 4 der Geschäftsordnung enthaltene Prinzip, dass die Dokumente vertraulich sind, solange die Gemeinsame Kontrollinstanz keine andere Entscheidung trifft, ins Gegenteil umgekehrt. Nunmehr sind in der Regel alle Dokumente zugänglich, Ausnahmen sind nur in Einzelfällen, z. B. zum Schutz der Sicherheit und öffentlichen Ordnung zulässig.

Auch die Protokolle der Sitzungen der Gemeinsamen Kontrollinstanz sollen auf der Website veröffentlicht werden.

Diese Bemühungen um mehr Transparenz entsprechen der innerhalb der EU-Institutionen angestrebten verbesserten Informationspolitik.

3.4.2

Stellungnahme zu Analysedateien

Für jede neue Analysedatei, die EUROPOL gemäß Art. 10 des EUROPOL-Übereinkommens einrichten will, muss nach Art. 12 des Übereinkommens eine Errichtungsanordnung erstellt werden. Diese soll u. a. den Zweck der Datei und die Art der zu speichernden Daten festlegen. Diese Anordnungen bedürfen der Zustimmung des Verwaltungsrates von EUROPOL, der verpflichtet ist, die Stellungnahme der Gemeinsamen Kontrollinstanz einzuholen.

Im Berichtszeitraum hat die Gemeinsame Kontrollinstanz sich zu drei Errichtungsanordnungen für Analysedateien geäußert. In allen Fällen hat die Gemeinsame Kontrollinstanz keine Änderungen des Inhalts der Errichtungsanordnungen gefordert.

3.4.3

Prüfung der Rechtmäßigkeit einer etwaigen Speicherung

Anlässlich des Ersuchens eines Bürgers, zu prüfen, ob die etwaige Speicherung seiner Daten bei EUROPOL rechtmäßig ist, hat die Gemeinsame Kontrollinstanz Vorschläge entwickelt, auf welche Weise dem Bürger in diesem Fall zu antworten ist.

Art. 24 Abs. 4 EUROPOL-Übereinkommen lautet:

Jede Person hat das Recht, die Gemeinsame Kontrollinstanz zu ersuchen, die Zulässigkeit und die Richtigkeit seiner etwaigen Speicherung, Erhebung, Verarbeitung und Nutzung von sie betreffenden Daten bei EUROPOL zu überprüfen.

Dieses Recht ist zu unterscheiden von dem an das BKA bzw. EUROPOL zu richtende Auskunftsbegehren nach Art. 19 der EUROPOL-Übereinkommen. Es ist weiter zu trennen von der Möglichkeit, sich bei der Gemeinsamen Kontrollinstanz über eine nicht befriedigende Antwort von EUROPOL zu beschweren (Art. 19 Abs. 7 EUROPOL-Übereinkommen).

Die Mehrheit der Delegationen in der Gemeinsamen Kontrollinstanz ist der Auffassung, dass bei dem Ersuchen nach Art. 24 Abs. 4 EUROPOL-Übereinkommen die Überprüfung der Rechtmäßigkeit der Speicherung im Vordergrund steht. Dem Betroffenen soll danach in den Fällen, in denen nichts über ihn gespeichert oder die Speicherung in Ordnung ist, nur mitgeteilt werden können, dass die Gemeinsame Kontrollinstanz nach erfolgter Prüfung festgestellt hat, dass EUROPOL in Übereinstimmung mit den EUROPOL-Übereinkommen gehandelt hat. Nur im Falle einer rechtswidrigen Speicherung soll dem Betroffenen die Tatsache der Speicherung zwangsläufig bekannt gemacht werden können.

3.4.4

Prüfung der Abkommen mit Drittstaaten

Die Übermittlung von personenbezogenen Daten an einen Staat, der nicht zur Europäischen Union gehört, setzt die Unterzeichnung eines formellen Abkommens zwischen EUROPOL und dem betreffenden Staat voraus. Dabei ist der zuständige Verwaltungsrat von EUROPOL verpflichtet, vor Abschluss eines derartigen Abkommens die Stellungnahme der Gemeinsamen Kontrollinstanz einzuholen. Bisher wurden bereits mit Bulgarien und Rumänien derartige Abkommen abgeschlossen, im Berichtszeitraum folgten Abkommen mit Kanada und Kroatien. Die Gemeinsame Kontrollinstanz hat sich in beiden Fällen zu den Abkommen geäußert und kam zu dem Ergebnis, dass aus Sicht des Datenschutzes keine Einwände gegen einen Abschluss der Abkommen durch EUROPOL bestehen.

3.4.5

Kontrolle von EUROPOL

Die Gemeinsame Kontrollinstanz hat im März 2005 wieder eine Kontrolle von EUROPOL durchgeführt. Der Bericht über diese Kontrolle ist vertraulich. Die Gemeinsame Kontrollinstanz diskutiert derzeit die schriftliche Stellungnahme von EUROPOL zu diesem Bericht.

4. Bund

4.1

Rechtsprechung des Bundesverfassungsgerichtes zum Kernbereich privater Lebensgestaltung

Das Bundesverfassungsgericht hat in einer Entscheidung zum Niedersächsischen Polizeigesetz seine Feststellungen aus dem Jahre 2004 zum Schutz des Kernbereichs privater Lebensgestaltung vor Eingriffen des Staates nochmals verdeutlicht.

Schon in seinen Entscheidungen vom 3. März 2004 zum so genannten Lauschangriff und zur Telekommunikationsüberwachung im Außenwirtschaftsgesetz hat das Bundesverfassungsgericht einen Kernbereich privater Lebensgestaltung definiert, der sich aus der Unantastbarkeit der Menschenwürde des Art. 1 GG ableitet (BVerfGE 109, 279 ff. und BVerfGE 110, 33 ff.). Über diese Entscheidungen sowie eine erste Einschätzung, inwieweit diese Auswirkungen auf bestehende Rechtsgrundlagen für staatliche Überwachungsmaßnahmen haben, habe ich im 33. Tätigkeitsbericht, Ziff. 4.1 berichtet.

Nunmehr hat das Bundesverfassungsgericht in einem Urteil vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz (1 BvR 668/04) daran angeknüpft und klargestellt, dass entsprechende Anforderungen für jegliche Art von verdeckten Ermittlungsmaßnahmen gelten.

Das Gericht hebt hervor, ein Erhebungsverbot bestehe, wenn in einem konkreten Fall Anhaltspunkte vorliegen, dass eine Überwachungsmaßnahme Inhalte erfassen könne, die zu dem definierten Kernbereich gehören. Ein wissentlicher Eingriff in den Kernbereich sei in keinem Fall zu rechtfertigen. Bloße Verwertungsverbote reichten in diesen Fällen nicht aus. Schließlich verdeutlicht das Bundesverfassungsgericht erneut, dass Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen wesentlicher Bestandteil der Regelungen zu verdeckten Ermittlungsmaßnahmen sind.

Zur Schutzwirkung des Art. 10 GG – Telekommunikationsgeheimnis – stellt das Gericht klar, dass sich diese auch auf die Informationen und Datenverarbeitungsprozesse bezieht, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen und von diesen

Gebrauch machen. Konkret: Das Niederschreiben von Gesprächsinhalten, die durch eine Telefonüberwachungsmaßnahme der Sicherheitsbehörde bekannt werden, unterliegt ebenfalls dem Schutz des Art. 10 GG. Dies gilt unabhängig davon, ob es sich um ein wörtliches Protokoll der technisch aufgezeichneten Daten handelt oder um eine Zusammenfassung in einem Vermerk. Konsequenz ist, dass solche Vorgänge entsprechend zu kennzeichnen sind. Damit kann sichergestellt werden, dass bei der Entscheidung, ob diese Daten an andere Stellen übermittelt werden dürfen, entsprechende Beschränkungen berücksichtigt werden können. Dem Empfänger ist eine entsprechende Kennzeichnung mitzuteilen und er hat dann ebenfalls die Beschränkungen in der Verwendung dieser Daten zu beachten.

In diesem Kontext weist das Gericht auch darauf hin, dass jeder Eingriff in das Telekommunikationsgeheimnis schwerwiegende Auswirkungen haben kann. Das gelte auch für die Verbindungsdaten. Damit würden zwar keine Inhalte der Kommunikation betroffen, aber häufig ließe sich auf Gewohnheiten von Personen schließen oder gar Bewegungsbilder erstellen.

Vom Gesetzgeber verlangt das Bundesverfassungsgericht, gerade auch dann wenn hochrangige Rechtsgüter betroffen sind, dass der Entscheidung über die Einführung bzw. Ausgestaltung von Eingriffsmaßnahmen ein Konzept zugrunde liegt, zur Aufklärung welcher Delikte ein bestimmtes Instrument zum Einsatz kommen soll.

Damit hat das Gericht selber nochmals verdeutlicht, dass dieser Maßstab über den Lauschangriff hinaus sowohl im Bereich der Strafverfolgung als auch der Gefahrenabwehr zu beachten ist. In diesem Sinne hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer EntschlieÙung vom 27./28. Oktober 2005 die Gesetzgeber in Bund und Ländern aufgefordert, ohne Abstriche die Vorgaben des Bundesverfassungsgerichts zum Schutz des Kernbereichs privater Lebensgestaltung umzusetzen (vgl. Ziff. 10.10).

4.1.1

Konsequenzen für das Land Hessen

Auch im HSOG besteht weiterhin Novellierungsbedarf, um den vom Bundesverfassungsgericht formulierten Anforderungen gerecht zu werden.

Bei der Novelle des HSOG im Jahre 2004 hat sich der Gesetzgeber bemüht, die vom Bundesverfassungsgericht formulierten Rahmenbedingungen zu verwirklichen. Dabei hat er sich nicht auf Regelungen zum Lauschangriff beschränkt, sondern es gab grundsätzliche Anpassungen für alle verdeckten Datenerhebungen. Das Ergebnis ist aus Sicht der verfassungsrechtlichen Anforderungen jedoch noch nicht zufriedenstellend. Teilweise hat der Gesetzgeber die Konsequenzen nicht gesehen, in anderen Punkten sind die getroffenen Änderungen nicht ausreichend.

Im 33. Tätigkeitsbericht (Ziff. 5.1.1.2) hatte ich schon auf diese Defizite hingewiesen. Angesprochen hatte ich folgende Gesichtspunkte: Eine einheitliche Definition für Straftaten mit erheblicher Bedeutung kann der unterschiedlichen Intensität der Grundrechtseingriffe bei den verschiedenen verdeckten Erhebungsmethoden nicht gerecht werden. Für die akustische Wohnraumüberwachung ist für Erkenntnisse aus dem Kernbereich privater Lebensgestaltung nur ein Verwertungsverbot und kein Erhebungsverbot ausgesprochen. Schließlich fehlen im Zusammenhang mit der Telekommunikationsüberwachung Regelungen zum Schutz des Kernbereichs völlig.

4.1.1.1

Daten aus dem Kernbereich privater Lebensgestaltung

Die Ausführungen in der Begründung zur letztjährigen HSOG-Novelle (LTDrucks. 16/2352) zeigen, dass der Gesetzgeber die Konsequenzen aus der Rechtsprechung des Bundesverfassungsgerichts nicht zutreffend bewertet hat. Dort wird im Zusammenhang mit der Einführung der Telekommunikationsüberwachung die Notwendigkeit eines Verwertungsverbotes damit begründet, dass Erkenntnisse, die sich auf eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person oder auf eine Straftat beziehen, nicht zum Kernbereich privater Lebensgestaltung gehören können. Unabhängig davon, dass auch dies nicht immer zutrifft – so hat der Bundesgerichtshof Selbstgespräche mit Ausführungen zu einer Straftat dem Kernbereich zugerechnet (BGH-Urteil vom 10. August 2005, NJW 2005, 3295 ff.) – lässt diese Regelung außer Acht, dass bei der Überwachung, insbesondere wenn sie durch technisches Aufzeichnen erfolgt, natürlich zunächst nicht nur die Gesprächspassagen erfasst werden, die direkte Aussagen zur Gefahrensituation beinhalten, sondern ggf. auch im nicht unerheblichen Umfang andere Gespräche. Für die Behandlung dieser Informationen ist eine Regelung notwendig. Diese muss

auch über ein Verwertungsverbot hinausgehen. Für die Fälle der Telekommunikationsüberwachung, in denen bei der Anordnung nicht sicher vorhersehbar ist, dass auch Gespräche aus dem Kernbereich erfasst werden, sagt das Bundesverfassungsgericht nunmehr ausdrücklich, dass diese unverzüglich zu löschen sind. Kommunikationsinhalte des höchstpersönlichen Bereichs dürfen nicht gespeichert werden (Rz. 164 von 1 BvR 668/04). Erst recht gilt dies für den Bereich des Lauschangriffs, für den schon der Gesetzgeber grundsätzlich die Möglichkeit, dass auch Informationen aus dem Kernbereich betroffen sein können, nicht ausgeschlossen hat.

Immer dann wenn eine Information, die durch verdeckte Ermittlungsmethoden erhoben wurde, als zum Kernbereich privater Lebensführung gehörig erkannt ist, muss diese sofort gelöscht werden, und zwar in allen vorhandenen Unterlagen.

4.1.1.2

Straftaten von erheblicher Bedeutung

Gerade für den Bereich der Telekommunikationsüberwachung zu präventiven Zwecken stellt das Bundesverfassungsgericht nunmehr erneut klar, dass es notwendig ist, die Auswahl der Straftaten den besonderen Anforderungen des Telekommunikationsgeheimnisses anzupassen. Dies ist auch eine originäre Aufgabe des Gesetzgebers. Dagegen hatte der Landesgesetzgeber die einheitliche Definition der Straftat mit erheblicher Bedeutung ausdrücklich mit einem notwendigen Spielraum für die Polizei begründet. Ein starrer Katalog sei schwer handhabbar. Damit sollten auch Sicherheitslücken vermieden werden (LTDrucks. 16/2352, S. 16 f). Wenn auch die Gründe von der Abkehr vom Katalog zu einer eher abstrakten Definition noch nachvollziehbar erscheinen, bleibt doch die Frage der Verhältnismäßigkeit der umschriebenen Straftaten als Grundlage für die einzelnen Eingriffsmaßnahmen offen.

4.2

Einführung des E-Passes

Obwohl bisher die notwendigen rechtlichen, organisatorischen und technischen Maßnahmen zur Einführung des so genannten E-Passes mit biometrischen Merkmalen noch nicht fertig gestellt

sind, werden bereits ab dem 1. November 2005 nur noch elektronisch lesbare Pässe herausgegeben.

Bereits mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I, S. 361 ff.) ist die Aufnahme weiterer biometrischer Merkmale in Reisepässe und Bundespersonalausweise ermöglicht worden. Mit Verordnung des Rates der Europäischen Union vom 13. Dezember 2004 (Nr. 2252/2004) wurden die Mitgliedstaaten verpflichtet, biometriegestützte Pässe für die Bürgerinnen und Bürger der Europäischen Union auszugeben.

Art. 1 Abs. 2 Verordnung Nr. 2252/2004 des Rates über Normen für Sicherheitsmerkmale und biometrische Daten in den von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten

Die Pässe und Reisedokumente sind mit einem Speichermedium versehen, das ein Gesichtsbild enthält. Die Mitgliedstaaten fügen auch Fingerabdrücke in interoperablen Formaten hinzu. Die Daten sind zu sichern, und das Speichermedium muss eine ausreichende Kapazität aufweisen und geeignet sein, die Integrität, die Authentizität und die Vertraulichkeit der Daten sicherzustellen.

Die Verordnung sieht vor, dass zunächst bis Mitte 2006 maschinenlesbare Gesichtsbilder in die Ausweisdokumente aufzunehmen sind. Als zweites biometrisches Merkmal sollen dann bis spätestens Anfang 2008 auch Fingerabdrücke in die Pässe integriert werden. Die beiden biometrischen Merkmale sollen gemäß den Vorgaben der internationalen zivilen Luftfahrtorganisation (ICAO) auf einem Funkchip (RFID-Chip) gespeichert werden.

Obwohl die Bundesrepublik Deutschland nach den europarechtlichen Vorgaben noch etwas Zeit gehabt hätte, die neue Form des Ausweises einzuführen, hat sie bereits zum 1. November 2005 mit der Ausgabe biometriegestützter Pässe begonnen. Zwar ist die Einführung dieser Pässe rechtlich auf Grundlage der EU-Verordnung möglich. Allerdings bedarf es – wie dies auch ausdrücklich in Art. 7 Nr. 1b) Terrorismusbekämpfungsgesetz geregelt ist – klarer rechtlicher Vorgaben insbesondere zur Zweckbindung bei der Verwendung biometrischen Daten.

§ 4 Abs. 4 Satz 1 PassG

Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Absatz 3 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt.

Eine derartige gesetzliche Regelung fehlt bisher.

Aus deutscher Sicht positiv zu bewerten ist dagegen, dass der Bundesgesetzgeber anders als der EU-Verordnungsgeber festgelegt hat, dass es keine zentrale Datenbank mit den für den E-Pass zu erhebenden biometrischen Daten geben wird, obwohl dies von der ICAO so gewünscht war. Die Bundesdruckerei erhält die biometrischen Daten lediglich zur Erstellung des Passes, hält sie dort aber nicht vor. Insofern gibt es keine Änderung zur bisherigen Verfahrensweise.

§ 4 Abs. 4 Satz 2 PassG

Eine bundesweite Datei wird nicht eingerichtet.

Die schnelle Umsetzung der Verordnung bereits zum 1. November 2005 wurde auch damit begründet, dass der neue Pass einen Gewinn an Sicherheit bringe. Dem ist entgegenzuhalten, dass aus Sicht der Bundesdruckerei und auch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bereits der bisherige deutsche Pass nahezu fälschungssicher sei. Insofern hätten durchaus die zunächst notwendigen rechtlichen und technisch-organisatorischen Rahmenbedingungen geklärt werden können.

RFID beim E-Pass

Der E-Pass unterscheidet sich von den herkömmlichen Pässen vor allem dadurch, dass ein RFID-Chip im Rückendeckel integriert ist, auf dem die Daten zur Person inklusive des digitalisierten Lichtbildes, zukünftig auch weitere biometrische Merkmale, gespeichert sind. Durch die Verwendung eines RFID-Chips können die Daten berührungslos aus geringer Entfernung ausgelesen werden.

In den Diskussionen wurde die Verwendung eines RFID-Chip als problematisch angesehen, da es dadurch Unbefugten möglich sei, die gespeicherten Daten ohne Wissen und Willen der

Betroffenen auszulesen. (Generelle Anmerkungen zu RFID habe ich in meinem 33. Tätigkeitsbericht, Ziff. 8.4 gemacht.) Bei der Konzeption des E-Passes, d. h. für die deutsche Ausprägung der Technik, wurden Sicherheitsvorkehrungen getroffen, von denen die Verantwortlichen annehmen, dass sie angemessen sind, um den Zugriff Unbefugter zu verhindern. Die wesentlichen Maßnahmen für die erste Generation des E-Passes von 2005, die die Anforderungen der „Basic Access Control“ umsetzen sollen, möchte ich hier skizzieren.

Basic Access Control

Von der ICAO formulierte Sicherheitsanforderungen an maschinenlesbare Ausweisdokumente.

- Der Chip ist passwortgeschützt.
Damit Daten vom Chip gesendet werden, muss das Lesegerät mit dem richtigen Passwort abfragen. Der Aufbau des Passworts ist allerdings bekannt. Es handelt sich um den Inhalt der MRZ (machine readable zone). Auch wenn diese von Pass zu Pass differiert, kann man sie hinsichtlich der Qualität nicht mit einem sorgfältig gewählten Passwort vergleichen.
- Die Datenübertragung zwischen Chip und Lesegerät erfolgt verschlüsselt.
Die gewählten Schlüssel werden in einem Challenge-Response-Verfahren ausgehandelt.

Challenge-Response-Verfahren

Verfahren zum Schlüsselaustausch, bei dem jeweils unterschiedliche Schlüssel für die Sicherung der Übertragung gewählt werden.

- Der RFID-Chip besitzt keine feste Kennung
Wird ein RFID-Chip von einem Lesegerät abgefragt, antwortet er üblicherweise mit einer festen Kennung. Hierdurch wäre es möglich, auch mit nicht zugelassenen Lesegeräten einen bestimmten Pass zu verfolgen. Der Chip im E-Pass meldet sich jedoch bei jeder Abfrage mit einer anderen, von einem Zufallszahlengenerator erzeugten Kennung.
- Geringe Leseentfernung
Es wurde ein RFID-Chip ausgewählt, der eine Leseentfernung von wenigen Zentimetern zulässt. Das Abhören der Kommunikation ist aus erheblich größerer Entfernung möglich.

Genauere Aussagen zur möglichen Lese- bzw. Abhörentfernung mit aufwändiger Technik stehen noch aus. Sie sollen vom BSI durch Tests ermittelt werden.

Für die zweite Stufe, wenn auch die Fingerabdrücke hinterlegt werden, sind weitere Sicherheitsmaßnahmen geplant. So sollen dann durch den Chip Zertifikate geprüft werden, die nur zugelassene Lesegeräte besitzen. Die Zertifikate werden eine beschränkte Gültigkeit haben.

4.3

Fußball-Weltmeisterschaft 2006

Nicht nur aus der Sicht des Sports, sondern auch sicherheitspolitisch stellt die Ausrichtung der Fußball-Weltmeisterschaft eine Herausforderung dar. Bei der Organisation eines solchen Großereignisses ergeben sich damit auch vielfältige datenschutzrechtliche Fragen.

Ein symbolträchtiges Großereignis wie die Fußball-Weltmeisterschaft 2006 ist mit erheblichen Sicherheitsrisiken verbunden. In erster Linie die Sicherheitsbehörden sind hier aufgerufen, die gebotenen Vorkehrungen zur Gefahrenabwehr und Risikoversorge zu treffen. Dazu hat ein Bund-Länder-Ausschuss der Innenministerkonferenz ein Sicherheitskonzept erarbeitet, dessen Kernstück ein polizeiliches Rahmenkonzept über den Einsatz und die Aufgaben der Polizeien der Länder und des Bundes darstellt. Dieses Rahmenkonzept hat datenschutzrechtlichen Anforderungen zu genügen und ist datenschutzkonform zu handhaben, auch wenn die sicherheitspolitischen Aspekte bislang weniger Aufmerksamkeit in der Öffentlichkeit fanden als die datenschutzrechtlichen Probleme.

Immerhin wurde in der Öffentlichkeit die Ticketvergabe bzw. die Gestaltung der Tickets mit den eingesetzten RFID-Chips diskutiert. Erhebliche datenschutzrechtliche Belange sind auch bei der Akkreditierung der Personen zu berücksichtigen, die rund um die Spiele für die Abwicklung eingesetzt werden. Das betrifft eine große Zahl von Personen (z. B. Würstchenverkäufer/innen, Ordnungskräfte, Medienvertreter/-innen).

Bei der Abwicklung der Fußball-Weltmeisterschaft sind aus Sicht des Datenschutzes noch weitere Umstände zu berücksichtigen. An der Abwicklung beteiligt sind verschiedenste Stellen in unterschiedlichen Rechtsformen. Bei der Fußball-Weltmeisterschaft handelt es sich um eine

Veranstaltung der „FIFA“. Die FIFA hat ihren Sitz in der Schweiz. Organisiert wird die WM von einem Organisationskomitee, das dem DFB, einem privatrechtlichen Verein, zugeordnet ist. Für die Wahrung der Sicherheitsbelange sind die Polizei und ggf. weitere Sicherheitsbehörden verantwortlich. Daraus ergeben sich auch unterschiedliche Zuständigkeiten im Bereich der Datenschutzaufsicht. Für den DFB mit Sitz in Frankfurt ist das Regierungspräsidium in Darmstadt zuständig. Dies gilt auch für das Organisationskomitee. Die Sicherheitsbehörden werden durch die jeweils zuständigen Datenschutzbeauftragten des Bundes und der Länder kontrolliert. Die Notwendigkeit einer Zusammenarbeit der jeweiligen Sicherheitsbehörden liegt auf der Hand. Zur Koordination dient eine Bund-Länder Arbeitsgruppe. Mit dieser arbeitet auch der DFB zusammen. Zur Wahrung des Datenschutzes müssen die Datenschutzbeauftragten dementsprechend ebenfalls ihre Aktivitäten koordinieren. Zu diesem Zweck hat sich schon seit dem letzten Jahr eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit den verschiedenen datenschutzrechtlichen Aspekten der Fußball-Weltmeisterschaft beschäftigt. Mein Anliegen ist es dabei, sachadäquaten, den besonderen Anforderungen dieses Großereignisses gerecht werdenden Datenschutz zu gewährleisten. Auch mit dem Regierungspräsidium in Darmstadt arbeiten meine Mitarbeiterinnen und Mitarbeiter eng zusammen. So gab es u. a. einen Ortstermin anlässlich des Confederations-Cups im Frankfurter Stadion, um dort einzelne Aspekte im Einsatz zu beurteilen.

4.3.1

Allgemeine Sicherheitsfragen

Wie bei allen solchen Großereignissen beschäftigen sich die Sicherheitsbehörden frühzeitig mit der Planung des Ereignisses. Das gilt – soweit Frankfurt als Spielort betroffen ist – für die hessische Polizei ebenso wie für alle sonst zu beteiligenden Sicherheitsbehörden. Polizeitaktische Erwägungen verbieten es, alle geplanten Sicherheitsmaßnahmen öffentlich zu machen. Andererseits besteht das Anliegen, die Öffentlichkeit nach Möglichkeit umfassend zu informieren. Das kann dann im Einzelfall dazu führen, dass öffentliche Äußerungen einzelner Beteiligter missverständlich ausfallen und deshalb zu Irritationen führen. Dies galt etwa im Anschluss an den Confederations-Cup für Aussagen zum Einsatz von Videoüberwachungsmaßnahmen. Hier ist die Rechtslage eindeutig: Soweit es um den Einsatz von Videokameras in den Innenstädten, etwa auf Plätzen mit Großbildleinwänden geht, gibt das HSOG den engen Rahmen für Überwachungsmaßnahmen vor. Ein spontaner Einsatz von mobilen Kameras ist somit praktisch

ausgeschlossen. Das Innenministerium hat mir in diesem Zusammenhang bestätigt, dass über die vorhandenen Anlagen hinaus keine zusätzlichen besonderen Überwachungsanlagen für den Zeitraum der Fußball-Weltmeisterschaft eingesetzt werden sollen. Daneben kommt die Anlage im Frankfurter Stadion – wie bei jedem Liga-Spiel – zum Einsatz, mit der das Geschehen im Stadionbereich überwacht werden kann. Damit wird zunächst, soweit notwendig, der Einsatz der Sicherheitskräfte im Stadion gesteuert. Je nach Situation werden auch die Aufnahmen einzelner Kameras gespeichert, um bestimmte Vorkommnisse zu dokumentieren bzw. um für sich ggf. anschließende strafrechtliche Verfahren Beweismaterial zu sichern.

4.3.2

Eintrittstickets

Im Hinblick auf das Verfahren des Erwerbs und die Gestaltung der Tickets sind aus datenschutzrechtlicher Sicht zwei Themen relevant. Diese betreffen:

- die Informationen, die ein Besucher angeben muss, um Tickets zu erwerben bzw. ein Stadion betreten zu können sowie
- den Einsatz der RFID-Chips, um Daten zu speichern und auszulesen.

Mit dieser Fragestellung hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Frühjahr des Jahres befasst (vgl. Ziff. 10.2).

Dass der Veranstalter eine Kontrolle haben möchte, wer an dieser Veranstaltung teilnimmt bzw. dass ausgesondert werden soll, wer als Störer bekannt ist und etwa auch schon mit einem Stadionverbot belegt wurde, ist aus meiner Sicht verständlich. Folglich ist es auch notwendig, die Personalien eines jeden Karteninhabers zu kennen. Nur so kann der Veranstalter die Personalien mit seinen Stadionverbotsdateien abgleichen. Auch die Verwendung der Ausweisnummer ist aus meiner Sicht nicht zu kritisieren. Ein Vergleich mit den bei der Bestellung angegebenen Daten und dem Ausweis beim Betreten des Stadions ist vielmehr zulässig. Der Speicherung dieses Datums steht auch das Personalausweisgesetz nicht entgegen. Das Personalausweisgesetz verbietet nur, die Ausweisnummer als Ordnungsmerkmal in der eigenen Datenverarbeitung einzusetzen. Damit ist jedoch nicht jegliche Verwendung bzw. Speicherung ausgeschlossen. So kann die Ausweisnummer gespeichert werden als Dokumentation, dass eine entsprechende Legitimation vorgelegt wurde.

Ein weiterer Kritikpunkt in diesem Verfahren wurde inzwischen vom DFB klargestellt. Erhoben werden die Personalien von *allen* Ticketinhabern, also auch für die so genannten Sponsorentickets. Die Sponsoren sind verpflichtet, bis zu einem bestimmten Zeitpunkt vor dem jeweiligen Spiel die Angaben über die Karteninhaber vorzulegen, so dass auch für diese noch die Überprüfung in der Stadionsverbotsdatei erfolgen kann. Wenn entsprechende Daten nicht vorliegen, bleibt das Ticket gesperrt; ein Betreten des Stadions ist nicht möglich.

Um Daten zu speichern und auslesen zu können, befindet sich auf dem Ticket ein RFID-Chip. Die grundsätzlich damit zusammenhängenden Probleme habe ich in meinem 33. Tätigkeitsbericht, Ziff. 8.4 beschrieben. Als wesentlicher Kritikpunkt wird in den Diskussionen die Möglichkeit genannt, ohne Wissen und Wollen des Besitzers die gespeicherten Daten auslesen zu können. Für eine datenschutzrechtliche Bewertung spielt es auch noch eine Rolle, um welche Daten es sich handelt.

Nach den mir vorliegenden Informationen wird ein RFID-Chip genutzt, der eine maximale Leseentfernung – das ist die Entfernung zwischen Lesegerät und Chip – von 15 cm hat. Der Datenaustausch zwischen dem Chip und einem Lesegerät kann allerdings aus größerer Entfernung abgehört werden. Ob es Möglichkeiten gibt, die Zugriffe auch über längere Strecken vorzunehmen, wird derzeit untersucht.

Die Daten selbst werden verschlüsselt gespeichert. Nur zum System gehörende Lesegeräte verfügen über den Schlüssel, um die Daten zu entschlüsseln. Sollte es dennoch unbefugten Personen gelingen, die Daten zu lesen und zu entschlüsseln, so erhalten sie damit keinen Namen, Anschrift oder Ähnliches, sondern eine Identifikationsnummer, die zu dieser Karte gehört. Die Daten zu einem Karteninhaber, zu denen die Identifikationsnummer seiner Karte gehört, sind auf dem Stadionrechner gespeichert. Über diese Nummer wird bei Kontrollen auf die Daten des Inhabers zugegriffen. Weitere auf der Karte gespeicherte Daten betreffen den Sitzplatz und die Information, ob mit der Karte bereits das Stadion betreten wurde.

Es ist denkbar, die Karte zu „verfolgen“, um Rückschlüsse über das Verhalten einer Person zu erlangen. Angesichts der kurzen Leseentfernung handelt es sich dabei um eine Information, die man auch ohne RFID-Chip erhält, wenn man der Person folgt. Außerdem wird diese Karte nicht

über einen längeren Zeitraum benutzt, was andernfalls im Zusammenhang mit RFID-Chips immer die Möglichkeit zur Bildung von Bewegungsprofilen impliziert.

Wenn die beschriebenen Schutzmaßnahmen konsequent umgesetzt sind, halte ich den Einsatz von RFID-Chips für akzeptabel.

4.3.3

Akkreditierung

Zur Durchführung eines großen Sportereignisses sind eine Fülle von organisatorischen Vorkehrungen zu treffen. Dazu gehören auch differenzierte Sicherheitsmaßnahmen. Eine Vielzahl von Personen wird im Umfeld der einzelnen Spiele tätig werden. Diese benötigen alle eine formale Akkreditierung. Der zu akkreditierende Personenkreis umfasst Mitarbeiter der FIFA und des Organisationskomitees, Angehörige der Mannschaften und Begleitdelegationen, Mitarbeiter und Berechtigte der offiziellen Partner des Veranstalters, Presseangehörige sowie Angehörige und Mitarbeiter des Fernsehens und Personen, die im Bereich Sicherheit und durch die Hilfsdienstorganisationen eingesetzt werden können einschließlich Polizeibeamte, Freiwillige und Servicebedienstete aller Sparten. Die Veranstalter rechnen mit bis zu 250.000 Akkreditierungsverfahren.

Die Akkreditierung muss beim Organisationskomitee beantragt werden. Dort wird geprüft ob Bedenken gegen die Akkreditierung bestehen. Diese können auf verschiedenen Gründen beruhen. Die Notwendigkeit, die Zahl der Akkreditierten zu beschränken ergibt sich schon aus Kapazitätsgründen. Wichtig sind vor allem aber auch Sicherheitsbelange. Ein wesentlicher Bestandteil des Akkreditierungsverfahrens ist eine Zuverlässigkeitsüberprüfung durch die Sicherheitsbehörden. Diese Zuverlässigkeitsprüfung ist auch aus meiner Sicht zwingend für die die Gewährleistung der Sicherheit der Veranstaltungen notwendig.

Datenschutzrechtlich wird eine derartige Zuverlässigkeitsüberprüfung vielfach für problematisch gehalten. Ausdrückliche gesetzliche Grundlagen für ein solches Verfahren gibt es nämlich nicht. Es ist auch nicht völlig mit anderen sicherheitsrechtlichen Zuverlässigkeitsprüfungen vergleichbar. Vielmehr handelt es sich eher um eine Erkenntnisabfrage bei den betroffenen Behörden. Dabei ist

zu bedenken, dass das Ergebnis nicht an eine öffentliche Stelle übermittelt wird. Das HSOG lässt in § 23 Abs. 1 zwar auch eine Übermittlung von Daten an private Dritte zu.

§ 23 HSOG

(1) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs übermitteln, soweit dies zur

1. Erfüllung gefahrenabwehrbehördlicher oder polizeilicher Aufgaben,
2. Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder
3. Verhütung oder Beseitigung einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist.

Wesentliche Voraussetzung dabei ist jedoch, dass diese Übermittlung im Einzelfall erforderlich ist. Auf die genannte Vorschrift lässt sich die Bearbeitung der hier in Frage stehenden Anfragen daher nicht allein stützen.

Für die Beteiligung des Verfassungsschutzes ergibt sich die gleiche Problematik. Auch hier fehlt eine ausdrückliche gesetzliche Grundlage.

Andererseits kann und will ich mich den besonderen Sicherheitsanforderungen bei diesem singulären Ereignis nicht verschließen. Deshalb habe ich mich – auch nach Erörterungen mit Vertretern des DFB, der Polizei und dem Regierungspräsidium Darmstadt als Aufsichtsbehörde für den Veranstalter – entschlossen, die Abwicklung der Akkreditierungen auf der Grundlage einer Einwilligungslösung zu akzeptieren.

Bei allen Bedenken, die man in diesem Zusammenhang vor allem auch in Bezug auf die Freiwilligkeit der Einwilligung haben kann, ist im Wesentlichen eine Lösung gefunden worden, die den Rechten aller Betroffenen gerecht wird. Gewiss kommt ohne Einwilligung in das Verfahren mancher Arbeitsvertrag nicht zu Stande. Der Eingriff hat indessen nicht einmal die Intensität einer unverhältnismäßigen Berufsausübungsregelung, sofern der Einsatz im Rahmen der WM-Einrichtungen nur einen geringen Teil der beruflichen Tätigkeit ausmacht. Der Einwilligungsdruk ist dann so niedrig, dass die Entscheidungsfreiheit nicht übermäßig eingeschränkt wird. Bei Ad-hoc-Beschäftigungen im Zusammenhang mit der WM spielt ebenfalls eine Rolle, dass es sich um ein einmaliges Ereignis handelt, während die Berufsfreiheit durch das Merkmal der andauernden Erwerbstätigkeit geprägt ist. Ferner ist das Problem der Freiwilligkeit

von Einwilligungen im Rahmen von Arbeitsverhältnissen nicht nur in diesem Kontext vorhanden. Ich verweise nur auf die Vorlage eines Führungszeugnisses bei Einstellungen im öffentlichen Dienst.

Das Akkreditierungsverfahren wird überwiegend über Internet durchgeführt. Dazu müssen die Bewerber für eine Akkreditierung zunächst ein Online-Antragsformular ausfüllen und es dem Organisationskomitee übersenden. Das Formular beinhaltet eine Einwilligungserklärung in die Zuverlässigkeitsüberprüfung und die zu diesem Zweck beabsichtigten gegenseitigen Datenübermittlungen zwischen dem Organisationskomitee und den Sicherheitsbehörden. Bei Arbeitnehmern erfolgt diese Beantragung durch den Arbeitgeber. Jeder erhält eine Datenschutzzinformation mit der die Bewerber über die Tatsache der Überprüfung, ihren Umfang und die Folgen sowie die dem Betroffenen zustehenden Rechte unterrichtet werden. Der Arbeitgeber muss gegenüber dem Organisationskomitee versichern, dass ihm die Einwilligungserklärungen seiner Mitarbeiter vorliegen.

Der DFB leitet die Personalien an das BKA weiter, das die Verteilung an die jeweils zuständige Polizeibehörde und an den Verfassungsschutz organisiert. Beim BKA werden auch die Ergebnisse der einzelnen Überprüfungen zusammengeführt und dann an das BKA zurückgemeldet. Dabei werden jedoch keine Details übermittelt, sondern nur Bedenken ja oder nein. Die Entscheidung über die Akkreditierung verbleibt beim Organisationskomitee. Das Verfahren hat im Dezember 2005 begonnen, die Überprüfung erfolgt jedoch erst etwa ab dem März 2006, um eine größtmögliche Aktualität der Zuverlässigkeitsüberprüfungen zu erreichen.

In der Datenschutzerklärung werden die Betroffenen darauf hingewiesen, dass sie sich an das Landeskriminalamt ihres Wohnsitzes wenden können, wenn sie mit dem Ergebnis nicht einverstanden sind. Soweit nicht das örtlich zuständige Landeskriminalamt sondern eine andere beteiligte Sicherheitsbehörde das negative Votum abgegeben hat, wird diese Stelle über das BKA ermittelt und dann der Betroffenen informiert. Für die Auskünfte und ggf. notwendige Berichtigungs- oder Löschungsansprüche gelten die jeweiligen gesetzlichen Regelungen.

Misslich ist allerdings, dass Beschäftigte, die über ihren Arbeitgeber akkreditiert werden sollen, nur indirekt von einer Ablehnung erfahren. Andererseits erfährt der Arbeitgeber durch die Ablehnung, dass bei Sicherheitsbehörden etwas über seinen Arbeitnehmer vorliegt. Der Weg des Betroffenen, konkrete Informationen zu erhalten und ggf. auch eine Korrektur zu erreichen, ist

nicht einfach und vermutlich meist auch langwierig. Der Versuch zu erreichen, dass in solchen Fällen die Betroffenen mindestens gleichzeitig mit ihren Arbeitgebern informiert werden, führte nicht zum Erfolg. Von Seiten des Organisationskomitees wurden dabei im Wesentlichen organisatorische Gründe geltend gemacht. Da das ganze Verfahren elektronisch abgewickelt werde, und Kommunikationsadressen von den einzelnen Arbeitnehmern nicht bekannt seien – für alle anderen Konstellationen auch nicht benötigt würden –, sei eine Vorabinformation nicht leistbar.

Abschließend möchte ich betonen, dass die datenschutzrechtlich pragmatische Vorgehensweise allein durch die Einmaligkeit der Fußball-Weltmeisterschaft in Deutschland begründet ist und nicht als Präzedenzfall für künftige Großveranstaltungen gesehen werden kann.

5. Land

5.1 Hessischer Landtag

5.1.1

Datenschutzbeauftragte für Fraktionen im Hessischen Landtag

Die Fraktionen im Hessischen Landtag verarbeiten auch personenbezogene Daten, die nicht unmittelbar parlamentarischen Zwecken dienen. Für diesen Bereich muss jede Fraktion einen Datenschutzbeauftragten bestellen.

Der Präsident des Hessischen Landtags hat sich mit der Frage an mich gewandt, ob die Fraktionen im Hessischen Landtag betriebliche Datenschutzbeauftragte bestellen müssen.

Zur Beantwortung dieser Frage war es erforderlich zu ermitteln, welche personenbezogenen Daten bei den Fraktionen für welche Zwecke verarbeitet werden. Von der Art der Daten, insbesondere aber von deren Zweck hängt es ab, ob spezialgesetzliche Vorschriften (z. B. die Datenschutzordnung des Hessischen Landtags) oder allgemeines Datenschutzrecht zur Anwendung kommt. Darüber hinaus kommt es darauf an, welchen Status die Fraktionen besitzen, ob sie als öffentliche oder nichtöffentliche Stellen gelten. Davon hängt nämlich ab, ob HDSG oder BDSG anzuwenden ist.

5.1.1.1

Datenverarbeitung zum Zweck der Wahrnehmung parlamentarischer Aufgaben

Die Fraktionen verarbeiten personenbezogene Daten z. B. im Zusammenhang mit kleinen und großen Anfragen, bei der Befassung mit Petitionen, in ihren Adressensammlungen, die für die parlamentarische Arbeit in allen ihren Ausprägungen wie z. B. die Benennung von Sachverständigen, die Kontaktpflege mit Berufsgruppen-, Wirtschafts- und Bevölkerungsrepräsentanten etc. bereitgehalten werden. Hierbei handelt sich um Datenverarbeitung im Zusammenhang mit der Wahrnehmung parlamentarischer Aufgaben. Für diesen Bereich gilt § 39 HDSG in Verbindung mit der Datenschutzordnung des Hessischen Landtags. Zwar sind die Fraktionen in § 39 HDSG nicht ausdrücklich erwähnt, sondern es ist nur

vom „Landtag“ die Rede. Unter den Begriff „Landtag“ sind aber nicht nur die Mitglieder des Hessischen Landtags zu verstehen. Die Fraktionen im Hessischen Landtag setzen sich aus Mitgliedern des Landtags zusammen und das Hessische Fraktionsgesetz bezeichnet sie als „Vereinigungen im Hessischen Landtag“ (§ 1 Hessisches Fraktionsgesetz). Die Geschäftsordnung des Hessischen Landtags (GO-HLT) regelt alle gängigen Facetten parlamentarischer Arbeit und sieht dementsprechend den Begriff des Parlaments auch umfassend. Sie enthält Regelungen nicht nur für das Parlament im engeren Sinn, sondern auch für seine Organe, zu denen auch die Fraktionen zählen (vgl. 2. Teil GO-HLT). Folgerichtig bezieht die auf Basis des § 112 GO-HLT und § 39 Abs. 1 Satz 2 HDSG erlassene Datenschutzordnung des Hessischen Landtags (DSO-HLT) in § 1 Abs. 2 die Datenverarbeitung für den Bereich der Wahrnehmung parlamentarischer Aufgaben durch die Fraktionen ausdrücklich mit ein.

§ 1 Abs. 2 DSO-HLT

Diese Datenschutzordnung gilt für den gesamten Bereich der Wahrnehmung parlamentarischer Aufgaben durch den Hessischen Landtag, seine Organe, seine Mitglieder, die Fraktionen sowie Mitarbeiterinnen und Mitarbeiter der Abgeordneten und Fraktionen. Eine Wahrnehmung parlamentarischer Aufgaben liegt vor, wenn es sich nicht um Verwaltungsangelegenheiten nach § 39a Abs. 1 Hessisches Datenschutzgesetz handelt.

Bei den o. g. Datenverarbeitungen handelt es sich um solche im Zusammenhang mit den parlamentarischen Aufgaben. Soweit dort personenbezogene Daten anfallen, gelten die speziellen Regeln der DSO-HLT, die den allgemeinen Datenschutzgesetzen vorgehen. Kontrollgremium für diesen Bereich ist nach § 11 DSO-HLT der jeweils am Anfang der Legislaturperiode bestimmte Ausschuss, derzeit der Hauptausschuss.

5.1.1.2

Datenverarbeitung für Verwaltungszwecke der Fraktionen

Die Fraktionen verarbeiten aber auch Daten, die nicht unmittelbar parlamentarischen Zwecken dienen. Dazu zählen die Daten ihrer eigenen Mitarbeiterinnen und Mitarbeiter, aber auch personenbezogene Daten im Zusammenhang mit der Beschaffung von Material, Vergabe von Werk- und sonstigen Verträgen durch die Fraktionen. Diese Datenverarbeitung dient letztlich zwar

auch der parlamentarischen Funktion der Fraktionen, weil sie die parlamentarische Arbeit unterstützt – wie auch die Landtagskanzlei das ausschließliche Ziel der Unterstützung des Parlaments hat. Gleichwohl ist die Verarbeitung der Mitarbeiterdaten und sonstigen im Zusammenhang mit reinen Verwaltungsarbeiten stehenden personenbezogenen Daten nicht unter den Begriff der Wahrnehmung von parlamentarischen Aufgaben zu fassen. Die DSO-HLT definiert diesen Begriff nämlich negativ; er umfasst alles, was „nicht Verwaltungsangelegenheiten i. S. d. § 39a Abs. 1 HDSG“ (heute § 39 Abs. 1 HDSG) ist. § 39 HDSG zitiert als Verwaltungsangelegenheiten ausdrücklich die „wirtschaftlichen Angelegenheiten“ und die „Personalverwaltung“.

§ 39 Abs. 1 Satz 1 HDSG

Mit Ausnahme der §§ 1 Abs. 1 Nr. 2, 25 und 38 gelten die Vorschriften dieses Gesetzes für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird, insbesondere wenn es sich um die wirtschaftlichen Angelegenheiten des Landtags, die Personalverwaltung oder die Ausführung von gesetzlichen Vorschriften, deren Vollzug dem Präsidenten des Landtags zugewiesen ist, handelt.

Aus diesem Grund fällt die Verarbeitung solcher personenbezogener Daten nicht unter den Geltungsbereich der DSO-HLT; deren Spezialvorschriften finden hier keine Anwendung.

5.1.1.3

Status der Fraktionen

Welche Datenschutzvorschriften für die Verarbeitung von personenbezogenen Daten in Verwaltungsangelegenheiten Anwendung finden (das BDSG oder das HDSG) hängt davon ab, ob es sich bei den Fraktionen um öffentliche oder nichtöffentliche Stellen handelt.

Das Bundesverfassungsgericht hat den Fraktionen verfassungsrechtlichen Status zuerkannt, sie als maßgebliche Faktoren politischer Willensbildung bezeichnet, die in die organisierte Staatlichkeit eingefügt seien und die parlamentarische Handlungsfähigkeit garantierten. Es hat sie dem staatsorganschaftlichen Bereich zugewiesen (BVerfGE 20, 56 [101, 104] = NJW 1966, 1499; BVerfGE 62, 194 [202] = NJW 1983, 343; BVerfGE 80, 188 [231] = NJW 1990, 373;

BVerfGE 85, 264 [287] = NJW 1992, 2545; BVerfGE 102, 224 [242] = NJW 2000, 3771). Ob die Fraktionen dem öffentlichen oder dem Privatrecht zuzuordnen sind, lässt sich nicht eindeutig beantworten (Zusammenstellung des Meinungsstandes in Ipsen, Rechtsschutz gegen Fraktionsausschluss, NJW 2005, 363). Die gesetzlichen Regelungen sind im Bund und in den Ländern nicht einheitlich und lassen alle deren Status im Unklaren (vgl. § 1 Hessisches Fraktionsgesetz, ebenso wie § 46 Abgeordnetengesetz des Bundes, der durch das so genannte „Fraktionsgesetz“ 1995 eingefügt wurde). Übereinstimmend ist allerdings geregelt, dass die Fraktionen Organe des jeweiligen Parlaments sind und einen eigenen Rechtsstatus mit aktivem und passivem Klagerecht haben.

Auch der Hessische Landtag hat in seiner Geschäftsordnung die Fraktionen als Organe des Landtags eingeordnet (vgl. Teil 2 GO-HLT). Den Begriff „Landtag“ in § 39 HDSG, der zusammen mit § 112 GO-HLT Basis für die DSO-HLT ist, hat er durch die Einbeziehung der Organe des Landtags in seine Datenschutzordnung weit interpretiert. Dies entspricht auch der Begrifflichkeit in § 38 HDSG, der als Auskunftsrecht des Landtags ausdrücklich auch das Auskunftsrecht der Fraktionen versteht und den Begriff „Landtag“ im Übrigen immer als die Fraktionen einschließend verwendet. Berücksichtigt man die Stellung der Fraktionen im Hessischen Landtag in der staatlichen Organisation und ihre Zugehörigkeit zur Legislative, so sind sie dem öffentlichen Recht – nämlich dem Parlamentsrecht – zuzuordnen. Auch ihre Zusammensetzung und ihre Aufgabenstellung verbietet eine Zuordnung zum Privatrecht. Gerade bei der Datenschutzkontrolle würde mit ihrer Zuordnung zum Privatrecht und damit der Klassifizierung als nichtöffentliche Stelle i. S. d. BDSG zudem eine Kontrolle der Exekutive über die Legislative postuliert, was dem verfassungsrechtlichen Prinzip der Gewaltenteilung zuwiderlaufen würde. Die Fraktionen im Hessischen Landtag sind deshalb öffentliche Stellen des Landes; sie sind unter den Begriff des Landtags im Sinne des § 39 HDSG zu subsumieren.

Nach § 39 HDSG gelten für die Fraktionen im Hessischen Landtag – soweit sie in Verwaltungsangelegenheiten tätig werden – die Vorschriften des Hessischen Datenschutzgesetzes.

5.1.1.4

Handlungsalternativen

Damit findet auch § 5 HDSG Anwendung: die Fraktionen im Hessischen Landtag haben Datenschutzbeauftragte für den Aufgabenbereich der Verwaltungsangelegenheiten zu bestellen. Dabei haben sie die Alternativen eine oder einen ihrer eigenen Beschäftigten zum Datenschutzbeauftragten nach § 5 Abs. 1 oder zusammen mit einer anderen öffentlichen Stelle eine oder einen gemeinsamen Datenschutzbeauftragten nach § 5 Abs. 3 Satz 2 HDSG zu bestellen.

§ 5 Abs. 3 Satz 2 HDSG

Mehrere Daten verarbeitende Stellen können gemeinsam einen ihrer Beschäftigten zum Datenschutzbeauftragten bestellen, wenn dadurch die Erfüllung seiner Aufgabe nicht beeinträchtigt wird.

Bestellen die Fraktionen eigene Datenschutzbeauftragte, sind die Anforderungen nach § 5 Abs. 1 HDSG zu beachten: Es muss sich um eine oder einen Beschäftigten der Fraktion mit entsprechender Sachkenntnis und Zuverlässigkeit handeln. Die Anbindung erfolgt unmittelbar an die Leitung. Durch die Tätigkeit, die weisungsfrei auszuüben ist, darf kein Interessenkonflikt mit den sonstigen Aufgaben entstehen. Benachteiligungen infolge dieses Amtes sind untersagt.

Stattdessen wäre es für die Fraktionen auch möglich, nach § 5 Abs. 3 Satz 2 HDSG eine oder einen Beschäftigten einer anderen öffentlichen Stelle mit deren Einverständnis zum gemeinsamen Datenschutzbeauftragten zu bestellen. Damit wäre es den Fraktionen – das Einverständnis der Kanzlei des Hessischen Landtags vorausgesetzt – auch möglich, den Datenschutzbeauftragten der Kanzlei mit diesem Amt zu betrauen, der die Anforderungen an Sachkenntnis und Zuverlässigkeit bereits mitbringt und bei dem Interessenkollisionen mit den sonstigen Aufgaben nicht zu erwarten sind.

5.2 Justiz

5.2.1

Moderne Justiz, Datenschutz und richterliche Unabhängigkeit

Auf der vom Hessischen Minister der Justiz am 13. Mai 2005 veranstalteten Modernisierungskonferenz zur zukünftigen Entwicklung der hessischen Justiz habe ich mich grundlegend zu den Grenzen der richterlichen Unabhängigkeit geäußert und dabei vor allem das Verhältnis von Datenschutzkontrolle und richterlicher Unabhängigkeit beleuchtet.

Ausgehend von einer zunehmenden Technisierung des Richterarbeitsplatzes auch im häuslichen Umfeld sind Sicherheits- und Datenschutzkonzepte auch dort umzusetzen. Solche Konzepte können zwar die richterliche Unabhängigkeit im Sinne einer Selbstbestimmung über Arbeitsmittel und -bedingungen berühren. Verfassungsgrund für die richterliche Unabhängigkeit und damit deren Kern ist aber die Gewährleistung insbesondere der sachlichen Unabhängigkeit, also der Freiheit von Weisungen beim Fällen der Entscheidungen. Die richterliche Unabhängigkeit ist kein Privileg für datenschutzfreie Räume, sondern muss sich in ein allgemeines Datenschutzkonzept integrieren, das sowohl der richterlichen Unabhängigkeit aber und vorrangig auch den datenschutzrechtlichen Interessen der Bürgerinnen und Bürger genügt. Die Gerichte sind dabei nicht vollständig meiner Aufgabenstellung entzogen; sie unterliegen außerhalb des richterlichen Kernbereichs meiner Kontrolle. Auch den Einsatz moderner Informationstechnologien am häuslichen Arbeitsplatz des Richters habe ich zu beobachten und bin insoweit auch zu kritischen Äußerungen berechtigt.

Meine Ausführungen im Einzelnen sind nachzulesen in der Veröffentlichung „Moderne Justiz, Datenschutz und richterliche Unabhängigkeit“ in der DuD 2005, 354 ff.

5.2.2

Verwechslungsgefahr bei Insolvenzbekanntmachungen im Internet

Bei der Entscheidung des Insolvenzgerichts, welche Daten wie zu veröffentlichen sind, ist sorgfältig abzuwägen zwischen den Interessen der Betroffenen, dass als Suchergebnis nicht schon zu viele Details offenbar werden, und den Interessen Dritter, die vor Verwechslungen mit einem Schuldner zu schützen sind.

Die von der Insolvenzordnung vorgeschriebenen öffentlichen Bekanntmachungen dürfen seit 2002 auch im Internet erfolgen. Die Mehrzahl der Bundesländer hat dazu eine gemeinsame Internetseite ins Leben gerufen, die technisch in Nordrhein-Westfalen betreut wird. Die inhaltliche

Verantwortung für die Zulässigkeit der einzelnen Eintragungen sowie die Dauer der Eintragung bleibt beim jeweils zuständigen Insolvenzgericht.

Eingetragen werden Beschlüsse über die Eröffnung, Entscheidungen über die Aufhebung oder Einstellung eines Insolvenzverfahrens, Anordnungen zu Sicherheitsmaßnahmen, Ankündigungen zur Restschuldbefreiung, Terminbestimmungen und Beschlüsse über die Festsetzung der Vergütung des Insolvenzverwalters, Treuhänders und der Mitglieder des Gläubigerausschusses.

Da diese Veröffentlichungen an die Stelle der öffentlichen Bekanntmachung etwa durch Aushang an der Gerichtstafel des jeweils zuständigen Insolvenzgerichts treten, ist für die Dauer der vom Gesetz vorgesehenen Veröffentlichung jedermann der Zugriff gestattet. Für darüber hinausgehende Auskünfte unterliegen die Insolvenzgerichte einer beschränkten Auskunftspflicht. Das bedeutet, dass Auskünfte zu einzelnen Verfahren nur unter bestimmten Voraussetzungen erteilt werden können. Wer nicht selbst Verfahrensbeteiligter ist, erhält Auskünfte nur bei Vorliegen eines rechtlichen Interesses. Bei der Frage, welche Auskünfte im Einzelnen erteilt werden können, sind sowohl datenschutzrechtliche als auch schuldnerische Belange zu berücksichtigen.

Das Verfahren zur Suche in den Insolvenzveröffentlichungen ist mehrstufig ausgestaltet. Soweit Daten zu Veröffentlichungen gesucht werden, die länger als zwei Wochen zurückliegen, muss zunächst das zuständige Insolvenzgericht sowie eine der Angaben Familienname, Firma, Sitz oder Wohnort des Schuldners oder das Aktenzeichen des Insolvenzgerichts angegeben werden. Dann erscheint eine Liste der (möglichen) Treffer. Aus dieser kann der Nutzer dann den interessierenden Fall aussuchen und sich für diesen die Details der Veröffentlichung anzeigen lassen.

Dieses Verfahren wurde aus zwei Gründen gewählt. Zum einen gelingt es so, die einzelnen Seiten übersichtlicher zu gestalten. Gleichzeitig kann sichergestellt werden, dass nicht sofort – vor allem wenn die Suche mehrere Treffer ergibt – Details zu den einzelnen Verfahren erkennbar sind. Der Nutzer muss (nochmals) eine Entscheidung treffen, welches das für ihn relevante Verfahren ist.

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, dass diese Gestaltung der Veröffentlichung im Einzelfall aber auch zu Nachteilen für Unbescholtene führen kann.

Was war geschehen? In einer Großstadt war für eine Firma, deren Inhaber einen oft vorkommenden Namen trug, ein Verfahren eingetragen. Das Suchergebnis war vergleichbar mit: Hans Schmidt, Frankfurt, AZ. XXXX.

In dieser Stadt gibt es aber eine Vielzahl von Firmeninhabern mit dem Namen Hans Schmidt. Einer von diesen hat sich über die Darstellung in der Veröffentlichung beschwert. Dabei hat er dargelegt, dass diese Veröffentlichung dazu geführt habe, dass er Schwierigkeiten mit Geschäftspartnern und Lieferanten bekommen habe. Offensichtlich würde über das weitere Schicksal seiner Firma spekuliert.

Das Anliegen des Eingebers, zusätzliche identifizierende Merkmale zu verwenden, ist verständlich. Ich habe daher dem Justizministerium empfohlen, schon auf der „Trefferliste“ für eine verbesserte Darstellung zu sorgen. Das Ministerium hat daraufhin den Insolvenzgerichten empfohlen, dies zumindest in Fällen mit häufig vorkommenden Namen zu tun. Sinnvoll erscheint dabei die zusätzliche Angabe der Straße. Damit kann die Unterscheidung verschiedener Personen mit gleichen Namen erleichtert und gleichzeitig den berechtigten Interessen aller Beteiligten Rechnung getragen werden.

5.3 Polizei und Strafverfolgung

5.3.1

Erfahrungen mit der Videoüberwachung, insbesondere in Frankfurt am Main

Beim Einsatz von Videoüberwachungsanlagen ist in jedem Einzelfall sorgfältig zu prüfen, ob die vom Gesetz vorgegebenen Rahmenbedingungen eingehalten werden.

5.3.1.1

Trends der Videoüberwachung in Hessen

Die Zahl der Videoüberwachungsanlagen auf Grundlage der Regelungen im HSOG steigt weiterhin. Wenn auch nicht so extrem wie häufig befürchtet. Für die Beurteilung, inwieweit ein Bewegen im öffentlichen Raum möglich ist ohne von irgendwelchen Überwachungskameras

erfasst zu werden, ist auch zu berücksichtigen, dass die Mehrzahl der Kameras in den hessischen Städten und Gemeinden nicht durch Polizei oder Gefahrenabwehrbehörden auf Grundlage des HSOG errichtet worden sind, sondern von privaten Stellen im Rahmen des BDSG.

Vermeehrt wird von Kommunen ein Kameraeinsatz zur Überwachung von Örtlichkeiten angestrebt, mit dem Schäden oder ordnungswidrigem Verhalten vorgebeugt werden soll, etwa zur Verhinderung von illegalem Müllabladen.

Bei der Überwachung öffentlicher Plätze setzt sich eine Tendenz fort, dass keine strikte Trennung zwischen Maßnahmen der Polizei und der Kommunen erfolgt. Die Entscheidung für eine Überwachung erfolgt häufig durch die kommunalen Gremien, die auch die wesentliche Finanzierung übernehmen. Die Überwachungsmonitore stehen dann aber oft bei der Polizei.

5.3.1.2

Videoüberwachung von Plätzen in Frankfurt am Main

In Frankfurt werden auf Veranlassung des Stadtparlaments durch die Polizei zwei Plätze überwacht: Seit einigen Jahren die Konstablerwache und nunmehr auch der Bahnhofsvorplatz. Dies habe ich zum Anlass genommen, mir den Umgang mit den Überwachungsanlagen im Polizeipräsidium Frankfurt näher anzuschauen.

Für die neuen Kameras am Hauptbahnhof konnte ich feststellen, dass dort sehr sorgfältig von den technischen Möglichkeiten Gebrauch gemacht wurde, solche Bereiche auszublenden, die nicht zu dem zu überwachenden Gebiet gehören. Das gilt insbesondere auch für die Beobachtung von Hauseingängen und Fenstern.

Anders stellt sich die Situation im Bereich der Konstablerwache dar. Dort erfassen die Kameras auch Balkone bzw. Fenster. Zudem geht die Reichweite der Kameras weit über das ursprünglich definierte Ziel, die Konstablerwache, hinaus. Dabei war außerdem festzustellen, dass der überwachte Bereich nicht mit der Beschilderung übereinstimmte, solche gab es nämlich nur an den Zugängen zum eigentlichen Platz „Konstablerwache“.

Nicht abschließend geklärt werden konnte bis jetzt, inwieweit innerhalb des Präsidiums Zugriff auf die Aufzeichnungsdaten gewährt werden kann. Ich habe gefordert, in einer Dienstanweisung

klarzustellen, wer Zugang zu diesen Daten bekommen kann. Dabei muss auch das Verfahren geregelt werden, wer über einen Zugriff entscheidet, einschließlich einer Dokumentation der vergebenen Zugriffsrechte.

5.3.2

Gelöscht und doch nicht gelöscht – Prüfung von Polizeidatenbeständen

Das Konzept der hessischen Polizei zur Löschung von personenbezogenen Daten nach Abschluss eines Verfahrens und Ablauf der verfügbaren Aufbewahrungsfrist genügt datenschutzrechtlichen Anforderungen, funktioniert aber nur in der Theorie. Eine Prüfung offenbarte Unstimmigkeiten und technische Mängel in der praktischen Umsetzung des Konzepts. Die Mängel sind noch nicht behoben.

5.3.2.1

Anlass der Prüfung

Einem Einwohner aus dem Westerwald habe ich im Jahre 2003 nach einer Überprüfung seiner Datenbestände bei der Polizei mitgeteilt, dass er die Datenspeicherung hinnehmen müsse. Die Datenspeicherung sei rechtmäßig. Erst im Mai des Jahres 2005 könne er mit der Löschung der zu seiner Person gespeicherten Daten rechnen. Im Juli 2005 wandte er sich nun erneut an mich und bat um die Prüfung, ob die Löschung seiner Daten erfolgt sei.

Ich prüfte beim Hessischen Landeskriminalamt das polizeiliche Auskunftssystem POLAS-HE und stellte fest, dass die Daten nach wie vor gespeichert waren. Ein Grund für die Fortdauer der Datenspeicherung war nicht ersichtlich.

5.3.2.2

Das Verfahren

Die Rechtsgrundlage für das Verfahren der Speicherung und Löschung in POLAS-HE enthalten §§ 20 Abs. 4 und 27 Abs. 4 HSOG und die auf dieser Grundlage vom Hessischen Ministerium des Innern und für Sport erlassene Prüffristenverordnung (PrüffristVO). Danach enthält jeder in

POLAS-HE gespeicherte Datensatz zwingend nach Abschluss der Ermittlungen ein so genanntes Aussonderungsprüfdatum, das nach in der PrüffristVO festgelegten Kriterien vergeben wird. Zum Aussonderungsprüfdatum muss geprüft werden, ob die Datenspeicherung gelöscht werden kann.

§ 2 PrüffristVO

(1) Bei Daten tatverdächtiger Personen betragen die Prüffristen

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

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

(2) Automatisiert verarbeitete Daten sind zu löschen und die dazugehörigen Unterlagen sowie die Akten sind zu vernichten, wenn kein Anlass für eine erneute Aufnahme in die Datensammlung entstanden ist.

(3) Die Löschung und die Vernichtung können unterbleiben, wenn es sich um eine Straftat mit erheblicher Bedeutung handelt und tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person solche Straftaten begehen wird. Die Gründe für die Verlängerung sind aktenkundig zu machen. Spätestens nach zwei Jahren, bei Kindern nach einem Jahr, hat eine erneute Prüfung nach den gleichen Maßstäben zu erfolgen.

(4) Löschung und Vernichtung können auch unterbleiben:

1. bei einer Sexualstraftat nach dem 13. Abschnitt des Strafgesetzbuches, ausgenommen den §§ 183a, 184, 184d und 184e des Strafgesetzbuches oder
2. bei einer sexuell bestimmten Straftat nach den §§ 211 bis 213 und 223 bis 228 des Strafgesetzbuches.

Spätestens nach fünf Jahren, bei Kindern nach zwei Jahren, hat eine Überprüfung nach Abs. 3 zu erfolgen.

(5) Tatverdächtige Person ist eine Person, die im Verdacht steht, eine rechtswidrige Tat im Sinne des § 11 Abs. 1 Nr. 5 des Strafgesetzbuches begangen zu haben, vorzubereiten oder vorbereitet zu haben.

§ 5 PrüffristVO

(1) Die Prüffrist beginnt mit dem letzten Ereignis, das die Speicherung begründet hat, in Fällen des § 2 nicht vor Entlassung der betroffenen Personen aus einer Justizvollzugsanstalt oder der Beendigung einer mit Freiheitsentzug verbundenen Maßregel der Besserung oder Sicherung. Ereignis im Sinne des Satz 1 ist in Fällen des § 3 Nr. 2 die Aufklärung der Vermisstensache. Sind die Daten zugleich in einer Verbunddatei des Bundeskriminalamtes gespeichert, richtet sich der Beginn der Prüffrist nach dem Ereignis, das die Speicherung in dieser Datei begründet hat.

(2) In den Fällen des § 4 beginnt die Frist mit der erstmaligen Speicherung zu dem jeweiligen Zweck.

(3) Hängt die Länge der Prüffrist vom Lebensalter der betroffenen Person ab, ist das Lebensalter im Zeitpunkt des Ereignisses maßgebend.

§ 6 PrüffristVO

(1) Die Prüfung nach den §§ 2 bis 4 obliegt der Daten verarbeitenden Stelle. Werden die Daten von einer Stelle automatisiert verarbeitet, die nicht die dazugehörigen Unterlagen führt, ist diejenige Stelle zuständig, die die Unterlagen führt.

(2) Die Daten verarbeitende Stelle unterstützt die in Abs. 1 Satz 2 genannten Stellen bei der Einhaltung der Fristen in geeigneter Weise.

Jeden Monat erfolgt eine Auswertung der Datenbank POLAS-HE, mit der eine Prüfliste erstellt wird. Diese enthält Fälle, in denen in vier Monaten das Aussonderungsprüfdatum verstreicht, die Person während der Dauer der Datenspeicherung nicht erneut in den Verdacht geraten ist, Straftaten begangen zu haben oder bei einer neuen Datenspeicherung kein späteres Aussonderungsprüfdatum verfügt wurde. Diese Liste wird der Akten führenden Stelle – das ist in der Regel das Polizeipräsidium, welches die Ermittlungen angestellt hatte – zur Verfügung

gestellt. Damit erhält diese die Möglichkeit, in nach der PrüffristVO begründeten Einzelfällen die Prüffrist zu verlängern. Liegen keine Gründe für die Verlängerung vor, bleibt es bei dem Datum, und diese Datensätze werden nach vier Monaten automatisch gelöscht. Den Akten führenden Stellen werden Listen der gelöschten Datensätze übersandt, denn sie müssen noch die dazugehörigen Kriminalakten vernichten. Auch evtl. vorhandene erkennungsdienstliche Unterlagen – Lichtbilder und Fingerabdrücke – müssen anhand dieser Löschlisten ausgesondert und vernichtet werden.

5.3.2.3

Die Prüfung

Durch die Verordnung und das Verfahren ist eigentlich sichergestellt, dass der Fall, wie unter Ziff. 5.3.2.1 beschrieben, überhaupt nicht vorkommen dürfte.

Solche Fälle wie sie auf Grund technischer Vorkehrungen ausgeschlossen sein sollten, sind mir jedoch seit der Einführung des polizeilichen Auskunftsverfahren POLAS-HE im Juli 2001 mehrmals aufgefallen. Ich habe deshalb das Präsidium für Technik, Logistik und Verwaltung (PTLV) gebeten, die Datenbank POLAS-HE für Zwecke der Datenschutzkontrolle auszuwerten und mir Datensätze aufzulisten, deren Aussonderungsprüfdatum im Juli 2005 zur Löschung führen sollte.

Einige Wochen nach Ablauf dieses Datums fragte ich beim PTLV die Liste der Datensätze mit den verstrichenen Aussonderungsprüfdaten ab. Das Ergebnis überraschte mich: Keiner der abgefragten Datensätze war gelöscht. Die weitere Analyse ergab ein etwas differenzierteres Bild:

Zu etwa einem Drittel der abgefragten Datensätze gab es zu den Personen zusätzliche Datenspeicherungen von Polizeibehörden anderer Bundesländer oder des Bundeskriminalamtes mit späteren Aussonderungsprüfdaten. In diesen Fällen hatten technische Vorkehrungen zu Recht bewirkt, dass sie nicht gelöscht waren. Sie waren also für meine Fehlersuche nicht aussagekräftig.

Zu einem weiteren Teil gab es zusätzliche Datenspeicherungen, bei denen offensichtlich dieselbe technische Vorkehrung bewirkte, dass die Datensätze nicht gelöscht wurden. Dabei handelte es sich aber nicht um Zuspeicherungen von anderen Polizeivollzugsbehörden, sondern um Zuspeicherungen von den kommunalen Ausländerbehörden über ausländerrechtliche

Entscheidungen. Im Gegensatz zu Entscheidungen anderer Polizeibehörden gibt es aber bei Entscheidungen von Ausländerbehörden keinen Rechtsgrund, der die Vernichtung einer ansonsten lösungsreifen polizeilichen Information hindert. Die Datensätze hätten deshalb nur noch die Speicherung der ausländerrechtlichen Entscheidungen nicht die polizeilichen Daten enthalten dürfen.

Bei einem weiteren Anteil waren die Datensätze als „überregional relevant“ gekennzeichnet. Diese Kennzeichnung bewirkt, dass der jeweilige Datensatz auch außerhessischen Polizeibehörden zur Verfügung steht. Damit – so das Landeskriminalamt – habe die Landesbehörde die Verfügungshoheit über den Datensatz aufgegeben. Der Anstoß zur Datenlöschung muss nun vom Bundeskriminalamt erfolgen. Ob und wann dieser Anstoß erfolgt, war dem Landeskriminalamt nicht bekannt.

Bei einer weiteren Reihe von Fällen, jetzt solche, die nicht „überregional relevant“ waren, war ein Datensatz im polizeilichen Auskunftssystem POLAS-HE tatsächlich nicht mehr vorhanden. Trotzdem zeigte das Auskunftssystem, mit dem gleichzeitig das bundesweite Informationssystem abgefragt wird, immer dann einen Treffer, wenn die Person erkennungsdienstlich behandelt worden war. Das erklärt sich daraus, dass das Bundeskriminalamt ein Mehrexemplar einer jeden erkennungsdienstlichen Behandlung erhält. Dies wiederum führt zu einer Datenspeicherung im INPOL, die nur auf Veranlassung des Bundeskriminalamtes gelöscht werden kann. Auch in diesen Fällen war dem Landeskriminalamt nicht bekannt, wann das Bundeskriminalamt die Löschung veranlasst. Offensichtlich sind die Fristen nicht identisch.

Bei einem letzten Teil von Vorgängen, bei denen das Aussonderungsprüfdatum verstrichen war, war das Versäumnis der Löschung nicht nachvollziehbar. Es war auch nach Einschätzung des Landeskriminalamtes eindeutig kein Grund für die unterbliebene Löschung ersichtlich.

Daraufhin habe ich einen weiteren Prüfungsansatz verfolgt. Einen vom Landeskriminalamt zu diesem Zweck erstellten Auszug aus der aktuellen Prüfliste habe ich gemeinsam mit meinen Gesprächspartnern bei der Polizei mit den zugehörigen Datensätzen verglichen. Wir stellten fest, dass nur ein Teil der aufgeführten Datensätze tatsächlich zur Prüfung anstand. Bei einem anderen Teil lag das Aussonderungsprüfdatum weit in der Zukunft oder in der Vergangenheit. Weshalb hier anscheinend Löschungen nachgeholt oder Datensätze vorzeitig überprüft werden sollten, war wiederum nicht zu erkennen. Auch einige Datensätze Verstorbener befanden sich auf der Prüfliste.

Nach einer internen Richtlinie sollen Daten Verstorbener im Regelfall zwei Jahre nach dem Tod ausgesondert werden. Doch in keinem dieser Fälle korrespondierte die reale Prüffrist mit dieser Vorschrift.

Schließlich habe ich die Richtigkeit der Löschliste geprüft. Das ist die Liste der Datensätze, die gelöscht sein sollten und bei denen nur noch die Akten ausgesondert werden müssen. Immerhin: Alle auf der Löschliste verzeichneten Datensätze waren auch tatsächlich gelöscht.

5.3.2.4

Ergebnis

Insgesamt ist das Ergebnis nicht zufrieden stellend. Fest steht nur, dass ein Datensatz, der auf der Löschliste steht, auch wirklich gelöscht ist. Auf die Prüfliste gelangen offensichtlich nicht alle und nicht nur Fälle, die sich nach den Rechtsvorschriften dort finden sollten. Personen, über die ein Datensatz in POLAS-HE gespeichert war, können auch nachdem das Aussonderungsprüfdatum verstrichen ist, nicht sicher sein, dass ihre Daten gelöscht und ihre Akten vernichtet sind. Das Landeskriminalamt hat bestätigt, dass solche Fehler seit Einführung von POLAS-HE immer wieder auftreten. Es war auch längst selbst auf sie aufmerksam geworden und hat auf den Missstand – allerdings bislang ohne sichtbaren Erfolg – beim Landespolizeipräsidium hingewiesen. Bis zum Redaktionsschluss dieses Berichts waren die Ursachen der Fehler nicht vollständig analysiert und nicht beseitigt. Ich habe das Landespolizeipräsidium auf meine Feststellungen hingewiesen und um dringliche Behebung des Missstandes gebeten. Über das Ergebnis werde ich in meinem nächsten Tätigkeitsbericht informieren.

5.3.3

Mangelndes Auskunftsverhalten der Staatsanwaltschaft bei dem Landgericht Frankfurt

Das Recht auf Auskunft beinhaltet nicht nur einen Anspruch auf Auskunft über die zur Person gespeicherten Daten, sondern auch eine Auskunft über die Herkunft der Daten, die Empfänger von Übermittlungen und den Zweck der Datenspeicherung. Auskunftsverlangen müssen nicht

begründet werden. Es ist daher rechtlich fehlerhaft, ein Auskunftsverlangen wegen fehlender Begründung einfach unbeantwortet zu lassen.

Mangelndes Auskunftsverhalten hessischer Staatsanwaltschaften auf Anfragen über Datenspeicherungen zur eigenen Person hatte ich bereits in meinem 31. Tätigkeitsbericht, Ziff. 3.4 und 33. Tätigkeitsbericht, Ziff. 5.2 geschildert. Die Staatsanwaltschaft bei dem Landgericht Frankfurt war einem Auskunftsverlangen nach § 491 Abs. 1 StPO erst nach über einem Jahr mit dem Übersenden eines Computerausdruckes der zur Person des Betroffenen gespeicherten Daten nachgekommen. Der Umfang des Auskunftsanspruches bei den Staatsanwaltschaften richtet sich auf Grund eines Verweises in § 491 Abs. 1 StPO nach § 19 BDSG.

§ 491 Abs. 1 StPO

Dem Betroffenen ist, soweit die Erteilung oder Versagung von Auskünften in diesem Gesetz nicht besonders geregelt ist, entsprechend § 19 BDSG Auskunft zu erteilen.

§ 19 BDSG

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden und
3. den Zweck der Speicherung.

...

Es muss also nicht nur Auskunft über die gespeicherten Daten erteilt werden, sondern auch über die Herkunft der Daten und die Empfänger von Datenübermittlungen, außerdem muss der Zweck der Datenspeicherung benannt werden. Diese Fragen hatte die Staatsanwaltschaft unbeantwortet gelassen. Ihre Beantwortung wurde dem Betroffenen auch ein Jahr nach seinem Auskunftsantrag von der Behörde erst in Aussicht gestellt, sobald es die Arbeitsbelastung zulasse. In diesem verzögerten und unvollständigen Beantworten der Anfrage hatte ich bereits eine Verletzung der Pflicht nach § 491 Abs. 1 StPO festgestellt (33. Tätigkeitsbericht, Ziff. 5.2.1.3).

Die Staatsanwaltschaft bei dem Landgericht Frankfurt hat nun ihren Rechtsverstoß erweitert: Etwa ein halbes Jahr später habe ich nachgefragt, ob dem Betroffenen mittlerweile Auskunft erteilt wurde. Der Behördenleiter teilte mir mit, eine (damals) in den Folgewochen durchgeführte Überprüfung habe ergeben, dass der Anfrager weder nach dem HDSG noch nach dem BDSG einen Anspruch auf die in seinem Schreiben erbetenen Auskünfte habe, weil seine Anfrage nicht schriftlich begründet gewesen sei. Von der Beantwortung seiner Fragen sei deshalb abgesehen worden.

Demgegenüber verlangen aber weder § 491 Abs. 1 StPO noch § 19 BDSG eine Begründung. Ich habe dieses Verhalten nun gegenüber dem Hessischen Ministerium der Justiz gemäß § 27 Abs. 1 HDSG beanstandet und gebeten, die Fragen des Betroffenen soweit als möglich zu beantworten.

Das Justizministerium hat die Staatsanwaltschaft bei dem Landgericht Frankfurt gebeten, meine Empfehlung, die Fragen soweit wie möglich zu beantworten, sehr ernsthaft zu bedenken. Dies führte zu einer erneuten Auskunftserteilung an den Betroffenen. Zu der Frage der Herkunft der Daten und der Empfänger evtl. Übermittlungen konnte sich die Staatsanwaltschaft bei dem Landgericht Frankfurt allerdings gerade einmal zu der Aussage bequemen: „In der Regel erhalten wir die Daten von den Polizeibehörden. Mit diesen Behörden tauschen wir auch Daten, wie z. B. die Aktenzeichen, aus.“

Diese Auskunft, sie war auch nach Ansicht des Justizministeriums sehr knapp, orientiert sich aber immerhin am Wortlaut des § 19 BDSG, wobei noch zum Zweck der Datenspeicherung zutreffend und hinreichend erklärt wurde, dass die Daten für Zwecke zukünftiger Strafverfahren sowie zur Vorgangsverwaltung gespeichert werden.

Das Justizministerium hat mir in seiner Stellungnahme auf meine Beanstandung nach § 27 Abs. 1 HDSG noch zugesagt, die Problematik des Umfangs des Auskunftsanspruches bei der Herbsttagung der Leitenden Oberstaatsanwälte seines Geschäftsbereiches zu erörtern. Nach meiner Ansicht sollte es möglich sein, den Anfragern z. B. mitzuteilen, dass sie angezeigt worden sind oder dass und welche Polizeibehörde die Daten recherchiert und übermittelt hat. Auch zur Frage evtl. Übermittlungen ist ggf. die Aussage geboten, dass die Daten z. B. an das Bundeszentralregister, das Zentrale Staatsanwaltschaftliche Verfahrensregister oder der Verfahrensausgang der Polizei übermittelt wurde. Sollte in diesem Zusammenhang ein überwiegendes öffentliches oder ein Geheimhaltungsinteresse eines Dritten der Auskunft an den

Betroffenen entgegenstehen, so ist dies auszudrücken. Die Anfrage einfach unbeantwortet zu lassen, ist jedoch nicht mit den Regelungen der §§ 491 StPO und 19 BDSG vereinbar.

5.3.4

Mangelnder Informationsaustausch zwischen Polizei und Justiz

Aus unterschiedlichen Gründen ist die Polizei sehr oft nicht darüber informiert, zu welchem Ergebnis die Justiz bei der strafrechtlichen Verfolgung der von ihr festgestellten Ermittlungsergebnisse kam. Stellt die Justiz fest, dass einem Beschuldigten kein strafrechtlicher Vorwurf gemacht werden kann, muss sie die Polizei informieren. Die Polizei muss diese Information verarbeiten und ihre Datenbestände bereinigen.

5.3.4.1

Einzelfälle

Wenn das Ergebnis der strafrechtlichen Verfolgung einer Tat von der Polizei nicht zur Kenntnis genommen wird, kommt es zu unzulässigen Datenspeicherungen. Die Gründe dafür sind unterschiedlich. Es gelingt auch nicht immer, die Ursache einer Fehlinformation zu lokalisieren. Hier vier Einzelfälle aus dem Berichtszeitraum:

- Einem jungen Mann aus Nordhessen wurde das Handy gestohlen. In der Folgezeit wurde die Handynummer mit einem Rauschgiftgeschäft in Verbindung gebracht. Er wurde als Inhaber der Handynummer festgestellt und gegen ihn wurde ein Verfahren wegen Verstoßes gegen das Betäubungsmittelgesetz eingeleitet. Für eine Tatbeteiligung von ihm konnte, von der ihm zuzuordnenden Handynummer abgesehen, kein Anhaltspunkt ermittelt werden. Die Staatsanwaltschaft bei dem Landgericht Marburg stellte das Verfahren nach § 170 Abs. 2 StPO ein.

§ 170 StPO

(1) Bieten die Ermittlungen genügenden 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. ...

Kurz danach geriet der Mann in eine Polizeikontrolle. Er hatte den Eindruck, dass er besonders intensiv kontrolliert wurde. Die Polizei erklärte ihm auf Nachfrage, dass er schließlich schon einmal wegen Rauschgifthandels in Erscheinung getreten sei. Er wandte sich an mich, legte die Mitteilung der Staatsanwaltschaft über die Einstellung des Verfahrens bei und fragte mich, ob er die Datenspeicherung hinnehmen muss. Beim Hessischen Landeskriminalamt stellte ich eine Datenspeicherung im polizeilichen Auskunftssystem POLAS-HE fest. Unter der Deliktsangabe „Verstoß gegen das Betäubungsmittelgesetz“ waren die Daten des Betroffenen registriert. Sie sollten zehn Jahre lang aufbewahrt werden. Ich bat das Polizeipräsidium Nordhessen unter Berücksichtigung des Verfahrensausganges die Erforderlichkeit der weiteren Aufbewahrung der Unterlagen und die Rechtmäßigkeit der Datenspeicherung zu überprüfen. Die Polizei prüfte und kam zu dem Ergebnis, dass die Datenspeicherung zu löschen und die Kriminalakte zu vernichten sei. Auf meine Frage, weshalb dies nicht bereits geschehen war, teilte das Polizeipräsidium Nordhessen mit, es sei nicht bekannt gewesen, dass und warum das Verfahren eingestellt worden war. Erst auf Grund meiner Nachfrage sei die Information über den Verfahrensausgang nebst Begründung bei der Staatsanwaltschaft eingeholt worden. Erst in Kenntnis dieser Information konnte die Löschung der Daten verfügt werden. Dabei ist die Informationsübermittlung in § 482 Abs. 2 StPO durchaus gesetzlich vorgeschrieben.

§ 482 Abs. 1 und Abs. 2 StPO

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

(2) Sie unterrichtet die Polizeibehörden 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.

Warum die Information nicht vorlag konnte nicht festgestellt werden. Entweder wurde Sie von der Staatsanwaltschaft nicht oder noch nicht übermittelt oder sie wurde übermittelt, aber von der Polizei nicht verarbeitet.

- Zweimal hatte ein Wiesbadener Einwohner unter falschen Personalien Waren im Versandhandel bestellt. Bei der Lieferung täuschte er vor, die andere Person zu sein, nahm die Ware entgegen, bezahlte aber nicht. Bevor die Wiesbadener Polizei auf die Betrugsanzeige des Versandunternehmens ermitteln konnte, dass der Täter falsche Personalien benutzte, waren die Ermittlungsverfahren gegen die Person, die die verwendeten Personalien tatsächlich führt, bereits eingeleitet und im polizeilichen Informationssystem gespeichert. Die Verfahren wurden an die Staatsanwaltschaft abgegeben. Die Staatsanwaltschaft bei dem Landgericht Wiesbaden stellte sie gemäß § 170 Abs. 2 StPO ein. Der tatsächliche Täter wurde wegen Betruges verurteilt.

Bei einem Besuch im Bundeskriminalamt wurde der Betroffene, dessen Personalien fälschlich verwendet wurden, aus Sicherheitsgründen an der Pforte abgewiesen. Er durfte die Behörde nicht betreten. Daraufhin wandte er sich an mich. Er vermutete, Datenspeicherungen über die ursprünglich gegen ihn eingeleiteten Ermittlungsverfahren könnten die Bedenken begründen. Ich stellte fest, dass die Vermutung zutraf. Die Polizei war nicht über die etwa ein halbes Jahr zurückliegende Verfahrenseinstellung wegen der Feststellung, dass ein anderer der Täter war, informiert. Der Grund, weshalb die Mitteilung nicht ergangen war, ließ sich nicht herausfinden. Die nachträglich eingeholte Information indes führte zur Löschung der Datenspeicherung und zur Vernichtung der Akte.

- Ein Mann aus Heidelberg geriet bei einer politischen Demonstration in eine Schlägerei. Von der Polizei in Frankfurt wurde wegen Körperverletzung gegen ihn ermittelt. Das Landgericht Frankfurt hat ihn wegen dieses Vorwurfs freigesprochen. Durch eine Auskunft über eigene Daten erlangte er Kenntnis von einer Datenspeicherung der Frankfurter Polizei. Er wandte sich an mich und fragte, ob er diese Datenspeicherung hinnehmen muss. Das Polizeipräsidium Frankfurt war von dem Freispruch des Betroffenen nicht informiert. Es hatte nach Abschluss der Ermittlungen eine Speicherdauer von zehn Jahren verfügt. Ich stellte dem Polizeipräsidium das mir von dem Betroffenen übersandte Gerichtsurteil zur Verfügung. Nach einer Rückfrage

bei den Frankfurter Justizbehörden löschte das Polizeipräsidium Frankfurt die Datenspeicherung und vernichtete die Kriminalakte. Das Geschehen lag zum Zeitpunkt meiner Überprüfung fünf Jahre, das Urteil drei Jahre zurück. Nachforschungen anzustellen, ob und warum die Mitteilung unterblieb bzw. ob sie mehrere Jahre zuvor erging aber nicht verarbeitet wurde, erschienen aussichtslos.

- Gegen mehrere Geschäftsinhaber eines Bewachungsunternehmens wurde ein Betrugsverfahren geführt. Betrügerische Machenschaften wurden auch ermittelt, gleichwohl wurde das Verfahren von der Staatsanwaltschaft wegen Geringfügigkeit eingestellt. Diesmal lag die Mitteilung über die bereits mehrere Jahre zurückliegende Entscheidung der Justizbehörde der Polizei vor. Sie führte korrekterweise nicht zur Löschung. Denn das Ermittlungsergebnis mit der Feststellung eines Betruges traf ja zu. Die Datenspeicherung der Polizei gelangte einem der Betroffenen zur Kenntnis. Er wandte sich an mich und behauptete, das Verfahren sei in seinem Falle nicht wegen Geringfügigkeit, sondern weil festgestellt wurde, dass er gar keine Straftat begangen habe, eingestellt worden. Ich bat die Polizei um Prüfung dieser Angabe. Sie teilte mir danach mit, die zuständige Staatsanwaltschaft habe die ursprüngliche Mitteilung, dass das Verfahren zwar eingestellt wurde, die Einstellungsform (wegen Geringfügigkeit) aber den Tatvorwurf bestätigte, noch einmal wiederholt. Daraufhin sah ich selbst bei der Staatsanwaltschaft den Datenbestand ein und tatsächlich: Der Informationsstand der Polizei schien zu stimmen. Er stimmte mit der Datenspeicherung im Staatsanwaltschaftlichen Verfahrensregister MESTA (s. 27. Tätigkeitsbericht, Ziff. 6.3) überein. Erst die Durchsicht der Akte der Staatsanwaltschaft brachte ein Versehen der Justizbehörde bei der Registratur des Verfahrens zu Tage. Während des Ermittlungsverfahrens stellte sich heraus, dass nur zwei der aus vier Personen bestehenden Geschäftsleitung des Unternehmens für den Betrug verantwortlich zu machen waren. Die anderen beiden Personen hatten keine Straftat begangen. Das Verfahren gegen diese beiden Beschuldigten wurde abgetrennt und nach § 170 Abs. 2 StPO eingestellt. Nur gegen die beiden anderen Geschäftsführer wurde weiter ermittelt und später das Verfahren wegen Geringfügigkeit aber unter Feststellung des Tatvorwurfs eingestellt. Im staatsanwaltschaftlichen Verfahrensregister MESTA wurde fälschlich festgehalten, das Verfahren sei gegen alle Beschuldigte wegen Geringfügigkeit eingestellt. Dies führte natürlich auch zu einer inhaltlich falschen Mitteilung an die Polizei. Die Staatsanwaltschaft korrigierte ihr Register und informierte die Polizei über die früheren falschen Mitteilungen. Die Polizei korrigierte ihre Datenbestände und sonderte die Akten über die beiden Geschäftsführer aus, gegen die kein Tatverdacht bestand.

5.3.4.2

Lösungsansatz und Fazit

Zurzeit produziert das Datenverarbeitungsverfahren der Staatsanwaltschaften MESTA nach der Registratur eines Verfahrensausganges einen elektronischen Datensatz, der an die Polizei übermittelt wird. Dieser Datensatz enthält ein Datenfeld, in dem die Art des Verfahrensausganges verschlüsselt übermittelt wird. So gibt es z. B. eine Schlüsselangabe für die Verurteilung eines Beschuldigten, ebenso wie für die Einstellung eines Verfahrens nach § 170 Abs. 2 StPO wegen mangelnden Tatverdachts. Einzelne Fehlleistungen, wie im letzten Einzelfall beschrieben, sind damit zwar nicht ausgeschlossen. Einem versehentlichen Unterlassen der Mitteilung nach § 482 Abs. 2 StPO sollte damit aber vorgebeugt sein. Nicht automatisiert erfolgt die Verarbeitung dieser Information durch die Polizei. Seit dem Jahre 2004 – damals von der Polizei als Übergangslösung eingeführt – werden diese Datensätze vom PTLV lediglich gesammelt und den einzelnen Polizeipräsidien elektronisch im polizeilichen Intranet zum Abruf zur Verfügung gestellt. Die Polizeipräsidien sollen diese Datensätze ausdrucken und manuell weiterverarbeiten. Diese manuelle Weiterverarbeitung birgt Fehlerquellen, die in einem Teil der aufgezeigten Einzelfälle ursächlich waren. Auch erfolgt die manuelle Weiterverarbeitung nicht immer tatsächlich in Form einer formellen Verarbeitung. Beim Polizeipräsidium Frankfurt beispielsweise werden nur Freisprüche und Verfahrenseinstellungen wegen mangelndem Tatverdacht formell verarbeitet. Alle anderen Verfahrensausgangsmittelungen werden lediglich ausgedruckt und chronologisch gesammelt abgeheftet.

Besser wäre es, den von der Staatsanwaltschaft übermittelten Datensatz elektronisch im Informationssystem der Polizei weiterzuverarbeiten. Beispielsweise könnten Freisprüche und Verfahrenseinstellungen wegen mangelndem Tatverdacht einen Automatismus anstoßen, der im Regelfall zur Löschung der Daten führt. Eine Einstellung wegen Geringfügigkeit oder unter Verweis des Anzeigerstatters auf den Privatklageweg sollte – ebenso wie eine Verurteilung – in das Informationssystem der Polizei übernommen werden. Es mangelt an einer solchen elektronischen Weiterverarbeitung der Information bei der Polizei. Bei Einführung der Übergangslösung hatte das PTLV eine entsprechende Zusage gemacht. Die Umsetzung steht immer noch aus.

5.4 Verfassungsschutz

5.4.1

Novellierung des hessischen Verfassungsschutzgesetzes

Das Hessische Gesetz über das Landesamt für Verfassungsschutz wird novelliert. Das Hessische Ministerium des Innern und für Sport hat mit mir Vorgespräche über gebotene und mögliche Änderungen geführt.

Spätestens seit den Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 (BVerfGE 109, 270; 110, 33) zur Wohnraumüberwachung bedarf es einer Änderung des Verfassungsschutzgesetzes. Auch das Urteil des Sächsischen Verfassungsgerichtshofs vom 21. Juli 2005 (NVwZ 2005, 1310 ff.) zum Großen Lauschangriff im sächsischen Verfassungsschutzgesetz bietet Anlass zur Diskussion.

Derzeit arbeitet das Hessische Ministerium des Innern und für Sport an einem derartigen Gesetzentwurf. In Vorgesprächen mit Vertretern des Ministeriums und mir wurde u. a. folgender Änderungsbedarf angesprochen:

- Das geltende Verfassungsschutzgesetz enthält in § 5 Abs. 2 sehr weit reichende Befugnisse für den Verfassungsschutz zum Abhören im Wohnungsbereich. Diese Befugnisse sind nach den Vorgaben des Bundesverfassungsgerichts einzuschränken. Nach den Ausführungen des Gerichts muss sichergestellt werden, dass ein absolut geschützter Kernbereich privater Lebensgestaltung vom Abhören ausgenommen wird. Falls es dennoch – nicht zielgerichtet, sondern unerwartet – zur Erhebung entsprechender Informationen kommt, muss die Überwachung abgebrochen und entsprechende Aufzeichnungen gelöscht werden.

Eine Wohnraumüberwachung bei Berufsheimnisträgern (Rechtsanwälten, Ärzten, Priestern, Pressevertretern) sollte – ähnlich wie im sächsischen Verfassungsschutzgesetz vom 10. April 2004 – nur dann möglich sein, wenn der Betroffene selbst Verdächtiger ist.

- Das hessische Gesetz ist eines der wenigen, das die Beobachtung von Bestrebungen und Tätigkeiten der organisierten Kriminalität dem Verfassungsschutz als Aufgabe zuweist. Dies darf nach meiner Auffassung aber allenfalls dann geschehen, wenn die zu bekämpfende organisierte Kriminalität ein Ausmaß erreicht hat, das die freiheitlich demokratische Grundordnung oder den Bestand der Sicherheit des Bundes oder der Länder tangiert. Diese Auffassung wird durch das o. g. Urteil des Sächsischen Verfassungsgerichtshofs gestützt. Danach ist es mit dem so genannten Trennungsgebot zwischen Polizei und Nachrichtendiensten nicht vereinbar, die Beobachtung der organisierten Kriminalität auch in den Fällen vorzusehen, in denen die Tätigkeit des Landesamtes nicht gleichzeitig den andern tradierten Aufgaben des Verfassungsschutzes dient.

- Eine weitere Forderung von mir betrifft den Umgang von personenbezogenen Daten in so genannten Sachakten. Diese werden im Gegensatz zu Akten, die zu Personen angelegt werden, zu bestimmten Ereignissen, Gruppierungen etc. geführt. In Sachakten können auch personenbezogene Daten auftauchen. Deren Löschung ist nach der derzeitigen Rechtslage unklar. Nach meinem Formulierungsvorschlag sind diese Daten nach den für Personenakten geltenden Vorschriften zu löschen, bzw. – wenn dies einen unverhältnismäßig großen Arbeitsaufwand erfordern würde – unterliegen sie einem absoluten Verwertungsverbot.

5.4.2

Gemeinsames Informations- und Analysezentrum für die Polizei und das Landesamt für Verfassungsschutz

Das Hessische Ministerium des Innern und für Sport plant, ein gemeinsames Informations- und Analysezentrum für Polizei und Verfassungsschutz aufzubauen.

Auf meine Nachfrage hat das Hessische Ministerium des Innern und für Sport bestätigt, dass ein gemeinsames Informations- und Analysezentrum errichtet werden soll, in dem Mitarbeiter der Polizei und des Verfassungsschutzes zusammenarbeiten. Damit soll eine Einrichtung beim Ministerium geschaffen werden, die Informationen zur politisch motivierten Kriminalität zusammenführt und für die Aufgabenwahrnehmung der Hausspitze aufarbeitet.

Ich habe mich in Gesprächen mit dem Hessischen Ministerium des Innern und für Sport dafür eingesetzt, dass nur die für die Ausübung der Fachaufsicht des Ministeriums erforderlichen Informationen von Polizei und Verfassungsschutz an das Gemeinsame Informations- und Analysezentrum übermittelt werden dürfen. Des Weiteren wird klargestellt, dass das Gemeinsame Informations- und Analysezentrum nur unter den im Verfassungsschutzgesetz vorgesehenen Voraussetzungen an die Polizeibehörden übermitteln darf.

Der Entwurf für eine Dienstanweisung, in der diese Festlegungen getroffen werden, liegt mir derzeit vor.

Im Rahmen meines Kontrollauftrags werde ich darauf achten, dass auf der Vollzugsebene auch künftig das datenschutzrechtliche Trennungsprinzip von Polizei und Verfassungsschutz eingehalten wird.

5.5 Verkehrswesen

5.5.1

Inhalt von Führerscheinakten – Speicherung im örtlichen Fahrerlaubnisregister

Benötigt ein Führerscheininhaber eine Karteikartenabschrift aus dem örtlichen Fahrerlaubnisregister, darf die Behörde nur die zur Bearbeitung des Antrags erforderlichen Daten übermitteln.

Wenn ein Fahrerlaubnisinhaber nicht mehr im Zuständigkeitsbereich der örtlichen Fahrerlaubnisbehörde wohnt, die ihm die Fahrerlaubnis erteilt hat, und er z. B. eine Änderung, Neuausstellung bei Verlust oder Wiedererteilung seiner Fahrerlaubnis beantragt, muss er der für ihn jetzt zuständigen Fahrerlaubnisbehörde eine so genannte Karteikartenabschrift der zuvor zuständigen Fahrerlaubnisbehörde vorlegen.

Mehrere Eingaben an meine Behörde im Berichtsjahr haben gezeigt, dass jedoch vor einer Übermittlung von Karteikartenabschriften aus dem Fahrerlaubnisregister die Behörden häufig nicht prüfen, welche Daten, die im örtlichen Fahrerlaubnisregister zu der betreffenden Person

gespeichert sind, für den Einzelfall erforderlich sind und deshalb übermittelt werden dürfen. So wurde z. B. einem Führerscheininhaber, der die Ausstellung eines Karteikartenführerscheins beantragt hatte, auf seinen Antrag hin eine Karteikartenabschrift mit Daten aus den Jahren 1963, 1967 und 1974 übersandt. Die Übermittlung der Daten aus den Jahren 1963 und 1967 war unter Beachtung der nachfolgend näher beschriebenen Lösungsfristen unzulässig.

Da das Datum der Erteilung bzw. der letzten Wiedererteilung – unabhängig davon, wie lange dies zurückliegt – als so genanntes Grunddatum nicht gelöscht werden darf, hätte in diesem Fall nur das Datum aus dem Jahr 1974 übermittelt werden dürfen, da zu diesem Zeitpunkt die letztmalige Wiedererteilung erfolgte.

Fahrerlaubnisbehörden führen im Rahmen ihrer örtlichen Zuständigkeit ein Register (örtliches Fahrerlaubnisregister), in dem u. a. Entscheidungen enthalten sind, die Bestand, Art und Umfang von Fahrerlaubnissen betreffen. Welche Daten darüber hinaus in diesen örtlichen Fahrerlaubnisregistern enthalten sein dürfen, ist in § 50 Abs. 2 StVG geregelt. Dies sind z. B. der Widerruf oder die Rücknahme der Fahrerlaubnis, Fahrverbote oder die Sicherstellung und Verwahrung von Führerscheinen. § 2 Abs. 9 StVG regelt, dass Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse aus diesen örtlichen Fahrerlaubnisregistern nach zehn Jahren zu vernichten sind, es sei denn, dass mit ihnen im Zusammenhang stehende Eintragungen im Verkehrszentralregister oder im zentralen Fahrerlaubnisregister nach den Bestimmungen für diese Register zu einem späteren Zeitpunkt zu tilgen oder zu löschen sind. In diesem Fall ist für die Vernichtung oder Löschung der spätere Zeitpunkt maßgeblich.

Sind in den örtlichen Fahrerlaubnisregistern Entscheidungen enthalten, die auch im Verkehrszentralregister einzutragen sind, gelten gemäß § 61 Abs. 3 StVG die in § 29 StVG geregelten Tilgungsfristen auch für die im örtlichen Fahrerlaubnisregister gespeicherten Eintragungen.

Zu den so genannten Grunddaten, die gemäß § 61 Abs. 1 StVG nicht gelöscht werden dürfen, gehört das Datum der Erteilung (also auch der Wiedererteilung) der Fahrerlaubnis. Konkret bedeutet dies, dass nach Ablauf der Tilgungs- und Lösungsfristen die Akten zwar vernichtet werden, die Chronologie der Fahrerlaubniserteilung (z. B. Erteilung am 17. Mai 1981, Entzug am

28. März 1983, Wiedererteilung am 10. Mai 1984) im örtlichen Fahrerlaubnisregister jedoch noch enthalten ist.

Sofern eine Karteikartenabschrift aus dem örtlichen Fahrerlaubnisregister benötigt wird, darf die Behörde jedoch nur die für den konkreten Einzelfall erforderlichen Daten übermitteln. Um dies zu gewährleisten, muss die Behörde vor einem Ausdruck der Karteikartenabschrift aus dem Register die gespeicherten Daten überprüfen. Enthält das Register Daten, die zur Bearbeitung des Antrags nicht erforderlich sind, müssen diese für den aktuellen Ausdruck und die anschließende Übermittlung gelöscht werden.

Ich habe die betroffenen Fahrerlaubnisbehörden auf die Einhaltung der gesetzlichen Bestimmungen hingewiesen und veranlasst, dass – in dem eingangs erwähnten Fall – dem Petenten eine korrekte Karteikartenabschrift übersandt wurde.

5.5.2

Nutzung von Bankverbindungsdaten aus der Kfz-Zulassung

Bankverbindungsdaten, die eine Zulassungsstelle anlässlich der Zulassung eines Fahrzeuges zur Sicherung der Kraftfahrzeugsteuer erhebt, sind Steuerdaten. Sie dürfen nicht zur Vollstreckung anderer Forderungen als in Kraftfahrzeug-Steuersachen an die Kreiskassen übermittelt werden.

Verschiedene Anfragen von Kreiskassenmitarbeitern machten mich auf eine unzulässige Datenweitergabe von Bankverbindungsdaten durch Zulassungsstellen aufmerksam.

Seit dem 1. Januar 2004 muss ein Fahrzeughalter bei der Zulassung eines Fahrzeuges bei einer hessischen Zulassungsstelle obligatorisch seine Bankverbindung mit der Ermächtigung zum Einzug der Kraftfahrzeugsteuer angeben (§ 13 Abs. 1 Satz 2 und Abs. 1a Kraftfahrzeugsteuergesetz i. V. m. § 1 der Verordnung über die Mitwirkung der Zulassungsbehörden bei der Verwaltung der Kraftfahrzeugsteuer). Die Zulassungsstellen fragen die Bankverbindungsdaten anlässlich der Zulassung eines Fahrzeuges für die Finanzverwaltung als Landesfinanzbehörde zur Sicherstellung des Kraftfahrzeugsteuer-Aufkommens ab. Bei den Zulassungsstellen sammelt sich somit ein Datenbestand über Bankverbindungen an, der Begehrlichkeiten bei den Kassen bzw. Vollstreckungsstellen der Kreisverwaltungen weckt.

Da die Daten ausschließlich für die Finanzverwaltung erhoben werden, handelt es sich um Steuerdaten, die dem Steuergeheimnis nach § 30 AO unterliegen.

Eine Datenübermittlung von den Zulassungsstellen an die Kreiskassen zur Vollstreckung von anderen öffentlichen Forderungen außerhalb des Kraftfahrzeugsteuerverfahrens ist zweckwidrig und verletzt das Steuergeheimnis. Es fehlt in diesem Fall an einer Rechtsgrundlage für die Zweckänderung. Daran ändert auch der Hinweis auf § 17a HVwVG nichts. Nach dieser Vorschrift darf eine Vollstreckungsbehörde Steuerdaten, die dem Steuergeheimnis unterliegen, nur dann zur Vollstreckung anderer Geldforderungen verwenden, wenn die Daten ihr zuvor aus einer Vollstreckung wegen Steuern oder steuerlicher Nebenleistungen bekannt geworden sind. Dies ist im Rahmen der Kraftfahrzeugsteuer-Vollstreckung bei den Kreiskassen nicht der Fall. Damit ist auch die Einrichtung eines allgemeinen automatisierten Zugriffsrechts auf die Bankverbindungsdaten bei den Zulassungsbehörden nicht zulässig.

Auf meinen Hinweis hin, hat das Hessische Ministerium für Wirtschaft und Verkehr mit Erlass vom 21. Juni 2005 die Rechtslage klargestellt.

5.6 Schulverwaltung

5.6.1

Neuerungen im Schulgesetz

Die seit 1. August 2005 wirksame Änderung des Hessischen Schulgesetzes bringt auch einige datenschutzrechtlich relevante Rechtsänderungen.

Nachdem ich mich schon im Rahmen des Gesetzgebungsverfahrens gegenüber dem Hessischen Kultusministerium zu Fragen der datenschutzrechtlichen Neuerungen im Entwurf des seit 1. Januar bzw. seit 1. August 2005 geltenden Schulgesetzes geäußert hatte, sind meine Anregungen überwiegend berücksichtigt worden. Wegen der praktischen Auswirkungen auf den Schulalltag seien hier einige wesentliche Punkte angesprochen:

5.6.1.1

Evaluierung in der Schule

Die Evaluierung hält auch Einzug in der Schule, nachdem sie bereits im Hochschulbereich zum Standardwerkzeug für die Verbesserung der Lehre fest etabliert worden ist.

Soweit die Lehrkräfte bei der Qualität des von ihnen betreuten Unterrichts evaluiert werden sollen – ein ausdrückliches Ziel hessischer Schulpolitik – greifen die an der Evaluierung beteiligten schulinternen oder externen Personen nicht nur auf schon vorhandene Schulverwaltungs- und Personalunterlagen zu den betroffenen Lehrkräften zurück; sie erheben zudem neue, zusätzliche Informationen durch Besuch und Beurteilung des Unterrichts. Da diese Daten über den herkömmlichen Rahmen von Schulverwaltungs- und Personaldaten hinausgehen, musste eine ausdrückliche und besondere Rechtsgrundlage für die Zulässigkeit der Verarbeitung dieser Daten geschaffen werden. Der neue § 83 Abs. 4 HSchulG versucht generalklauselartig, alle Varianten der Datenverarbeitung im Rahmen der Evaluierung einzufangen.

§ 83 Abs. 4 HSchulG

Zur Evaluation der Schulen nach § 98 können Schulen und die Schulaufsichtsbehörden oder von ihnen beauftragte Dritte methodisch geeignete Verfahren einsetzen und durch Befragungen, Erhebungen und Unterrichtsbeobachtungen gewonnene Daten verarbeiten. Die Betroffenen werden vorab über das Ziel des Vorhabens, die Art der Beteiligung an der Untersuchung, die Verarbeitung ihrer Daten sowie über die zur Einsichtnahme in die Daten und Ergebnisse Berechtigten informiert. Personenbezogene Daten für diese Zwecke dürfen ohne Einwilligung der Betroffenen verarbeitet werden, wenn das öffentliche Interesse an der Durchführung eines von der obersten Schulaufsichtsbehörde veranlassten oder genehmigten Vorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck des Vorhabens auf andere Weise nicht oder nur mit einem unverhältnismäßigen Aufwand erreicht werden kann. Unter diesen Voraussetzungen dürfen personenbezogene Daten auch Dritten, die mit der externen Evaluation beauftragt sind, überlassen werden. § 33 Abs. 2 und 3 des Hessischen Datenschutzgesetzes gilt entsprechend.

Im Mittelpunkt steht dabei die für die betroffenen Lehrkräfte notwendige Transparenz der jeweiligen Ziele und Abläufe der Evaluierungsschritte (s. Satz 2). Ausdrücklich zu regeln war

auch die Variante, dass im Falle der Evaluierung durch externe Personen die Überlassung der vorhandenen Daten an diese zulässig ist, unabhängig davon, ob es sich dabei um ein Auftragsverhältnis oder ein Forschungsprojekt handelt.

5.6.1.2

Bild- und Tonaufnahmen des Unterrichts

Bild- und Tonaufnahmen greifen besonders weit in die Persönlichkeitsrechte ein. Von einer solchen Dokumentation des Unterrichts sind sowohl die Schüler als auch die jeweils eingesetzten Lehrkräfte betroffen.

Abs. 5 des § 83 HSchulG lässt Bild- und Tonaufzeichnungen vom Unterricht ausdrücklich nur für Zwecke der Qualitätsentwicklung und zur Lehreraus- und -fortbildung zu, postuliert die Informationspflicht und ein Widerspruchsrecht der Betroffenen.

§ 83 Abs. 5 HSchulG

Für Zwecke der Lehreraus- und -fortbildung sowie der Qualitätsentwicklung des Unterrichts dürfen Bild- und Tonaufzeichnungen des Unterrichts erfolgen, wenn die Betroffenen rechtzeitig über die beabsichtigte Aufzeichnung und den Aufzeichnungszweck schriftlich informiert worden sind und nicht widersprochen haben. Die Aufzeichnungen sind spätestens nach fünf Jahren zu löschen, soweit schutzwürdige Belange der Betroffenen nicht eine frühere Löschung erfordern.

Es bleibt abzuwarten, ob diese Regelungen alle in der künftigen Praxis entstehenden datenschutzrechtlichen Probleme auffangen und befriedigend lösen können. Ich werde die Praxis weiter beobachten.

5.6.1.3

Nutzung privater IT-Geräte für Schulzwecke

5.6.1.3.1

Private IT-Geräte in der Schule

Die Fassung des alten § 83 Abs. 5 HSchulG verbot ausdrücklich die Nutzung privater DV-Geräte (Handheld, Notebook, Laptop, Handy) zu Schulverwaltungszwecken in der Schule. Dieses Verbot stellte sich aber im Schulalltag als nicht mehr zeitgemäß heraus, weil die Automatisierung auch im Schulverwaltungsbereich voranschreitet und die Ausstattung von Schule und Lehrkräften mit DV-Geräten oftmals hinter den Bedürfnissen zurückbleibt. Außerdem besteht die Notwendigkeit, viele Verwaltungsaufgaben mit Personenbezug IT-unterstützt auch zu Hause zu erledigen.

Gleichwohl trägt die Schule die datenschutzrechtliche Verantwortung für die IT-Nutzung in der Schule. Eine Öffnung für die Nutzung fremder IT in der Schule hat der Gesetzgeber deshalb unter den Vorbehalt gestellt, dass die notwendigen Datensicherheitsmaßnahmen eingehalten werden.

§ 83 Abs. 7 HSchulG

Die automatisierte Verarbeitung personenbezogener Daten darf in der Schule nur mit schuleigenen Datenverarbeitungsgeräten erfolgen, es sei denn, dass die Beachtung der erforderlichen Datensicherheitsmaßnahmen gewährleistet ist.

Sie müssen grundsätzlich den gleichen Sicherheitsstandard gewährleisten, wie sie die schuleigene IT-Ausstattung einzuhalten hat. Es wird also auch dem Datenschutzbeauftragten der Schule obliegen, diesen Aspekt zu prüfen und die Lehrkräfte entsprechend zu informieren und beraten.

5.6.1.3.2

Nutzung privater IT-Geräte für Schulungszwecke außerhalb der Schule

Die alte Fassung des § 83 Abs. 5 HSchulG sah vor, dass die Zulässigkeit der Nutzung schulfremder, vor allem eigener DV-Geräte der Lehrkräfte zu Hause von der schriftlichen Genehmigung der Schulleitung abhängig war. Die Details dazu regelte § 2 der „Verordnung zur Verarbeitung personenbezogener Daten in Schulen“ vom 30. November 1993 (ABl. des HKM 1994 S. 114).

Diese Regelung ist in der neuen Fassung des HSchulG entfallen. Grund hierfür war, dass sie weitgehend nicht eingehalten wurde, weil sie entweder nicht bekannt war oder bewusst negiert

wurde. Das deckt sich auch mit meinen Feststellungen (vgl. 33. Tätigkeitsbericht, Ziff. 5.5.2). Es wird aber gleichwohl eine Maßnahme der Schulleitung notwendig bleiben, das Problem zu lösen, wie die IT-Sicherheit auch im heimischen Bereich der Lehrkräfte sichergestellt werden kann.

Nach entsprechenden Äußerungen des Hessischen Kultusministeriums ist zu erwarten, dass zumindest bei der notwendigen Anpassung der oben erwähnten Rechtsverordnung Regularien hierzu aufgenommen werden. Es bleibt abzuwarten, ob damit das Bewusstsein der Lehrkräfte über ihre Verantwortung für die IT-Sicherheit auch zu Hause nachhaltig gestärkt werden kann. Die Gefährdungslage für die Schulverwaltungsdaten (Noten, Gutachten u. Ä) auf dem heimischen PC der Lehrkraft nimmt z. B. schon dann erheblich zu, wenn die Lehrkraft den PC auch für das Internet nutzt. Hier sind jedenfalls effiziente Schutzmaßnahmen zu treffen (z. B. verschlüsselte Speicherung, Einsatz mobiler Datenträger).

5.6.2

Folgerungen der IT-Sicherheitsleitlinie für die Schulen

Die IT-Sicherheitsleitlinie der Landesregierung, die einen einheitlichen IT-Sicherheitsstandard gewährleisten soll, gilt auch an hessischen Schulen. Das Hessische Kultusministerium wird Muster für Sicherheitskonzepte entwickeln und den Schulen zur Verfügung stellen.

Im 33. Tätigkeitsbericht habe ich mich in Ziff. 8.2.1 mit der Sicherheitsleitlinie beschäftigt. Sie wurde sowohl dort in Ziff. 11 als auch im Staatsanzeiger 2004, auf S. 3827 veröffentlicht und trat am 1. Dezember 2004 in Kraft.

Die IT-Sicherheitsleitlinie gilt für die rd. 2000 Schulen in Hessen. Bei meinen Prüfungen habe ich festgestellt, dass sie zumeist den Schulleitungen nicht bekannt war. Das Hessische Kultusministerium hat sie weder in seinem Amtsblatt veröffentlicht noch die Schulleitungen über ihre Existenz informiert.

Daraufhin habe ich mit dem Hessischen Kultusministerium Kontakt aufgenommen, um das weitere Vorgehen zu vereinbaren. In den Gesprächen wurde mir zugesagt, dass das Hessische Kultusministerium allen Schulen ausführliche Informationen über die Sicherheitsleitlinie und die daraus resultierenden Änderungen zukommen lässt.

Die wesentlichen Punkte werden nachstehend dargestellt:

5.6.2.1

Bestellung eines IT-Sicherheitsbeauftragten

Die Schulen haben bereits heute einen Datenschutzbeauftragten (§ 5 Abs. 1 HDSG) und oftmals auch einen IT-Beauftragten (freiwillige Benennung). Zukünftig müssen sie auch einen IT-Sicherheitsbeauftragten bestellen.

Nr. 5.2 IT-Sicherheitsleitlinie

Verantwortlichkeiten

Ein Sicherheitsmanagement besteht aus dem bzw. der IT-Sicherheitsbeauftragten, den Zuständigen für die Fachanwendungen, für den IT-Service und für den IT-Betrieb. Es ist damit zu betrauen, gemäß den Sicherheitsvorgaben die Sicherheit im Umgang mit der IT und den Schutz der Daten und Informationen zu gewährleisten. Ebenso gehört es zu seinen Aufgaben, das IT-Sicherheitskonzept fortzuschreiben und Maßnahmen umzusetzen, die ein angemessenes und dem Stand der Technik entsprechendes IT-Sicherheitsniveau sicherstellen. Der behördliche Datenschutzbeauftragte unterstützt den Dienststellenleiter bei der Umsetzung der IT-Sicherheit. Ihm ist deshalb die Teilnahme an den Beratungen des IT-Sicherheitsmanagements zu ermöglichen, soweit er dies wünscht.

Die Aufgaben dieser drei Funktionsträger sind klar abzugrenzen. Der behördliche Datenschutzbeauftragte darf nicht IT-Sicherheitsbeauftragter sein. Die Funktion des IT-Beauftragten und des Sicherheitsbeauftragten kann aber von einer Person wahrgenommen werden.

5.6.2.2

Erstellung eines Sicherheitskonzeptes

Es war schon immer erforderlich, einen angemessenen Sicherheitsstandard zu gewährleisten. Einige Schulträger haben auch schon in der Vergangenheit für ihre Schulen Sicherheitskonzepte für den

Schulverwaltungsbereich realisiert. Seit 1. Dezember 2004 müssen alle Schulen Sicherheitskonzepte erstellen.

Nr. 4.1 IT-Sicherheitsleitlinie

Maßnahmen

Für bereits betriebene und für geplante Informationstechnik sind IT-Sicherheitskonzepte zu erstellen. Im Rahmen dieses Verfahrens sind die personalvertretungsrechtlichen Beteiligungsrechte zu wahren.

Dem IT-Sicherheitsbeauftragten obliegt die Aufgabe, diese IT-Sicherheitskonzepte koordinierend zu erstellen, deren Umsetzung zu planen und zu überprüfen. Ziel ist es, einen landeseinheitlich hohen Sicherheitsstandard zu erreichen.

Mit Hilfe dieser Konzepte, die nach den Vorgaben der IT-Sicherheitsleitlinie entsprechend dem IT-Grundschutzhandbuch erstellt werden müssen, können technische, infrastrukturelle und organisatorische Sicherheitsmaßnahmen optimal aufeinander abgestimmt werden. Die vom BSI empfohlenen Sicherheitsmaßnahmen eignen sich, systematisch nach Sicherheitslücken zu suchen, vorhandene Sicherheitsmaßnahmen zu überprüfen und neue in das Sicherheitskonzept einzuplanen.

In den Schulen, wo die Unterstützung durch den Schulträger fehlte, habe ich in der Regel keine Sicherheitskonzepte vorgefunden. Dies lag daran, dass das Personal in den Schulen nicht die fachliche Qualifikation aufweisen kann, die zur Erstellung eines Sicherheitskonzeptes erforderlich ist.

Gemeinsam mit dem Hessischen Kultusministerium habe ich nun einen Weg aus der Misere gesucht.

Das Hessische Kultusministerium sagte mir zu, Musterkonzepte zu erarbeiten und diese den Schulen zur Verfügung zu stellen. Ich habe ihm meine Unterstützung zugesagt.

Im nächsten Jahr werde ich prüfen, ob diese Vereinbarungen eingehalten wurden.

5.7 Bibliotheken

5.7.1

Speicherung von Lesernamen bei Bibliotheken

Die Angabe der Lesernamen zum Buchtitel in Bibliothekssystemen kann nur mit schriftlicher Einwilligung der Bibliotheksnutzer erfolgen.

Im Rahmen einer datenschutzrechtlichen Anfrage wurde ich erstmals mit einem Sachverhalt konfrontiert, der in der Praxis von öffentlichen Bibliotheken nicht ungewöhnlich sein dürfte: Der datenschutzrechtliche Grundsatz der Erforderlichkeit gebietet, dass der Titel des entliehenen Buches unter dem Namen der Entleiher in Bibliothekssystemen zu löschen ist, wenn der Entleihvorgang – mit der Rückgabe des Buches – abgeschlossen ist. Damit wird die Erstellung eines Leserprofils vermieden, da anderenfalls über eine längere Zeit die Titel aller entliehenen Bücher im System erhalten blieben.

Bei zahlreichen Lesern besteht allerdings der Wunsch, die entliehenen Buchtitel zu speichern, um die zweimalige Ausleihe eines Buches zu vermeiden. Denn nur so ist bei der wiederholten Leihe ein entsprechender Hinweis durch das Bibliothekspersonal möglich. Diese Datenspeicherung sah das System in dem angefragten Fall nicht vor, es konnte jedoch um dieses Merkmal ergänzt werden.

Da es sich bei diesem zusätzlichen Merkmal, das über die tatsächliche Entleihzeit eines Buches hinaus dauerhaft gespeichert werden sollte, ebenfalls um ein personenbezogenes Datum handelt, kann die nach § 7 Abs. 1 HDSG gebotene Rechtsgrundlage dazu nur in der schriftlichen Einwilligung des betroffenen Entleihers liegen, der diese Eintragung ausdrücklich wünscht.

§ 7 Abs. 1 HDSG

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

1. eine diesem Gesetz vorgehende Rechtsvorschrift sie vorsieht oder zwingend voraussetzt,
2. dieses Gesetz sie zulässt oder

3. der Betroffene ohne jeden Zweifel eingewilligt hat.

Denn diese Datenspeicherung wurde weder von der hier vorgelegten Bibliothekssatzung vorgesehen noch ist sie nach § 11 Abs. 1 HDSG für die Aufgabenerfüllung der Bibliothek erforderlich.

§ 11 HDSG

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

Ich habe daher die anfragende Bibliothek gebeten, für solche Fälle einen Vordruck für eine solche Einwilligungserklärung bereitzuhalten.

5.8 Gesundheitswesen

5.8.1

Elektronische Speicherung und Langzeitarchivierung von Krankenakten im Krankenhaus

Auch in Hessen speichern immer mehr Krankenhäuser (Teil-)Krankenakten in elektronischer Form. Meine Dienststelle hat zahlreiche Krankenhäuser beraten, welche datenschutzrechtlichen Aspekte bei der Entwicklung von Konzepten für die Digitalisierung und Langzeitarchivierung zu beachten sind.

5.8.1.1

Notwendigkeit eines Gesamtkonzepts

In diesem Jahr habe ich vermehrt Anfragen von Krankenhäusern erhalten, die neue Konzepte für die Führung und Archivierung ihrer Krankenakten planen. Die Krankenhäuser bzw. Ärzte sind

rechtlich verpflichtet, die wesentlichen Abläufe einer Behandlung in der Krankenakte zu dokumentieren. In vielen Krankenhäusern wird die rechtlich relevante Dokumentation noch in Papierform geführt. Parallel dazu werden vielfach Teile der Behandlungsdaten elektronisch im Krankenhauskommunikationssystem oder in peripheren Anwendungen gespeichert. In einem Teil der Krankenhäuser werden die (Papier-)Krankenakten digitalisiert und mikroverfilmt; oft verbunden mit einer Vernichtung der Papierakte. Hier stellt die mikroverfilmte Krankenakte die rechtlich relevante Dokumentation dar.

Mit der Digitalisierung und Mikroverfilmung der Krankenakten war bisher vor allem eine Reduktion der Kosten der Archivierung angestrebt worden. Vor diesem Hintergrund wurden in der Regel Vorgehensweisen entwickelt, bei denen die ältesten und voraussichtlich nur noch selten oder gar nicht benötigten Krankenakten digitalisiert und mikroverfilmt wurden. Daten über einen aktuellen Behandlungsfall sind heute in vielen Krankenhäusern nur teilweise in elektronischer Form vorhanden. Sie werden dann oft ausgedruckt und in Papierform in der Krankenakte abgelegt. Angestrebt wird aber in neuerer Zeit vielfach auch eine zeitnahe Digitalisierung aktueller Behandlungsdaten, sodass z. B. auch für die behandelnden Ärzte zur Arbeitserleichterung die komplette Krankenakte online verfügbar ist.

Bei der Einführung einer (vollständigen) digitalen bzw. elektronischen Krankenakte ist die Erstellung eines Gesamtkonzepts zur Digitalisierung und Langzeitarchivierung erforderlich, das auch die datenschutzrechtlichen Aspekte berücksichtigen muss. Zu klären sind insbesondere die folgenden Fragen:

- Sollen künftig alle Dokumente elektronisch gespeichert werden?
- Zu welchem Zeitpunkt sollen die Dokumente digitalisiert werden?
- Wie soll sichergestellt werden, dass sämtliche zu einem Behandlungsfall erstellte/eingegangene Dokumente zu einer Krankenakte zusammengeführt werden können?
- Wer gibt ein Papierdokument frei zur Digitalisierung und was bedeutet diese Freigabe?
Es muss geklärt werden, wer diese Aufgabe wahrnehmen soll und für welche Aspekte damit die Verantwortung übernommen wird.
- Wer soll die Berechtigung erhalten, Papierdokumente zu scannen?

In Betracht kommen kann nur ein begrenzter besonders vertrauenswürdiger Personenkreis. Sofern die Aufgabe des Scannens gemäß § 12 Abs. 1 HKG i. V. m. § 4 HDSG als Auftragsdatenverarbeitung an einen externen Dienstleister vergeben werden soll, müssen alle Arbeits- und Verarbeitungsschritte datenschutzgerecht organisiert und dokumentiert werden.

- Soll die Original-Papierakte nach der Digitalisierung vernichtet werden?
Wenn ja, wie soll dem Prozessrisiko begegnet werden, das entsteht, wenn die Originalunterlagen im Prozess nicht mehr vorgelegt werden können?
- Wie lange sollen digitale elektronisch gespeicherte Behandlungsdaten im aktuellen Online-Speicher zur Verfügung stehen? Wie sollen die Daten nach dieser Phase archiviert werden?
- Wie sollen die Rechte der Patientinnen und Patienten auf Berichtigung, Sperrung, Löschung ihrer Daten sowie auf Auskunft und Einsicht realisiert werden?
- Welche Personen im Krankenhaus sollen auf welche Daten wie lange Zugriff erhalten?
- Wie soll die Löschung unzulässig gespeicherter bzw. nicht mehr für das Krankenhaus erforderlicher (und vom zuständigen Archiv i. S. d. HArchivG abgelehnter) Daten realisiert werden?

5.8.1.2

Fälschungssicherheit

Bei der Speicherung und Archivierung von Krankenakten ist zu berücksichtigen, dass es zu rechtlichen Auseinandersetzungen über die Behandlung und Schadensersatzforderungen von Patientinnen und Patienten gegenüber dem behandelnden Arzt und dem Krankenhaus kommen kann. Einen Haftungsprozess kann ein Arzt bzw. ein Krankenhaus im Regelfall nur gewinnen, wenn keine Kunstfehler begangen wurden und dies mittels der Behandlungsdokumentation in der Krankenakte bewiesen werden kann. Bei einer elektronischen Speicherung ist ohne elektronische Signatur (s. dazu noch unten Ziff. 5.8.1.2.2) grundsätzlich eine spurenlose nachträgliche Veränderung der Behandlungsdokumentation möglich. Mit einer elektronisch gespeicherten Krankenakte kann vor Gericht nicht wie mit unterschriebenen Schriftstücken ein Urkundenbeweis angetreten werden. Gemäß § 416 ZPO erbringen unterschriebene Dokumente als Privaturkunden den Vollbeweis dafür, dass der Erklärungsinhalt des Schriftstücks vom Unterzeichner stammt. Die freie Beweiswürdigung des Gerichts gemäß § 286 ZPO ist eingeschränkt, das Gericht kann die Unterschrift des Schriftstücks nicht frei würdigen, es hat bezüglich seiner Echtheit keinen Ermessensspielraum. Der neu gefasste § 371 Abs. 2 Satz 2 ZPO stellt klar, dass elektronische Schriftstücke nicht den gleichen Beweiswert haben wie unterschriebene Schriftstücke, sie unterliegen dem Beweis durch Augenschein und damit der freien richterlichen Beweiswürdigung i. S. v. § 286 ZPO. Der Beweis muss durch Vorlegung oder Übermittlung der Datei angetreten werden. Zur Beweisaufnahme muss das elektronische Dokument auf einem Computer des

Gerichts sichtbar gemacht werden. Der behandelnde Arzt kann in diesem Fall mittels der Behandlungsdokumentation eine konkrete Behandlung des Patienten nur schwer beweisen.

Als Problemlösung habe ich mit den Krankenhäusern verschiedene Verfahrensweisen diskutiert.

5.8.1.2.1

Erstellung eines Mikrofilms

Eine Mikroverfilmung von Krankenakten zur Langzeitarchivierung wird bereits seit Jahren von vielen Krankenhäusern – im Wesentlichen mit dem Ziel der Platzersparnis – durchgeführt. Eine Mikroverfilmung wird grundsätzlich auch als geeignet angesehen zur Beweisführung im Prozess. Es werden auch bereits technische Lösungen angeboten für eine Automatisierung wesentlicher Funktionen der Langzeitarchivierung mit Mikrofilm. Allerdings muss im Prozess bewiesen werden, dass die Übereinstimmung der ursprünglichen Krankenakte mit der Abbildung auf Mikrofilm von dem Krankenhaus sichergestellt wurde. Diese Übereinstimmung kann durch verschiedene Verfahren sichergestellt werden.

5.8.1.2.1.1

Hybrid-Verfahren

Beim Hybrid-Verfahren wird gleichzeitig die Original-Papierakte digitalisiert und analog der Mikrofilm mittels Kamera von der Original-Papierakte belichtet. Auf dem Mikrofilm entsteht damit ein 100%iges Abbild der Krankenakte (einschließlich leerer Rückseiten, die leeren Rückseiten werden im digitalen Abbild ausgeblendet). Das Verfilmungsprotokoll wird zur Sicherheit mit auf dem Mikrofilm abgelegt. Damit stellt die Kamera die Übereinstimmung des Films mit der Original-Papierakte sicher und durch die zeitgleiche Digitalisierung wird die Übereinstimmung von Bild und elektronischem Abbild erreicht. Manipulationen sind lediglich vor dem Vorgang des Scannens (durch Verwendung einer falschen Vorlage) möglich. Ein Problem gibt es allerdings bei dem Hybrid-Verfahren: Durch die Gleichzeitigkeit der Digitalisierung und Mikroverfilmung besteht das Risiko, dass Seiten durch versehentlichen Doppeleinzug oder schlechte Qualität nicht auffindbar oder schlecht lesbar sind. Korrekturen sind aufwändig, da eventuell komplette Scanläufe wiederholt werden müssen.

5.8.1.2.1.2

COM-Verfahren

Beim COM-Verfahren (Computer Output on Mikrofilm) wird mittels eines herkömmlichen Scannens die Original-Papierakte zunächst digitalisiert. Das elektronische Abbild der Akte wird dann in einem zweiten, darauf folgenden, d. h. zeitversetzten Arbeitsgang auf den Mikrofilm aufgebracht, nachdem bei einem evtl. Doppeleinzug von Seiten eine automatische Korrektur erfolgte und ein Mitarbeiter die Qualität der Speicherung überprüft und bei Bedarf ein erneutes Scannen von Seiten mit einer anderen Einstellung veranlasst hat. Der Mikrofilm ist somit ein Abbild der elektronischen Krankenakte, nicht jedoch ein Abbild von der Original-Papierakte. Es besteht daher die Unsicherheit, ob während der Speicherung bis zur Erstellung des Mikrofilms eine Manipulation am elektronischen Abbild stattgefunden hat. Diese Unsicherheit nimmt mit der Dauer der elektronischen Speicherung zu, sodass unter dem Gesichtspunkt der Fälschungssicherheit eine möglichst kurze Zeitspanne bis zur Erstellung des Mikrofilms wünschenswert ist. Für diese Zeitspanne muss die grundsätzlich bestehende Unsicherheit durch die eingesetzte Technik und organisatorische Maßnahmen minimiert werden, sodass in einem Prozess vor Gericht überzeugend dargelegt werden kann, dass das gescannte und elektronisch gespeicherte Dokument vor der Erstellung des Mikrofilms nicht verfälscht wurde. Gegenüber dem Hybrid-Verfahren muss daher beim COM-Verfahren der Ausschluss von Manipulationen durch aufwändigere technisch-organisatorische Maßnahmen sichergestellt werden. Solche Maßnahmen können z. B. sein:

- Restriktive Vergabe von Zutrittsrechten zu den Räumen mit den Rechnern, auf denen die Daten gespeichert werden.
- Nutzung der Rechner nur für das COM-Verfahren.
- Installation allein der hierfür benötigten Programme.
- Zugriffsrechte für die Rechner haben nur Personen, die das Verfahren bedienen.

Auch beim COM-Verfahren ist eine Verfälschung des Original-Papierdokuments vor der Digitalisierung und Mikroverfilmung grundsätzlich denkbar.

Mit der Mikroverfilmung kann daher keine vollkommene Fälschungssicherheit gewährleistet werden.

Probleme können auch entstehen, wenn ein Krankenhaus die Fälschungssicherheit seiner Krankenakte mittels Mikroverfilmung gewährleisten will, einzelne Dokumente der Krankenakte aber überhaupt nicht mehr in Papierform erstellt wurden, sondern ausschließlich in elektronischer Form mit elektronischer Signatur vorliegen.

Ein schlichtes Ausdrucken von einem elektronischen Dokument mit qualifizierter elektronischer Signatur kann kein (Papier-)Dokument mit gleichwertiger Beweisfunktion erzeugen:

Wenn die Signatur eines elektronischen Dokuments berechnet wird, werden alle Bits einbezogen; d. h. die Änderung eines Bits führt bereits zu einem anderen Ergebnis. Bei den „üblichen“ Dokumententypen, zum Beispiel das doc-Format von Microsoft Word, gibt es viele verborgene Informationen, die nicht ausgedruckt werden. Im Ergebnis liefern Dokumente, die sich in vielen Bits unterscheiden, gleiche Ausdrücke. Es gibt daher keine Möglichkeit, aus einem Ausdruck das zugrunde liegende elektronische Dokument Bit für Bit zu rekonstruieren. Die Rückführung in ein signiertes elektronisches Dokument ist nicht möglich.

Der OCR-lesbare Ausdruck eines elektronischen Dokuments, der alle Bits (hexadezimale Darstellung) umfasst und aus dem das elektronische Dokument rekonstruiert werden kann, wäre denkbar, kann aber nur bei wenigen Dokumentformaten sinnvoll sein. Für die heute gebräuchlichen Dokumentformate ist es keine Lösung.

Durch die Mikroverfilmung wird die Wirkung der elektronischen Signatur aufgehoben. Die Nachweise der Urheberschaft, der Authentizität und Integrität gehen verloren.

5.8.1.2.2

Elektronische Signatur von Dokumenten der Krankenakte

In meinem 24. Tätigkeitsbericht, Ziff. 17.1 und meinem 30. Tätigkeitsbericht, Ziff. 4 habe ich die Vor- und Nachteile eines elektronisch signierten Dokuments im Vergleich zu einem per Hand unterschriebenen Dokument beschrieben. Für elektronische Dokumente kann man feststellen, dass wesentliche Anforderungen an die Fälschungssicherheit und die eindeutige Urheberschaft, also Wahrung der Integrität und Authentizität, nur mit einer elektronischen Signatur erreicht werden können. Für elektronische Dokumente im Krankenhaus, die im Rahmen der Behandlung

(Laborbefunde, Arztbriefe etc.) erzeugt werden, kommt dabei die elektronische Signatur für jedes einzelne Dokument in Betracht.

Die elektronische Signatur ermöglicht eine rechtssichere und beweiskräftige Archivierung. Elektronische Dokumente ohne Signatur unterliegen der freien richterlichen Beweiswürdigung nach § 286 ZPO. Je nach Fallkonstellation hängt es vom Vorliegen weiterer unterstützender Tatsachen ab, ob der Beweis mit den elektronischen Dokumenten erbracht werden kann oder nicht. Zwar kann durch aufwändige technische und organisatorische Maßnahmen eine Manipulation von elektronischen Dokumenten weitgehend ausgeschlossen werden. Im gerichtlichen Verfahren müssen aber u. U. umfangreiche Gutachten eingeholt werden, um die Qualität der Sicherheitsmaßnahmen und damit die Fälschungssicherheit zu beurteilen. Der Ausgang des Verfahrens ist daher mit Unsicherheiten verbunden. Demgegenüber hat der Gesetzgeber mit den neuen Regelungen der §§ 292a ZPO, 126a BGB eine Beweiserleichterung für elektronisch signierte Dokumente geschaffen, die die beweisrechtliche Würdigung ähnliche voraussehbar machen soll wie die eines (Papier-)Schriftstücks.

Für die tägliche Arbeit bieten signierte elektronische Dokumente einige Vorteile. Sie erlauben es, die Arbeit und die IT weiter zu verzahnen, ohne einige Vorteile von Papierdokumenten wie das Erkennen der Urheberschaft und die Wahrung der Integrität zu verlieren. Sie werden auch durch die Entwicklung bei der Telematik im Gesundheitswesen an Bedeutung gewinnen. In absehbarer Zeit werden Dokumente, die den Patienten betreffen, qualifiziert signiert per E-Mail übertragen werden.

Bei der Langzeitarchivierung elektronischer Dokumente ergeben sich allerdings Probleme. Mit der Zeit sind die Dokumente im Unterschied zu Papierdokumenten immer weniger für Beweise geeignet, da die verwendeten Algorithmen und Schlüssel „schwächer“ werden, d. h. Fälschungen werden eher möglich, und die zur Überprüfung nötigen Verzeichnisse und Unterlagen sind vielleicht nicht mehr vorhanden.

Weiterhin gibt es bei allen elektronischen Dokumenten eine Schwachstelle. Um die Dokumente am Bildschirm ansehen oder ausdrucken zu können, muss die richtige Hard- und Software vorhanden sein. Die Datenträger müssen also gelesen werden können und das Dokumentenformat muss richtig verarbeitet werden können. Diese Anforderung muss für die gesamte Dauer der Archivierung erfüllt werden. Bei einer Archivierungsdauer von mehreren Jahrzehnten sind das

erhebliche Anforderungen an die Technik: Am Beispiel eines Textdokuments, das im Wordperfect-Format auf einer 5,25-Zoll-Diskette gespeichert ist und als Ausdruck vorgelegt werden soll, kann man sich den Aufwand vorstellen. In der Regel wird davon ausgegangen, dass die Daten in regelmäßigen Abständen auf andere Datenträger und ggf. andere Formate umkopiert werden. Dabei kann jedoch in einigen Konstellationen das Dokument verändert werden, weshalb die Signatur nicht mehr als gültig erkannt würde.

Um diese und andere Schwierigkeiten zu erkennen und Lösungen zu erarbeiten, wurde z. B. das Projekt ARCHISIG [(www.archisig.de; Rossnagel/Schmücker (Hrsg.), Beweiskräftige elektronische Archivierung. Bieten elektronische Signaturen Sicherheit? Economica 2006] gestartet. Dabei beschränkte man sich auf Fragen, die mit einer elektronischen Archivierung signierter Dokumente zusammenhängen. Ob und wie eine Mikroverfilmung zusätzlich machbar und erforderlich ist, gehörte nicht zum Projektumfang. Im Ergebnis wurde ein Konzept entwickelt, wie elektronisch signierte Dokumente Signaturgesetz-konform archiviert werden können und dabei trotzdem Anpassungen an Änderungen der Technik möglich sind. Im Folgeprojekt ARCHISAFE (www.archisafe.de) werden die Fragestellungen insbesondere in technischer Hinsicht vertieft. Die Frage, ob mit diesem Konzept auch sichergestellt ist, dass die Dokumente über viele Jahrzehnte lesbar und die ursprünglichen Signaturen prüfbar bleiben, kann aber nur durch die Praxis beantwortet werden.

5.8.1.3

Nachweis der Urheberschaft

Im Gegensatz zur Original-Papierkrankenakte kann eine mikroverfilmte Krankenakte ebenso wie eine elektronische Krankenakte keinen sicheren Nachweis der Urheberschaft eines Dokuments erbringen. Durch das Filmen bzw. Scannen geht der Unterschriftencharakter verloren; es ist z. B. keine graphologische Begutachtung möglich. Soweit ein Krankenhaus davon ausgehen muss, dass die Urheberschaft eines Dokuments zukünftig evtl. noch einmal nachgewiesen werden muss, bleibt es erforderlich, das Dokument im (Papier-)Original weiter vorzuhalten.

5.8.1.4

Langfristige Verfügbarkeit

Die Mikroverfilmung, bei der lediglich Lupe, Licht und Auge für das Lesen der Dokumente erforderlich sind, kann auf jeden Fall eine langfristige Verfügbarkeit der Krankenakte gewährleisten. Der Mikrofilm ist als dauerhaftes Speichermedium bewährt, während für die elektronische Archivierung keine vergleichbaren Erfahrungen existieren (s. o. Ziff. 5.8.1.2.2). Dies sollte bei Entscheidungen berücksichtigt werden.

5.8.2

Aktuelle Entwicklung des Neugeborenen-Screenings

In der gesetzlichen Krankenversicherung ist ein erweitertes Neugeborenen-Screening eingeführt worden. In Hessen können die Eltern wählen zwischen diesem Angebot der gesetzlichen Krankenversicherung und einem vom Hessischen Sozialministerium geförderten, darüber hinausgehenden Screening. Der Umgang mit den Daten und Restblutproben ist noch nicht vollständig geklärt.

In meinem 32. Tätigkeitsbericht (Ziff. 14.2) hatte ich bereits ausführlich dargelegt, dass eine zentrale bevölkerungsbezogene Speicherung der Daten und Aufbewahrung der Restblutproben erhebliche datenschutzrechtliche Brisanz hat und die rechtlichen Rahmenbedingungen für das Neugeborenen-Screening daher mehrfach Gegenstand öffentlicher Diskussionen waren. Es ist unerlässlich endlich zu klären und festzulegen, in welchem Umfang, zu welchem Zweck und in welchem Verfahren Daten und Blutproben gewonnen werden, wer zu welchem Zweck Zugang dazu hat und wann die Daten bzw. Proben gelöscht und vernichtet werden. Seit diesem Bericht ist das Verfahren in den verschiedenen Zusammenhängen weiter diskutiert worden.

5.8.2.1

Neues Standardverfahren in der gesetzlichen Krankenversicherung

Am 21. Dezember 2004 hat der Gemeinsame Bundesausschuss der Ärzte und Krankenkassen eine Änderung der Kinder-Richtlinien (Richtlinien des Bundesausschusses der Ärzte und Krankenkassen über die Früherkennung von Krankheiten bei Kindern bis zur Vollendung des

6. Lebensjahres) beschlossen. Nach dem aktuellen Text (www.g-ba.de) haben Neugeborene einen Anspruch auf Teilnahme am erweiterten Neugeborenen-Screening (Anlage 2, § 3). Die Zielkrankheiten, auf die auf freiwilliger Basis gescreent wird, sind in der Richtlinie abschließend aufgeführt (§ 5). Darüber hinaus enthält die Richtlinie detaillierte Festlegungen des gesamten Verfahrens. Aus datenschutzrechtlicher Sicht sind insbesondere die folgenden Regelungen relevant:

- Soweit technisch die Erhebung von Daten über weitere Krankheiten nicht unterdrückt werden kann, sind diese Daten unverzüglich zu vernichten (§ 5 Abs. 3).
- Die im Rahmen des Screenings erhobenen Daten dürfen ausschließlich zu dem Zweck verwendet werden, die in der Richtlinie aufgeführten Zielkrankheiten zu erkennen und zu behandeln (§ 5 Abs. 3).
- Die Eltern (Personensorgeberechtigten) des Neugeborenen sind vor der Durchführung des Screenings eingehend mit Unterstützung eines Informationsblatts zu Sinn, Zweck und Ziel des Screenings aufzuklären. Die Einwilligung oder Ablehnung zumindest eines Elternteils ist zu dokumentieren (§ 4).
- Die Restblutproben sind spätestens nach drei Monaten zu vernichten (§ 15 Abs. 3).

Damit liegt aus datenschutzrechtlicher Sicht eine korrekte und klare Regelung für das jetzt von der gesetzlichen Krankenversicherung vorgesehene Neugeborenen-Screening vor. Die Hessische Krankenhausgesellschaft bzw. die Krankenhäuser sehen jedoch die Richtlinie für sich nicht als verbindlich an, da ihrer Auffassung nach der Gemeinsame Bundesausschuss in der konkreten Zusammensetzung für die Krankenhäuser nicht zuständig war. Auch das Screening-Zentrum sieht die in der Richtlinie festgelegten Fristen offenbar nicht als verbindlich an.

Die unklare Entwicklung ist insgesamt (auch) aus Datenschutzsicht nicht glücklich, da die dringend notwendige – und eigentlich auch angestrebte – Transparenz für die Bürgerinnen und Bürger dadurch wieder in Frage gestellt ist. Vor diesem Hintergrund habe ich das Hessische Sozialministerium im September 2005 um Stellungnahme zur rechtlichen Situation gebeten. Eine Antwort liegt mir noch nicht vor.

5.8.2.2

Erweitertes hessisches Screening -Angebot

In Hessen können die Eltern das dargestellte Standardverfahren der gesetzlichen Krankenversicherung für ihr Neugeborenes wählen oder sich für die Teilnahme an dem vom Sozialministerium geförderten so genannten erweiterten hessischen Screening entscheiden. Dieses so genannte erweiterte hessische Verfahren sieht jetzt ein Screening auf 31 in der Elterninformation konkret benannte Zielkrankheiten vor. Es handelt sich ausschließlich um behandelbare Zielkrankheiten.

Auch für dieses Angebot ist jetzt die schriftliche Einwilligung der Eltern nach vorheriger Information vorgesehen. Nach den Vorstellungen des Hessischen Sozialministeriums und des Screening-Zentrums sollen die Restblutproben künftig zehn Jahre aufbewahrt werden, und zwar für Behandlungs-, Qualitätssicherungs- und Forschungszwecke. Der Zeitraum von zehn Jahren wird insbesondere deshalb als sinnvoll angesehen, weil manche der Erkrankungen, auf die gescreent wird, erst spät sichtbar werden können. In den Fällen, in denen bei den gescreenten Kindern mit negativem Befund später doch Krankheiten auftreten (derartige Fälle sind in Hessen bereits vorgekommen), ist eine Klärung der Ursache (falsches Blut auf der Karte, falsche Personenzuordnung der Karte, falsche Messung im Labor, fehlerhaftes Messverfahren) nur mit Hilfe der Originalblutproben möglich. Die Ursachen können später nicht mittels einer erneuten Blutentnahme bei den Betroffenen geklärt werden, weil sich das Blut des Neugeborenen innerhalb kurzer Zeit verändert und die ursprünglichen Untersuchungen daher nicht wiederholt werden können. Eine Ursachenklärung ist sowohl für evtl. Haftungsansprüche der Betroffenen wie auch für eine Kontrolle und Weiterentwicklung des Screening-Verfahrens von Bedeutung.

Wie im 32. Tätigkeitsbericht bereits berichtet, habe ich die Vorschläge des Hessischen Sozialministeriums und des Screening-Zentrums akzeptiert unter der Bedingung, dass

- die medizinischen Daten und die Blutproben der negativ gescreenten Kinder im Screening-Zentrum nach kurzer Frist pseudonymisiert werden,
- die persönlichen Daten der Kinder sich in einem rechtlich, räumlich und personell vom Screening-Zentrum getrennten Treuhänder befinden und
- die Zwecke, zu denen der Treuhänder auf Anfrage depseudonymisieren darf, konkret und verbindlich festgelegt sind.

Im Herbst 2005 wurde unter meiner Mitwirkung ein Treuhändervertrag entworfen und die Landesärztekammer hat ihre grundsätzliche Bereitschaft erklärt, beim Neugeborenen-Screening

als Treuhänder zu fungieren. Ein unterschriebener Treuhändervertrag liegt mir jedoch noch nicht vor.

5.8.3

Rahmenbedingungen für den Aufbau von Biobanken

Der Vorstand des Universitätsklinikums Frankfurt hat auf der Grundlage meiner Beratung Rahmenbedingungen für den Aufbau und Betrieb von Biobanken beschlossen, die insbesondere datenschutzrechtliche Anforderungen festlegen.

In meinem 33. Tätigkeitsbericht (Ziff. 5.8.1) hatte ich dargelegt, dass die Gewinnung, Aufbewahrung und Verwendung von Blut- und Gewebeproben zunehmend Gegenstand von öffentlichen Diskussionen ist. Insbesondere auch vor dem Hintergrund der ständig zunehmenden Möglichkeiten, Blut- und Gewebeproben genetisch zu analysieren, bedarf es der Klärung der zivilrechtlichen, strafrechtlichen und nicht zuletzt auch datenschutzrechtlichen Vorgaben. Der Vorstand des Universitätsklinikums Frankfurt hat auf der Grundlage meiner Beratung am 24. August 2005 Rahmenbedingungen für den Aufbau von Biobanken im Universitätsklinikum beschlossen, die die datenschutzrechtlichen Anforderungen erfüllen. Das Universitätsklinikum hat damit einen Schritt in Richtung Klarheit und Transparenz vorgenommen, der in vielen anderen Stellen noch aussteht. Die Rahmenbedingungen wurden im Hinblick auf über das Datenschutzrecht hinausgehende Fragen auch mit der Ethikkommission diskutiert.

Bei dem künftigen Aufbau langfristig angelegter Biobanken für die Forschung als Grundlage für noch nicht konkretisierte wissenschaftliche Studien sind lt. Beschluss die folgenden rechtlichen, organisatorischen und technischen Punkte zu beachten:

1. Verantwortliche Daten verarbeitende Stelle i. S. d. Datenschutzrechts

Verantwortliche Daten verarbeitende Stelle ist das Universitätsklinikum. Der Klinikträger ist verantwortlich für die Einhaltung des Datenschutzrechts sowie die weiteren rechtlichen Vorgaben. Die Projektleiter erarbeiten und dokumentieren das Datenschutzkonzept für die Biobanken.

2. Einschaltung des internen Datenschutzbeauftragten und des Hessischen Datenschutzbeauftragten

Das Datenschutzkonzept für die Biobanken ist dem internen Datenschutzbeauftragten zur Kenntnis zu geben. Er berät die Projektleiter. Projektleiter oder interner Datenschutzbeauftragter schalten bei Bedarf den Hessischen Datenschutzbeauftragten ein.

3. Einschaltung der Ethikkommission

Der Projektleiter muss grundsätzlich die Ethikkommission beteiligen. Dies kann je nach Einzelfall nach oder ggf. vor Beratung durch den Datenschutzbeauftragten geschehen.

4. Aufbewahrung/Speicherung der Proben/Daten im Universitätsklinikum

Eine langfristige namentliche Aufbewahrung, Speicherung und Verwendung der Proben/Daten ist für die Forschung im Regelfall nicht erforderlich und daher unzulässig. Die Proben und Daten sind vor der Aufnahme in die Bio-/Datenbank

- entweder vollständig zu anonymisieren, d. h. jede Möglichkeit einer Zuordnung zum individuellen Spender/Betroffenen ist auszuschließen - z. B. für die Grundlagenforschung.
- oder sicher zu codieren, – wenn für die Forschung eine Zuordnung zum Spender/Betroffenen möglich bleiben soll –, d. h. der Name und andere Identifikationsmerkmale sind durch einen Code zu ersetzen. Diesen Code können ausschließlich besonders hierfür berechtigte Personen in vorher festgelegten Bedarfsfällen mit Hilfe einer Zuordnungsliste dem Spender/Betroffenen wieder zuordnen. Die Zuordnungsliste ist besonders geschützt aufzubewahren. Je nach Dimension und Sensitivität des Projekts kann im Einzelfall eine Aufbewahrung der Zuordnungsliste bei einem externen Treuhänder erforderlich sein.

5. Technische und organisatorische Datensicherheitsmaßnahmen

Die Proben und Daten sind durch technische und organisatorische Maßnahmen vor dem unberechtigten Zugriff Dritter sicher zu schützen (abschließbare Räume bzw. Schränke, Passwortvergabe, Verschlüsselung, Abschottung von Internetzugang, möglichst zweite Codierung vor der Weitergabe codierter Proben/Daten an externe Dritte etc.).

6. Inhalt der Aufklärung der Spender

Eine Einwilligung ist nur rechtswirksam, wenn die Betroffenen vorher hinreichend konkret über den geplanten Umfang und Zweck der Biobanken aufgeklärt wurden („informed

consent“). Aus der Aufklärung der Spender müssen daher folgende Punkte ersichtlich sein:

- Verantwortliche Daten verarbeitende Stelle, verantwortlicher Projektleiter
- Zweck der Biobank
- Umfang der Probensammlung/Datenspeicherung
(Wird im Rahmen der Biobank ein spezieller Datensatz erhoben? Wird ein aus der Krankenakte extrahierter Datensatz gespeichert? Oder wird über das Pseudonym bei Bedarf ein Zugang zur Krankenakte ermöglicht?)
- Kreis der Personen, die Zugang/Kennntnis erhalten von personenbezogenen Daten
(keine Namen, sondern Funktionen/Rollen)
- Form der Aufbewahrung/Speicherung der Proben/Daten:
Inwieweit werden die Proben/Daten anonymisiert oder codiert aufbewahrt/verwendet?
Mögliche Anlässe und Berechtigte zu einer Re-Identifizierung der Spender?
- Weitergabe von Proben/Daten an externe Stellen außerhalb des Universitätsklinikums nur mit Einwilligung des Spenders und nur in anonymisierter oder pseudonymisierter Form
- Hinweis auf die Freiwilligkeit der Einwilligung und die Möglichkeit des Widerrufs der Einwilligung
- Hinweis darauf, dass aus der Verweigerung der Einwilligung keine Nachteile für den Spender entstehen
- Klärung der Frage, ob der Spender (auf Wunsch) über evtl. Forschungsergebnisse informiert wird/sich informieren kann
- keine Rechte des Spenders bei Patentanmeldungen/gewerblichen Nutzungen.

5.8.4

Unzulässige Verarbeitung von Versichertendaten in Vietnam

Die Verarbeitung personenbezogener Gesundheitsdaten im Rahmen so genannter Disease-Management-Programme (DMP) erfolgt durch eine Datenstelle, die von einem privaten Dienstleister betrieben wird. In der in Hallstadt (bei Bamberg) angesiedelten Datenstelle ist es zu gravierenden vertraglichen und datenschutzrechtlichen Verstößen durch den privaten Auftragnehmer gekommen, die von einem ehemaligen Mitarbeiter publik gemacht worden sind.

5.8.4.1

Zielsetzung und Organisation der Disease-Management-Programme

DMP verfolgen verschiedene Ziele: Zunächst geht es darum, Behandlungsziele zu formulieren. Danach muss die Therapie festgelegt werden. Schließlich gilt es, die Kooperation der Versorgungsträger untereinander zu beschreiben. Am Ende soll eine gezieltere und damit bessere Versorgung von chronisch Kranken erreicht werden.

Verschiedene Krankenkassen innerhalb Hessens, darunter auch die AOK Hessen, haben eine Arbeitsgemeinschaft (ARGE) Diabetes mellitus Typ 2 gebildet, der auch der Verband der Hausärzte in Hessen sowie die Kassenärztliche Vereinigung angehören. Die ARGE vertritt die Interessen der sie bildenden Gruppen und tritt rechtlich als Empfänger der ärztlichen Dokumentationen auf, welche die Hausärzte erstellen. Die ARGE hat die Datenverarbeitung selbst an eine so genannte Datenstelle abgegeben, die im Auftrag der ARGE die Bearbeitung der Daten, die Übermittlung an die im DMP-Vertrag festgelegten Stellen sowie die Speicherung der Daten übernimmt.

5.8.4.2

Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag ist im Regelfall mit der Kenntnisnahme personenbezogener Daten durch den Auftragnehmer verbunden. Der Gesetzgeber hat das zwar erlaubt, in § 80 SGB X jedoch strikte Vorgaben für die Auftragsdatenverarbeitung festgelegt, weil es sich bei den Sozial- bzw. Gesundheitsdaten um besonders sensitive, dem Sozialgeheimnis nach § 35 SGB I unterliegende Daten handelt.

§ 80 SGB X

...

(2) Eine Auftragsdatenverarbeitung für die Erhebung, Verarbeitung oder Nutzung von Sozialdaten ist nur zulässig, wenn der Datenschutz beim Auftragnehmer nach der Art der zu erhebenden, zu verarbeitenden oder zu nutzenden Daten den Anforderungen genügt, die für den Auftraggeber

gelten. Der Auftrag ist schriftlich zu erteilen, wobei die Datenerhebung-, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftraggeber ist verpflichtet, erforderlichenfalls Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zu erteilen. Die Auftragserteilung an eine nicht öffentliche Stelle setzt außerdem voraus, dass der Auftragnehmer dem Auftraggeber schriftlich das Recht eingeräumt hat,

1. Auskünfte bei ihm einzuholen,
2. während der Betriebs- oder Geschäftszeiten seine Grundstücke oder Geschäftsräume zu betreten und dort Besichtigungen oder Prüfungen vorzunehmen und
3. geschäftliche Unterlagen sowie die gespeicherten Sozialdaten und Datenverarbeitungsprogramme einzusehen,

soweit es im Rahmen des Auftrags für die Überwachung des Datenschutzes erforderlich ist.

...

(4) Der Auftragnehmer darf die zur Datenverarbeitung überlassenen Sozialdaten nicht für andere Zwecke verarbeiten oder nutzen und nicht länger speichern, als der Auftragnehmer schriftlich bestimmt.

5.8.4.3

Vertrag zwischen der ARGE Hessen und der Firma systemform mediocard GmbH

Innerhalb der Ablauforganisation der DMP hat die Firma systemform die Einrichtung und den Betrieb der Datenstelle übernommen. In der Datenstelle werden die eingehenden Dokumentationsbögen, die von den behandelnden Ärzten zusammen mit den Patienten ausgefüllt werden, und die umfangreiche medizinische Informationen z. B. über eine Diabetes mellitus Typ 2-Erkrankung enthalten, elektronisch erfasst, bearbeitet und in so genannte Teildatensätze zerlegt. Die Teildatensätze werden von der Datenstelle an die Krankenkassen und eine „Gemeinsame Einrichtung“ übermittelt. Die Gemeinsame Einrichtung nutzt diese (pseudonymisierten) Daten zu Zwecken der Qualitätskontrolle und Qualitätssicherung.

In dem Vertrag, den die ARGE mit der Firma systemform abgeschlossen hatte, waren Rechte und Pflichten von Auftraggeber und Auftragnehmer – so wie es der § 80 SGB X vorsieht – dezidiert geregelt. U. a. war auch festgelegt, dass eine Datenverarbeitung außerhalb der Grenzen der

Bundesrepublik Deutschland ausgeschlossen war. Allerdings war vereinbart worden, dass ein Unterauftragnehmer, die Firma GHP Document Services GmbH, für die Firma systemform die Dienstleistung übernehmen sollte.

Der Datenschutzbeauftragte der ARGE Hessen sowie die Vertreter des Datenschutzes der ebenfalls beteiligten Arbeitsgemeinschaften Sachsen, Hamburg, Schleswig-Holstein, Thüringen und Bayern waren im März 2004 in Hallstadt, um sich beim Auftragnehmer, also der GHP Document Services GmbH, vor Ort über die Ablauforganisation innerhalb der Datenstelle zu informieren sowie die getroffenen Datensicherheitsmaßnahmen in Augenschein zu nehmen. Bei diesem Informationsbesuch war ein Mitarbeiter meines Hauses zugegen. Die zeitliche begrenzte Inaugenscheinnahme der Datenverarbeitung gab damals keinen Anlass zur Kritik.

5.8.4.4

Hinweis eines Datenstellen-Mitarbeiters

Ende Januar 2005 erhielt mein Mitarbeiter den Anruf von einem ehemaligen Systemadministrator der Datenstelle. Der Anrufer schilderte fast unglaubliche Sachverhalte, welche die Rechtmäßigkeit der dort stattfindenden Datenverarbeitung in größte Zweifel brachte.

Er warf dem Geschäftsführer und führenden Mitarbeitern der GHP vor, für erhebliche Mängel im Zusammenhang mit der Verarbeitung von DMP-Daten verantwortlich zu sein. Folgende Vorwürfe wurden im Einzelnen erhoben:

- Keine Protokollierung und Dokumentation der inneren und äußeren DMP-Datenflüsse,
- Unverschlüsselte Übermittlung von personenbezogenen DMP-Daten (Dokumentationsbögen) über eine offene Datenleitung an ein Tochterunternehmen der GHP in Vietnam,
- Verarbeitung dieser Daten dort und Rückübermittlung an die GHP nach Deutschland,
- Allgemeiner Zugriff aller GHP-Mitarbeiter auf die DMP-Daten sowie
- Abschaltung bzw. Abbau der seinerzeit installierten Firewall.

Die telefonisch erhobenen Anschuldigungen präzisierete der Anrufer in den nächsten Tagen dann mit einer schriftlichen Stellungnahme. Zusätzlich konnte er mir auf meine Bitte hin ein File-Transfer-Protokoll übermitteln, aus dem sich das Volumen der nach Vietnam übermittelten Daten nachvollziehen ließ.

Mein Mitarbeiter hat unverzüglich den Datenschutzbeauftragten der ARGE Hessen von den Vorwürfen gegen den Betreiber der Datenstelle unterrichtet. Zusammen mit dem Datenschutzbeauftragten der ARGE Sachsen erfolgte bereits wenige Tage später eine Überprüfung der Datenverarbeitung vor Ort sowie die Konfrontation der verantwortlichen Mitarbeiter mit den Vorwürfen.

5.8.4.5

Erste Einlassung der GHP zu den Vorfällen

Sowohl der Geschäftsführer der GHP als auch dessen DV-Leiter bestritten die Vorwürfe. Sie wiesen vor allem die personenbezogene Übermittlung von DMP-Bögen, also der vom Arzt zusammen mit dem Patienten ausgefüllten Erst- und Folgedokumentationsbögen von sich. Sie erklärten gegenüber den ARGE-Datenschutzbeauftragten, dass eine „pseudonymisierte“ Übermittlung der Bögen stattgefunden habe, ohne die Merkmale Name des Versicherten, Krankenversicherungsnummer oder der Name des Arztes. Dazu sei, so die Einlassung von GHP, der obere Teil des Bogens „abgeschnitten“ und ausschließlich der inhaltliche Teil (ohne Personenbezug) zu dem Rechenzentrum nach Vietnam, einem Tochterunternehmen von GHP, übermittelt worden. Die Übermittlung habe man zu Testzwecken vorgenommen, um die OCR-Software, mit deren Hilfe die zu elektronischen Bildern (TIF-Dateien) umgewandelten Dokumentationsbögen gelesen werden, kontinuierlich zu kalibrieren, um so eine störungsfreie Verarbeitung in Deutschland sicherzustellen. Die Übermittlung, so wurde weiter behauptet, sei verschlüsselt erfolgt. Eine Firewall sei stets installiert und funktionsfähig gewesen. Allerdings konnte man keine Protokollierungen vorweisen, um die Darstellung nachvollziehbar zu machen. Begründet wurde dieser Mangel mit technischen Problemen und der Person des ehemaligen Mitarbeiters, der mich eingeschaltet hatte. Dieser habe in seiner Funktion als Systemadministrator, so die Version der GHP, eigenmächtig und unbemerkt die Abschaltung der Protokollierung vorgenommen.

Die Vertreter der ARGE kritisierten, dass auch die Übermittlung nicht personenbezogener Daten zu Testzwecken nach Vietnam hätten dem Auftraggeber angezeigt und von diesem genehmigt werden müssen. Die GHP-Holding, unter deren Dach der Subunternehmer GHP firmiert, reagierte auf die Vorfälle mit der Entlassung des Geschäftsführers von GHP, sah aber sonst keinen weiteren Handlungsbedarf.

5.8.4.6

Ergebnisse eines weiteren Prüftermins

Zur weiteren Bewertung des Sachverhaltes wurde drei Wochen später ein erneuter Gesprächstermin angesetzt, bei dem einer meiner Mitarbeiter ebenfalls zugegen war. Dabei wurden offen gebliebene Fragen angesprochen sowie weitere Mitarbeiterbefragungen durchgeführt. Am Ende der Veranstaltung ergab sich ein völlig anderes Bild und die Erkenntnis, dass beim ersten Prüftermin vom Geschäftsführer der GHP und seinem verantwortlichen Mitarbeiter die wahren Sachverhalte manipuliert und verschleiert wurden. Im Einzelnen wurde Folgendes festgestellt:

- Eine personenbezogene Übermittlung von DMP-Daten an das Rechenzentrum in Vietnam, einem Tochterunternehmen der GHP, fand bis zum 31. Januar 2005 statt. Die Behauptungen des Subunternehmers bzw. der Firma systemform, die Pseudonymisierung habe seit Ende März 2004 stattgefunden und damit ab dem Zeitpunkt des Datentransfers, entsprachen nicht den nachweisbaren Fakten. Die Mitarbeiterbefragung ergab nämlich, dass der Auftrag zur Erstellung des entsprechenden Programms am 31. Januar, also unmittelbar vor der Prüfung der ARGE-DSB in der Datenstelle, erging. In einer Art „Nacht-und-Nebel-Aktion“ programmierte der Mitarbeiter das Tool, welches am nächsten Tag präsentiert wurde und das angeblich bereits seit März 2004 im Einsatz gewesen war.
- Die Übermittlung der Daten fand unverschlüsselt und auf einer offenen Datenleitung statt. Dies ergibt sich ohne Zweifel aus dem mir zur Verfügung stehenden File-Transfer-Protokoll. Die Behauptungen der GHP entsprachen auch in diesem Punkt nicht der Wahrheit.
- Dass die Daten personenbezogen zum Zwecke der kontinuierlichen Verarbeitung und Rückübermittlung nach Vietnam transferiert wurden, ergibt sich sowohl aus dem File-Transfer-Protokoll als auch den Aussagen des ehemaligen Systemadministrators. Außerdem ist die eingesetzte OCR-Software im fraglichen Zeitraum nicht weiter gepflegt bzw. aktualisiert worden. Das war deshalb nicht erforderlich, weil ja die Erfassung der Bögen zu den entsprechenden Teildatensätzen von zahlreichen Datentypistinnen in Vietnam vorgenommen wurde. Eine Rückübermittlung der aufbereiteten Daten (die bis zum heutigen Tage bestritten wird) fand ausweislich des Protokolls ebenfalls statt. Nur dies ergibt im

Übrigen auch den Sinn, zehntausende von DMP-Bögen als TIF-Dateien nach Vietnam zu schicken.

- Eine Protokollierung bzw. Dokumentation des Datentransfers bzw. der Verarbeitung erfolgte nicht. Deshalb waren die Beschuldigten auch nicht in der Lage, die Vorwürfe substantiiert entkräften zu können.

Im Gegenteil: nach dem ersten Prüfbesuch der ARGE-Datenschutzbeauftragten wurde von GHP explizit zugesichert, die Protokollierung wieder einzuschalten. Die GHP hatte behauptet, sie habe erst zu diesem Zeitpunkt festgestellt, dass der ehemalige Mitarbeiter sie ausgeschaltet habe. Die zweite Prüfung ergab, dass die Protokollierung nach wie vor ausgeschaltet war.

- Ebenso bestätigt ist, dass bis Ende Februar 2005 keine funktionsfähige Firewall installiert war. Dies ergibt sich aus der Tatsache, dass keinerlei Firewall-Logdateien vorhanden waren und keine Hardware präsentiert werden konnte. Erst nach dem zweiten Prüfbesuch wurden entsprechende Investitionen getätigt.

5.8.4.7

Reaktion der Öffentlichkeit

Nur kurze Zeit nach dem Bekanntwerden der Datenschutzverstöße in der Datenstelle wurde die Öffentlichkeit aufmerksam. In den nächsten Wochen hatte mein Mitarbeiter zahlreiche Journalistenanfragen zu beantworten sowie Eingaben besorgter Bürger und Ärzte zu bearbeiten. Das Presseecho war für den Betreiber der Datenstelle ebenso vielfältig wie verheerend. Kein Wunder auch, stand doch die Verarbeitung sensibler medizinischer Daten der DMP stets im kritischen Blickpunkt insbesondere der Ärzte. Auch ein bundesweit ausgestrahlter Filmbeitrag beschäftigte sich mit dem Thema. In der Tat handelte es sich hier um eine ebenso einmalige wie datenschutzrechtlich gravierende Konstellation von Verstößen eines privaten Auftragnehmers gegen sowohl vertragliche als auch rechtliche Vorgaben.

5.8.4.8

Reaktion der ARGE

Das Krisenmanagement der Datenschutzbeauftragten der ARGE von Hessen und Sachsen, welche im Wesentlichen die Prüfungen vor Ort durchführten, gibt keinen Anlass zur Kritik. Ein enger Kontakt und Informationsaustausch zwischen ihnen und meiner Dienststelle war stets gewährleistet. Die Vertreter der ARGE, also Kassenvertreter, Hausärzteverband und Kassenärztliche Vereinigung, haben in mehreren Sitzungen die Aspekte, die sich aus den Feststellungen ergaben und die in diversen Prüfberichten zusammengetragen worden waren, diskutiert. An einer dieser Sitzungen nahm mein Mitarbeiter teil, um die Feststellungen der Datenschutzbeauftragten der ARGE zu unterstützen und eine dem Informationsstand angemessene Bewertung abzugeben.

5.8.4.9

Rechtliche Bewertung des Hessischen Datenschutzbeauftragten

Ich habe in zwei umfangreichen Stellungnahmen am 17. März und 28. April 2005 dem Vorstand der AOK Hessen, einem der größeren Mitglieder der ARGE Hessen, meine rechtliche Bewertung des Sachverhaltes mitgeteilt. In meinem ersten Brief bin ich auf die datenschutzrechtlichen Verstöße und Defizite der Datenverarbeitung in Hallstadt eingegangen und habe eine umgehende Beseitigung der Mängel gefordert. Ohne eine Beseitigung der Mängel hätte die Einstellung der Datenverarbeitung erfolgen müssen. In einem zweiten Brief bin ich auf die Reorganisation der Datenstelle sowie die realisierten Verbesserungen zur Einhaltung des technischen und organisatorischen Datenschutzes gemäß der Anlage zu § 78a SGB X eingegangen. Die Reorganisation war im April 2005 zwar noch nicht abgeschlossen, doch war das Bemühen der Verantwortlichen unverkennbar, endlich die Dinge so anzupacken und zu gestalten, wie dies der Gesetzgeber vorgeschrieben hat. Das Vertrauen in die Zuverlässigkeit des Auftragnehmers bleibt jedoch beeinträchtigt. Dennoch habe ich unter Berücksichtigung der realen Sachzwänge (die Beauftragung eines anderen Unternehmens war organisatorisch nicht zu bewältigen) meine Bedenken zurückgestellt. Allerdings habe ich Wert darauf gelegt, dass das Unternehmen regelmäßig, in kurzen Zeitabständen und in der Regel unangemeldet überprüft wird. Dies hat – auch im eigenen Interesse – die ARGE gewährleistet.

Mit meinen Kollegen in den ebenfalls betroffenen Ländern habe ich einen steten Kontakt gepflegt und Informationen weitergegeben. Meine rechtliche Bewertung der Situation wurde von den anderen Datenschutzbeauftragten geteilt.

5.8.4.10

Weitere Entwicklungen

Im März 2005 schaltete sich auch die Aufsichtsbehörde für den Datenschutz im privaten Bereich in Bayern, die Regierung von Niederbayern, ein und stellte nach Auskunft des dortigen Mitarbeiters einen Strafantrag wegen Verletzung des Datenschutzes. Gleichzeitig gab es nach meinem Kenntnisstand mehrere Privatpersonen bzw. Ärzte, die Strafanzeige gegen systemform mediacard stellten. Dies hat dazu geführt, dass die Staatsanwaltschaft in Bamberg ein Verfahren eröffnete und die zuständige Kriminalinspektion Bamberg mit den Ermittlungen beauftragte. Diese trat an mich heran und bat um Überlassung der bei mir gelagerten Unterlagen. Diese habe ich der Kriminalpolizei Bamberg unverzüglich übermittelt. Die weitere Entwicklung des Verfahrens ist zum jetzigen Zeitpunkt nicht abzusehen.

5.8.4.11

Grundsätzliche Konsequenzen für die Datenverarbeitung durch Dritte im Gesundheitsbereich?

Der geschilderte Fall hat anschaulich gezeigt, welchen potenziellen Risiken und Gefahren eine Verarbeitung personenbezogener Daten durch Dritte unterliegt. Dieses Instrumentarium, dessen sich sowohl nach dem § 80 SGB X als auch dem § 4 Abs. 2 HDSG öffentliche Stellen bedienen können, sollte man deshalb aber nicht grundsätzlich in Frage stellen. Es hat sich jedoch einmal mehr gezeigt, dass sowohl unmissverständliche und detaillierte Vertragsregelungen ebenso notwendig sind wie die Ausübung der Kontrollrechte, die der Auftraggeber sich schriftlich zusichern lassen muss. Auch sind die Anforderungen an einen Auftragnehmer zu spezifizieren und dieser sorgfältig auszuwählen. Eine vor allem bei länger andauernden Vertragsverhältnissen unregelmäßige, aber stete Kontrolle ist besonders wichtig. Dennoch ist der Auftraggeber trotz aller Sorgfaltspflichten nicht davor geschützt, dass betrügerische oder gar kriminelle Aktivitäten nicht unmittelbar erkannt werden. Einen absoluten Schutz gibt es nicht, doch kann man mit der Beachtung der von mir genannten Schutzmechanismen das potenzielle Risiko minimieren.

5.8.5

Schuleingangsuntersuchungen –

Der Informationsbedarf der Gesundheitsämter kommt einem Wildwuchs gleich

Die hessischen Gesundheitsämter verwenden für Schuleingangsuntersuchungen unterschiedliche Fragebogen. Einige der verwendeten Formulare enthalten Fragen, die nicht von den rechtlichen Grundlagen gedeckt werden. Auf meine Anregung werden die Gesundheitsämter mit meiner Mitwirkung einen landesweit einheitlichen Fragebogen unter Beachtung des rechtlichen Rahmens entwickeln.

Vom schulärztlichen Dienst der hessischen Gesundheitsämter werden im Rahmen der Schuleingangsuntersuchung schulpflichtiger Kinder unterschiedliche Dateninhalte erhoben, die oftmals nicht den rechtlichen Vorgaben entsprechen, die sich z. B. aus § 71 HSchulG oder der Verordnung über die Zulassung und Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege vom 7. Februar 2000 ergeben.

§ 71 HSchulG

1. Soweit zur Vorbereitung einer Entscheidung nach diesem Gesetz schulärztliche oder schulpsychologische Untersuchungen sowie sonderpädagogische Überprüfungen erforderlich werden, sind die Kinder, Jugendlichen und volljährigen Schülerinnen und Schüler verpflichtet, sich untersuchen zu lassen und an wissenschaftlich anerkannten Testverfahren teilzunehmen.
2. Kinder und Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler haben die für die Untersuchungen erforderlichen Angaben zu machen. Kinder, Jugendliche und volljährige Schülerinnen und Schüler dürfen dabei in der Regel nicht befragt werden über Angelegenheiten, die ihre oder die Persönlichkeitssphäre ihrer Eltern oder Angehörigen betreffen.
3. Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler sind über die Untersuchungen und Testverfahren vorher näher zu informieren. Ihnen ist Gelegenheit zur Besprechung der Ergebnisse und zur Einsicht in die Unterlagen zu geben.

4. Für Untersuchungen im Rahmen der Schulgesundheitspflege gelten Abs. 1 bis 3 entsprechend. Dabei können auch röntgenologische Untersuchungen sowie percutane und intracutane Tuberkuloseproben angeordnet werden.

§ 2 Abs. 1 der Verordnung über die Zulassung und Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege

Regelmäßige schulärztliche Untersuchungen finden anlässlich der Einschulung statt und sind danach in vierjährigen Abständen bis zum Ende der Schulausbildung der Schülerinnen und Schüler zulässig. Die Untersuchungen dienen der Gesunderhaltung, Entwicklungsbeurteilung und der Krankheitsfrüherkennung und schließen eine Beratung zur Veranlassung notwendiger Folgemaßnahmen und eine Impfberatung ein.

5.8.5.1

Die Beschwerden von Eltern schulpflichtiger Kinder

Im Berichtszeitraum erreichten mich verschiedene Beschwerden von Eltern, deren schulpflichtige Kinder von den Gesundheitsämtern zur Schuleingangsuntersuchung eingeladen worden waren. So wurde mit der Bekanntgabe des Untersuchungstermins ein Fragebogen mitgeschickt, der ausgefüllt zur Untersuchung mitgebracht werden sollte. In dem Bogen wurden Angaben zur sozialen und gesundheitlichen Anamnese des Kindes erhoben. Die Problematik besteht nun darin, dass die Inhalte der erhobenen Informationen von Gesundheitsamt zu Gesundheitsamt stark differieren. So wurde in einem Fall z. B. der vom Vater ausgeübte Beruf oder Angaben zur Schwangerschaft erfragt. Dabei sollte die Frage beantwortet werden, ob es u. a. zu einer Zangengeburt gekommen war oder aber eine Saugglocke verwendet werden musste. Auch sollte Angaben über „Auffälligkeiten“ im ersten Lebensjahr, wie z. B. das Tragen von Spreizhöschen, gemacht werden. Diese Inhalte führten dazu, dass von den Eltern hinterfragt wurde, ob man zur Auskunft solcher intimen persönlicher Details verpflichtet sei.

Auch die Aufforderung, zur Untersuchung den Impfpass des Kindes mitzubringen, stieß zunächst auf Unverständnis. Dabei leiten sich aus § 34 Abs. 11 Infektionsschutzgesetz (IfSG) eindeutige Vorgaben ab, welche die Gesundheitsbehörde befugt, diese Daten zu erheben.

§ 34 Abs. 11 IfSG

Bei Erstaufnahme in die erste Klasse einer allgemein bildenden Schule hat das Gesundheitsamt oder der von ihm beauftragte Arzt den Impfstatus zu erheben und die hierbei gewonnenen aggregierten und anonymisierten Daten über die oberste Landesgesundheitsbehörde dem Robert-Koch-Institut zu übermitteln.

5.8.5.2

Unterschiedliche Informationsanforderungen der Gesundheitsämter und mangelnde Hinweise auf die Rechtsgrundlagen für die Datenerhebung

Wenig nachvollziehbar ist, dass Art und Umfang der verlangten Informationen stark differiert. Während man sich bei der Stadt Frankfurt mit einem wenige Fragen umfassenden Bogen begnügte, forderte der Kreis Bergstraße ein Mehrfaches an Angaben von den Betroffenen ein.

Hinweise zur Rechtsgrundlage für die Datenerhebung fehlen ebenso in den Anschreiben an die Eltern wie Informationen zur Datenverarbeitung sowie zu Aufbewahrungsfristen bzw. der Dauer der Speicherung dieser Unterlagen. In einem Fragebogen war die Rechtsgrundlage falsch bzw. unvollständig zitiert.

5.8.5.3

Konsequenzen

Die wiederholt geäußerte Kritik betroffener Eltern hat mich veranlasst, das Thema im Rahmen einer Amtsleiterkonferenz der hessischen Gesundheitsämter zu thematisieren. Meine dort vertretene Auffassung, wonach es erforderlich ist, einen landesweit einheitlichen Standard der Datenerhebung anzustreben, wurde positiv aufgenommen. Dazu sollte ein landesweit einheitlicher Erhebungsbogen entwickelt werden, mit dem die erforderlichen Informationen im Rahmen der Schuleingangsuntersuchung abgefragt werden. Der hierfür zuständige Fachkreis der Schulärzte der Gesundheitsämter wurde beauftragt, die entsprechenden Voraussetzungen zu schaffen. In diesem Zusammenhang habe ich meine Mitwirkung hinsichtlich der Ausgestaltung des

Fragebogens, insbesondere was die rechtlichen Informationen zur Datenerhebung und -verarbeitung betrifft, zugesagt. Über die Ergebnisse werde ich im 35. Tätigkeitsbericht berichten.

5.8.6

Neue Datenverarbeitungsprojekte des Medizinischen Dienstes der Krankenversicherung Hessen

Im Berichtsjahr habe ich mit dem Medizinischen Dienst der Krankenversicherung in Hessen die datenschutzrechtlichen Anforderungen an verschiedene neue Datenverarbeitungsprojekte diskutiert. Einige Fragen sind weiterhin klärungsbedürftig.

5.8.6.1

Einsatz von Laptops durch die Gutachter des MDK

Vor allem im Bereich der Pflege wurden medizinische Informationen über den Patienten bislang händisch in einen Formularvordruck aufgenommen. Die Inhalte des Formulars dienten als Basis für das vom Gutachter zu erstellende medizinische Gutachten. Seit geraumer Zeit können sich die einzelnen Mitarbeiter jeweils eines Laptops bedienen. Die erhobenen Daten, die bislang per Hand auf Papier eingetragen wurden, werden nun in ein elektronisches Formular, das als Eingabemaske zur Verfügung steht, erfasst.

Die elektronische Ver- bzw. Bearbeitung personenbezogener Daten erfordert technische und organisatorische Maßnahmen zu Datenschutz und Datensicherheit, wie sie sich insbesondere aus der Anlage zu § 78a SGB X und § 10 Abs. 2 HDSG ableiten. Schließlich werden medizinische Daten, die der ärztlichen Schweigepflicht unterliegen, auf einem elektronischen Speichermedium abgelegt. Diese Informationen müssen vor einem Zugriff unbefugter Dritter angemessen und wirksam geschützt werden. Gerade bei Laptops gibt es das Diebstahlrisiko, das beachtet werden muss. Deshalb ist es z. B. unumgänglich, solche besonders sensiblen personenbezogenen (Gesundheits-)Daten nur verschlüsselt auf der Festplatte zu speichern. Selbstverständlich ist unter Zuhilfenahme einer entsprechenden Schutzsoftware auch der Zugang zum Betriebssystem zu sichern. Derartige Sicherheitsmaßnahmen waren jedoch zum Zeitpunkt meiner Gespräche mit dem

MDK über Art und Umfang der Nutzung dieses Mediums nicht realisiert. Erschwerend kam hinzu, dass in der Vergangenheit bereits zwei von etwa 90 durch Gutachter außer Haus eingesetzter Laptops gestohlen wurden. Ich habe deshalb dem MDK gegenüber eine unmittelbare Umsetzung der erforderlichen Sicherheitsmaßnahmen gefordert, die nach Auskunft der Geschäftsleitung inzwischen realisiert ist. Danach hat man das Produkt „SafeGuard Easy“ auf alle mobilen Rechner aufgespielt, die im Außendienst eingesetzt werden. Hinzu kommt, dass durch die technische Abteilung beim MDK für jeden Laptop eine besondere Kennung vergeben wurde und der jeweilige Nutzer ein zusätzliches, individuelles Passwort eingeben muss, um die Anwendung zu starten.

5.8.6.2

Übermittlung der Gutachten per E-Mail an den MDK

Das Schreiben der Gutachten und deren sichere Speicherung auf dem Laptop ist jedoch nur ein Teil des Gesamtverfahrens. Ein anderer Aspekt, der datenschutzrechtliche Fragen beinhaltet, ist die sichere Übermittlung vom einzelnen Gutachter auf den zentralen Server des MDK in die Hauptverwaltung nach Oberursel.

Die Übergabe der Gutachten soll mit Hilfe des Abgleichs der persönlichen Notes-Mail-Datenbank über Wählleitungen von unterwegs oder vom heimischen Arbeitsplatz aus erfolgen. In dieser Datenbank sind für den Gutachter die jeweiligen Aufträge enthalten, die dieser abarbeiten soll. Um die Vermittlung technisch sicherzustellen, wurde auf die Laptops, die alle standardmäßig mit internen Modems ausgestattet sind, die hierfür notwendige Software (Lotus Notes) aufgespielt. Da alle beim MDK benutzten PC mit dieser Software arbeiten, ist die erforderliche Kompatibilität der Technik mit den beim MDK-Hessen bestehenden Notes-Systemen gewährleistet.

Hinsichtlich der Anforderungen an die Sicherheit des Verfahrens, dass technisch auf dem mit der AOK bereits seit Jahren praktizierten elektronischen Austausch von Pflegegutachten basiert, gelten die gleichen Sicherheitsstandards. Es wird dadurch sichergestellt, dass die Daten nur verschlüsselt übertragen werden.

5.8.6.3

Projekt „Sicherer E-Mail-Verkehr mit externen Gutachtern“

Bislang wurden die Gutachten, die von externen Gutachtern im Auftrag des MDK gefertigt wurden, von diesen in unregelmäßigen Abständen per Diskette der zuständigen Geschäftsstelle überbracht. Nunmehr will man sich eines elektronischen Transfers der geschriebenen Gutachten bedienen. Die Übergabe der Pflegegutachten soll mit Hilfe des Programms „OpenPGP“ oder des S/MIME-Protokolls erfolgen (vgl. 28. Tätigkeitsbericht, Ziff. 10.1 und Orientierungshilfe zum Einsatz kryptografischer Verfahren unter www.datenschutz.hessen.de). Die Weitergabe der Daten erfolgt nur von einer bestimmten Person (Absender) an eine andere festgelegte Person (Empfänger). Durch die Verwendung eines an die Person des Empfängers gebundenen privaten Schlüssels ist es unbefugten Dritten nicht möglich, die ausgetauschten Dateninhalte zu entschlüsseln und zur Kenntnis zu nehmen. Die Geschäftsführung hat mich über den Beginn der Testphase in Kenntnis gesetzt. Nach deren Abschluss sollen die Ergebnisse ausgewertet und mir zur datenschutzrechtlichen Bewertung vorgelegt werden.

5.8.6.4

Einsatz des Programms KQP II

Entsprechend den Vorgaben des § 53a SGB XI wurden für den Bereich der sozialen Pflegeversicherung gemeinsame und einheitliche Richtlinien über die von den Medizinischen Diensten zu übermittelnden Berichte und Statistiken, zur Qualitätssicherung der Begutachtung und Beratung sowie über das Verfahren zur Durchführung von Qualitätsprüfungen verbindlich festgeschrieben.

Der MDK Hessen hat, um den Richtlinien Rechnung zu tragen, vom MDK Westfalen Lippe ein Programm (KQP I) erworben und dieses modifiziert (Version KQP II). Danach erfolgt über einen Zufallsgenerator die Auswahl eines fertig gestellten Gutachtens. Die inhaltliche Bewertung des Gutachtens (Qualität, inhaltliche Konsistenz) soll durch das jeweilige Pflegeteam vor Ort erfolgen. Nach den Vorstellungen der Geschäftsführung sollte dies jedoch nicht durch eine zuvor autorisierte Person, z. B. den Teamleiter selbst, erfolgen. Vielmehr sieht eine Formulierung im Organisationshandbuch des MDK hierzu vor, dass in Form einer „Eigenregelung“ das Team den Qualitätssicherer selbst bestimmt. Dies müsste nicht die Person des Teamleiters sein. Vielmehr

könne hierfür auch ein anderes Mitglied des Teams, das etwa sechs bis acht Köpfe zählt, bestimmt werden. Die datenschutzrechtliche Brisanz besteht darin, dass die Qualitätssicherung gutachterbezogen erfolgt und die Bewertung arbeitsrechtliche Konsequenzen haben kann. Das bedeutet, dass der Qualitätssicherer die jeweils bestimmte Person sowohl den Namen des Gutachters als auch die medizinischen Inhalte der Unterlage zur Kenntnis erhält. Die Verantwortung der Qualitätskontrolle soll nach dem Willen der Geschäftsleitung künftig innerhalb der Teams als „selbst steuernde und selbst organisierende Einheiten“ erfolgen. Dies entspricht der Formulierung im Organisationshandbuch des MDK. Das gesamte Verfahren entspricht jedoch nicht datenschutzrechtlicher Transparenz, Objektivität und Nachvollziehbarkeit des Verfahrens. Es bedarf der Präzisierung, wer unter welchen Voraussetzungen mit welchen Konsequenzen personenbezogene Daten vom Gutachten und Patienten verarbeiten muss bzw. darf.

Eine gutachterbezogene Übermittlung der Qualitätskontrolle an die Hauptverwaltung erfolgt nicht. Dort werden nur die vom Qualitätssicherer geprüften Gutachten (ohne Namensbezug) eingesehen und auf ihre inhaltliche Plausibilität und Qualität hin überprüft.

Ich habe die Geschäftsleitung gebeten, das Organisations-Handbuch hinsichtlich der gutachterbezogenen Auswertung innerhalb der jeweiligen Teams zu präzisieren. Eine Antwort des MDK liegt mir noch nicht vor.

5.8.7

Datenschutzrechtliche Probleme der Auftragsdatenverarbeitung für die Erfassung von ärztlichen Gutachten des Medizinischen Dienstes der Krankenversicherung Hessen

Der MDK Hessen lässt durch ein Tochterunternehmen des MDK Sachsen-Anhalt ärztliche Gutachten schreiben. Bei einer Prüfung vor Ort musste ich feststellen, dass die mir vom MDK schriftlich dargelegten Modalitäten der Datenverarbeitung mit der Praxis nicht übereinstimmten. Insbesondere war die Verantwortung für Datenschutz und Datensicherheit nicht klar zugeordnet. Auch war ein wesentlicher Teil der in den Verträgen festgelegten Verfahrensanforderungen, nämlich die Pseudonymisierung der übermittelten Sprachdiktate, nicht umgesetzt.

5.8.7.1

Das Verfahren

Bislang wurden die von Gutachtern des MDK Hessen diktierten Gutachten von eigenen Kräften in den jeweiligen Geschäftsstellen oder aber externen Schreibbüros gefertigt. Vom Volumen her geht es dabei um etwa 100.000 Gutachten, die jährlich in den verschiedenen Bereichen (Pflege, Arbeitsunfähigkeit, Hilfsmittel, Rehabilitation u. a.) anfallen. Die Geschäftsleitung des MDK Hessen hat nun sämtliche Schreibarbeiten, die in diesem Zusammenhang anfallen, an den MDK Sachsen-Anhalt übertragen. Davon verspricht man sich eine erhebliche Verkürzung der Laufzeiten für die Erstellung eines Gutachtens. Die Diktate werden in digitaler Form als Dateianhang zu einem ISmed-Auftrag vom ISmed-System des MDK in Hessen über eine bestehende Datenleitung verschlüsselt (Lotus-Notes) zu einem separaten ISmed-Server in die Räume des MDK Sachsen-Anhalt übertragen. Dabei handelt es sich um den Server, der auch für die digitale Archivierung (s. 33. Tätigkeitsbericht, Ziff. 5.8.2) genutzt wird. Von dort werden die Sprachdiktate auf einen zweiten „hessischen“ Server in die Zentrale des MDK Sachsen-Anhalt übertragen. Dieser Server repliziert nun die Aufträge auf eine spezielle Notes-Datenbank, die auf einem weiteren Server im Serverraum der MDK-Hauptverwaltung liegt. Auf diesem so genannten Schreibpool-Server sind die Diktate sowohl aus Hessen als auch Sachsen-Anhalt zentral abgelegt. Auf diese Diktate greifen insgesamt 26 Schreibkräfte zu. Nach dem Schreiben werden die nunmehr geschriebenen Gutachten als Textdatei an den ursprünglichen ISmed-Auftrag angehängt und auf umgekehrtem Weg auf den zentralen Server des MDK Hessen in Oberursel (verschlüsselt) zurückgeschickt. Damit verbunden ist eine E-Mail an den jeweiligen Gutachter bzw. die Geschäftsstelle mit dem Hinweis, dass auf das fertig geschriebene Gutachten zugegriffen werden kann. Danach werden die Gutachten durch entsprechende Systemvorgaben gelöscht.

5.8.7.2

Vertragliche Aspekte der Auftragsdatenverarbeitung und Rechtsverhältnisse der Auftragnehmer untereinander

Bei dem vom MDK vergebenen Auftrag handelt es sich um eine Datenverarbeitung im Auftrag i. S. v. § 80 SGB X (vgl. hierzu auch Ziff. 5.8.4 sowie 33. Tätigkeitsbericht, Ziff. 5.8.2).

Der MDK Hessen hat einen Dienstleistungs- sowie einen Datenschutzvertrag mit dem MDK Sachsen-Anhalt abgeschlossen. In dem Datenschutzvertrag sind Rechte und Pflichten von

Auftragnehmer und Auftraggeber geregelt. U. a. ist festgelegt, dass sich der Auftragnehmer, also der MDK Sachsen-Anhalt, eines Unterauftragnehmers bedient. Eine solche Möglichkeit räumt der § 80 Abs. 2 Satz 2 SGB X einem Auftragnehmer ausdrücklich ein. Bei diesem Unterauftragnehmer handelt es sich um die MedFlex GmbH, die eine hundertprozentige Tochter des MDK Sachsen-Anhalt ist. Die MedFlex GmbH, die sich personell aus ehemaligen Mitarbeitern des MDK Sachsen-Anhalt rekrutiert, ver- bzw. bearbeitet die Daten (also die digitalen Sprachdiktate) im Auftrag der Mutter (also des MDK Sachsen-Anhalt). Bei meiner Prüfung musste ich feststellen, dass die in den Verträgen festgelegte klare Zuordnung der Verantwortlichkeiten in der Praxis nicht umgesetzt war. Ich habe vor Ort eine personelle, organisatorische und technische Verquickung der rechtlich getrennten Institutionen MDK Sachsen-Anhalt und MedFlex GmbH vorgefunden. So erfolgt die technische Betreuung des Verfahrens, dessen Administrierung sowie das Krisenmanagement der MedFlex GmbH durch den Systemadministrator des dortigen MDK. Der Server der MedFlex GmbH stand zusammen mit dem technischen Equipment des MDK Sachsen-Anhalt in einem Raum. Die Geschäftsführung residierte ebenso in den Räumen des MDK wie die Schreibkräfte, die in einzelnen Geschäftsstellen untergebracht waren. Die technische Ausstattung war vom dortigen MDK angemietet.

Auf Grund dieser Konstellation ist keine nachvollziehbare Zuordnung bezüglich der Verantwortung für Datenschutz und Datensicherheit vorhanden. Denn für die Sicherheit des Verfahrens z. B. muss der Unterauftragnehmer in Haftung genommen werden können. Technisch basiert dies aber auf der Grundlage des Handelns des Systemadministrators des MDK Sachsen-Anhalt.

5.8.7.3

Vertraglich vorgesehene Pseudonymisierung findet nicht statt

In dem zwischen dem MDK Hessen und dem MDK Sachsen-Anhalt geschlossenen Datenschutzvertrag war eine Pseudonymisierung der Gutachten ausdrücklich vereinbart. Hierzu heißt es in § 2 Abs. 7 des Vertrages: „Die Diktate erfolgen ohne Nennung des Namens, des Geburtsdatums und der Adresse des Versicherten, um die Möglichkeit der Identifizierung des Patienten bzw. Versicherten auszuschließen. Die Gutachten, die beim MDK in Hessen extern

bearbeitet und elektronisch versandt werden, werden mit einem Schlüssel an Stelle des Namens versehen.“

Mit Schreiben vom 22. September 2005 hatte mir der Geschäftsführer des MDK Hessen dies nochmals ausdrücklich bestätigt und die einzelnen Verfahrensschritte beschrieben.

Bei meiner Prüfung musste ich feststellen, dass eine Pseudonymisierung, wie vertraglich geregelt und in dem Brief beschrieben, nicht stattfand. Durchaus nachvollziehbare technische und organisatorische Probleme haben eine Realisierung nicht möglich gemacht. Allerdings ist es nicht akzeptabel, dass mir der Sachverhalt unzutreffend dargelegt wurde und ich erst vor Ort und im Rahmen meiner Überprüfung von diesem wesentlichen Umstand Kenntnis erlangt habe. Nur vier Wochen vor der Prüfung erhielt ich den Brief des Geschäftsführers des MDK Hessen, in dem dieser mir Vorgänge (der Pseudonymisierung) beschrieb, die tatsächlich nie realisiert wurden.

5.8.7.4

Bewertung des Verfahrens und datenschutzrechtliche Defizite

Das Verfahren selbst erscheint mir den erforderlichen Ansprüchen an Datenschutz und Datensicherheit zu entsprechen. Problematisch sind jedoch die Aspekte der nicht erfolgten Pseudonymisierung sowie der technischen, organisatorischen und personellen Vermengung von Zuständigkeiten des MDK Sachsen-Anhalt und der MedFlex GmbH. Bezüglich der fehlenden Pseudonymisierung erscheinen mir die Argumente des MDK Hessen, wonach der zu betreibende Aufwand unverhältnismäßig zu den erzielten Schutzmaßnahmen ist, schlüssig zu sein. Das Sozialgesetzbuch schließt im Rahmen einer Auftragsdatenverarbeitung die Kenntnisnahme von personenbezogenen Sozialdaten durch den Auftragnehmer auch nicht aus. Nicht akzeptabel ist jedoch, dass ich erst im Rahmen meiner Prüfung vor Ort von dem Verzicht auf die Pseudonymisierung Kenntnis erlangt habe. Hinzu kommt, dass der geschlossene Datenschutzvertrag die Pseudonymisierung als rechtlichen Bestandteil der Datenverarbeitung explizit beinhaltet.

Das Rechtsverhältnis zwischen MDK Sachsen-Anhalt und der MedFlex GmbH sowie die Aufgabenverteilung, Nutzung der technischen Ressourcen, Einsatz des Personals etc. ist für eine ordnungsgemäße Datenverarbeitung so nicht darstellbar. Eine Veränderung der Strukturen erscheint mir deshalb unumgänglich zu sein.

5.8.7.5

Konsequenzen

Der MDK Hessen hat mich in verschiedenen Punkten nicht über die tatsächlichen Verhältnisse informiert. Ich habe den MDK aufgefordert, hierzu Stellung zu nehmen. Darüber hinaus habe ich dem MDK mitgeteilt, dass eine nachvollziehbare räumliche, personelle und organisatorische Trennung zwischen Auftragnehmer (MDK Sachsen-Anhalt) und Unterauftragnehmer (MedFlex GmbH) unerlässlich ist. Eine klare Zuordnung der Verantwortlichkeit ist Voraussetzung für die weitere Fortsetzung der Auftragsdatenverarbeitung.

Ich habe dies dem Geschäftsführer des MDK in einem Schreiben deutlich gemacht und das Sozialministerium hierüber informiert. Unabhängig hiervon behalte ich mir auch künftig vor, kurzfristig und unangemeldet den Datenverarbeiter, also die MedFlex GmbH, aufzusuchen, um die Einhaltung der Vorgaben zu einem angemessenen Schutz der Sozialdaten zu überprüfen.

5.9 Sozialwesen

5.9.1

Hartz IV – Vorlage von Kontoauszügen

Das behördliche Verlangen, Kontoauszüge der letzten drei bis sechs Monate vorzulegen, ist als bisher auch schon im Sozialhilferecht übliche Standardmaßnahme bei der Entscheidung über die Gewährung von Arbeitslosengeld II zulässig.

Fast alle Eingaben von Bürgerinnen und Bürgern betreffend Hartz IV (SGB II) betrafen die Frage, ob sie verpflichtet sind, die Kontoauszüge der letzten drei bis sechs Monate vorzulegen.

Die Mitwirkungsobliegenheiten im Sozialrecht sind vor allem in den §§ 60 ff. SGB I geregelt. Was die Vorlage von Kontoauszügen betrifft, ist insbesondere § 60 SGB I von Bedeutung.

§ 60 Abs. 1 SGB I

Wer Sozialleistungen beantragt oder erhält hat

1. alle Tatsachen anzugeben, die für die Leistung erheblich sind, ...
3. Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen ...

Kontoauszüge sind Beweisurkunden im Sinne dieser Vorschrift, deren Vorlage die Behörde verlangen kann. Deren Überprüfung dient der Aufklärung der finanziellen Verhältnisse, da die Einkommens- und Vermögensverhältnisse bei der Entscheidung über die Gewährung von Arbeitslosengeld II zu berücksichtigen sind (§§ 11, 12 SGB II).

Zu Recht hat beispielsweise jüngst das Sozialgericht München ausdrücklich darauf hingewiesen, dass für die Feststellung, inwieweit Einkommen und Vermögen vorhanden sind, der letzte Kontoauszug nicht genügt, da die Kontenbewegungen der letzten Monate zur vollständigen Ermittlung von Einkommen und Vermögen erforderlich sind (Beschluss vom 9. September 2005, Az. S 50 AS 472/05 ER). Aus zurückliegenden Kontenbewegungen wird z. B. ersichtlich, ob und inwieweit Zuwendungen Dritter geflossen sind, größere Beträge transferiert und sonstige leistungserhebliche Transaktionen vorgenommen wurden (etwa Beiträge zu einer Kapitallebensversicherung).

Vor diesem Hintergrund ist auch eine Entscheidung des Hessischen Landessozialgerichts (Beschluss vom 22. August 2005, Az. L 7 AS 32/05 ER) abzulehnen, in der das Gericht das Verlangen nach den Kontoauszügen der letzten Monate anders als das Sozialgericht Frankfurt in der ersten Instanz für rechtswidrig hält. Freilich ist dem Landessozialgericht beizupflichten, dass die Erhebung von Daten nicht „im Belieben der Verwaltung“ steht, aber bei der Frage der Erforderlichkeit einer Datenerhebung hat die Verwaltung einen gewissen Beurteilungsspielraum (vgl. auch Voelzke in Hauck/Noftz, SGB II § 50 Rdnr. 9 m. w. N.), der bei dem Verlangen nach Kontoauszügen der letzten Monate sicher nicht überschritten wird. Völlig zu Recht hat sich dann auch das Sozialgericht München im oben erwähnten, nach der Entscheidung des Landessozialgerichts getroffenen Beschluss ausdrücklich gegen die Rechtsansicht des Landessozialgerichts Darmstadt ausgesprochen, und diese Ansicht des Landessozialgerichts steht auch im Widerspruch zur überwiegenden Auffassung der Datenschutzbeauftragten des Bundes und der Länder, die das Verlangen nach Kontoauszügen im Bereich des SGB II und auch des SGB XII (Sozialhilfe) prinzipiell für zulässig hält.

Es ist auch zulässig, Kopien der Kontoauszüge zu den Akten zu nehmen, um beispielsweise die korrekte Sachbearbeitung jederzeit nachprüfen zu können (vgl. auch Voelzke in Hauck/Noftz, SGB II § 60 Rdnr. 44).

Allerdings ist es ein datenschutzrechtlich berechtigtes Anliegen von Antragstellerinnen und Antragstellern, dass nach Überprüfung der Kontoauszüge nicht relevante Angaben ggf. geschwärzt werden. Denn die vom Sozialgericht München in besagtem Beschluss geäußerten Bedenken, dass bei Vorlage geschwärzter Kontoauszüge ein Verdacht auf beabsichtigten Leistungsmissbrauch nahe liege, bestehen nach Überprüfung der ungeschwärzten Kontoauszüge nicht mehr.

Ich habe die Eingeberrinnen und Eingebere über die beschriebene Rechtslage informiert.

5.9.2

Unzulässiger Inhalt von Wohngeld-Antragsformularen

Es ist unzulässig, bei der Entscheidung über einen Antrag auf Gewährung von Wohngeld Angaben zu verlangen, deren Erhebung vom Wohngeldgesetz nicht gedeckt ist.

Ein Bürger beschwerte sich mit seiner Eingabe darüber, dass er neben seinem Antrag auf Gewährung von Wohngeld eine formularmäßige „Ergänzende Erklärung“ ausfüllen sollte, die die durchschnittlich monatlich aufgewandten Beträge für den Lebensunterhalt des Antragstellers und der zu seinem Haushalt gehörenden Personen betraf. In dem Formular wurden Beträge für Ernährung, persönliche Dinge des täglichen Lebens, Neuanschaffung von Bekleidung und vieles andere mehr erfragt. Der Antragsteller wurde zugleich darauf hingewiesen, dass er kein Wohngeld erhalte, falls die ergänzende Erklärung nicht ausgefüllt werde.

Wird Wohngeld beantragt, besteht für die Antragsteller eine sozialrechtliche Mitwirkungspflicht (§ 60 SGB I). Damit verbunden ist die Obliegenheit, der Wohngeldstelle Auskunft über die Einnahmen und über andere für das Wohngeld maßgebende Umstände zu geben (§ 25 Abs. 1 WoGG). Vor diesem Hintergrund ist es unzulässig, vom Antragsteller Informationen zu verlangen, die weder Einnahmen noch für das Wohngeld maßgebende Umstände betreffen. Es ist

beispielsweise unerheblich, welche Beträge speziell für Ernährung, für persönliche Dinge des täglichen Lebens und die Neuanschaffung von Bekleidung aufgewandt werden. Diese Thematik habe ich bereits in meinem 22. Tätigkeitsbericht, der freilich schon zwölf Jahre zurückliegt, ausführlich dargelegt (Ziff. 11.2). Der Hinweis der Wohngeldstelle, ihr sei der Vordruck während eines Seminars des Kommunalen Bildungswerkes e. V. in Berlin im Jahr 2002 übergeben worden und sie habe daher keinen Grund gesehen, an der datenschutzrechtlichen Zulässigkeit des Vordrucks zu zweifeln, ist sicher nachvollziehbar. Bloß wird in dem verteilten Vordruck am Ende betont, dass die Angaben „freiwillig“ sind, also eben nicht der Mitwirkungspflicht unterliegen. Genau hiergegen hat aber die Wohngeldstelle verstoßen. Offenbar hat sich diese unzulässige Praxis, wie die Wohngeldstelle angedeutet hat, bei den Wohngeldstellen auch anderer Kommunen wieder eingeschlichen, sodass ein erneuter Hinweis auf die Rechtslage erforderlich ist.

Die Wohngeldstelle des Landkreises, über die sich der Antragsteller beschwert hatte, hat zugesagt, das Formular „Ergänzende Erklärung“ nicht mehr zu verwenden; dies habe ich dem Eingebener mitgeteilt.

5.9.3

Datenschutzrechtliche Rahmenbedingungen im Bereich der Jugendgerichtshilfe

Das Jugendamt – Jugendgerichtshilfe – ist verpflichtet, bei seiner Tätigkeit im Jugendstrafverfahren auf die Mitwirkung des Jugendlichen zu achten.

Ein Jugendamt hat angefragt, inwieweit datenschutzrechtliche Vorgaben bei der Mitwirkung im Jugendstrafverfahren zu beachten sind.

Datenschutzrechtlicher Ausgangspunkt ist § 61 Abs. 3 SGB VIII (Kinder- und Jugendhilfe), der bestimmt, dass für die Erhebung, Verarbeitung und Nutzung von Sozialdaten durch das Jugendamt bei der Mitwirkung im Jugendstrafverfahren die Vorschriften des Jugendgerichtsgesetzes maßgebend sind. Das hat zur Konsequenz, dass insoweit also weder der allgemeine Sozialdatenschutz (§§ 67 ff. SGB X) noch das bereichsspezifische Sozialdatenschutzrecht gemäß dem Kinder- und Jugendhilferecht (§§ 61 ff. SGB VIII) anwendbar sind.

Für das Jugendamt gelten bei seiner Tätigkeit im Jugendstrafverfahren in erster Linie die §§ 38 und 43 JGG.

§ 38 Abs. 2 JGG

Die Vertreter der Jugendgerichtshilfe bringen die erzieherischen, sozialen und fürsorgerischen Gesichtspunkte im Verfahren vor den Jugendgerichten zur Geltung. Sie unterstützen zu diesem Zweck die beteiligten Behörden durch Erforschung der Persönlichkeit, der Entwicklung und der Umwelt des Beschuldigten und äußern sich zu den Maßnahmen, die zu ergreifen sind. ...

§ 43 Abs. 1 JGG

Nach Einleitung des Verfahrens sollen sobald wie möglich die Lebens- und Familienverhältnisse, der Werdegang, das bisherige Verhalten des Beschuldigten und alle übrigen Umstände ermittelt werden, die zur Beurteilung seiner seelischen, geistigen und charakterlichen Eigenart dienen können. Der Erziehungsberechtigte und der gesetzliche Vertreter, die Schule und der Auszubildende sollen, soweit möglich, gehört werden. Die Anhörung der Schule oder des Auszubildenden unterbleibt, wenn der Jugendliche davon unerwünschte Nachteile, namentlich den Verlust seines Ausbildungs- oder Arbeitsplatzes, zu besorgen hätte.

Nach ihrem Wortlaut sehen diese Regelungen Datenerhebung, Verarbeitung und Nutzung auch ohne Mitwirkung der betroffenen Jugendlichen vor. Wegen deren aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG abgeleiteten Rechts auf informationelle Selbstbestimmung ist das Jugendamt bei seiner Tätigkeit im Jugendstrafverfahren aber verpflichtet, den Jugendlichen jedenfalls in der Regel die Mitwirkung zu ermöglichen, soweit es um ihre personenbezogenen Daten geht. In diesem Sinne sind die Jugendämter zu einer verfassungskonformen Anwendung der §§ 38, 43 JGG verpflichtet. So sind etwa Datenerhebungen bei Dritten sowie Datenübermittlungen an Dritte ohne die Einwilligung der Betroffenen nur ausnahmsweise zulässig.

In diesem Sinne habe ich das Jugendamt über eine datenschutzorientierte Anwendung des Jugendgerichtsgesetzes unterrichtet.

In der Folgezeit ist § 61 Abs. 3 SGB VIII und damit der Verweis auf §§ 38 und 43 JGG durch das Gesetz zur Weiterentwicklung der Kinder- und Jugendhilfe mit Wirkung zum 1. Oktober 2005 aufgehoben worden. Dies hat zur Folge, dass nunmehr das Sozialdatenschutzrecht des Kinder- und Jugendhilfegesetzes, §§ 61 ff. SGB VIII, auch für die Jugendgerichtshilfe gilt.

Datenschutzrechtlich ist das eine Verbesserung. So ist nunmehr gesetzlich geregelt, dass etwa die Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen nur zulässig ist, wenn die Erhebung beim Betroffenen nicht möglich ist oder die jeweilige Aufgabe ihrer Art nach eine Erhebung bei anderen erfordert, die Kenntnis aber erforderlich ist für die Wahrnehmung der Aufgaben der Jugendgerichtshilfe (§§ 52, 62 Abs. 3 Nr. 2 c) SGB VIII).

5.10 Personalwesen

5.10.1

E-Beihilfe

Die Einführung der digitalen Beihilfebearbeitung (E-Beihilfe) lässt sich mit datenschutzrechtlichen Vorgaben in Einklang bringen.

Die Hessische Landesregierung möchte die Beihilfeverwaltung durch den Einsatz moderner Informationstechnologie, durch Zentralisierung, Organisationsoptimierung und durch Anpassung des hessischen Beihilferechts effizienter gestalten. E-Beihilfe bezeichnet das Konzept und das Verfahren für die elektronische Bearbeitung von Beihilfeanträgen. Hierfür hat das Regierungspräsidium Kassel eine zentrale Verwaltungseinheit aufgebaut, die optimal auf die Aufgabenstellung zugeschnitten werden soll.

Der Ablauf ist wie folgt geplant:

- Im Posteingang werden die Eingänge zum Scannen vorbereitet. Neue Scantechnik und Texterkennungssoftware sorgen für die Erfassung aller eingehenden Dokumente.
- Das System klassifiziert die Antragsunterlagen (Antragsformular, Arztrechnungen, Rezepte, etc.), erkennt die Daten und leitet sie weiter. Beim anschließenden maschinellen

- Datenabgleich mit Regeln und Informationen aus Datenbanken werden Abweichungen automatisch gemeldet. Unklare und nicht erkannte Daten werden manuell ergänzt.
- Sämtliche Vorgänge werden vollständig durch das System verwaltet. Es besteht aus einer Integration des weiterentwickelten Fachanwendungsprogramms „Elba“ mit dem Dokumentenmanagementsystem DOMEA.
 - Die Erteilung des Beihilfebescheides und die Auszahlungen erfolgen automatisch nach Prüfung und Freigabe durch die Sachbearbeiter, ebenso wie der Druck und Versand der Beihilfebescheide über eine zentrale Druckstraße in Wiesbaden.
 - Kundenanfragen sollen im neuen Kundenzentrum beantwortet werden.

Das Projekt, in der Hessischen Landesverwaltung die E-Beihilfe einzuführen, begann im Frühjahr 2004. In die Gespräche war ich von Anfang an einbezogen, um das Projekt aus der Sicht des Datenschutzes beratend zu begleiten. Das Projekt ist datenschutzrechtlich brisant, weil es um sensible Daten von Landesbediensteten geht.

Das im HBG geregelte Personalaktenrecht lässt die automatisierte Verarbeitung von Beihilfedaten (§ 107a HBG) zu, nämlich in § 107g Abs. 2 HBG.

§ 107g Abs. 2 HBG

Personalaktendaten im Sinne von § 107a dürfen automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet und genutzt werden.

Das für die datenschutzrechtliche Bewertung der E-Beihilfe erforderliche Verfahrenverzeichnis (§ 6 HDSG), insbesondere die Vorabkontrolle (§ 6 Abs. 1 Nr. 11 HDSG), wurde mir im Dezember 2004 vorgelegt.

5.10.1.1

Die Vorabkontrolle

Die Bewertung aus Datenschutzsicht stützt sich auf die Vorabkontrolle einschließlich der Befassung mit dem Entwicklungssystem in Kassel und einer Überprüfung des Rechenzentrums der HZD in Hünfeld.

Die elektronische Erfassung und Speicherung der Anträge als solche stellen eine organisatorische Änderung der bisherigen Arbeitsweise und die Bereitstellung eines neuen Arbeitsmittels dar, die über die bisherige nur teilweise elektronische Beihilfebearbeitung (Elba-Verfahren) hinausgehen.

Mit der Einführung der E-Beihilfe ändert sich im Wesentlichen Folgendes:

- Der Antragsteller fügt seinem Antrag keine Originale, sondern nur noch Kopien von Rechnungen und Rezepten bei. Diese Kopien werden in elektronische Dokumente überführt und das Papier vernichtet. Diese elektronischen Dokumente werden zur Bearbeitung zeitlich begrenzt gespeichert (zehn Wochen). Im Übrigen gelten die gesetzlichen Speicherfristen.
- Gleichzeitig mit der Einführung des neuen Verfahrens wird die Verarbeitung von 16 dezentralen Beihilfestellen auf eine zentrale Beihilfestelle konzentriert. Dies erfolgt schrittweise nach einem Migrationsplan.

Als Vorteile werden eine schnellere Bearbeitung, geringere Kosten, geringere Betrugsmöglichkeiten durch zentrale Speicherung aller Beihilfeanträge und nunmehr eine völlig strikte Trennung von Beihilfe- und Personalsachbearbeitung angeführt. Der Verfügbarkeit, Integrität und Vertraulichkeit der Daten wird in der Vorabkontrolle Rechnung getragen, insbesondere ist die Übertragungsverschlüsselung (Server/Client) vorgesehen.

5.10.1.2

Umsetzung der Datenschutzmaßnahmen

Im Januar 2005 begann der Probetrieb nur mit der Buchstabengruppe K und L der Beihilfestelle Kassel.

Die Umsetzung der in der Vorabkontrolle angeführten Maßnahmen zur Datensicherheit (Verfügbarkeit, Integrität und Vertraulichkeit der Daten) wurde von mir fortlaufend im Jahr 2005 kontrolliert.

Die erste Prüfung fand Anfang März 2005 statt.

Bei dieser Überprüfung musste ich erhebliche Unterschiede zwischen dem Konzept und der Umsetzung feststellen und wurde mit neuen datenschutzrechtlichen Fragestellungen konfrontiert.

Die wichtigsten Punkte werden im Folgenden aufgelistet:

1. In dem Verfahrensverzeichnis wurde auf ein zu erstellendes Infrastrukturpapier zur Datensicherheit verwiesen. Dieses war noch nicht fertig gestellt.
2. In dem Verfahrensverzeichnis wurde auf das immer noch in Arbeit befindliche BSI-konforme Grundschutzkonzept der HZD Bezug genommen. Dieses lag noch nicht vor.
3. Die organisatorischen Maßnahmen, die die Arbeit der Administratoren vor Ort beschreiben, waren weder abschließend festgeschrieben noch umgesetzt.
4. Das Programm befand sich in einem Teststadium und war noch nicht fertig entwickelt. Neben zahlreichen Programmfehlern (Bugs) waren auch wichtige Funktionen (Löschen der Images nach zehn Wochen, korrekte Bearbeiterangabe, korrekte Sachmittelzuweisung etc.) noch nicht verfügbar.
5. Das Entwicklungssystem enthielt eine Kopie der Echtdaten und befand sich in Kassel in einem unzureichend geschützten Bereich, statt wie aus Gründen der deutlich höheren Datensicherheit geboten in der HZD Hünfeld.
6. Die Verfügbarkeit des Systems war zu diesem Zeitpunkt nicht sichergestellt.

Daraufhin setzte ich dem Projektteam eine Frist von sechs Wochen, um die wesentlichen Mängel abzustellen. Für den Umzug des Entwicklungssystems nach Hünfeld wurde eine Frist bis zum Juli 2005 vereinbart. Gleichzeitig teilte ich mit, dass ich der geplanten Ausweitung des Verfahrens auf weitere Buchstabenbereiche angesichts dieser gravierenden Mängel widersprechen müsse.

Bei der zweiten Überprüfung Anfang Mai 2005 waren die Mängel, insbesondere zu den Ziffern

3. Administrationskonzept
4. Programmfehler (mit Ausnahme der endgültigen Löschung von Belegen)

5. Räumliche Sicherungsmaßnahmen
6. Verfügbarkeit des Systems

abgestellt. Deshalb habe ich dem Wunsch der Projektleitung entsprochen und einer Migration weiterer Buchstabenbereiche zugestimmt.

Die mir bei diesem Besuch vorgelegten Konzepte

- IT-Sicherheitskonzept für den Teilverbund „E-Beihilfe“ der HZD (aktualisiert)
 - Administrationskonzept
 - Benutzungsvereinbarung Betrieb E-Beihilfe des Hessischen Innenministeriums mit der HZD
- waren Grundlage für einen weiteren Prüfbesuch im Juli 2005. Die sich aus den Konzepten ergebenden Fragen wurden mit den Projektmitarbeitern direkt vor Ort besprochen. Zu diesem Zeitpunkt wurden die Löschfunktionen konsequent eingesetzt, und ich erhielt das überarbeitete Verfahrenverzeichnis.

Ungeachtet dessen waren folgende datenschutzrechtliche Aspekte nach der dritten Überprüfung im Juli 2005 noch nicht abschließend geklärt:

- Das IT-Sicherheitskonzept für den Teilverbund „E-Beihilfe“ der HZD war fortgeschrieben worden, enthielt aber noch offene Punkte. Das Konzept wird bis zur vollständigen Migration aller Beihilfestellen kontinuierlich fortgeschrieben werden.
- Das Administrationskonzept befindet sich in der Überarbeitung.
Die Benutzungsvereinbarung Betrieb E-Beihilfe befindet sich in der Endabstimmung.
- Das Entwicklungssystem befand sich immer noch in Kassel. Die vereinbarte Frist für diesen Umzug nach Hünfeld war Ende Juli 2005 abgelaufen. Die Projektleitung informierte mich, dass der Umzug aus technischen und organisatorischen Gründen noch nicht möglich war. Allen Beteiligten war klar, dass aus Gründen der Datensicherheit auf Dauer die Entwicklung nicht in Kassel bleiben kann.
- Der Serverraum wurde zwischenzeitlich sowohl mit einer Sicherheitstür als auch einem Zutrittskontrollsystem gesichert. Für die weitere Entwicklung in Kassel wurde daher eine Übergangsfrist bis Ende Juni 2006 zugesagt.

Für einige Punkte war eine Frist bis Mitte September 2005 gesetzt. Da die ausstehenden Unterlagen mir termingerecht vorlagen und keinen Anlass zu datenschutzrechtlicher Kritik boten, hatte ich keine datenschutzrechtlichen Bedenken gegen eine weitere Migration der Beihilfestellen Darmstadt, Gießen, Hünfeld und Michelstadt.

5.10.1.3

Nutzung durch Dritte

Neu ist die geplante Inanspruchnahme des E-Beihilfe-Verfahrens durch Dritte. Interesse haben die Beamtenversorgungskassen (BVK) Kassel und Darmstadt sowie der Städte Frankfurt und Darmstadt bekundet.

Es bestehen gegen die Systemnutzung durch andere öffentliche Stellen des Landes Hessen grundsätzlich keine rechtlichen Bedenken, da dies durch § 92 Abs. 3 HBG abgedeckt ist. Wichtig dabei ist die Frage der Ausgestaltung der Nutzung. Insbesondere muss sichergestellt sein, dass die Datenbestände externer öffentlicher Stellen bei der Systemnutzung hinreichend abgeschottet sind. Das Regierungspräsidium Kassel müsste über die Aufgabenregelung und Ausgestaltung einen Vertrag mit den Dritten schließen. Der Dritte selbst z. B. die BVK muss ein eigenes Verzeichnis erstellen und mir vorlegen.

Für das weitere Vorgehen wurde vereinbart, dass beabsichtigte Systemnutzungen durch Dritte mir vor Vertragsabschluss angezeigt und Konzepte mit Beschreibung der Art und Weise der Anbindung vorgelegt werden.

5.10.1.4

Ausblick

Die Option, Beihilfeanträge elektronisch abzusenden, kann heute technisch noch nicht realisiert werden, da die virtuelle Poststelle im Land Hessen noch nicht vorhanden ist. Langfristig ist dies aber geplant. Hierfür sind bereits sinnvolle technische Lösungen angedacht, und die verschlüsselte Kommunikation ist in der neuen Beihilfeverordnung (§ 17 Abs. 1a HBeihVO) schon ausdrücklich vorgesehen.

Der nächste Informationsbesuch ist für Januar 2006 vorgesehen.

5.10.2

Datenschutzrechtliche Begleitung der Einführung der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung

Bei den Arbeiten für die Einführung der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung war ich sowohl bei den entwickelten Konzepten für den Einsatz als auch in Einzelfragen der Anpassung der Software auf die Anforderungen der hessischen Landesverwaltung beteiligt. Dabei war eine Vielzahl komplexer datenschutzrechtlicher Fragestellungen zu lösen. Auch künftig wird die Prüfung und Beratung in diesem Bereich einen Schwerpunkt meiner Tätigkeit bilden.

Die Einführung der Personalverwaltungssoftware SAP R/3 HR in der hessischen Landesverwaltung ist komplex und mit einem erheblichen Aufwand verbunden. Die große Zahl der Konzepte, die im Rahmen der „Neuen Verwaltungssteuerung“ und für die neu einzuführende und an vielen Stellen auf die hessische Landesverwaltung anzupassende SAP-Software erstellt wurden, konnten von mir nur im Rahmen der zur Verfügung stehenden personellen Ressourcen geprüft und datenschutzrechtlich bewertet werden. Die aus meinen Prüfungen und der Mitarbeit in den Gremien resultierenden datenschutzrechtlichen Hinweise und Forderungen wurden, soweit ich dies auf Grund der Vielfalt der Probleme und Fragestellungen abschließend beurteilen kann, regelmäßig beachtet und sowohl in die Konzepte als auch in die jeweiligen Programmversionen eingearbeitet.

Bei der Erstellung des Berechtigungskonzepts war ich von Anfang an inhaltlich beteiligt.

Natürlich habe ich während der Entwicklungsphase und des Einsatzes des SAP-Systems Fehler festgestellt, von denen ich nur die wichtigsten beispielhaft beschreibe.

5.10.2.1

Personaldaten im landesweiten Zugriff

Ich wurde darauf aufmerksam, dass bei bestimmten Konstellationen Personaldaten auch von Dienststellen aufgerufen werden konnten, bei denen dieses Personal nicht beschäftigt war. Bei richtiger Eingrenzung der Zugriffsberechtigungen hätte ein Zugriff nicht möglich sein dürfen. Umfangreiche Überprüfungen ergaben, dass es sich um einen konzeptionellen Fehler handelte. Durch die im System hinterlegten Zugriffsberechtigungen soll sichergestellt werden, dass nur die Personal führenden Dienststellen auf die Daten der bei ihnen beschäftigten Personen zugreifen können. Dies wird über die jeweilige Dienststellennummer bzw. über die organisatorische Zuordnung (strukturelle Berechtigung) einer Planstelle zu einer Dienststelle gesteuert. In Fällen der Versetzung von Bediensteten wurden die Daten der Betroffenen auf einer so genannten „Dummstelle“ gespeichert, auf die alle Dienststellen Zugriff hatten. Dies war nach Auffassung der Entwickler notwendig, weil die aufnehmende Dienststelle ansonsten keinen Zugriff auf den Datensatz haben konnte, um diesen in ihren Bestand aufzunehmen.

Meine datenschutzrechtlichen Einwände gegen diese Verfahrensweise führten dazu, dass der „Fehler“ zunächst analysiert wurde. Es wurde eine zweite Fehlerquelle festgestellt, nämlich wenn z. B. eine Planstelle gelöscht wurde, diese aber noch mit einem Personaldatensatz verknüpft war. In diesen Fällen wurden die Personaldaten automatisch durch das System mit der „Dummstelle“ verknüpft, was auch dazu führte, dass sie im landesweiten Zugriff waren.

Die von den Entwicklern zunächst vorgeschlagenen Lösungen waren alle datenschutzrechtlich nicht zufrieden stellend. Inzwischen wurden die Berechtigungen für den Zugriff auf diese „Dummstelle“ im System so hinterlegt, dass ein Zugriff nur noch für ganz bestimmte Mitarbeiterinnen und Mitarbeiter des Hessischen Competence Centers (HCC) möglich ist, die die Datensätze auf Anforderung der jeweils zuständigen Personal führenden Dienststellen von der „Dummstelle“ in deren Zugriff stellen. Ein landesweiter Zugriff bei diesen Fallkonstellationen ist zukünftig ausgeschlossen.

5.10.2.2

Nicht genutzte Berechtigungen (inaktive User)

Im Rahmen einer Prüfung des Systems habe ich festgestellt, dass eine nicht unerhebliche Anzahl von Personen (1022) mit Zugangsberechtigung für das SAP-System (Usern) seit mehr als 90 Tagen das System nicht genutzt hatten, also inaktiv waren. Als Gründe hierfür kamen in Betracht: Lange Krankheitszeiten bzw. Langzeitabwesenheiten, User mussten nur im Vertretungsfall aktiv werden und dieser Fall war lange nicht eingetreten, User waren versetzt worden, ausgeschieden, bzw. ihnen war inzwischen eine andere Aufgabe übertragen worden, die den Zugang zum System nicht mehr notwendig machte.

Der entsprechende Hinweis an die Gesamtprojektleitung wurde dort zwar aufgenommen, führte aber nicht dazu, dass entsprechende Maßnahmen kurzfristig ergriffen wurden.

Daraufhin habe ich ca. 100 User telefonisch nach den Gründen für ihre Inaktivität am SAP-System befragt. Sie gaben als Gründe an: Zwischenzeitliche Versetzungen, Übernahme neuer Aufgaben innerhalb der Dienststelle, Langzeiterkrankungen mit der großen Wahrscheinlichkeit der Pensionierung oder, dass ihnen nicht bekannt war, dass sie einen Zugang zum System hatten.

Zugriff auf personenbezogene Daten darf nur Personen eingeräumt werden, wenn und soweit dieser für die übertragene Aufgabe erforderlich ist (§ 11 HDSG). Gerade mit Berechtigungen für den Zugriff auf Personaldaten ist besonders sorgfältig umzugehen. Ich habe mich deshalb erneut an die Gesamtprojektleitung gewandt und gefordert, alle User, die länger als 90 Tage inaktiv waren zunächst einmal zu sperren. Die Gesamtprojektleitung ist – nachdem sie alle User über die beabsichtigte Maßnahme informiert hat – dieser Forderung nachgekommen.

Zukünftig muss durch geeignete Maßnahmen sichergestellt werden, dass User, die eine andere Aufgabe übernehmen bzw. zu einer anderen Dienststelle wechseln oder aus dem Dienst ausscheiden, sofort als Zugangsberechtigte aus der Berechtigungsdatei gelöscht werden.

5.10.2.3

Standardsuchhilfe

Im Rahmen einer Prüfung „vor Ort“ habe ich festgestellt, dass es Zugriffsberechtigten, die das Veranstaltungsmanagement bearbeiten, das zur Organisation von zentralen Fortbildungsmaßnahmen für die Fortbildung der Landesbediensteten genutzt wird, möglich war,

auf den gesamten Personaldatenbestand der Landesverwaltung zuzugreifen. Es werden unter anderem die Teilnehmerdaten verarbeitet. Dies erfolgt unter direktem Zugriff auf die in SAP HR gespeicherten Personaldaten. Dieses Problem war um so schwerwiegender zu bewerten, als auch die Daten des Personals der „sicherheitsrelevanten Bereiche“ der Landesverwaltung, wie z. B. der Polizei, des Landeskriminalamtes und des Landsamtes für Verfassungsschutz im allgemeinen Zugriff des Veranstaltungsmanagements waren.

Ich habe zusammen mit Vertreterinnen und Vertretern der genannten Bereiche die Angelegenheit analysiert und entsprechende Forderungen zur Behebung dieses Missstandes gestellt.

Inzwischen ist die so genannte „Standardsuchhilfe“ des SAP-Systems für das Veranstaltungsmanagement abgeschaltet und durch eine entsprechende „Suchmaske“ ersetzt worden. Dadurch wird sichergestellt, dass nur Datensätze einzelner, für konkrete Veranstaltungen angemeldeter Personen, aufgerufen werden können.

5.10.2.4

Zugriff auf Personaldaten von Bediensteten nachgeordneter Behörden

Die Ressorts der Hessischen Landesregierung haben die Zuständigkeiten für das Personal sehr unterschiedlich geregelt. So ist ein Ressort als Personal führende Stelle für alle Personalfälle im nachgeordneten Bereich ab der Besoldungsstufe A 15 zuständig während andere Ressorts ab A 13 oder A 14 bzw. ab BAT I oder BAT II zuständig sind. Einzelne Ressorts machen die Zuständigkeiten nicht nur an der Besoldungsstufe oder an der BAT-Einstufung fest, sondern an Funktionen wie z. B. Dienststellenleitung. Weiterhin sind die Zuständigkeiten für die Genehmigungen bestimmter Personalmaßnahmen wie z. B. Gewährung von Urlaub nach § 85a HBG sehr unterschiedlich geregelt.

Diese unterschiedlichen Festlegungen in den Zugriffsberechtigungen im SAP-System abzubilden ist faktisch unmöglich.

Ich habe anlässlich einer Überprüfung der Zugriffsberechtigungen festgestellt, dass ein Ministerium für zwei User Berechtigungen vergeben hat, die Zugriffe auf Daten **aller** Bediensteten des nachgeordneten Bereichs erlauben. Begründet wird dies damit, dass das

Ministerium Personal führende Dienststelle für alle Bediensteten ab der Besoldungsgruppe A 15 ist und einen Zugriff auf diese Datensätze haben muss. In den Personaldatensätzen im SAP-System ist zurzeit kein Merkmal hinterlegt, das eine entsprechende Zugriffsbeschränkung im Rahmen der Berechtigungsvergabe ermöglicht.

Ich habe gefordert, diese Zugriffsberechtigungen sofort zu löschen.

Nach langen Diskussionen mit Vertretern des Ministeriums habe ich für eine Übergangszeit zugestimmt, dass diese Zugriffe (technisch) weiterhin möglich sind. Voraussetzung für meine Zustimmung war allerdings, dass den beiden Bediensteten des Ministeriums per Dienstanweisung untersagt wird, auf andere als ihrer Zuständigkeit unterliegende Datensätze zuzugreifen, und dass alle Zugriffe protokolliert werden. Außerdem ist sicherzustellen, dass so schnell als möglich ein entsprechendes Merkmal in den Personaldatensätzen im SAP-System hinterlegt wird, um eine datenschutzgerechte Zugriffssteuerung zu gewährleisten. Eine weitere Voraussetzung ist die Vereinheitlichung der Zuständigkeitsanordnungen aller Ressorts, um landeseinheitlich gewährleisten zu können, dass ein entsprechendes Merkmal in den betreffenden Datensätzen gespeichert werden kann, über das die Zugriffsberechtigung steuerbar ist.

Zwischenzeitlich hat der Kabinettsausschuss „Verwaltungsreform und Verwaltungsinformatik“ beschlossen, dass unverzüglich ein entsprechendes Merkmal für die Zugriffssteuerung in die Datensätze aufgenommen werden soll. Weiterhin wurde beschlossen, dass die Zuständigkeitsanordnungen der Ressorts im Bereich des Personalwesens standardisiert werden sollen, um klare Strukturen zu haben, die sauber im SAP-System abgebildet werden können.

Inzwischen wurde ein entsprechendes Konzept erarbeitet, sodass ich davon ausgehe, dass die entsprechenden Hinterlegungen im SAP-System zeitnah erfolgen werden.

5.10.2.5

Fazit und Ausblick

Die Praxis hat gezeigt, dass die Anforderungen der sehr unterschiedlichen Verwaltungsstrukturen der hessischen Landesverwaltung im SAP-System nicht ohne Probleme abzubilden sind. Dies zeigt sich deutlich an der sehr großen Zahl von Änderungsanträgen der einzelnen Dienststellen.

Diese Anträge werden mir, soweit sie datenschutzrechtliche Relevanz haben und vom Landesreferenzmodell abweichen, zur Stellungnahme vorgelegt.

Ich werde in den nächsten Jahren das SAP-System vermehrt vor Ort prüfen um sicherzustellen, dass die in den Konzepten und im Verfahrensverzeichnis beschriebenen Zugriffsberechtigungen tatsächlich hinterlegt und eingehalten werden.

Ebenso werde ich prüfen, ob Auswertungen des Datenbestandes nur für User möglich sind, die diese konkret zur Erfüllung der ihnen übertragenen Aufgaben und im Rahmen ihrer Zuständigkeit benötigen.

5.10.3

Bekanntgabe von Bediensteten, die Altersteilzeit beantragt haben, an den Personalrat

Dienststellen sind nicht befugt, dem Personalrat die Bediensteten bekannt zu geben, die Altersteilzeit beantragt haben.

Eine Kommune hat angefragt, ob sie dem Personalrat Auskunft geben müsse, welche Bediensteten Gewährung von Altersteilzeit beantragt haben.

Ein dahingehender Informationsanspruch könnte sich möglicherweise aus § 77 HPVG ergeben, der das Mitbestimmungsrecht des Personalrats im Rahmen seiner Beteiligung in Personalangelegenheiten betrifft. Beispielsweise bestimmt der Personalrat mit in Personalangelegenheiten der Beamten bei Ablehnung eines Antrags auf Teilzeitbeschäftigung oder Beurlaubung nach §§ 85a oder 85f HBG (§ 77 Abs. 1 Nr. 1i HPVG); Gleiches gilt in Personalangelegenheiten der Angestellten und Arbeiter (§ 77 Abs. 1 Nr. 2f HPVG).

Die Anfrage der Kommunen zielte aber auf das Thema Altersteilzeit, die in § 85b HBG geregelt ist; diese Norm wird indessen bei der Mitbestimmung – anders als §§ 85a oder 85f HBG – gerade nicht aufgeführt. Von daher lässt sich aus den Regelungen über die Mitbestimmungsrechte des Personalrats in Personalangelegenheiten kein Informationsanspruch des Personalrats ableiten.

Ebenso wenig besteht ein solcher Anspruch mit Blick auf die Vorschrift, die die Mitwirkung des Personalrats in Personalangelegenheiten betrifft, § 78 HPVG. Denn danach umfasst die Mitwirkung Nebentätigkeitsgenehmigungen, vorzeitige Versetzungen in den Ruhestand, fristlose Entlassungen, außerordentliche Kündigungen sowie Kündigungen während der Probezeit. Die Altersteilzeit ist hier jedoch nicht aufgeführt.

Ungeachtet des fehlenden Informationsanspruchs des Personalrates bleibt es den Bediensteten selbstverständlich unbenommen, in Fragen der Altersteilzeit den Personalrat aus eigener Initiative zu konsultieren, wenn ihnen das opportun erscheint.

Ich habe die Kommune über die Rechtslage informiert.

5.10.4

Datenübermittlung durch den Polizeiärztlichen Dienst an die Polizeiverwaltung

Medizinische Daten dürfen vom Polizeiärztlichen Dienst nur im Rahmen der Erforderlichkeit an die polizeiliche Personalverwaltung übermittelt werden.

5.10.4.1

Der Ausgangsfall

Ein in den Ruhestand versetzter Polizeivollzugsbeamter beschwerte sich darüber, dass Gutachten des Polizeiärztlichen Dienstes, die zu seiner Person im Zusammenhang mit einer versorgungsrechtlichen Auseinandersetzung erstellt worden waren, der Personal verwaltenden Stelle des Polizeipräsidiums in Offenbach übermittelt, dort verwendet und in die Personalakte aufgenommen wurden.

Die datenschutzrechtliche Problematik ergibt sich aus den Inhalten solcher Gutachten. Diese enthalten in der Regel Angaben zur Anamnese, einer Verlaufsbeschreibung des Krankheitsbildes, Ergebnisse medizinischer Einzeluntersuchungen (z. B. Blutwerte) und vieles andere mehr. Hinzu kommen die verschiedenen fachlich-inhaltlichen Aspekte solcher Gutachten. So kann es einerseits

um Aussagen zu körperlichen Schädigungen gehen, die Auswirkungen auf die weitere Verwendung des Betroffenen haben. Andererseits kann Untersuchungsgegenstand auch die psychische Verfassung eines Betroffenen sowie deren Auswirkungen, z. B. auf die weitere Dienstfähigkeit, sein. In jedem Fall handelt es sich um ärztliche Unterlagen, die zunächst einmal der Schweigepflicht durch den Arzt unterliegen. Aus Sicht der Personal führenden Stelle war die Einsichtnahme in die Gutachten und Verwendung der Informationen zulässig. Es sei erforderlich, so deren Argumentation, die Inhalte der Gutachten zur Kenntnis zu nehmen und daraus ggf. eigene Schlüsse zu ziehen. Auch war man der Ansicht, dass sogar im vorprozessualen Stadium einer Auseinandersetzung zwischen dem Betroffenen und der Personal führenden Stelle nur dann eine „Chancengleichheit der Parteien“ gegeben sei, wenn die Personalverwaltung eine inhaltliche Auseinandersetzung mit dem Gutachteninhalt vornehmen könne. Bei jeder kontroversen Diskussion polizeiärztlicher Feststellungen zwischen Betroffenen und Behörde sei deshalb die volle Kenntnis vorhandener Gutachten erforderlich. Dies ergebe sich auch aus § 51 Abs. 1 Satz 3 HBG, wonach Beamte sich im Rahmen einer Versetzung in den Ruhestand bei Dienstunfähigkeit oder auf Antrag bzw. Weisung der Behörde ärztlich untersuchen lassen müssten. Gemäß Satz 4 der Vorschrift habe der Arzt der Behörde sein Gutachten sowie entsprechend der für Amtsärzte geltenden Rechtsvorschriften auch die Angaben zur Vorgeschichte und den Untersuchungsbefund mitzuteilen.

5.10.4.2

Verfahrensweise bei anderen Polizeipräsidiën

Die grundsätzliche Bedeutung der Eingabe hat mich dazu veranlasst, weitere Personal führende Stellen bei den Polizeipräsidiën aufzusuchen und deren Verfahrensweise im Umgang mit ärztlichen Gutachten zu ermitteln. Dabei ergaben sich signifikant unterschiedliche Handhabungen, die vor allem in der Organisationsstruktur des polizeiärztlichen Dienstes begründet liegen. Andererseits hatten die Verwaltungsleiter selbst unterschiedliche Auffassungen zur Kenntnisnahme und Verwendung der Gutachten.

Im Polizeipräsidium Frankfurt selbst ist ein polizeiärztlicher Dienst untergebracht. Dieser ist zunächst für den Bereich Frankfurt zuständig. Daraus resultiert insbesondere die ordnungskonforme Umsetzung der restriktiven Vorgaben der Polizeidienstverordnung 300, wonach ärztliche Unterlagen beim Arzt bzw. dessen Hilfspersonal zu verbleiben haben. Die

Personalverwaltung in Frankfurt erhält demnach zunächst einmal ausschließlich die Untersuchungsergebnisse im Hinblick auf die Polizeidiensttauglichkeit bzw. Nichttauglichkeit eines bzw. einer Betroffenen sowie Hinweise über eine ggf. mögliche Weiterverwendung. Hierzu wird vom Polizeiarzt auf einem Formular eine Beurteilung über die Dienstfähigkeit abgegeben. Im Weiteren wird Stellung dazu genommen, durch welche Umstände die Gesundheitsschäden entstanden sind, bevor eine sozialmedizinische Bewertung sowie eine Tätigkeitsbewertung vorgenommen werden. Dabei wird u. a. festgestellt, ob das Führen eines Dienst-Kfz oder die Teilnahme an der Schießausbildung möglich sind. Diese Informationen genügen der Behörde zunächst, um eine den ärztlichen Empfehlungen entsprechende Verwendung des Untersuchten sicherzustellen. Beim Polizeipräsidium Südhessen sah man ebenfalls keine Erforderlichkeit, unmittelbaren Einblick in das ärztliche Gutachten zu nehmen. Allerdings ist man dort praktisch dazu gezwungen, da vom Polizeiärztlichen Dienst kein zusammengefasstes Ergebnis an die Behörde zugestellt, sondern von vornherein das komplette Gutachten übermittelt wird. Infolgedessen bleibt nur die Möglichkeit, den als vertrauliche Arztsache gekennzeichneten Umschlag zu öffnen, um die Ergebnismitteilung zu erfahren. Das Polizeipräsidium Südhessen verfügt über keinen eigenen Arzt. Deshalb ist man auf externe Kräfte bei der Bereitschaftspolizei in Mühlheim (Main) bzw. dem Polizeipräsidium Frankfurt angewiesen. Da die Ärzte dort offensichtlich keine Aktenbestände zu Beamten externer Dienststellen führen können bzw. wollen, erhält der Auftraggeber die vollständigen Akten bzw. Gutachten zur weiteren Verwendung. In einem so genannten Unterordner C wird das Gutachten nach der Kenntnisnahme in einem verschlossenen Umschlag abgelegt.

Das Polizeipräsidium Nordhessen verfügt wie Südhessen über keinen eigenen ärztlichen Dienst. Von den externen Polizeiärztlichen Diensten wird neben dem Gesamtgutachten eine zusammengefasste Beurteilung mitgeliefert, die Aufschluss über die Dienstfähigkeit des Untersuchten gibt. Allerdings wird es in Kassel bislang so gehandhabt, dass die ausführlichen Gutachten im Hinblick auf ein zukünftiges Verwendungsgespräch mit dem Betroffenen eingesehen werden.

5.10.4.3

Datenschutzrechtliche Bewertung

Die unterschiedliche Handhabung der Polizeiärzte im Umgang mit dem Gutachten ist problematisch. Nach den Vorgaben unter Ziff. 2.5.1 der Polizeidienstverordnung 300 darf nur Ärzten und deren Hilfspersonal, die mit der Vorbereitung dienstrechtlicher Entscheidungen befasst sind, das Gutachten zugänglich sein. Nach Ziff. 2.5.2 ist der Behörde ein „Gesundheits- oder Tauglichkeitszeugnis“ zu überlassen, welches nur das abschließende Beurteilungsergebnis enthält. Die Organisationsstruktur des Dienstes in Hessen und der Umstand, dass nicht jede Personal führende Stelle auf einen eigenen Dienst zurückgreifen kann, haben ganz offensichtlich zu der differentiellen Handlungsweise beigetragen. Dem steht jedoch sowohl die allgemeine und für jeden Arzt verbindliche Schweigepflicht einerseits sowie die klare Regelung der Polizeidienstverordnung 300 entgegen.

Die entscheidende datenschutzrechtliche Fragestellung, sieht man einmal von dem Thema der Übermittlung kompletter Gutachten an den Auftraggeber ab, betrifft den Zeitpunkt der Kenntnisnahme dieser Unterlagen. Dabei geht es nicht, wie u. a. ebenfalls argumentiert darum, der Behörde die Befugnis abzuspochen, Gutachten zu veranlassen oder ihr ein Verwertungsverbot aufzuerlegen, wenn die tatsächlichen Umstände, wie z. B. der Erlass eines Widerspruchsbescheides oder die verwaltungsgerichtliche Aufarbeitung einer unterschiedlichen Bewertung von Betroffenen und Dienstherren, dies erforderlich machen.

Der Zeitpunkt der Erforderlichkeit zur Kenntnisnahme medizinischer Sachverhalte, die zunächst einmal der ärztlichen Schweigepflicht unterliegen, berührt den datenschutzrechtlichen Kern der Diskussion.

Gemäß § 107 Abs. 4 HBG darf der Dienstherr Daten nur im Rahmen der Erforderlichkeit erheben.

§ 107 Abs. 4 HBG

Der Dienstherr darf personenbezogene Daten über Bewerber, Beamte und ehemalige Beamte nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt.

Es ist keineswegs so, dass § 51 Abs. 1 Satz 4 HBG bedeutet, dass ausführliche Gutachten dem Auftraggeber zu übermitteln sind.

§ 51 Abs. 4 HBG

Der Arzt teilt der Behörde sein Gutachten sowie in entsprechender Anwendung der für Amtsärzte geltenden Rechtsvorschriften auch die Angaben zur Vorgeschichte und den Untersuchungsbefund mit.

Bei dieser Vorschrift ist von dem Grundsatz auszugehen, dass dem Dienstherrn lediglich ein zusammengefasstes Ergebnis der Untersuchungen mitzuteilen ist. Davon unberührt bleibt dessen Möglichkeit, zusätzliche Informationen beim Arzt durch gezielte Nachbefragungen zu erheben. Ebenso wie in der Polizeidienstverordnung 300 ergibt sich dieser Grundsatz auch für Amtsärzte aus § 18a Abs. 1 Satz 1 und 2 der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens (DVO). Nach der Anlage 2 der DVO sind die Angaben zur Vorgeschichte, die verschiedenen Untersuchungsbefunde sowie die Diagnose nicht in ein amtsärztliches Zeugnis aufzunehmen; sie verbleiben beim Gesundheitsamt. Nur wenn konkrete Zweifel an der Vollständigkeit oder an der Aussagefähigkeit des Gesundheitszeugnisses oder des darin festgestellten Ergebnisses der Beurteilung bestehen, kann der Dienstherr weitergehende Angaben fordern. Diese Vorschriften gelten auch für einen Privatarzt, der mit einem Gutachten beauftragt wird. Hat die Behörde insgesamt Zweifel an der Aussage des Arztes bzw. Polizeiarztes, so kann sie weitere, ggf. externe Ärzte beauftragen zur Beurteilung des medizinischen Sachverhaltes. Die restriktiven Regelungen zur Daten- und Informationsweitergabe tragen unmittelbar dem Recht auf informationelle Selbstbestimmung, Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG, Rechnung und schränken die Datenübermittlung auf das jeweils Erforderliche ein. Vor diesem Hintergrund habe ich mit dem Leiter des Hessischen Polizeiärztlichen Dienstes die Rechtslage erörtert und die Notwendigkeit betont, die Handlungsweise des Hessischen Polizeiärztlichen Dienstes der Rechtslage anzupassen. Er hat mir zugesagt, dass der Polizeiärztliche Dienst zukünftig rechtskonform verfahren wird; d. h., dass die Datenübermittlungen strikt auf das erforderliche Maß reduziert werden.

Der leitende Polizeiarzt hat in einem Erlassentwurf, den er dem Hessischen Innenministerium zur Prüfung zugeleitet hatte, den Umgang mit dem Gutachter geregelt. Danach werden die von den verschiedenen Polizeiärztlichen Dienststellen durchgeführten Untersuchungen und die daraus

erstellten Gutachten künftig an den Leiter des Polizeiärztlichen Dienstes übermittelt. Dort werden die Gutachten zentral abgelegt. Die jeweiligen Auftraggeber der Untersuchung über die Polizeidiensttauglichkeit, also die Personalabteilungen der zuständigen Dienststellen der Polizei, erhalten zunächst nur ein zusammengefasstes Ergebnis. Erst im weiteren Verlauf einer möglichen Auseinandersetzung vor dem Verwaltungsgericht erhält die Personal führende Stelle auf Anforderung das komplette Gutachten. Das Hessische Innenministerium hat dem Vorschlag des Leitenden Polizeiarztes zugestimmt. Mit der Umsetzung dieser Maßnahmen wird ein wesentlicher Schritt zur Verbesserung der Rechte hessischer Polizeibeamtinnen und -beamter realisiert.

Was den konkreten Ausgangsfall betrifft, war die Einsichtnahme in die Einzelgutachten zum damaligen Zeitpunkt erforderlich. Denn es war zu einer verwaltungsgerichtlichen Auseinandersetzung über die ärztlich festgestellten Befunde und die hieraus resultierenden Konsequenzen betreffend der versorgungsrechtlichen Ansprüche des Betroffenen gegenüber dem Dienstherrn gekommen. Dies habe ich dem Betroffenen mitgeteilt.

5.11 Finanzwesen

5.11.1

Darf das Finanzamt Geschäftspost an die Privatanschrift des Einzelunternehmers versenden?

Auch wenn die ungenaue Adressierung von Finanzamtspost im Einzelfall zu Problemen führen kann, muss sie für die Dauer der technischen Entwicklung neuer DV-Programme hingenommen werden.

Ein Einzelunternehmer aus Südhessen wandte sich an mich, weil sein Finanzamt auch geschäftliche Korrespondenz zur Lohnsteuer von Mitarbeitern sowie zur Umsatzsteuer regelmäßig an seine Privatadresse verschickte. Er könne nicht ausschließen, dass so Familienmitglieder Einsicht in diese Post erhalten.

Meine Recherchen bei dem betroffenen Finanzamt und der Oberfinanzdirektion Frankfurt ergaben, dass im Grundinformationsdienst der Finanzverwaltung für jeden Steuerpflichtigen

dessen Wohnadresse gespeichert wird. Alle derzeit genutzten DV-Programme greifen unabhängig von der bearbeiteten Steuerart grundsätzlich auf diese Adresse zurück. Hierbei ist jede natürliche Person ein einziges Steuersubjekt, unabhängig davon, für welche Steuerarten sie steuerrechtlich in Erscheinung tritt. Eine Unterscheidung zwischen privater und geschäftlicher Post wird vom Finanzamt nur dann getroffen, wenn der Einzelunternehmer verheiratet ist und gemeinsam veranlagt wird. In diesen Fällen werden private Steuerunterlagen an die Eheleute und geschäftliche Unterlagen an den Unternehmer allein adressiert, aber in beiden Fällen wird die private Adresse verwendet. Es ist jedoch fraglich, ob diese feine Unterscheidung von den Adressaten wahrgenommen wird.

Als Alternative wird dem Steuerpflichtigen die Möglichkeit eingeräumt, einen so genannten Zustellbevollmächtigten in den Grundinformationsdienst eintragen zulassen. Im Allgemeinen sind dies Steuerberater, es könnte aber auch die Unternehmensadresse angegeben werden. In diesem Fall würde auch die private Finanzamtspost an die Geschäftsadresse verschickt. Wieder mit dem Risiko, dass Unbefugte Einsicht in Briefe des Finanzamtes erlangen könnten.

Diese begrenzten technischen Möglichkeiten der derzeit genutzten DV-Verfahren mit den hier beschriebenen Problemen sind der Finanzverwaltung bekannt. Sie werden mit dem Einsatz der in der Entwicklung befindlichen Stammdatenverarbeitung für alle Steuerpflichtigen behoben werden. Das neue Verfahren wird unterschiedliche Zustelladressen für verschiedene steuerliche Vorgänge einer Person vorsehen. Den Betroffenen habe ich informiert.

6. Kommunen

6.1

Forderungsmanagement von Kommunen

Die Einbeziehung von privaten Inkassobüros und Auskunftsteilen ist bei privatrechtlichen Forderungen von Kommunen rechtlich zulässig. Öffentlich-rechtliche Forderungen sind hingegen von der Kommune selbst zu verfolgen.

Die angespannte Haushaltslage der Kommunen verleitet zu immer neuen Experimenten, mit denen Geld in die leeren kommunalen Kassen geholt werden soll. So wird jetzt erwogen und teilweise auch praktiziert, private Inkassobüros mit der Beitreibung kommunaler Forderungen zu beauftragen. Erfolg bei der Realisierung von Forderungen verspricht man sich ferner aus Verträgen mit der SCHUFA, um so deren Adressbestände zum Auffinden säumiger Schuldner nutzen zu können.

6.1.1

Einbeziehung von Inkassobüros und Übertragung von Forderungen

Wenn Forderungen verkauft werden, werden in den meisten Fällen auch personenbezogene Daten der Schuldner gegenüber dem Inkassobüro offenbart. Bei der Beurteilung der Frage, ob dies datenschutzrechtlich zulässig ist, ist zu unterscheiden zwischen privatrechtlichen und öffentlich-rechtlichen Forderungen.

6.1.1.1

Privatrechtliche Forderungen

Auch Gemeinden schließen zahlreiche privatrechtliche Verträge wie z. B. Miet- und Pachtverträge ab. Forderungen aus solchen Verträgen können von der öffentlichen Hand unter den gleichen rechtlichen Bedingungen abgetreten werden, wie dies ein privater Vermieter tun könnte. Die Rechtsverhältnisse unterscheiden sich in diesem Fall nicht. Im rein privatrechtlichen Handlungsrahmen einer Kommune gehen die §§ 398 ff. BGB als spezialgesetzliche

Übermittlungsnormen denen des HDSG vor. Etwas anderes gilt lediglich dann, wenn zusätzliche datenschutzrechtliche Bestimmungen zu beachten sind, etwa wenn es sich um Miet- oder Pachtforderungen gegenüber eigenen Bediensteten aus der vergünstigten Überlassung von Wohnungen/Grundstücken handelt.

6.1.1.2

Öffentlich-rechtliche Forderungen

Der „Verkauf“ von kommunalen öffentlich-rechtlichen Forderungen ist hingegen rechtlich als Übertragung von Hoheitsgewalt zu verstehen. Dadurch gehen Datenzugriffsrechte auf Private über, ohne dass eine förmliche Beleihung erfolgt. Anders als bei einer Beauftragung Dritter verbleiben der Kommune beim Verkauf auch keine Steuerungsmöglichkeiten mehr. Im Übrigen hat der Gesetzgeber die Vollstreckung zugunsten der Gemeinden dahingehend geregelt, dass sie durch eigene Vollziehungsbeamte oder die des Kreises durchgeführt werden (§ 16 HessVwVG). Ein Verkauf öffentlich-rechtlicher Forderungen ist damit datenschutzrechtlich unzulässig.

6.1.2

Vereinbarung mit der SCHUFA

Da säumige Schuldner ihren melderechtlichen Verpflichtungen häufig nicht nachkommen, ist auch beabsichtigt, den Adressdatenbestand der SCHUFA zu nutzen, die häufig genauere Informationen hat als die Meldebehörden. Die Besonderheit eines Vertragsabschlusses mit der SCHUFA besteht darin, dass dieser hinsichtlich der Übermittlung von Daten und ihrer Nutzung auf Gegenseitigkeit beruht. D. h., will eine Kommune den Datenbestand der SCHUFA nutzen, muss sie sich ihrerseits verpflichten, Daten über ihre Schuldner zur Verfügung zu stellen. Diese Daten stehen dann auch anderen Vertragspartnern der SCHUFA zur Verfügung.

Bei der Bewertung einer Anfrage zum Abschluss eines Vertrages mit der SCHUFA habe ich ebenfalls eine Unterscheidung zwischen privatrechtlichen und öffentlich-rechtlichen Forderungen vorgenommen. Soweit es um die Adressdatenermittlung im Zusammenhang mit privatrechtlichen Forderungen geht, habe ich dem „normalen“ Vertragsverfahren mit der SCHUFA zugestimmt. D. h. die Kommune ist berechtigt, Abfragen nach Adressen über säumige Schuldner

vorzunehmen. Der Tatbestand der Anfrage wird dann auch allen anderen Vertragspartnern der SCHUFA bekannt, nicht allerdings wer angefragt hat. Als Gegenleistung verpflichtet sich die Kommune, alle titulierten Forderungen namentlich mit Vollstreckungsinhalt an die SCHUFA zu melden, und zwar unabhängig davon, ob im Einzelfall eine Anfrage zur Adressermittlung an die SCHUFA erfolgte. Nach erfolgreicher Beitreibung erfolgt seitens der Kommune ein Erledigungsvermerk an die SCHUFA.

Bei der Beitreibung öffentlich-rechtlicher Forderungen habe ich einem Vertragsabschluss mit der SCHUFA und damit der Möglichkeit der Nutzung der Adresdaten unter folgenden Bedingungen zugestimmt:

Bei der SCHUFA wird nur der Tatbestand der Anfrage zu einem bestimmten Schuldner den anderen Vertragspartnern zur Verfügung gestellt. Nicht gespeichert werden die anfragende Stelle, Daten über das Schuldverhältnis oder Art der Forderung.

6.2

Prüfung des Online-Abrufs von Privaten aus dem Liegenschaftskataster

Die Überprüfung von Teilnehmern am automatisierten Abrufverfahren aus dem Liegenschaftskataster hat ergeben, dass die Vorgaben des Hessischen Landesamtes für Bodenmanagement und Geoinformationen nur unzureichend umgesetzt waren. So haben die Abrufer nicht dokumentiert, warum sie im Einzelfall auf das Kataster zugegriffen haben.

Mit Gesetz vom 20. Juni 2002 hat der Landesgesetzgeber die Möglichkeit geschaffen, Daten aus dem Liegenschaftskataster auch in automatisierter Form abzurufen (s. a. 31. Tätigkeitsbericht, Ziff. 21). Dies gilt auch für den Abruf von personenbezogenen Daten. Der automatisierte Abruf bedarf der Genehmigung durch das Hessische Landesamt für Bodenmanagement und Geoinformationen. Dieses prüft, ob der Antragsteller ein berechtigtes Interesse i. S. v. § 16 Abs. 2 Vermessungsgesetz (HVG) hat.

§ 16 Abs. 2 HVG

Die Einsicht in die personenbezogenen Daten sowie das Erteilen von entsprechenden Auskünften und Auszügen ist nur zulässig, wenn der Nutzer ein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft macht.

Dieses berechnigte Interesse muss auch bei jedem einzelnen Abruf im automatisierten Verfahren vorliegen. Bei der Prüfung durch das Hessische Landesamt für Bodenmanagement und Geoinformationen, ob ein Antragsteller die Genehmigung für den automatisierten Abruf erhält, findet zunächst eine grundsätzliche Prüfung statt, ob überhaupt ein berechtigtes Interesse vorliegt. Um überprüfen zu können, ob dann im einzelnen Abruffall das berechnigte Interesse an der Kenntnis der Daten vorgelegen hat, muss der Teilnehmer am Abrufverfahren dokumentieren, warum er Daten zu einer bestimmten Person abgerufen hat. D. h., jedem getätigten Abruf personenbezogener Daten muss ein konkreter Geschäftsfall zugeordnet und ein entsprechender Nachweis für den Zeitraum von zwölf Monaten aufbewahrt werden. Darauf werden die Nutzer des Verfahrens in dem Genehmigungsbescheid hingewiesen. Das Hessische Landesamt für Bodenmanagement und Geoinformationen seinerseits protokolliert sämtliche getätigten Abrufe.

§ 16a Abs. 4 HVG

Die Abrufe sind zum Zweck der Kontrolle zu protokollieren. Dabei werden die Benutzererkennung, Datum und Uhrzeit, der Verwendungszweck (Aktenzeichen oder Bearbeitungs- oder Auftragsnummer) und die Ordnungsmerkmale der abgerufenen Daten (Gemarkungsname und -nummer, Flur- und Flurstücksnummer oder Grundbuchblattnummer) erfasst.

Die abrufenden Stellen müssen sich zudem schriftlich bereit erklären, eine Kontrolle der Anlage und ihrer Benutzung durch die Genehmigungsbehörde zu dulden.

Bereits kurz nach In-Kraft-Treten des Gesetzes hatte ich mit dem Hessischen Ministerium für Wirtschaft, Verkehr und Landesentwicklung vereinbart, mehrere Institutionen, denen eine Abrufberechnigung personenbezogener Daten aus dem Liegenschaftsbuch erteilt worden ist, daraufhin zu überprüfen, ob die getätigten Abrufe innerhalb des bei Antragstellung benannten Verwendungszwecks erfolgt sind und auch nur für diesen weiterverarbeitet werden.

Diese Überprüfung wurde im Berichtszeitraum zusammen mit Vertretern des Wirtschaftsministeriums und des Landesamtes für Bodenmanagement und Geoinformationen bei berechtigten Abrufern durchgeführt.

Die Überprüfung ergab, dass die Abrufer ihre beim Landesamt protokollierten Abrufe in keinem Fall einem konkreten Geschäftsvorfall zuordnen konnten. Die Nutzer des Verfahrens haben sich insoweit nicht an die rechtlichen Vorgaben, die das Landesamt mit seinem Genehmigungsschreiben mitgeteilt hatte, gehalten. Die überprüften Stellen haben zugesichert, die Dokumentation in Zukunft ordnungsgemäß durchzuführen. Da anzunehmen war, dass andere abrufberechtigte Stellen ihrer Dokumentationsverpflichtung ebenfalls nicht nachgekommen sind, ist seitens der Vermessungsverwaltung beabsichtigt, alle zugelassenen Direktabrufener nochmals schriftlich auf ihre Verpflichtung zur Dokumentation hinzuweisen. Neu zugelassene Direktabrufener in Geodaten online sollen im Zulassungsschreiben noch deutlicher als bisher auf die Möglichkeit der Überprüfbarkeit hingewiesen werden. Im Übrigen ist beabsichtigt, bei den bereits geprüften Nutzern im ersten Quartal 2006 einen Nachprüfungstermin vorzunehmen.

6.3

Wahlstatistik

Stimmzettel, die mit statistischen Hinweisen wie „Mann“ und „geboren von 1948 bis 1960“ gekennzeichnet sind, verletzen nicht das Wahlgeheimnis.

Vor der Bundestagswahl 2005 erhielt ich Anfragen zum Wahlgeheimnis von besorgten Bürgern, die auf ihrem mit den Briefwahlunterlagen zugesandten Stimmzettel Kennzeichnungen wie „Mann“ und „geboren von 1948 bis 1960“ entdeckten.

Die Kennzeichnung von Stimmzetteln findet nicht nur bei der Bundestagswahl, sondern auch bei Landtagswahlen und Kommunalwahlen statt. Das Wahlgeheimnis wird durch diese besondere Kennzeichnung einiger Stimmzettel jedoch nicht verletzt, solange die gesetzlichen Vorgaben aus dem Wahlstatistikgesetz (WStatG) für Bundestagswahlen, aus § 72 Landeswahlordnung für Landtagswahlen bzw. aus § 66 Hessisches Kommunalwahlgesetz (KWG) für kommunale Wahlen berücksichtigt werden.

§ 2 WStatG

(1) Aus dem Ergebnis der Wahlen gemäß § 1 sind unter Wahrung des Wahlgeheimnisses in ausgewählten Wahlbezirken repräsentative Wahlstatistiken über

- a) die Wahlberechtigten, Wahlscheinvermerke und die Beteiligung an der Wahl nach Geschlecht und Geburtsjahresgruppen,
 - b) die Wähler und ihre Stimmabgabe für die einzelnen Wahlvorschläge nach Geschlecht und Geburtsjahresgruppen sowie die Gründe für die Ungültigkeit von Stimmen
- als Bundesstatistik zu erstellen.

(2) In die Statistik nach Absatz 1 Buchstabe b sind ausgewählte Briefwahlbezirke einzubeziehen. Ein Briefwahlbezirk wird bestimmt durch die dem Briefwahlvorstand zugewiesene Zuständigkeit nach Wahlbezirken, die auf der Grundlage von § 2 Abs. 3 des Bundeswahlgesetzes oder von § 3 Abs. 2 des Europawahlgesetzes gebildet worden sind.

§ 72 LWO

(1) Die von den Wahlorganen ermittelten Wahlergebnisse (§§ 58, 66, 67) werden vom Statistischen Landesamt dokumentiert und ausgewertet. Dabei werden insbesondere Veränderungen im Verhältnis zu vorangegangenen Wahlen ermittelt und die Ergebnisse in unterschiedlichen regionalen Gliederungen dargestellt.

(2) Das Statistische Landesamt teilt den Gemeindebehörden spätestens am vierunddreißigsten Tage vor der Wahl die nach § 48 Abs. 2 des Gesetzes bestimmten Wahlbezirke mit und gibt ihnen die Erhebungsmerkmale sowie die Unterscheidungsbezeichnungen für die Stimmzettel oder die Wahlgeräte bekannt. Die Gemeindebehörde unterrichtet die zuständigen Wahlvorstände über die Durchführung der repräsentativen Wahlstatistik.

(3) Die Auswertung der Wahlbeteiligung nach Geburtsjahresgruppen und Geschlecht (§ 48 Abs. 2 Satz 1 Buchst. a des Gesetzes) erfolgt durch das Statistische Landesamt, das sich dazu der jeweiligen Gemeindebehörde bedient. Die Gemeindebehörden übersenden dem Statistischen Landesamt im Anschluss an die Feststellung des Wahlergebnisses die nach seiner Anleitung ausgefüllten Erhebungsbögen.

(4) Für die Erstellung der Wahlstatistik über die Geschlechts- und Altersgliederung der Wahlberechtigten und Wähler unter Berücksichtigung der Stimmabgabe für die einzelnen Wahlvorschläge (§ 48 Abs. 2 Satz 1 Buchst. b des Gesetzes) sind dem Statistischen Landesamt im Anschluss an die Feststellung des Wahlergebnisses auf Anforderung zu übersenden:

von der Gemeindebehörde:

1. das Wählerverzeichnis,
2. die eingenommenen Wahlscheine,
3. alle Stimmzettel, soweit sie nicht der Wahlniederschrift beigelegt sind;

vom Kreiswahlleiter:

die Wahlniederschriften der ausgewählten Bezirke mit allen Unterlagen.

Nach Abschluss der Auswertung gibt das Statistische Landesamt den einzelnen Dienststellen die genannten Unterlagen zurück.

§ 66 KWG

(1) Die Ergebnisse der Gemeinde- und Kreiswahlen, der Wahlen der Bürgermeister und Landräte, der Bürgerentscheide und der Ausländerbeiratswahlen sind als Landesstatistik zu bearbeiten.

(1a) Das Hessische Statistische Landesamt kann in repräsentativ ausgewählten Wahlbezirken Wahlstatistiken über das Stimmverhalten der Wähler nach § 18 Abs. 1 als Landesstatistiken erstellen.

(2) Der Gemeindevahlleiter kann in repräsentativ ausgewählten Wahlbezirken Wahlstatistiken über

- a) die Wahlbeteiligung nach Geburtsjahresgruppen und Geschlecht,
 - b) Geschlechts- und Altersgliederung der Wahlberechtigten und der Wähler unter Berücksichtigung der Stimmabgabe für die einzelnen Wahlvorschläge
- als Kommunalstatistiken erstellen.

(3) Erhebungsmerkmale für die Statistiken nach Abs. 2 sind Geschlecht, Geburtsjahresgruppe, Teilnahme an der Wahl, Wahlscheinvermerk, abgegebene Stimme, ungültige Stimme. Hilfsmerkmal ist der Wahlbezirk. Für die Statistik nach Abs. 2 Buchst. a sind höchstens zehn Geburtsjahresgruppen zu bilden, in denen jeweils mindestens drei Geburtsjahrgänge zusammenzufassen sind. Für die Statistik nach Abs. 2 Buchst. b sind höchstens fünf Geburtsjahresgruppen zu bilden, in denen jeweils mindestens sieben Geburtsjahrgänge zusammenzufassen sind.

(4) Die Statistik nach Abs. 2 Buchst. a wird durch Auszahlung der Wählerverzeichnisse, die Statistik nach Abs. 2 Buchst. b unter Verwendung von Stimmzetteln mit Unterscheidungsbezeichnungen nach Geschlecht und Geburtsjahresgruppe oder unter Verwendung entsprechend geeigneter Wahlgeräte durchgeführt.

(5) Die für die Statistik nach Abs. 1a und 2 ausgewählten Wahlbezirke müssen wenigstens 400 Wahlberechtigte umfassen. Wählerverzeichnisse und gekennzeichnete Stimmzettel dürfen nicht zusammengeführt werden. Für die Vernichtung der Stimmzettel gelten die wahlrechtlichen Vorschriften. Ergebnisse für einzelne Wahlbezirke dürfen nicht bekannt gegeben werden.

(6) Die Durchführung der Statistiken nach Abs. 1a und 2 ist nur zulässig, wenn das Wahlgeheimnis gewahrt bleibt.

Alle Ergebnisse von Wahlen werden unter Wahrung des Wahlgeheimnisses statistisch ausgewertet. In ausgesuchten Wahlbezirken sind Wahlstatistiken über Wahlberechtigte, Wahlscheinvermerke und Beteiligung an der Wahl nach Geschlecht und Geburtsjahresgruppen, Stimmabgaben für einzelne Wahlvorschläge nach Geschlecht und Geburtsjahresgruppen sowie über die Gründe für die Ungültigkeit von Stimmen zu erstellen.

Diese Statistiken können nur mit Hilfe von amtlichen Stimmzetteln erstellt werden, die zusätzlich Unterscheidungsmerkmale nach Geschlecht und Geburtsjahresgruppen enthalten. Für die Bundestagswahl trifft der Bundeswahlleiter im Einvernehmen mit den Landeswahlleitern und den statistischen Landesämtern die Auswahl der Stichprobenwahlbezirke (§ 3 WStatG). Für Landtagswahlen teilt das Statistische Landesamt den Gemeindebehörden die statistisch auszuwertenden Wahlbezirke mit und gibt die Erhebungsmerkmale sowie die Unterscheidungsbezeichnungen für die Stimmzettel oder die Wahlgeräte bekannt. Für

Kommunalwahlen wählt das Hessische Statistische Landesamt repräsentative Wahlbezirke für Wahlstatistiken aus.

§ 3 WStatG

Die Auswahl der Stichprobenwahlbezirke und der Stichprobenbriefwahlbezirke trifft der Bundeswahlleiter im Einvernehmen mit den Landeswahlleitern und den statistischen Ämtern der Länder. Es dürfen nicht mehr als jeweils fünf vom Hundert der Wahlbezirke und der Briefwahlbezirke des Bundesgebietes und nicht mehr als jeweils zehn vom Hundert der Wahlbezirke und der Briefwahlbezirke eines Landes an den Statistiken nach § 2 teilnehmen. Ein für die Statistiken nach § 2 Abs. 1 ausgewählter Wahlbezirk muss mindestens 400 Wahlberechtigte, ein für die Statistik nach § 2 Abs. 1 Buchstabe b ausgewählter Briefwahlbezirk mindestens 400 Wähler umfassen. Für die Auswahl der Stichprobenbriefwahlbezirke ist auf die Zahl der Wähler abzustellen, die bei der vorangegangenen Bundestags- oder Europawahl ihre Stimme durch Briefwahl abgegeben haben. Die Wahlberechtigten sind in geeigneter Weise darauf hinzuweisen, dass der Wahlbezirk oder der Briefwahlbezirk in eine repräsentative Wahlstatistik einbezogen wird.

Für die Bundestagswahl sind nach § 2 Abs. 2 WStatG auch Briefwahlbezirke in die Statistik einzubeziehen. Es dürfen nach § 3 WStatG nicht mehr als fünf Prozent der Wahlbezirke und der Briefwahlbezirke des Bundesgebietes an den Statistiken teilnehmen. Darüber hinaus müssen die ausgewählten Wahlbezirke mindestens 400 Wähler umfassen. Hierbei wird auf die Zahl der Wähler der vorangegangenen Bundestagswahl abgestellt. Die Regelungen in der Landeswahlordnung und im Hessischen Kommunalwahlgesetz sind entsprechend.

Ich habe die Anfragenden darüber informiert, dass die Verwendung der gekennzeichneten Stimmzettel datenschutzrechtlich nicht zu beanstanden ist, da aufgrund der Vorgabe der gesetzlichen Regelungen zur Mindestzahl der betroffenen Wähler je Wahlkreis das Wahlgeheimnis gewahrt bleibt.

7. Sonstige Selbstverwaltungskörperschaften

7.1 Hochschulen

7.1.1

Datenschutzrechtliche Fragen bei der Privatisierung des Universitätsklinikums Gießen und Marburg

Als Hessischer Datenschutzbeauftragter habe ich die Aufgabe, die Privatisierung des Universitätsklinikums Gießen und Marburg zu begleiten und darauf zu dringen, dass die datenschutzrechtlichen Rahmenbedingungen bei dem Verfahren eingehalten werden. Diese Aufgabe kann ich allerdings nur wahrnehmen, wenn mir die Informationen zu dem von der Landesregierung angestrebten Verfahren umfassend und rechtzeitig zur Verfügung gestellt werden. Leider war dies in den vergangenen Monaten nicht der Fall. Es ist dadurch auch zu Verstößen gegen das Datenschutzrecht gekommen.

2004 hat die Landesregierung beschlossen, die Universitätskliniken Gießen und Marburg zu einer gemeinsamen Anstalt des öffentlichen Rechts zusammenzuführen und das dann entstandene Universitätsklinikum Gießen und Marburg in die Trägerschaft eines privaten Krankenhausbetreibers zu überführen. Mit dem Gesetz über die Errichtung des Universitätsklinikums Gießen und Marburg (UK-Gesetz vom 16. Juni 2005, GVBl. I Nr. 14, 432) wurde der erste Schritt vollzogen. Die neue Anstalt des öffentlichen Rechts mit dem Namen „Universitätsklinikum Gießen und Marburg“ arbeitet mit den nicht fusionierten Fachbereichen Medizin der beiden Universitäten Gießen und Marburg zusammen. Mit dem Gesetzentwurf zur Änderung des Gesetzes für die hessischen Universitätskliniken und anderer hessischer Vorschriften wird eine Optimierung des Zusammenwirkens zwischen den Universitätskliniken und der Universität und eine Sicherung der Belange von Forschung und Lehre bei einem wirtschaftlich geführten Universitätsklinikum in privater Rechtsform angestrebt. Eine von der Landesregierung eingesetzte Steuerungsgruppe unter Vorsitz des Hessischen Ministeriums für Wissenschaft und Kunst befasst sich mit den weiteren Änderungen der gesetzlichen Regelungen und der Ausgestaltung eines strukturierten Bieterverfahrens. Geplant ist eine Überführung des Universitätsklinikums in eine gemeinnützige GmbH zum 1. Januar 2006 und ein darauf folgender Verkauf von 95 % der Anteile der GmbH an einen privaten Partner.

Für die Durchführung des Bieterverfahrens wurden eine Anwaltskanzlei und eine Wirtschaftsprüfungsgesellschaft eingeschaltet. Die Wirtschaftsprüfungsgesellschaft wurde mit der Einrichtung eines so genannten Datenraums beauftragt, in dem sich potenzielle Erwerber über das Universitätsklinikum informieren können. In einer der Arbeitsgruppensitzungen sicherten mir das Hessische Ministerium für Wissenschaft und Kunst und die beteiligten Unternehmen ausdrücklich meine frühzeitige Beteiligung zu.

Zwischen den von der Landesregierung beauftragten Anwälten und mir wurde im Juli 2005 vereinbart, dass mit mir abgestimmt wird, welche Unterlagen der Wirtschaftsprüfungsgesellschaft für die Einrichtung des so genannten Datenraums übergeben werden, damit die Einhaltung der datenschutzrechtlichen Vorschriften sichergestellt ist.

In der Folgezeit wurde jedoch weder von der Anwaltskanzlei noch von der Wirtschaftsprüfungsgesellschaft wieder Kontakt mit meinem Hause aufgenommen. Nachdem ich zufällig über Dritte erfahren hatte, dass der Datenraum bereits eingerichtet und den potenziellen Erwerbern zur Verfügung gestellt wurde, haben meine Mitarbeiter sofort am 31. August in dem bei der Wirtschaftsprüfungsgesellschaft eingerichteten Datenraum eine Prüfung durchgeführt. Dabei stellte sich heraus, dass in den Unterlagen personenbezogene Personaldaten enthalten waren, deren Weitergabe an die potenziellen Erwerber rechtlich unzulässig und für das Verfahren auch offensichtlich nicht in personenbezogener Form notwendig war. Abschließend wurde am 31. August mit der Vertreterin der Anwaltskanzlei und dem Vertreter der Wirtschaftsprüfungsgesellschaft vereinbart, dass ich vor Einrichtung eines so genannten erweiterten Datenraumes für die Endphase des Bieterverfahrens rechtzeitig informiert werde und Gelegenheit erhalte, die Unterlagen vor einer Terminvergabe für die potenziellen Erwerber überprüfen zu können. Am 1. September frühmorgens wurde dann eine Mitarbeiterin meiner Dienststelle telefonisch von der Anwaltskanzlei darüber unterrichtet, dass am 2. September der so genannte erweiterte Datenraum (mit zusätzlichen 14 Ordnern Datenmaterial) einem potenziellen Erwerber zur Verfügung gestellt werden soll. Mir wurde angeboten, die Unterlagen vorher in Frankfurt (Sitz der Wirtschaftsprüfungsgesellschaft) oder Wiesbaden zu überprüfen. Ein Mitarbeiter von mir ist daraufhin sofort nach Frankfurt gefahren mit dem Ergebnis, dass erneut Verstöße festgestellt wurden. Es liegt auf der Hand, dass diese Verfahrensweise keine angemessene Form der Einbeziehung des Hessischen Datenschutzbeauftragten darstellt.

Dies habe ich gegenüber der Landesregierung kritisiert. Die von mir geforderte Stellungnahme liegt noch nicht vor. Im weiteren Verfahren wurde mein Haus nicht beteiligt.

Auch nach erfolgtem Verkauf bleibt es bei der Zuständigkeit des Hessischen Datenschutzbeauftragten gemäß § 24 HDSG, da keine vollständige materielle Privatisierung erfolgt. Insbesondere bleibt die alleinige Verantwortung für alle Belange von Forschung und Lehre bei Land, Universität und Fakultät. Das privatisierte Universitätsklinikum soll u. a. mit der Aufgabe der Unterstützung der Fachbereiche bei der Aufgabenerfüllung in Forschung und Lehre beliehen werden und es muss sich im Rahmen der Krankenversorgung an den Erfordernissen von Forschung und Lehre ausrichten. Es liegt auch ein öffentlicher Daseinsvorsorgeauftrag vor (vgl. die eingehenden Ausführungen dazu im 33. Tätigkeitsbericht, Ziff. 2.1.1 und in diesem Tätigkeitsbericht, Ziff. 2.1.2.3).

7.1.2

Anwendung der IT-Sicherheitsleitlinie des Landes auf die Hochschulen

Die IT-Sicherheitsleitlinie der Landesregierung soll auch den IT-Sicherheitsstand in hessischen Hochschulen verbessern.

Die im Staatsanzeiger 2004, S. 3829 veröffentlichte IT-Sicherheitsleitlinie habe ich im 33. Tätigkeitsbericht, Ziff. 8.2.1 näher erläutert. Sie gilt zunächst nur für die Behörden der Landesverwaltung. Da die hessischen Hochschulen nur in geringen Bereichen (z. B. Liegenschaftsverwaltung) Teile der Landesverwaltung darstellen, im Übrigen aber als Körperschaften des öffentlichen Rechts rechtlich selbstständig sind, war die Frage zu klären, in welchem Umfang die Leitlinie auch für die Hochschulverwaltung gelten sollte. Das Hessische Ministerium für Wissenschaft und Kunst hat gegenüber den Hochschulen durch Erlass vom 23. Mai 2005 die Auffassung vertreten, wegen des allgemeinen Grundsatzes der Einheitlichkeit der Verwaltung sollte die IT-Sicherheitsleitlinie für alle Bereiche der Hochschulverwaltung gelten. Deshalb liegt es nun auch bei den Hochschulen, die einzelnen Forderungen aus dieser Leitlinie konkret umzusetzen.

Im Mittelpunkt stehen dabei zwei zentrale Punkte:

– **Bestellung eines IT-Sicherheitsbeauftragten**

Gemäß Ziff. 5.2 der Sicherheitsrichtlinie muss jede Hochschule neben dem nach § 5 Abs. 1 HDSG notwendigen Datenschutzbeauftragten einen IT-Sicherheitsbeauftragten bestellen.

– **Erstellung eines Sicherheitskonzeptes**

Gemäß Ziff. 4.1 der Sicherheitsrichtlinie muss jede Hochschule ein eigenes Sicherheitskonzept vorweisen können. Dieses Konzept umfasst die gesamte Hochschulverwaltung. Soweit einzelne Fachbereiche und/oder Abteilungen schon Teilkonzepte haben, müssen diese in das Gesamtkonzept integriert werden.

Als Reaktion auf den Erlass haben einige Hochschulen bereits Arbeitsgruppen gebildet, die sich mit dem Thema IT-Sicherheit beschäftigen und deren Aufgabe die Erarbeitung des IT-Sicherheitskonzeptes ist. Mitglieder dieser Arbeitsgruppen sind der IT-Sicherheitsbeauftragte, der Datenschutzbeauftragte und der Leiter des Hochschulrechenzentrums.

Es bleibt zu hoffen, dass diese Konzept-Erstellung zügig voranschreitet, um baldmöglichst die IT-Sicherheitslage an den hessischen Hochschulen wirksam zu verbessern.

7.2 Sparkassen

7.2.1

Prüfung der Netzwerksicherheit bei Sparkassen

Die in zwölf hessischen Sparkassen überprüften Computernetzwerke hatten jeweils ein hohes Sicherheitsniveau.

Im Jahr 2005 haben meine Mitarbeiter in zwölf hessischen Sparkassen die Sicherheit der Computernetzwerke überprüft. Gravierende Mängel konnten nicht festgestellt werden. Im Gegenteil: Die überprüften Netzwerke wiesen ausnahmslos einen hohen Sicherheitsstandard auf.

7.2.1.1

Prüfungsvorbereitung und -verlauf

Den Prüfungen ging eine Meinungsverschiedenheit mit dem Sparkassen- und Giroverband Hessen-Thüringen voraus. Der Verband war der Ansicht, dass den Hessischen Datenschutzbeauftragten eine Schadensersatzpflicht treffe, sollten die Prüfungen zu Netzwerkstörungen führen und daraus Schäden entstehen. Ich habe demgegenüber deutlich gemacht, dass für von meinen Mitarbeitern bei Prüfungen verursachte Schäden eine Schadensersatzpflicht des Landes Hessen lediglich im Rahmen der allgemeinen Grundsätze des Staatshaftungsrechts in Betracht kommt.

In Vorgesprächen mit dem Sparkassen- und Giroverband Hessen-Thüringen und der Sparkasseninformatik GmbH & Co KG (SI) wurden zunächst die Netzwerkstruktur und die Zuständigkeiten für die einzelnen Abschnitte des Sparkassennetzwerks geklärt. Die SI betreibt das so genannte Primärnetz, das der Anbindung der einzelnen Kreditinstitute an die zentralen Anwendungen, die im Wege der Auftragsdatenverarbeitung ebenfalls von der SI an verschiedenen Standorten in Deutschland bereitgestellt werden, dient. Die so genannten Sekundärnetze der einzelnen Sparkassen werden entweder noch in Eigenregie betrieben oder von der SI verwaltet. In jedem Fall hat die SI die Sparkassen vertraglich verpflichtet, bei allen am Netz angeschlossenen Komponenten bestimmte sicherheitsrelevante Standards einzuhalten.

Da zunächst die Netzwerksicherheit in den Sparkassen überprüft werden sollte, beschränkten sich die Prüfungen auf die Sekundärnetze. Die Auswahl der Sparkassen erfolgte nach repräsentativen Gesichtspunkten.

In den zentralen Vorgesprächen wurden auch einige Eckpunkte zum Prüfungsablauf festgelegt, um sicherzustellen, dass die Prüfung den Geschäftsbetrieb nicht mehr als unvermeidbar beeinträchtigte. Der sich daraus abzeichnende Prüfungsablauf wurde den ausgewählten Instituten im Rahmen individueller Vorbereitungsstermine dargestellt. Diese Termine wurden auch dazu genutzt, die notwendigen Informationen über die Netzwerkdetails der einzelnen Häuser und deren Serverlandschaft zu gewinnen. Durch diese Vorgehensweise war es möglich, die Prüfungen jeweils auf einen Tag zu begrenzen und trotzdem einen aussagefähigen Querschnitt an Komponenten zu prüfen. Bei den insgesamt zwölf Terminen kam es erfreulicherweise auch nur zu

einer einzigen Serverstörung, bei der die Anwendungssoftware durch den Portscan unmittelbar zum Absturz gebracht wurde.

Bei der von meinen Mitarbeitern eingesetzten Prüfsoftware handelte es sich um ein Instrument zur automatisierten Schwachstellenanalyse (vgl. 30. Tätigkeitsbericht, Ziff. 14.5 und 32. Tätigkeitsbericht, Ziff. 19.3). Damit können die Systemeinstellungen verschiedener Betriebssysteme und aktiver Netzwerkkomponenten ermittelt und die TCP/IP-Ports überprüft werden. Bei der Parametrisierung der einzelnen Prüfläufe wurde auf die Option, die es erlaubt Angriffe auf Systeme zu simulieren, bewusst verzichtet, um auch im Interesse der Sparkassenkunden den Betrieb nicht zu gefährden.

7.2.1.2

Ergebnisse

Auch wenn keine gravierenden Mängel bei den geprüften Netzwerkkomponenten festgestellt werden konnten, so waren doch einige wiederkehrende Defizite zu verzeichnen:

7.2.1.2.1

Nullsessions

Die so genannte „Nullsession“ (auch „anonymer Zugriff“ genannt) bietet bei Windows-Betriebssystemen die Möglichkeit, anonym, d. h. ohne Authentifizierung durch Domäne, Benutzername und Passwort auf einige Bereiche eines Windows-Systems lesend zuzugreifen. Dies sind im Wesentlichen eine Liste der Benutzer- und Gruppennamen, die Netzwerkfreigaben und die Systemregistrierung. Hierüber lassen sich auf einfache Art und Weise Informationen über ein Windows-System, das über ein Netzwerk erreichbar ist, beschaffen.

Durch Deaktivieren des anonymen Zugriffs lassen sich diese Informationen vor potenziellen Angreifern auf einfache Weise verbergen, was in den neueren Windows-Versionen (Windows 2003) auch standardmäßig der Fall ist.

Bei älteren, kritischen Systemen sollte der anonyme Zugriff daher nach ausgiebigem Test aller Anwendungen nachträglich deaktiviert werden.

7.2.1.2.2

Installation nicht benötigter Komponenten

Teilweise wurden auf den untersuchten Systemen installierte Dienste und Anwendungen vorgefunden, die für den täglichen Betrieb nicht benötigt werden. Dies gilt besonders für mit dem Betriebssystem Windows 2000 betriebene Server, da dieses Betriebssystem grundsätzlich alle Dienste und Anwendungen installiert und der Administrator alle nicht benötigten Komponenten nachträglich manuell deinstallieren muss.

Da permanent neue Schwachstellen bei Anwendungen und Diensten festgestellt werden, gilt die generelle Aussage, dass jede überflüssige Applikation ein potenzielles Einfallstor für Angreifer darstellt und daher unverzüglich entfernt werden sollte.

7.2.1.2.3

Patch-Management

Sofern die Möglichkeit eines zentralen Patch-Managements besteht (Windows-Anwendungen: SMS, SUS, WSUS, weitere Anwendungen von Drittanbietern) sollte diese auch genutzt werden.

Dies beinhaltet selbstverständlich einen Test der Anwendungen vor dem Rollout der Patchpakete.

7.2.1.2.4

Berechtigungen

Grundsätzlich gilt, dass für Ordner und Netzwerkfreigaben nur die Berechtigungen vergeben werden sollen, die für den ordnungsgemäßen Betrieb nötig sind. Dies gilt besonders nach dem Ausscheiden von Mitarbeitern und Änderungen in der Organisation.

Beachtet werden sollte, dass die Berechtigungen entweder auf Ordner- oder Freigabeebene gesetzt werden, da ansonsten die Fehlersuche bei Zugriffsproblemen erschwert wird.

7.2.1.2.5

Administrative Gruppen

Neben den Gruppen „Administratoren“ und „Domänen-Admins“ gibt es weitere Gruppen mit sicherheitskritischen Funktionen, die periodisch auf Aktualität geprüft werden sollten: Dies sind die Konten- und Sicherungsoperatoren. Kontenoperatoren haben im Bereich der Benutzerverwaltung erweiterte Rechte, Sicherungsoperatoren im Rahmen des Dateizugriffs bei der Sicherung.

7.2.1.2.6

SNMP

SNMP stellt ein wichtiges Protokoll zur Netzwerküberwachung dar. Da die Sicherheit dieses Protokolls nur auf den so genannten „Community-Namen“ basiert, sollten die im Protokoll selbst standardmäßig implementierten Communities „public“ (Lesezugriff auf die SNMP-Informationen) und „private“ (Schreibzugriff auf die SNMP-Informationen) durch eigene, nicht zu triviale Community-Namen ersetzt werden.

Ferner sollte der Zugriff auf die SNMP-Informationen über Zugriffskontrolllisten (ACL) und Firewall-Einstellungen auf die nötigen Mitarbeiter bzw. Systeme beschränkt werden.

7.2.1.2.7

TCP/IP

Die Windows-Programme „Traceroute“ und „ping“ stellen eine wichtige Komponente des ICMP-Protokolls dar und sind für den Betrieb eines Netzwerks und die Fehlersuche unerlässlich.

Gleichwohl lassen sich über diese Befehle wesentliche Netzwerkinformationen beschaffen: Der Befehl „ping“ prüft die generelle Erreichbarkeit eines Systems im Netzwerk. Da die

Antwortpakete unter anderem einen Zeitstempel enthalten, lässt sich somit die Systemzeit dieses Systems ermitteln, welche einen Ansatzpunkt für zeitbasierte Kryptographie-Komponenten (Kerberos) darstellen kann.

„Traceroute“ dient ebenfalls der Überprüfung der Erreichbarkeit, hier werden zusätzlich noch die Netzwerkknoten, die auf dem Weg zum Zielsystem passiert werden, aufgelistet. Damit lassen sich wertvolle Informationen über die Topologie eines Netzwerks gewinnen.

Es ist daher zu empfehlen, ICMP nur auf das lokale Netzwerk zu beschränken und ICMP-Zugriffe nach/von außerhalb des lokalen Netzes auf geeignete Weise zu reglementieren (Paketfilter, Firewall).

7.2.1.2.8

TCP/IP-Dienste

Auf fast allen untersuchten Windows NT-Systemen fanden sich die so genannten „Einfachen TCP/IP-Dienste“, eine Sammlung von Netzwerkdiensten (z. B. „echo“ und „chargen“).

Für diese Dienste gilt das zu Ziff. 7.2.1.2.2 Gesagte: Sofern sie nicht benötigt werden, sollten sie deinstalliert werden.

7.2.1.2.9

Netzwerkdienste Oracle-Datenbanken

Datenbanken stellen einen wesentlichen Teil ihrer Funktionalität im Netzwerk bereit. Bei den untersuchten Oracle-Datenbanken wurde festgestellt, dass der Dienst „TNS-Listener“ ohne Passwort zugänglich war. Damit waren unter bestimmten Voraussetzungen DoS-Angriffe auf die Datenbank möglich, was insbesondere unter dem Gesichtspunkt der Verfügbarkeit ein Problem darstellt.

DoS-Angriffe

Massenhafte, teilweise unsinnige Anfragen an den Server, die zum Stillstand der Anwendung oder des Servers bzw. zum Absturz des Servers führen.

Da sich dieser Dienst auf einfache Weise über eine Passwort-Authentifizierung absichern lässt, sollte dies auch umgesetzt werden.

7.2.1.2.10

Microsoft SQL-Server

Bereits vor ca. zwei Jahren wurde publiziert, dass die Installation des Microsoft SQL-Servers in seiner damaligen Fassung ein wesentliches Problem beinhaltet: Die Installationsroutine ließ es seinerzeit zu, dem administrativen Benutzer „sa“ (System Attendant) kein Passwort zuzuweisen (dies ist bei den aktuellen SQL-Server-Versionen nicht mehr möglich).

Problematisch ist vor allem, dass dieses Sicherheitsproblem vor allem bei älteren Installationen mittlerweile im wahrsten Sinne des Wortes „vergessen“ wurde. Trotz des Bekanntmachens dieser Schwachstelle wurden noch einige SQL-Server-Installationen aufgefunden, deren Benutzer „sa“ ohne Passwortschutz war.

Sofern daher ältere MS SQL-Server-Installationen im Netz vorhanden sind, sollte diese Einstellung unverzüglich überprüft werden.

7.2.1.2.11

Dokumentation

Besonders dann, wenn eine Anzahl von netzwerkfähigen Eigenentwicklungen in einem Netzwerk betrieben wird, ist eine Dokumentation dieser Komponenten unerlässlich. In der heutigen Zeit umfasst die Masse der Schadsoftware trojanische Pferde und Backdoor-Programme, die Verbindungen zu fremden Server aufnehmen, um Informationen von den befallenen Rechnern dorthin zu übertragen. Selbst wenn die für die Übertragung verwendeten Ports an Netzübergängen durch eine Firewall blockiert werden, hilft eine Liste der im lokalen Netz zulässigen Ports (inkl.

der Server, die die Dienste bereitstellen und ggf. der Clients, die diese Dienste legitim nutzen dürfen) Anomalien im Netzwerkverkehr aufzuspüren und zu beseitigen.

7.2.1.2.12

Sonstige Feststellungen

Im Rahmen der Prüfung wurden zwei weitere Problemfelder von grundsätzlicher Bedeutung untersucht: DNS-Zonenübertragung und SMTP-Relaying.

Zonenübertragung ist der Austausch von Informationen zwischen DNS-Servern (Domain Name System). DNS stellt einen wesentlichen Eckpfeiler der TCP/IP-Kommunikation dar, es ist deshalb unerlässlich DNS-Informationen (so genannte Zonen) aus Gründen der Ausfallsicherheit mehrfach vorzuhalten. Die Zonen-Informationen werden auf einem primären Server gepflegt und bei Änderung an die sekundären Server übertragen; dies wird als Zonenübertragung (oder Zonentransfer) bezeichnet. Standardmäßig reglementiert ein DNS-Server diesen Transfer nicht, d. h. jeder, der die zur Initialisierung notwendigen Befehle kennt, kann diese von einem DNS-Server abrufen. Da diese Zoneneinträge – analog zu den Ausführungen im Punkt 7 – wesentliche Informationen eines Netzwerks darstellen, sollte die Berechtigung für Zonenübertragungen über die Einstellungen des DNS-Servers reglementiert werden.

SMTP-Relaying (Weiterleitung) ist eine Grundeinstellung aller Mailserver. Sofern diese Einstellung am Server nicht geändert wird, kann über einen solchen Server eine Nachricht mit jeder beliebigen Absenderadresse an jeden beliebigen Empfänger versandt werden. Dies ist einer der Gründe, warum Spam im heutigen Internet eine solche Bedeutung hat: Sofern das Weiterleiten auf einem Server eingeschränkt ist, ist es nur noch möglich eine Mail über diesen Server zu transportieren, wenn entweder der Absender oder der Empfänger ein Benutzer auf dem System ist.

Die Einstellungen des lokalen Mailservers sollten dahingehend überprüft werden und – falls möglich – sollte diese Weiterleitungsmöglichkeit deaktiviert werden.

8. Entwicklungen und Empfehlungen im Bereich der Technik und Organisation

8.1

Sachstand zur Zentralisierung der IT

In diesem Jahr habe ich mit der Landesverwaltung weitere Schritte vereinbart, um potenzielle Sicherheitsrisiken strikt zentraler IT-Architekturen in den Griff zu bekommen.

In meinem 32. Tätigkeitsbericht habe ich die Probleme beschrieben, die sich aus meiner Sicht für eine IT-Architektur ergeben, bei der alle Daten zentral gespeichert werden sollen. Dieser Ansatz wird für die Hessische Landesverwaltung z. B. für ein Dokumentenmanagementsystem (DMS) verfolgt, welches Auslöser für die Diskussion war. Ergänzend ist eine Terminalserver-Architektur eingeführt bzw. geplant; d. h. die Benutzer bearbeiten die Daten, ohne dass die Dateien auf den Arbeitsplatzrechner übertragen werden. Die Technik wird in Richtung Web-basierter Zugriffe fortentwickelt.

Bei der Diskussion mit der Landesverwaltung über die Konsequenzen aus diesen Planungen wurde schnell klar, dass es unterschiedliche Sichten auf ein und denselben Sachverhalt gibt. In einem Workshop wurde Mitte des Jahres versucht, einvernehmlich die Probleme zu beschreiben, sie zu bewerten und von beiden Seiten akzeptierte Lösungswege zu erarbeiten. Dies ist weitgehend gelungen. Die wesentlichen Ergebnisse des Dialogs stellen sich wie folgt dar:

8.1.1

Übergreifende Aspekte

Das Konzept, die IT in Hessen zu zentralisieren, habe ich nicht prinzipiell in Frage gestellt. Dieser Ansatz und die Maßnahmen, eine ausreichende Verfügbarkeit zu gewährleisten, sind in erster Linie eine politische Entscheidung. Aus datenschutzrechtlicher Sicht sind aber die Gefahren des Zugriffs durch unbefugte Dritte auf die Daten zu betrachten und die Prinzipien der Erforderlichkeit, der informationellen Gewaltenteilung und der Differenzierung von sensiblen und weniger sensiblen Daten anzuwenden.

8.1.2

Verschlüsselung

Um die unbefugte Kenntnisnahme durch Dritte, zu denen auch die Mitarbeiter eines Dienstleisters zählen können, zu kontrollieren, bietet sich die Verschlüsselung an.

Es wurde folgender Konsens erzielt:

1. Eine Verschlüsselung der Daten ist nicht obligatorisch.
Es gibt Daten, die zentral unverschlüsselt gespeichert werden können.
2. Die Dienststellen erhalten die Option, die aus ihrer fachlichen Sicht sensiblen Daten oder Daten, die aus datenschutzrechtlichen Gesichtspunkten ein hohes Schutzbedürfnis tragen,
 - unter einen spezifischen Zugriffsschutz zu stellen und
 - zu verschlüsseln oder lokal zu speichern.

Ich habe meine Beratung angeboten, wenn Dienststellen Fragen bezüglich der Einschätzung der Kritikalität von Daten haben.

3. Es sollen Maßnahmen vorgesehen werden, die die Dienststellen zu Punkt 2 unterstützen.

Es wurde festgestellt, dass Produkte verfügbar sind, mit denen die o. g. Anforderungen erfüllt werden können und festgelegt, diesen Aspekt unter Berücksichtigung der organisatorischen Gesichtspunkte weiter zu vertiefen und mit dem Ziel zu verfolgen, geeignete Produkte zu finden.

8.1.3

Signatur

Zum Thema Signatur wurden zwei Aspekte vertieft diskutiert:

- Freischaltung des Windows-Log-on und der fortgeschrittenen Signatur mit der gleichen PIN
Es bestand Konsens, dass durch die Nutzung der gleichen PIN sowohl zur Anmeldung als auch zur Freischaltung der fortgeschrittenen Signatur Probleme auftreten, die im Widerspruch zu den Anforderungen des Signaturgesetzes stehen.

Es sollen Vorstöße sowohl in Richtung auf die Hersteller als auch den Gesetzgeber unternommen werden, um bessere Rahmenbedingungen zur Nutzung einer Smartcard sowohl für ein Single-Sign-On (SSO) als auch für die Erstellung fortgeschrittener Signaturen zu schaffen.

Das Thema konnte nicht abschließend behandelt werden, insbesondere konnte das Problem der Freischaltung von zwei Zertifikaten mit einer PIN nicht gelöst werden. Da weiterer Klärungsbedarf besteht, wird der Dialog fortgesetzt.

- Erstellung der Signatur in einer Windows-Terminal-System-Umgebung
Dieser Punkt konnte nicht geklärt werden. Ich bin mit der Landesregierung im Gespräch, um eine einvernehmliche Lösung zu finden.

8.1.4

Dokumentenmanagementsystem

Es waren noch nicht alle Fragen und zukünftigen Fragestellungen erkennbar. Entsprechend müssen Lösungen noch entwickelt werden. Bei dem schrittweisen Herangehen an dieses Thema wurden die Punkte Verschlüsselung und Recherche- und Leserecht betrachtet:

- Der Punkt Verschlüsselung war bereits als übergeordnete Fragestellung behandelt.
- Bei der Einführung in den Ministerien bleibt es den Häusern und der Diskussion mit den jeweiligen behördlichen Datenschutzbeauftragten überlassen, die besonders schützenswerten Datenbereiche zu definieren und von der Übernahme in das DMS oder von der Recherche auszunehmen. Von zentraler Stelle soll dazu eine Hilfestellung gegeben werden. Dabei soll beachtet werden, dass es besonders schützenswerte Daten aus der Sicht des Datenschutzes und aus fachlicher Sicht gibt.
- Zum Punkt Recherche- und Leserecht wurde für die Einführung eines DMS im nachgeordneten Bereich eine prozessorientierte Vorgehensweise vereinbart, um prozessindividuell die Vergabe von differenzierten Zugriffsrechten auf Daten der nachgeordneten Behörde im Rahmen der Dienstobliegenheiten festzulegen. Es bestand Konsens, dass es keine generelle Zugriffsberechtigung auf Daten nachgeordneter Behörden

geben darf.

Als besonders sensibel sind insbesondere die Bereiche Personal, Steuern, Polizei und Staatsanwaltschaft zu betrachten.

8.1.5

Stand Ende des Jahres

Die Absichtserklärungen der Tagung waren ermutigend. Leider liegen weitergehende Ergebnisse noch nicht in dem Umfang vor, wie es alle Beteiligten gehofft hatten. Aus Zeitmangel oder anderen Gründen konnten die vereinbarten Schritte noch nicht oder erst mit einiger Verspätung ergriffen werden. Das Fraunhofer SIT sollte hinsichtlich der Verschlüsselung eine Marktanalyse vornehmen, um potenziell geeignete Produkte zu finden und ihre Eignung unter den Hessischen Rahmenbedingungen zu untersuchen. Bei Redaktionsschluss lag ein Angebot vor. Der Auftrag war jedoch noch nicht vergeben.

Ich werde in den verschiedenen Projekten darauf achten, dass nur solche Daten verarbeitet werden, für die auch die erforderlichen technischen Voraussetzungen bezüglich der Speicherung und Signatur vorhanden sind.

8.2

Sachstand zur Einführung eines Dokumentenmanagementsystems in der Hessischen Landesverwaltung

Die Einführung eines einheitlichen Dokumentenmanagementsystems in der Hessischen Landesverwaltung ist komplex und schwierig, insbesondere gilt es eine Vielzahl datenschutzrechtlicher Probleme zu bewältigen. In die Problembewältigung bin ich frühzeitig eingebunden, so dass die datenschutzrechtliche Beratung und die antizipierende Kontrolle ineinander fließen.

8.2.1

Allgemeines

Die Hessische Landesregierung hat im Jahr 2003 beschlossen, für die Landesverwaltung ein Dokumentenmanagementsystem (DMS) flächendeckend in Hessen einzuführen. Von mehreren zur Auswahl stehenden Produkten fiel die Wahl auf das Produkt DOMEA der Firma Opentext.

Das DMS ist Kernelement aller E-Government-Projekte des Landes und eine der großen Projektdomänen neben NVS, Portal und HCN2004. In den unterschiedlichen Projekten müssen die Schnittstellen zu den verschiedenen Projektdomänen berücksichtigt werden. Hierbei handelt es sich um ein komplexes technisches Umfeld.

8.2.2

Einführungsstrategie in Stufen

Die Einführung von DOMEA erfolgt in mehreren Stufen:

- Umstellung der Poststellen und Registraturen
(Einscannen und registratorische Erfassung der eingehenden Post)
- Sachbearbeitung
- Workflow und Archivierung der Unterlagen.

Zunächst soll DOMEA in den Ministerien, später auch in den nachgeordneten Behörden eingeführt werden.

8.2.3

Vorabkontrolle

§ 7 Abs. 6 HDSG verlangt für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung eine gutachtliche Bewertung der einzelnen Gefahren für das informationelle Selbstbestimmungsrecht unter den Aspekten der rechtlichen Zulässigkeit sowie der technischen und organisatorischen Datensicherheit (Vorabkontrolle). Durchzuführen ist die

Vorabkontrolle von demjenigen, der für den Einsatz oder die wesentliche Änderung des Verfahrens zuständig ist. DOMEA soll in den Ressorts landeseinheitlich eingeführt werden. Die Konzeption und die Gesamtsteuerung dieser Einführung liegt beim Hessischen Ministerium des Innern und für Sport. Gleichwohl bleiben die Ressorts aber für ihren Bereich die nach dem Hessischen Datenschutzgesetz verantwortlichen Daten verarbeitenden Stellen. Bei der Konzeption der Vorabkontrolle in § 7 Abs. 6 HDSG waren solche Szenarien, wie sie bei landeseinheitlichen Verfahren oder bei Entscheidung des Ressorts für den nachgeordneten Bereich häufig anzutreffen sind, bereits absehbar. Deshalb trifft die Pflicht zur Erstellung der Vorabkontrolle denjenigen, der für den Einsatz zuständig (nicht verantwortlich) ist. Insoweit das Hessische Innenministerium zentrale Vorgaben für den Einsatz des Verfahrens macht, hat es folglich auch die Vorabkontrolle zu erstellen. Ähnlich wie bei den gemeinsamen Verfahren nach § 15 HDSG den Federführer trifft das Innenministerium hier die Pflicht, die Vorabkontrolle durchzuführen, sofern sie nicht durch Detailvorgaben der jeweiligen Ressorts für ihren Bereich ergänzt werden muss. Dies wurde mit der Erstellung eines **Musters** für die jeweilige Stufe bewältigt, in dem die generellen Vorgaben behandelt und die von den Ressorts zu ergänzenden Angaben gekennzeichnet sind, die jeweils in die Schlussbewertung einzubeziehen sind. Dieses Muster gibt den Rahmen für die einzelnen Ressorts, überlässt es ihnen aber, die bei ihnen jeweils zu bewertenden Gefahren und die Gegenmaßnahmen detailliert im Rahmen ihrer eigenen Ergänzung zu beschreiben. Außerdem müssen die Ressorts, soweit die einzelnen Einführungsschritte die dort vorhandene IT-Sicherheitsstruktur verändern, ihr eigenes nach § 10 Abs. 2 HDSG und Nr. 5.2 der IT-Sicherheitsleitlinie notwendiges Sicherheitskonzept fortschreiben. Die Muster der Vorabkontrolle der einzelnen Einführungsschritte stimmt das Hessische Ministerium des Innern und für Sport wegen der zahlreichen, teils neuen datenschutzrechtlichen Fragestellungen mit mir ab.

8.2.4

Sachstand

8.2.4.1

Einscannen und registratorische Erfassung der eingehenden Post

Aus datenschutzrechtlicher Sicht galt es, schon in dieser Phase die besonderen Anforderungen des HDSG an eine umfassende automatisierte Dokumentenerfassung zu berücksichtigen; zahlreiche materiellrechtliche und IT-sicherheitstechnische Fragen waren zu lösen.

Bei der Erfassung von Dokumenten in einem Dokumentenmanagementsystem sind Datenschutzbestimmungen zu berücksichtigen, weil personenbezogene Daten verarbeitet werden. Diese sind bei den meisten Dokumenten in Form von Anschriften darüber hinaus ggf. aber auch in den Dokumenteninhalten enthalten. Wie bei jeder Verarbeitung personenbezogener Daten ist deshalb auch hier zu beachten, dass diese Daten nur von Berechtigten und zu den Zwecken verarbeitet werden dürfen, für die sie erhoben wurden bzw. zulässigerweise weiterverarbeitet werden dürfen. Deshalb sind spezifische Vorkehrungen gegen unbefugte Kenntnisnahme und Verfälschung zur Gewährleistung der technischen und organisatorischen Datensicherheit nach § 10 HDSG sowie zur Wahrung ihrer Zweckbestimmung nach § 13 HDSG erforderlich. Beim Einscannen musste technisch sichergestellt werden, dass Vertraulichkeit und Integrität der Daten gewährleistet wird. Aus meinem Haus wurde daher die Forderung erhoben, die Daten verschlüsselt an die HZD zu übertragen; dies gilt sowohl direkt nach dem Einscannen als auch für den Abruf der Daten durch den Registrator. Dieser Forderung wurde Rechnung getragen.

Bereits im November 2004 wurde mir die Muster-Vorabkontrolle für diese erste Phase der DOMEA-Einführung (Einscannen und registratorische Erfassung der eingehenden Post) vorgelegt, die dann den Ressorts zur Übernahme und ressortspezifischen Ergänzungen überlassen wurde.

Ein wichtiger Punkt der ressortspezifischen Festlegungen in dieser Phase war - ausgehend von einer Analyse der typischerweise anfallenden Dokumente im jeweiligen Ressort - die Festlegung, welche Art von Dokumenten der eingehenden Post nicht eingescannt werden dürfen. Dazu zählen Dokumente, für die ein Verbot der automatisierten Verarbeitung besteht. In diese von jedem Ressort verbindlich aufzustellende Liste (sog. Negativliste) waren - ausgehend davon, dass die derzeit im Landeskonzept für DOMEA vorgesehenen technischen und organisatorischen Maßnahmen die datenschutzrechtlichen Anforderungen nur für Dokumente mit einfachem bis mittlerem Schutzbedarf abdecken - auch Dokumente aufzunehmen, die einen höheren Schutzbedarf haben.

Dazu zählen z. B.

- Unterlagen, die Personalakten zuzuordnen sind,
- Verschlussachen,
- Unterlagen mit besonders hoher Sensibilität.

Die nach dem bisherigen Stand zu erwartenden Dokumente lassen weit überwiegend Arten und Mengen personenbezogener Daten erwarten, die einen mittleren Schutzbedarf erfordern. Höherer Schutzbedarf besteht z. B. für Unterlagen mit Personalaktenbezug. Deshalb habe ich gefordert, diese auszunehmen oder sie zusätzlich gegen unbefugte Kenntnisnahme abzusichern, z.B. durch Verschlüsselung bei der Speicherung. Z. Zt. ist eine solche Verschlüsselung noch nicht vorgesehen. Der Vorschlag, das Fraunhofer Institut mit der Untersuchung der Verschlüsselungsmöglichkeiten zu betrauen, wie er zwischen mir und der Projektleitung E-Government vereinbart wurde, war bis Redaktionsschluss noch nicht umgesetzt. Unter günstigen Umständen ist Mitte nächsten Jahres mit Ergebnissen zu rechnen.

Die derzeit erstellte Vorabkontrolle bezieht sich ausschließlich auf die Einbeziehung von Dokumenten einfachen und mittleren Schutzbedarfs in DOMEA. Sollen künftig auch Dokumente mit sensibleren personenbezogenen Daten im Dokumentenmanagementsystem verwaltet werden, so ist zunächst eine darauf bezogene, spezifische Vorabkontrolle durchzuführen, die die rechtlichen Voraussetzungen, Risiken, Maßnahmen beschreibt und bewertet.

Die Ressorts begannen ab November sukzessive damit, die Poststellen und die Registraturen umzustellen und die Post einzuscannen. Aufgrund von technischen Problemen kam es bei der Umstellung zu einer Verzögerung von einem halben Jahr. Die eingescannten Dokumente konnten nicht ordnungsgemäß den verschiedenen Ministerien zugeordnet werden. Der Fehler wurde behoben und die Umstellung war Ende August abgeschlossen.

8.2.4.2

Sachbearbeitung

Die zweite Phase der DOMEA-Einführung ermöglicht den automatisierten Zugriff auf die bereits eingescannten Dokumente im Rahmen der Sachbearbeitung (sog. Sachbearbeiterclient)

Die zunächst notwendige Vorabkontrolle wurde im Berichtsjahr insoweit vorbereitet, als - unter meiner Mitwirkung - das Hessische Innenministerium wiederum eine Muster-Vorabkontrolle erstellte, die den Ressorts dann zur weiteren Ergänzung und Änderung überlassen werden wird.

Die praktische Einführung dieser 2. Phase soll - nach einem Probelauf - im Jahr 2006 erfolgen. Für die Testphase mit Echtdateien habe ich - da die Vorkontrolle noch nicht abschließend vorlag - der Gesamt-Projektleitung verschiedene datenschutzrechtliche Rahmenbedingungen vorgegeben.

Die wegen der Komplexität des Verfahrens umfangreiche Vorabkontrolle widmet sich einer Fülle von materiellrechtlichen und datensicherheitstechnischen Einzelfragen und Bewertungen.

Wegen der weit reichenden praktischen Bedeutung seien hier folgende Punkte herausgegriffen:

– **Rollen- und Berechtigungskonzept**

Der Sachbearbeiterclient ermöglicht einen komfortablen Umgang mit allen eingescannten Unterlagen innerhalb der Verwaltungsarbeit. Zunächst soll er aber nur die Abläufe ersetzen, die nach bewährten organisatorischen Grundsätzen für die Papierakte gelten. Insoweit war zu gewährleisten, dass der lesende und schreibende Zugriff auf die jeweils für die Sachbearbeitung erforderlichen Dokumente beschränkt wird. Das der Vorabkontrolle zugrunde liegende technische Berechtigungskonzept stellt dieses mit der Erstellung eines individuellen Nutzungsprofils eines jeden Bediensteten sicher, es ermöglicht aber auch die schnelle automatisierte Datenweitergabe im Rahmen der notwendigen Beteiligung anderer am Vorgang, etwa im Rahmen der Mitzeichnung oder der Stellvertretung.

Das erstellte Muster-Berechtigungskonzept des jeweiligen Ressorts ist den eigenen Organisationsplan anzupassen; dieses war im Berichtsjahr noch nicht abgeschlossen. Soweit das Rollen- und Berechtigungskonzept nicht auf technischen Voreinstellungen, sondern auf organisatorischen Vorgaben beruht, erfordert die notwendige Beschränkung der Zugriffe auf den datenschutzrechtlich zulässigen Umfang eine entsprechende Schulung der Bediensteten. Dies habe ich als ausdrückliche Voraussetzung für den Einsatz gefordert.

– **Recherche**

Ein in der Verwaltungspraxis willkommener Vorteil eines DMS-Systems wie DOMEA wird in der Möglichkeit gesehen, automatisiert in dem vorhandenen Datenbestand des Ressorts über Stichworte und Metadaten nach bestimmten Dokumenten und Informationen zu recherchieren. Bedenkenlos ist die Recherchemöglichkeit bei Dokumenten, die überhaupt keinen Personenbezug haben. Bei Dokumenten mit personenbezogenen Daten darf diese technische Möglichkeit jedoch nicht das zentrale datenschutzrechtliche Prinzip der Erforderlichkeit faktisch unterlaufen, wonach ein Dokument nur lesen darf, wer es für seine

Sachbearbeitung tatsächlich auch benötigt. Deshalb ist das Rechercherecht programmtechnisch beschränkt auf das Leserrecht des einzelnen Bediensteten.

Über den geäußerten Wunsch, das Rechercherecht wegen vielseitiger Bedürfnisse zu erweitern, wird im Jahr 2006 entschieden. Nachgedacht wird sowohl über eine Volltextrecherche, die datenschutzrechtlich wegen der personenbezogenen Inhaltsdaten des Dokumentes hinsichtlich der Berechtigungen restriktiver zu handhaben ist, als auch über eine sog. Metadatenrecherche. Diese ermöglicht über die Eingabe von Metadaten das Auffinden von gesuchten Dokumenten durch Angabe der sie kennzeichnenden Metadaten, ohne ihren Inhalt zu öffnen. Es gibt aus der Verwaltungspraxis berechnete Anforderungen, Recherchen auch über den Kreis der unmittelbar mit der Bearbeitung eines Vorgangs befassten Beschäftigten hinaus zuzulassen. Wie bereits erläutert, sind die Recherchemöglichkeiten für alle Bediensteten bei Dokumenten, die überhaupt keinen Personenbezug haben unkritisch; datenschutzrechtlich betrachtet werden nur Dokumente mit Personenbezug. Eine Volltextrecherche kann über den Kreis der berechtigten Bediensteten hinaus datenschutzrechtlich nicht zugelassen werden. Bei der Metadatenrecherche werden dagegen weniger Daten offenbart und sie lässt ein gestuftes Konzept der Recherche und der anschließenden Einzelfallprüfung durch den zuständigen Bediensteten zu, ob ein berechtigter Zugriff eröffnet werden kann. Der möglichen Eröffnung einer Metadatenrecherche ist bereits im vorliegenden Konzept durch die Auflage Rechnung getragen, dass sensible Informationen in die jeweiligen Metadaten nicht aufgenommen werden dürfen. Die technische Umsetzung einer übergreifenden Metadatenrecherche kann frühestens mit dem übernächsten Release (08/2006) erfolgen.

8.3

Probleme der Passwortverwaltung in Rechenzentren

Eine der zentralen Maßnahmen, um die IT-Sicherheit zu gewährleisten, ist eine sichere Anmeldeprozedur. Sie basiert heute meist noch auf geheimen Passwörtern. Um nicht große Sicherheitslücken zu schaffen und Unbefugten den Zugang zu eröffnen, sind für das Zurücksetzen von Passwörtern strikte Regelungen von Anwendern und Rechenzentren zu beachten.

8.3.1

Der Fall

Der Datenschutzbeauftragte eines Rechenzentrums hat mich gefragt, wie man das Zurücksetzen von Passwörtern datenschutzgerecht organisiert. Auslöser war ein Fall, in dem der Sachbearbeiter einer Kommune am Telefon der Hotline mitteilte, dass er sein Passwort vergessen habe und man es ihm zurücksetzen solle. Der zuständige Rechenzentrumsmitarbeiter bat im Gespräch um ein Fax, in dem dies bestätigt wird. Daraufhin nahm der vor Ort anwesende Bürgermeister das Telefon zur Hand und äußerte sich sehr lautstark und fordernd. Er war der Meinung, dass es kein Problem sein könne, sofort und ohne irgendwelche Formulare zu reagieren.

Da sehr oft Unverständnis oder Unmut über die vom Rechenzentrum geforderten Abläufe geäußert wurden, wurde überlegt, wie sie geändert werden können, ohne die IT-Sicherheit oder den Datenschutz zu gefährden.

8.3.2

Die Ausgangslage

Die IT-Landschaft hat sich in den letzten Jahren gewandelt. Nachdem eine Entwicklung von Rechenzentren mit einem Großrechner zu dezentralen Strukturen durchlaufen ist, findet jetzt wieder eine Rezentralisierung statt. Es handelt sich in der Regel um eine IT-Architektur, bei der im Zentrum viele Server, also Rechner, stehen. Während der ganzen Zeit hat es aber Verfahren gegeben, die durch die Rechenzentren betrieben wurden. Es gab und gibt eine ganz klare Tendenz, dass immer mehr Benutzer online auf zentrale Verfahren und Ressourcen zugreifen. Damit einher geht neben anderen ein technisch organisatorisches Problem, das mich seit längerer Zeit beschäftigt:

Obwohl es andere, bessere Möglichkeiten gibt um sicherzustellen, dass nur zugelassene Personen als Benutzer mit einem IT-System oder Verfahren arbeiten können (vgl. 30. Tätigkeitsbericht, Ziff. 14), wird meist mit Benutzererkennung und Passwort gearbeitet. Die Anforderungen an Passwörter und deren Verwaltung habe ich in mehreren meiner Tätigkeitsberichte beschrieben. Sie stimmen mit den Vorgaben überein, die das Bundesamt für Sicherheit in der Informationstechnik

im Grundschutzhandbuch formuliert hat. Ein praktisches Problem ist dabei die Aufforderung, Passwörter nicht aufzuschreiben aber nach einer Zeitdauer von etwa 30 bis 90 Tagen zu wechseln. Sie führt dazu, dass regelmäßig Passwörter vergessen werden. Vergisst der Benutzer sein Passwort, muss es zurückgesetzt werden. An dieser Stelle beginnt das Problem, wenn in einem Rechenzentrum hunderte oder tausende Personen als berechnigte Benutzer registriert sind. Das Problem lässt sich durch folgende Fragen umreißen:

- Wie stelle ich fest, ob die Person, die die Zurücksetzung wünscht, auch die ist, der die Benutzerkennung zugeordnet ist?
Da die Benutzer nicht arbeiten können solange sie kein neues Passwort haben, soll die Prüfung meist sofort und unbürokratisch erfolgen.
- Wie teile ich das neue Passwort so mit, dass Unbefugte es nicht zur Kenntnis bekommen?
- Wie dokumentiere ich diesen Vorgang?

Die vorhandene Technik und die vertraglichen Grundlagen bilden dabei einen Rahmen.

8.3.3

Lösungsansätze

Wie erkenne ich die Person?

Wenn es technisch möglich ist, die Funktion Passwörter zurückzusetzen nicht nur zentral, sondern stattdessen unmittelbar durch die Vor-Ort-Betreuung in einer kleineren Organisationseinheit vorzunehmen, sollte davon Gebrauch gemacht werden. Die Größe der Organisationseinheit sollte so überschaubar sein, dass ein Betreuer vor Ort die möglichen Benutzer an der Stimme erkennt und somit die erste Frage selbst beantworten kann.

Wenn der Auftraggeber diese Funktion nicht übernehmen will, muss das Rechenzentrum sie übernehmen. Das gilt auch, wenn die Technik nicht geeignet ist die Funktion zu dezentralisieren.

Die Sicherheitsanforderungen an die Prozedur beim Zurücksetzen eines Passwortes unterscheiden sich auf den ersten Blick nicht von denen beim Anlegen einer Benutzerkennung. Es kommt eine Mitteilung an, wonach eine Kennung angelegt werden soll bzw. ein Passwort zurückgesetzt werden soll. Diese Anfrage muss verifiziert werden. Im Vertrag oder in Konzepten wird für das

Anlegen in vielen Fällen ein Formular bereitgehalten, das von einem berechtigten Vertreter des Kunden unterschrieben werden muss. Analog gibt es bei Eingaben per E-Mail die Möglichkeit zu fordern, dass diese elektronisch signiert sind; diese Technik ist aber erst selten am Arbeitsplatz verfügbar.

Im Unterschied zum erstmaligen Anlegen einer Benutzererkennung ist die Grundsatzentscheidung, dass die betreffende Person für das System berechtigt ist, bereits gefallen und zudem muss sofort gehandelt werden. Der Mitarbeiter benötigt in der Regel umgehend ein neues Passwort, damit er überhaupt arbeiten kann.

Eine formularunterstützte Abarbeitung der Zurücksetzung des Passwortes ist aus verschiedenen Gründen problematisch: Zum einen ist der Unterzeichner des Formulars oft nicht sofort greifbar. Im Regelfall müssen Betroffene also selbst die Mitteilung absenden können. Selbst wenn sie E-Mails signieren können, hilft das nicht immer weiter. Falls es sich um das Passwort zur Anmeldung am System handelt, steht das Mailsystem der betroffenen Person gar nicht zur Verfügung.

Als Lösung wird daher meist ein Ablauf favorisiert, bei dem das Zurücksetzen telefonisch angefordert werden kann. Am Telefon bereitet es den Rechenzentrumsbefragten aber Probleme, Gesprächspartner zu identifizieren, wenn sie für hunderte oder tausende Kundenmitarbeiter oder -mitarbeiterinnen zuständig sind. Die wesentliche Frage ist also, wie man Telefonpartner identifizieren kann, die man nicht persönlich kennt.

Als erste Maßnahme kann mit einer hinterlegten Telefonnummer der Bedienstete des Kunden direkt oder über eine Zentrale zurückgerufen werden. Wie im Internet gebräuchlich, kann zusätzlich eine oder besser mehrere Kontrollfragen mit einem Bezug zu Betroffenen und deren – nicht offensichtlichen – Antworten hinterlegt sein. Diese Fragen müssen am Telefon richtig beantwortet werden. Ein weiterer Ansatz benutzt ein biometrisches Sprechererkennungsverfahren; d. h. durch Technik wird der Gesprächspartner an der Stimme erkannt. Dabei muss der Anrufer bestimmte Wörter sprechen. Wenn ihn das System identifiziert hat, wird das Passwort zurückgesetzt.

Für beide Lösungen muss das System mit Informationen gefüttert werden. Dies kann am sinnvollsten beim Anlegen einer Benutzererkennung erfolgen. Im ersten Fall werden die besonderen

Fragen und Antworten des Mitarbeiters mitgegeben. Dabei sollten Fragen, wie nach dem Deutschen Fußballmeister, vermieden werden, deren Antwort im Lexikon stehen. Im zweiten Fall wird z. B. eine temporäre Kennung mitgegeben, unter der der Mitarbeiter Sprechproben gegenüber dem System abgeben kann.

Wie wird das Passwort bekannt gegeben?

Handelt es sich nicht um das Passwort zur Anmeldung am System, so kann es per E-Mail, soweit verfügbar, zugestellt werden. Ansonsten könnte es am Telefon gesagt werden oder in einem verschlossenen Umschlag ähnlich wie ein PIN-Brief direkt oder über den örtlichen Ansprechpartner ausgegeben werden. Der letzte Ansatz hat dabei die aus praktischer Sicht immer wieder angeführten Nachteile, dass er höhere Kosten verursacht und die Laufzeit in der Regel zu lang ist. In der Praxis wird es die Regel sein, dass das Passwort am Telefon gesagt wird. Das Passwort muss dann bei der ersten Anmeldung geändert werden.

Was wird protokolliert?

Selbstverständlich muss das Rechenzentrum alle Fälle mit Datum und Uhrzeit dokumentieren, in denen das Passwort zurückgesetzt wurde. Dies wird oft im Rahmen einer umfassenderen Kundenbetreuung geschehen, weshalb auch die Tätigkeit selbst und die Art des Kontakts erfasst werden müssen. Außerdem sollte der Mitarbeiter und ggf. der Auftraggeber informiert werden, damit Unregelmäßigkeiten erkannt werden können. Wenn die Passwörter dezentral verwaltet werden, müssen die Abläufe ebenfalls protokolliert werden.

8.3.4

Fazit

Wie leicht zu erkennen ist, sind die möglichen Verfahren aufwändig zu organisieren. Von den Benutzern werden sie oft als Hindernis, wenn nicht sogar als Schikane empfunden. Gerade an dieser Stelle müssen aber adäquate Maßnahmen ergriffen werden, damit die

Sicherheitsvorkehrungen nach § 10 HDSG nicht mit einfachen Mitteln überwunden werden können.

8.4

Telearbeitsplätze in der Hessischen Landesverwaltung

Die Überprüfungen von Telearbeitsplätzen in drei obersten Landesbehörden ergaben ein unterschiedliches Bild. Teils war die Vereinbarung zur Einführung alternierender Telearbeit vorbildlich umgesetzt. Teils müssen aus datenschutzrechtlicher Sicht Nachbesserungen vorgenommen werden.

Die Hessische Landesregierung hat im Jahr 2003 einen Kriterienkatalog zur Einführung der alternierenden Telearbeit erstellt, an dessen Erarbeitung ich beteiligt war (StAnz. 2003, S. 2748). Ich habe darüber ausführlich in meinem 32. Tätigkeitsbericht berichtet (Ziff. 2.1). In diesem Zusammenhang hatte ich angekündigt, dass ich beabsichtige, an einigen Arbeitsplätzen die korrekte Umsetzung dieser Kriterien zu prüfen. Dies habe ich im vergangenen Berichtszeitraum in die Tat umgesetzt.

Überprüft wurden Telearbeitsplätze in drei obersten Landesbehörden. Dabei wurden zunächst die technischen Vorgaben mit den für die Telearbeit verantwortlichen Bediensteten erörtert und dann im Gespräch mit den Telearbeitenden die Details ihrer Arbeit am häuslichen Arbeitsplatz besprochen und überprüft. Thematisiert wurden sowohl technische Schwierigkeiten, räumliche Sicherheitsmaßnahmen als auch organisatorische Fragestellungen. Um ein möglichst einheitliches Bild zu erlangen, habe ich die Überprüfung an Hand eines Fragenkatalogs (s. Abb. 2) durchgeführt.

Die Überprüfung ergab kein einheitliches Bild. Gemeinsam war allerdings allen überprüften Telearbeitsplätzen, dass keine aus datenschutzrechtlicher Sicht „brisanten“ Daten verarbeitet wurden, was nach dem Wortlaut des Kriterienkatalogs durchaus auch möglich wäre.

Abb. 2

Fragen und Anforderungen an Telearbeiterinnen und Telearbeiter

		Zutreffendes bitte nachfolgend ankreuzen	Ja	Nein	z.T.
1. Allgemeines					
1.1	Verlief die Telearbeit für Sie problemlos?				
1.1.1	<u>Technik</u> Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	<u>Abläufe</u> Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	<u>Sonstiges</u> Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Gab es Begehungen hinsichtlich				
1.2.1	<u>Arbeitsschutz</u> Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	<u>Gesundheitsschutz</u> Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	<u>Datenschutz</u> Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	<u>Datensicherheit</u> Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Sind Mitbewohner über die Zutrittsmöglichkeiten zu Kontrollzwecken informiert und haben diese akzeptiert? Erklärung:				
1.4	Waren Wartungs-, Einrichtungs- oder Reparaturarbeiten zu Hause bisher nicht nötig? Erklärung:				

1.5	Sind die Voraussetzungen des ursprünglichen Antrags auf Telearbeit noch gegeben? Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Wenn nein, wurden die Prüfungen erneut vorgenommen? (Ziff. 6.4 der Vereinbarung der Landesregierung) Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Arbeitsmittel					
2.1	Sind die Arbeitsmittel im Eigentum des Landes Hessen? Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ist eine Zugriffsschutzsoftware vorhanden? Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	
2.3	Findet eine private Nutzung nicht statt? Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Sind die Arbeitsmittel vor dem Zugriff durch Dritte geschützt? Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Wer hat Zugang zum Raum? Erklärung:				
2.4.2	Sind der Raum/die Möbel verschlossen? Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Sind weitere Maßnahmen ergriffen? Wenn ja, welche. Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Datenschutz „Vertrauliche Daten und Informationen gegenüber Dritten sind in der häuslichen Arbeitsstätte so zu schützen, dass ein unbefugter Zugriff zu und ein unberechtigter Zugriff auf die Daten wirksam verhindert wird ...“					
3.1	Wurden Sie über die einschlägigen Vorschriften informiert, die einzuhalten sind? Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	3.1.1	Umgang mit Pass- und Codewörtern Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	3.1.2	Prozeduren zur Benutzung von Netzen, Mailsystemen und Rechnern Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	3.1.3	Wo was zu speichern ist Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	3.1.4	Umgang mit dem „Papierkorb“ und temporären Dateien Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Dritte dürfen keinen Einblick in Dateien oder Akten erhalten. Wie gehen Sie vor?				
	3.2.1	Tägliches Arbeiten Erklärung:			
	3.2.2	Besuch Erklärung:			
	3.2.3	Feiern Erklärung:			
3.3	Besondere Aufmerksamkeit ist bei personenbezogenen und äußerst sensiblen Daten geboten; z.B. Personal-, Disziplinar-, Steuer- und Beihilfeangelegenheiten. Gehen Sie mit solchen Daten um? Erklärung:		<input type="checkbox"/>	<input type="checkbox"/>	
	3.3.1	Wenn ja, wo werden die Daten gespeichert? (Server in der Dienststelle, lokal auf dem Telearbeitsrechner, ...) Erklärung:			
	3.3.2	Bei lokaler Speicherung: Werden die Daten verschlüsselt gespeichert? Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Werden personenbezogene Daten verschlüsselt übertragen?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Erklärung:				
3.5	Für nicht elektronische Akten				
	3.5.1	Werden die Akten in einem verschließbaren Schrank aufbewahrt? Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	3.5.2	Erfolgt der Transport in verschlossenen Behältnissen? Erklärung:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8.4.1

Technische Ausstattung/Konfiguration

In allen Fällen handelte es sich um Rechner, die im Eigentum des Dienstherrn waren. Sie waren komplett ausgestattet; weder private Soft- noch Hardware wurden genutzt. Die drei Dienststellen hatten allerdings unterschiedlich Lösungsansätze bei der Ausgestaltung des Arbeitsplatzes. Eine Behörde setzte darauf, dass die Telearbeitenden sowohl zu Hause als auch in der Dienststelle am selben PC arbeiten und haben ihnen deshalb einen Laptop zur Verfügung gestellt, der jeweils von der Dienststelle nach Hause und wieder zurück zu transportieren ist. In einer anderen Lösung wurden Rechner bei den Bediensteten zu Hause fest installiert. In der Behörde stand ihnen ein weiterer Rechner zur Verfügung. Im dritten Fall erhielten die Bediensteten für den heimischen Arbeitsplatz einen Laptop zum dortigen Verbleib.

Alle Telearbeitsplätze waren mit Windows als Betriebssystem ausgerüstet. Die Benutzerrechte im System waren stark eingeschränkt, so dass keine Änderungen am Betriebssystem durch die Telearbeitenden vorgenommen werden konnten. USB- und andere Schnittstellen waren blockiert. Beispielsweise wäre ein Rechner bei Anschluss eines USB-Sticks automatisch heruntergefahren worden und hätte erst durch den Systemadministrator wieder gestartet werden können.

Es war in allen Fällen einheitliche Vorgabe, dass zu bearbeitende Daten grundsätzlich auf dem Server der Dienststelle abzulegen sind und nicht auf der Festplatte. Diese Vorgabe wurde dort durchbrochen, wo die Verbindung zur Dienststelle nicht über DSL, sondern ISDN hergestellt wurde; denn das Antwortzeitverhalten bei ISDN-Anschlüssen ließ bei der Arbeit mit großen Dateien stark zu wünschen übrig. Die Kommunikation mit der Dienststelle erfolgte in allen Fällen verschlüsselt über ein VPN (virtual private network) mit einem von der HZD angebotenen Verfahren, das den Vorgaben des Kriterienkatalogs der Landesregierung entspricht und dort als Standard vorgesehen ist.

Die Festplatten der genutzten Geräte waren bei einer Behörde verschlüsselt, in den beiden anderen geprüften Behörden unverschlüsselt. Der Verzicht auf eine Festplattenverschlüsselung traf auch auf die Lösung mit den hin und her zu transportierenden Laptops zu. Gerade vor dem Hintergrund, dass – wie oben beschrieben – auch Daten auf der Festplatte gespeichert werden, weil das Antwortzeitverhalten bei ISDN-Anschlüssen zu schlecht ist, kann der Transport der Daten ohne Verschlüsselung nicht akzeptiert werden. Die Gefahr, dass ein Laptop gestohlen wird, ist

vergleichsweise groß. Im Falle eines Diebstahls wäre dann ein Zugang zu den gespeicherten Daten möglich. Von der betroffenen Dienststelle wurde argumentiert, dass es Schwierigkeiten mit der Festplattenverschlüsselung gebe und man insoweit auf eine landeseinheitliche Lösung warte. Dieser Argumentation kann ich nicht folgen, da die Verschlüsselung der Festplatte bei dem ortsgelassenen Laptop an einem Telearbeitsplatz ohne Schwierigkeiten funktionierte. Ich habe insoweit Nachbesserung gefordert.

8.4.2

Zusätzliche Ergebnisse der Prüfungen vor Ort

In allen geprüften Fällen ergaben die räumlichen Gegebenheiten der Telearbeitsplätze keinen Grund zur Beanstandung. Es gab bei der Überprüfung der zur Verfügung gestellten Rechner keine Anhaltspunkte dafür, dass diese entgegen den Vorgaben privat genutzt werden. Auffällig war allerdings, dass in fast allen geprüften Fällen im „Papierkorb“ der Rechner teilweise monatealte Daten gespeichert waren, die zur Aufgabenerfüllung am Telearbeitsplatz nicht mehr erforderlich waren. Dabei handelte es sich teilweise um Daten, die nach den Anweisungen gerade nicht auf der Festplatte des Telearbeitsplatzes, sondern auf dem Server der Dienststelle gespeichert sein sollten. Ich habe in meinem Prüfbericht deshalb angeregt, die Telearbeitenden nochmals schriftlich darauf hinzuweisen, dass keine Daten im „Papierkorb“ gespeichert werden, sondern dieser in kurzen Zeitabständen geleert werden muss.

8.4.3

Fazit

Teilweise sind die Vorgaben aus dem Kriterienkatalog zur Einrichtung von Telearbeitsplätzen vorbildlich umgesetzt. In einem Fall sind aus meiner Sicht dringend Nachbesserungen bei den Datensicherungsmaßnahmen erforderlich. Dies habe ich den überprüften Dienststellen entsprechend mitgeteilt.

8.5

Orientierungshilfe „Datenschutz in drahtlosen Netzen“

Bereits im 31. Tätigkeitsbericht, Ziff. 12 habe ich mich ausführlich mit dem Thema „Mobile Computing“ beschäftigt. Da das Thema weiter an Aktualität gewonnen hat, wurde im Jahr 2004 auf meine Anregung vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe zu dieser Thematik erarbeitet. Sie beleuchtet neben technischen auch rechtliche Aspekte.

Der AK Technik hat gemeinsam mit dem AK Medien die Orientierungshilfe „Datenschutz in drahtlosen Netzen“ erarbeitet, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zustimmend zur Kenntnis genommen hat. Sie kann auf meiner Homepage unter der URL <http://www.datenschutz.hessen.de/o-hilfen/OHWLAN.pdf> abgerufen werden.

Die Orientierungshilfe richtet sich an behördliche Datenschutzbeauftragte, IT-Verantwortliche und Administratoren, die sich mit der Planung, dem Aufbau und dem Betrieb dieser Netze befassen.

Nähere Erläuterungen zu dem technischen Inhalt erfolgen unter Ziff. 8.5.1 und zu den rechtlichen Aspekten unter Ziff. 8.5.2.

8.5.1

Technische Aspekte

Die Orientierungshilfe beschreibt verschiedene Technologien der drahtlosen Kommunikation, gibt einen Überblick über mögliche Gefährdungen bei der Nutzung von drahtlosen Netzen und beschreibt die aus technischer Sicht erforderlichen und geeigneten Schutzmaßnahmen.

Folgende Themen werden dort im Einzelnen behandelt:

In **Kapitel 2** wird auf Wireless Local Area Networks (WLAN) eingegangen. Diese Art von drahtlosen Netzen hat sich in vielen Bereichen etabliert. WLAN sind leicht zu installieren und die

erforderlichen Sicherheitsmechanismen zum Schutz von sensiblen personenbezogenen Daten stehen in neueren WLAN-Komponenten zum größten Teil bereits standardmäßig zur Verfügung.

Bluetooth ist ein Industriestandard für drahtlose Vernetzung von Geräten. Er bietet eine drahtlose Schnittstelle, über die sowohl Kleingeräte wie Mobiltelefone und PDAS als auch Computer und Peripheriegeräte miteinander kommunizieren können. Bereits im 31. Tätigkeitsbericht, Ziff. 12.1.1.2.2 habe ich mich zu den datenschutzrechtlichen Fragen des Einsatzes dieser Technologie geäußert. Das **Kapitel 3** der Orientierungshilfe setzt sich weiterführend mit den Gefährdungen und den Risiken bei der Nutzung von Bluetooth-Netzen auseinander und gibt Empfehlungen zum datenschutzgerechten Einsatz.

Eine weitere Möglichkeit Daten auszutauschen ist die Nutzung einer Infrarotschnittstelle. Diese wird in **Kapitel 4** näher erläutert. Im Vergleich zu WLAN und Bluetooth-Netzen erfolgt der Datenaustausch nur über kurze Distanzen.

Kapitel 5 beschreibt mögliche Gefährdungen und Schutzmaßnahmen, die beim Einsatz mobiler Endgeräte, wie z. B. Tastaturen, Mäusen und Personal Digital Assistants zu berücksichtigen sind.

Im **Kapitel 6** werden allgemein gültige Sicherheitsmaßnahmen (u. a. Firewall, Verschlüsselung, Virenschutz) beschrieben, die grundsätzlich in allen Funknetzen umgesetzt werden können.

8.5.2

Rechtliche Aspekte

Welche datenschutzrechtlichen Anforderungen beim Einsatz mobiler Netze (WLAN, Bluetooth, Infrarotschnittstellen usw.) zu beachten sind, hängt in erster Linie nicht von der Technik ab, sondern von ihrem Zweck und der Umgebung, in der sie eingesetzt werden.

Beim Einsatz von WLAN lassen sich zwei Konstellationen unterscheiden, die jeweils unterschiedliche datenschutzrechtliche Auswirkungen haben:

- Für die öffentliche Nutzung bestimmte WLAN-Zugänge (Hot Spots), z. B. in Flughäfen, Bahnhöfen, Messe- und Kongresszentren, aber auch Hotels usw. oder

- für eine geschlossene Benutzergruppe bestimmte (betriebs- oder behördeninterne) WLAN, z. B. innerhalb von Unternehmen, Krankenhäusern, Universitäten, Behördenstandorten.

8.5.2.1

Hot Spots

Betreibt eine Stelle einen WLAN-Zugang, der jedem zur Verfügung steht, der sich im Wirkungsbereich des Zugangs befindet und der nicht ausschließlich für eine geschlossene Benutzergruppe gedacht ist, so betreibt sie einen Telekommunikationsdienst für die Öffentlichkeit. Zudem handelt es sich um geschäftsmäßiges Erbringen von Telekommunikation i. S. v. § 3 Nr. 10 TKG. Hierfür reicht das nachhaltige, also nicht nur vorübergehende Angebot aus. Auf Kostenpflichtigkeit oder Gewinnerzielungsabsicht kommt es nicht an. Dies bedeutet, dass sowohl das Fernmeldegeheimnis als auch die datenschutzrechtlichen Vorschriften der §§ 88 ff. TKG gelten. Als Anbieter von Telekommunikationsdiensten für die Öffentlichkeit kommen auf den Betreiber des Access Points außerdem weit reichende Pflichten zur Wahrung der öffentlichen Sicherheit nach den §§ 108 ff. TKG zu.

Der drahtlose Übertragungsweg dient hauptsächlich der Internetkommunikation. Somit wird der Betreiber des Access Points zum Zugangsdienstanbieter, der u. a. IP-Adressen an die Nutzerrechner vergibt. Da § 2 Abs. 2 Nr. 3 TDG Angebote zur Nutzung des Internets ausdrücklich als Teledienst definiert, sind die TCP- und IP-Ebene bereits zur Dienstebene zu zählen. Der Betreiber des Access Points erbringt demnach nicht nur einen Telekommunikations-, sondern auch einen Teledienst. Er hat daher zusätzlich die Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) zu beachten.

Aus eher technischer Sicht wird allerdings die Meinung vertreten, dass TCP/IP-Übertragung noch zur so genannten Transportebene zu rechnen sei und es sich damit um Telekommunikation i. S. v. § 3 Nr. 22 TKG handle. Erst auf höheren Schichten (insbesondere http) sei von einem Teledienst auszugehen. Nach dieser Auffassung wären nur die datenschutzrechtlichen Vorschriften des Telekommunikationsrechts anzuwenden.

8.5.2.1.1

Pflichten nach dem TKG

Der Anbieter eines Access Points für die Öffentlichkeit hat eine Reihe von Anforderungen zu erfüllen:

- Anbieter haben das Fernmeldegeheimnis (§ 88 TKG) zu wahren. Diesem unterliegt nicht nur der Inhalt der Kommunikation, sondern auch deren näheren Umstände (wer hat wann wie lange mit wem kommuniziert). Nur in Ausnahmefällen dürfen sich Anbieter Kenntnis vom Inhalt und den näheren Umständen der Telekommunikation verschaffen und haben dabei eine strikte Zweckbindung zu beachten.
- Anbieter drahtloser Kommunikation dürfen Bestandsdaten der Nutzer nach § 95 TKG nur verarbeiten, wenn dies im Rahmen eines Vertragsverhältnisses erforderlich ist. Werden Hot Spots für WLAN-Zugänge beispielsweise auf einem Flughafen kostenfrei oder auf Prepaid-Basis bereitgestellt, erfordern die vertraglichen Beziehungen zum Anbieter in der Regel keine Kenntnis irgendwelcher vertraglicher Daten. Bestandsdaten dürfen dann nach § 95 TKG nicht erhoben werden. Eine Pflicht zur Bestandsdatenerhebung nach § 111 TKG (Kundenverzeichnis für Auskunftersuchen der Sicherheitsbehörden) besteht hier generell nicht, da der Betreiber des Hot Spots keine Rufnummern vergibt.
- Verkehrsdaten darf der Anbieter nur unter den Voraussetzungen des § 96 TKG verarbeiten. Zu diesen Daten zählen IP-Adressen, Beginn und Ende der Nutzung nach Datum und Uhrzeit, Datenmengen, Standortinformationen. Die Daten sind nach Beendigung der Verbindung unverzüglich zu löschen, es sei denn, sie sind zu Abrechnungszwecken, zur Erstellung von Einzelverbindungsnachweisen, zur Bekämpfung von Störungen und Missbrauch der Anlagen und Dienste oder zum Mitteilen ankommender Verbindungen erforderlich.
- Ob und welche Daten für Abrechnungszwecke i. S. v. § 97 TKG erforderlich sind, hängt davon ab, ob eine Abrechnung stattfindet und wenn ja, welches Abrechnungsverfahren gewählt wurde. Aus datenschutzrechtlicher Sicht sind Verfahren auf Guthabenbasis (Prepaid) zu bevorzugen, da diese wesentliche Vorteile im Hinblick auf Datenvermeidung und Datensparsamkeit besitzen.

- Standortdaten dürfen zur Bereitstellung standortbezogener (Mehrwert-)dienste (location based services) nach § 98 TKG nur mit Einwilligung des Nutzers verarbeitet werden.
- Der Anbieter hat nach § 109 TKG umfangreiche technische Maßnahmen zum Schutz des Fernmeldegeheimnisses sowie gegen unerlaubte Zugriffe zu treffen. Hierzu gehört z. B. der Einsatz von Verschlüsselungsverfahren. Die Maßnahmen haben sich nach dem Stand der Technik zu richten und müssen in einem angemessenen Verhältnis zum Schutzbedarf stehen.
- Als Anbieter eines Telekommunikationsdienstes für die Öffentlichkeit ist der Betreiber des Access Points verpflichtet, die in § 109 Abs. 2 und 3 TKG beschriebenen weiteren technischen und organisatorischen Maßnahmen einzuhalten; u. a. ist ein Sicherheitsbeauftragter zu bestellen und es ist ein Sicherheitskonzept zu erstellen.
- Wer ein drahtloses Netz für die Öffentlichkeit betreibt, ist nach § 110 TKG grundsätzlich verpflichtet, auf eigene Kosten Maßnahmen zur Umsetzung staatlicher Überwachungsmaßnahmen zu treffen. Inwieweit der Verordnungsgeber von der Ermächtigung in § 110 Abs. 2 lit. c TKG Gebrauch macht, aus Gründen der Verhältnismäßigkeit auf die genannte Verpflichtung zu verzichten, ist noch offen.

8.5.2.1.2

Pflichten nach dem TDDSG

Da die Bereitstellung eines Access Points für drahtlose Internetzugänge auch ein Teledienst ist, sind neben den Vorschriften des TKG auch die datenschutzrechtlichen Bestimmungen des TDDSG zu beachten.

Auch für die Pflichten nach dem TDDSG ergeben sich gegenüber der drahtgebundenen Kommunikation keine rechtlich relevanten Unterschiede:

- Die zulässige Erhebung von Bestandsdaten richtet sich nach § 5 TDDSG. Hier gilt entsprechend das oben zu § 95 TKG Gesagte.

- Nutzungsdaten über die Inanspruchnahme des Dienstes sind entsprechend § 6 Abs. 4 TDDSG nach Ende der Nutzung grundsätzlich zu löschen, wenn sie nicht für Abrechnungszwecke erforderlich sind (zur Protokollierung s. u.).
- Der Anbieter hat die in § 4 Abs. 4 TDDSG vorgeschriebenen technischen und organisatorischen Vorkehrungen zu treffen:
 - Möglichkeiten zum jederzeitigen Abbruch der Verbindung
 - Möglichkeit der Löschung von Nutzungsdaten
 - Sicherung der Vertraulichkeit.
- Der Grundsatz der Datenvermeidung und Datensparsamkeit ist zu beachten. Es sind - soweit technisch möglich und zumutbar - anonyme und pseudonyme Nutzungsmöglichkeiten zu schaffen (§ 4 Abs. 6 TDDSG).

8.5.2.1.3

Protokollierung von Verkehrs- und Nutzungsdaten

Strittig ist, in welchem Umfang bei der Inanspruchnahme von Informations- und Kommunikationsdiensten personenbezogene Verkehrs- oder Nutzungsdaten gespeichert werden dürfen.

Eine regelmäßige automatische Speicherung personenbezogener Protokolldaten ist zunächst an § 96 TKG und § 6 TDDSG zu messen. Entscheidend ist, ob die Daten zu Abrechnungszwecken erforderlich sind. Ist dies nicht der Fall, sind personenbezogene Log-Files grundsätzlich nach Ende der Verbindung unverzüglich zu löschen (§ 96 Abs. 2 Satz 2 TKG, § 6 Abs. 4 TDDSG).

Welche Daten bei der Erbringung kostenpflichtiger Dienste erforderlich sind, hängt vom Bezahlverfahren ab. Für Abrechnungszwecke dürfte eine Speicherung von IP-Adressen in der Regel nicht erforderlich sein. Die Radius-Server authentifizieren die Nutzer anhand der Nutzerkennung und des Passwortes. Zudem können Zeitpunkt der An- und Abmeldung protokolliert werden. Dies dürfte für die Abrechnung der Nutzung in der Regel ausreichen.

Eine regelmäßige Speicherung der IP-Adressen kann außerdem als Datensicherheitsmaßnahme gestützt auf § 109 TKG und § 10 HDSG in Betracht kommen. Diese Auffassung ist allerdings unter den Datenschutzkontrollbehörden umstritten.

8.5.2.2

WLAN für geschlossene Benutzergruppe

Die drahtlose Übertragungstechnik mittels WLAN wird in der Praxis zunehmend zur Erleichterung der internen Kommunikation innerhalb von Betrieben oder Behörden eingesetzt. Dabei haben nur Nutzer innerhalb einer definierten Nutzergruppe (in der Regel die Beschäftigten des Betriebes/der Behörde) einen Zugang zum Netzwerk. Die Technologie ermöglicht einen Verzicht auf aufwändige Verkabelung und kann die Kosten für betriebs- oder behördeninterne Netzwerke erheblich reduzieren. Dieses Einsatzszenario dürfte weitaus häufiger sein als die Bereitstellung von Access Points für die Öffentlichkeit.

Aus datenschutzrechtlicher Sicht sind beim betriebs- bzw. behördeninternen Einsatz von WLAN zwei Varianten zu unterscheiden, aus denen sich unterschiedliche rechtliche Folgen ergeben:

- Nutzung des Access Points ausschließlich für betriebliche bzw. dienstliche Zwecke erlaubt.
- Nutzung des Access Points für private und dienstliche Zwecke erlaubt.

8.5.2.2.1

Nutzung nur für dienstliche Zwecke

Ist die Nutzung des Access Points nur für dienstliche Zwecke erlaubt, ist die Stelle, die ihn betreibt, kein Anbieter im Sinne des Telekommunikations- oder Teledienstrechts. Es fehlt hier an dem von den gesetzlichen Bestimmungen vorausgesetzten Merkmal, dass es sich bei Anbieter und Nutzer um zwei verschiedene Rechtssubjekte handelt. Der Arbeitgeber oder Dienstherr stellt lediglich ein Arbeitsmittel zur Verfügung.

Er ist deshalb weder an das Fernmeldegeheimnis des TKG noch an die datenschutzrechtlichen Vorschriften des TKG bzw. des TDDSG gebunden, sondern muss lediglich die einschlägigen landesrechtlichen Vorschriften für Personaldatenverarbeitung beachten.

8.5.2.2.2

Nutzung für dienstliche und private Zwecke

Erlaubt der Betreiber des Access Points den Mitgliedern der geschlossenen Benutzergruppe auch die Nutzung für private Zwecke, erbringt er geschäftsmäßig Telekommunikationsdienste i. S. v. § 3 Nr. 10 TKG. In diesem Falle treten die Nutzer dem Anbieter (in der Regel ihrem Arbeitgeber) als Privatrechtssubjekte gegenüber, nicht in ihrer beruflichen bzw. dienstlichen Funktion als Beschäftigte. Es besteht also ein Anbieter-Nutzer-Verhältnis im Sinne des Telekommunikationsrechts. Wenn es sich zudem um ein nachhaltiges Angebot handelt, sind also die Voraussetzungen von § 3 Nr. 10 TKG erfüllt. Auf die Kostenpflichtigkeit kommt es nicht an.

Ebenso verhält es sich bei der erlaubten Nutzung des Access Points durch eine definierte Gruppe betriebs- oder behördenfremder Personen. Dies ist beispielsweise bei der Nutzung des WLAN durch Patienten eines Krankenhauses oder auch durch Gäste eines Hotels der Fall. Solange sich die Möglichkeit der Nutzung auf solche fest umrissenen Gruppen beschränkt, liegt ein zwar geschäftsmäßiges Erbringen, aber noch kein Angebot für die Öffentlichkeit vor.

Datenschutzrechtlich bedeutet dies, dass sowohl das Fernmeldegeheimnis als auch die datenschutzrechtlichen Vorschriften der §§ 88 ff. TKG und die Vorschriften des TDDSG anzuwenden sind. Das TKG enthält zwar einige wenige Erleichterungen für geschlossene Benutzergruppen, die jedoch für den Betrieb eines WLAN kaum relevant sind.

Pflichten, die ausschließlich für Anbieter, die Dienste für die Öffentlichkeit erbringen, gelten, spielen bei betriebs- oder behördeninternen WLAN keine Rolle. Die erhöhten Anforderungen zur Einhaltung technischer und organisatorischer Maßnahmen nach § 109 Abs. 2 und 3 TKG müssen daher nicht eingehalten werden. Anbieter behördeninterner WLAN sind auch nicht verpflichtet, auf eigene Kosten Vorkehrungen zur Überwachung der Kommunikation nach § 110 TKG zu treffen.

8.6

Voice over IP (VoIP) – weit mehr als Internet-Telefonie

Mit den aktuellen DSL-Angeboten der Internet-Provider wird häufig die Nutzung eines Freikontingentes zur Internet-Telefonie verbunden. Dabei ist zu bezweifeln, dass die Vertraulichkeit von derartigen Telefongesprächen i. S. d. Fernmeldegeheimnisses immer gewährleistet ist.

Mit ihrer Entschließung „Telefonieren mit Internet-Technologie (Voice over IP – VoIP)“ hat die 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (vgl. Ziff. 10.9) auf die besonderen Risiken hingewiesen, die mit dem Telefonieren über das Internet verbunden sind. Neben den verschiedenen Möglichkeiten, das Netz zu stören und sich Leistungen zu Lasten anderer zu erschleichen, stellt das Ausspähen von Kommunikationsverbindungen und -inhalten das größte Gefährdungspotenzial dar.

Unter deutlich anderen Blickwinkeln begleiten das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Bundesnetzagentur sowie die zuständigen Stellen der Europäischen Union die ausgeprägte Tendenz zur allgemeinen Nutzung der Sprachdatenübertragung über IP-basierte Netze. Während das BSI mit seiner Studie zur Sicherheit von Voice over Internet Protocol (VoIPSEC; <http://bsi.de/Literat/Studien/VoIP/index.htm>) den professionellen Anwendungsbereich der Technologie in den Vordergrund seiner Sicherheitsbetrachtungen stellt, sind die Bundesnetzagentur und die EU bemüht, dem Zukunftsmarkt eine freie Entwicklung zu ermöglichen und nur an unvermeidbaren Punkten regulierend einzugreifen. Die Bundesnetzagentur hat dazu die Ergebnisse einer umfangreichen Anhörung in einem Eckpunktepapier (<http://www.bundesnetzagentur.de/media/archive/3210.pdf> vom September 2005) zusammengefasst.

8.6.1

Was ist VoIP?

Genau genommen ist die Sprachdatenübertragung ein Spezialfall der Übertragung von Echtzeitverbindungen (Audio, Video oder zeitkritische Daten) in paketorientierten Transportnetzen.

Entgegen dem heute üblichen leitungsorientierten Sprachkanal im ISDN (Integrated Services Digital Network), bei dem die digitalisierten Sprachdaten – vereinfacht dargestellt – über einen vermittelten Kanal von Teilnehmer zu Teilnehmer übertragen werden, schickt man bei VoIP Datenpakete mit einem Gesprächsabschnitt, der Zieladresse und einer laufenden Nummer auf die Reise durch ein Netz, das auf dem Internet-Protokoll (IP) basiert. Dabei können die Pakete auf unterschiedlichsten Wegen zum jeweiligen Empfänger übertragen und dort an Hand der laufenden Nummer wieder in der richtigen Reihenfolge zusammengesetzt werden. Damit die Verständlichkeit zwischen den Gesprächspartnern gewährleistet ist, muss allerdings ein großer Teil der Pakete innerhalb einer bestimmten Frist beim Empfänger ankommen. Um dies sicherzustellen und alle grundsätzlichen, zum Teil sehr komplexen, Voraussetzungen zu schaffen, hat sich seit rund einem Jahrzehnt eine ganze Protokollfamilie (H 323) für die Übertragung von Echtzeitverbindungen in IP-Netzen etabliert.

Bei der eingangs angesprochenen Internet-Telefonie kommt dagegen eher das Session Initiation Protocol (SIP) zum Einsatz.

Wegen der allgemein prognostizierten Einsparpotenziale, die mit dem Systemwechsel zu VoIP einhergehen sollen, entwickeln sich neben dem Anwendungsumfeld, bei dem überwiegend private Nutzer ein analoges oder ISDN-Telefon an einem preisgünstigen Gateway betreiben, die Bereiche professioneller lokaler Netze am schnellsten. Dabei werden Netze ganz oder abschnittsweise in VoIP-Technik aufgebaut und die Verbindung zur herkömmlichen Technik wird entweder über lokale Gateways oder über einen VoIP-Provider realisiert.

Daneben eignet sich VoIP auch zur Kopplung von lokalen Telekommunikationsanlagen, wenn z. B. eine schon vorhandene IP-basierte Verbindung zwischen verschiedenen Standorten mitbenutzt werden kann. Inwieweit sich VoIP auch als Übertragungstechnik für den so genannten Backbone-Bereich gegen alternative Technologien durchsetzen kann, ist letztendlich eine Frage der Wirtschaftlichkeit.

Langfristig wird die heute bekannte Telefon- und Vermittlungstechnik durch VoIP abgelöst werden und die Kunden, die noch mit alter analoger oder digitaler Technik telefonieren, werden über ein geeignetes Gateway in der Vermittlungsstelle an die neuen Strukturen angebunden.

8.6.2

Gefährdungen

Neben den künftig genutzten Protokollen werden die sich noch entwickelnden Strukturen einen maßgeblichen Einfluss auf die Sicherheit der schützenswerten Telekommunikationsdaten haben. Große Telekommunikationsdiensteanbieter werden voraussichtlich selbst kontrollierte dedizierte IP-Netze betreiben. Die Rahmenbedingungen für die Vertraulichkeit von Gesprächsdaten und -inhalten werden sich in diesem Umfeld nicht wesentlich ändern.

Entgegen der heutigen Situation mit vergleichsweise wenigen regional agierenden Telekommunikationsdiensteanbietern ist zu erwarten, dass es bei VoIP eine weitaus größere Zahl Betreiber von regional begrenzten Anlagen bzw. Netzen (Firmennetze, Campusnetze von Hochschulen, Industrie und Gewerbeparks, Netze von Kommunen usw.) geben wird, die aber aus wirtschaftlichen Gründen neben der Telekommunikation alle bisher genutzten Anwendungen auf dem gleichen Netz betreiben müssen. Hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit steigen damit die Anforderungen an das Netz z. T. erheblich.

Zu den bekannten Bedrohungen, denen ein IP-Netz ohnehin ausgesetzt ist, kommen nun noch die speziellen Risiken, die sich mit der zusätzlichen Nutzung ergeben. Dabei gibt es auch in einem gemeinsamen Netz nahe liegende Wechselwirkungen. So legt z. B. ein erfolgreicher Denial of Service-Angriff auf bestimmte Domain Name Server, mit dem eine Überlastungssituation herbeigeführt wird, eben auch den davon abhängigen Telefondienst einer Firma oder Behörde lahm. In empfindlichen Aufgabenbereichen ist daher bei der Einführung von VoIP auf eine logische oder physikalische Entflechtung im Netz zu achten, um eine entsprechende Verfügbarkeit sicherzustellen. In bestimmten Zusammenhängen kann es auch notwendig sein, einzelne sonst benötigte Leistungsmerkmale abzuschalten, die erst mit der zusätzlichen Nutzung von VoIP in diesem Netz ein Sicherheitsrisiko darstellen.

An diesen nur angedeuteten Beispielen wird deutlich, dass die Nutzung von VoIP eine Fülle von Einzelfragen aufwirft, die ich aber an dieser Stelle – allein die BSI-Studie umfasst über 140 Seiten – nicht umfassend darstellen kann.

Einen Punkt will ich aber gesondert anführen.

Während die administrativen Oberflächen einer dem deutschen Recht entsprechenden herkömmlichen Telekommunikationsanlage nur in Sonderfällen das Mitschneiden/Mithören ermöglichen, ist dieses Leistungsmerkmal bei VoIP-Komponenten schlecht zu unterdrücken bzw. für den Betreiber unzugänglich zu machen.

8.6.3

Fazit

Der gegenwärtige Stand der Entwicklung zeigt, dass eine unbedarfte, allein an Einsparungseffekten orientierte Einführung und Nutzung von VoIP mit vielen Risiken verbunden ist. Nur mit einer umfassenden Analyse möglicher Bedrohungen und dem Einsatz geeigneter technischer Maßnahmen diesen zu begegnen, lässt sich VoIP sicher und ohne zusätzliches Risiko auch für bestehende IP-Dienste betreiben.

Die Anbieter von IP-Telefonie sind zur Wahrung des Fernmeldegeheimnisses verpflichtet und haben, soweit sie einen Telekommunikationsdienst erbringen, die Datenschutzbestimmungen des TKG einzuhalten. Dabei sind sie ganz wesentlich davon abhängig, dass die am Markt verfügbaren Produkte die dafür notwendigen Voraussetzungen bieten.

8.7

Kein Kopierschutz bei Internetveröffentlichungen

Die Veröffentlichung von Daten im Internet bedeutet, dass sie in der Regel auch kopiert werden können. Es ergeben sich dann Probleme, wenn diese Daten nur für eine bestimmte Zeit zur Verfügung stehen dürfen oder nur zur Einsicht bestimmt sind.

8.7.1

Ausgangslage

Unter dem Stichwort E-Government werden in der Verwaltung viele Abläufe automatisiert. Ein Ziel ist es, den Service für die Bürger zu verbessern. So wurde und wird intensiv darüber nachgedacht, welche Informationen über das Internet zur Verfügung gestellt werden können. Als wichtige und viele Bürgerinnen und Bürger interessierende Informationsquellen wurden die öffentlichen Bekanntmachungen der Gerichte eingestuft. So können z. B. die Bekanntmachungen in Insolvenzangelegenheiten oder die Terminbestimmungen für Zwangsversteigerungen in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem erfolgen (§ 9 InsO).

§ 9 InsO

(1) Die öffentliche Bekanntmachung erfolgt durch Veröffentlichung in dem für amtliche Bekanntmachungen des Gerichts bestimmten Blatt oder in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem; die Veröffentlichung kann auszugsweise geschehen. Dabei ist der Schuldner genau zu bezeichnen, insbesondere sind seine Anschrift und sein Geschäftszweig anzugeben. Die Bekanntmachung gilt als bewirkt, sobald nach dem Tag der Veröffentlichung zwei weitere Tage verstrichen sind.

(2) Das Insolvenzgericht kann weitere und wiederholte Veröffentlichungen veranlassen. Das Bundesministerium der Justiz wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die Einzelheiten der Veröffentlichung in einem elektronischen Informations- und Kommunikationssystem zu regeln. Dabei sind insbesondere Lösungsfristen vorzusehen sowie Vorschriften, die sicherstellen, dass die Veröffentlichungen

1. unversehrt, vollständig und aktuell bleiben,
2. jederzeit ihrem Ursprung nach zugeordnet werden können,
3. nach dem Stand der Technik durch Dritte nicht kopiert werden können.

(3) Die öffentliche Bekanntmachung genügt zum Nachweis der Zustellung an alle Beteiligten, auch wenn dieses Gesetz neben ihr eine besondere Zustellung vorschreibt.

Da die bislang übliche Veröffentlichung in Tageszeitungen oder im Bundesanzeiger schon einem großen Personenkreis zugänglich war, sah man in einer Veröffentlichung im Internet kein besonderes Problem, wenn verhindert wird, dass die Daten einfach zu kopieren sind. Dem wurde dadurch entsprochen, dass in den rechtlichen Vorgaben ein Kopierschutz gefordert wird. Auf die Problematik hatte ich schon im 30. Tätigkeitsbericht, Ziff. 7.1 hingewiesen.

Die Praxis hat gezeigt, dass die gesetzliche Vorgabe jedoch bei den datenbankbasierten Abfragesystemen Probleme bereitet. Das liegt insbesondere daran, dass auch die Möglichkeit besteht, auf eine Abfrage eine Liste der Ergebnisse zu erhalten. Die Datenschutzbeauftragten des Bundes und der Länder sind zu dem Schluss gekommen, dass ein wirksamer Kopierschutz, der nicht nur Laien daran hindert sich unzulässige Kopien der Daten zu verschaffen, zurzeit technisch nicht realisierbar ist.

8.7.2

Technischer Kopierschutz

8.7.2.1

Betrachtete Lösungsansätze

Bei den Betrachtungen wurden mehrere Lösungsmöglichkeiten untersucht.

– Wahl eines Datenformats mit Kopierschutz

Es wurde überlegt, die Daten zum Zeitpunkt der Übertragung in das pdf-Format zu konvertieren und das Dokument mit den bei pdf-Dokumenten möglichen Sicherheitseinstellungen zu versehen, die das Kopieren und Drucken unterbinden. Diese Schutzmechanismen wirken, wenn die vom Hersteller angebotene Darstellungssoftware benutzt wird. Es gibt jedoch auch Programme, die die Einstellungen ignorieren.

– Wahl einer anderen Präsentationslogik

Die Darstellung der Daten erfolgt mit einem Java-Applet, d. h. einem kleinen in Java geschriebenen Programm, das keine Kopier- und Druckfunktion besitzt. Das Programm würde zusammen mit den Daten vom Webserver heruntergeladen. Diese Lösung bedingt

spezielle Einstellungen beim Internetbrowser, die mit vorgegebenen Sicherheitseinstellungen kollidieren können. Außerdem gilt auch hier, dass versierte Nutzer die Sperren umgehen können, was man bei Stellen mit kommerziellem Interesse unterstellen kann.

Dieser Ansatz gewährleistet auch keine barrierefreie Internetnutzung. Wenn Personen mit einem eingeschränkten Sehvermögen Programme benutzen, die ihnen den Text lesbar darstellen, z. B. in Brailleschrift, so funktionieren diese Programme höchstwahrscheinlich nicht. Insofern gibt es einen Zielkonflikt zwischen Kopierschutz und Barrierefreiheit.

8.7.2.2

Digital Rights Management als datenschutzfreundliche Technik

Bei meinen Überlegungen zu einer Lösung verfolge ich einen weiteren möglichen Weg. Das Digital Rights Management (DRM) bzw. das Enterprise Rights Management könnte in absehbarer Zukunft die beschriebenen Ziele erfüllen. Die zugrunde liegende Technik ist jedoch aus Sicht des Datenschutzes nicht ohne Tücken; sie kann nur auf Basis des Trusted Computing (TC) ihre Funktionen sicher erfüllen. Wie ich in meinem 32. Tätigkeitsbericht unter der Ziff. 18.1 beschrieben habe, sind mit den genannten Technologien Risiken für den Nutzer verbunden.

Prinzipiell kann verhindert werden, dass Kopien von Dokumenten erstellt werden und einem Dokument kann eine Gültigkeitsdauer vergeben werden. Nach Ablauf der Gültigkeit wäre ein Zugriff auf das Dokument nicht mehr möglich. Es kann natürlich nicht verhindert werden, dass der Bildschirm abfotografiert und das Bild bearbeitet wird oder dass die Bildschirmanzeige abgeschrieben wird.

Da es aus Datenschutzsicht keinen Zwang geben sollte, DRM-Systeme für den Zugriff auf Informationen der Verwaltung scharf zu schalten, muss es auch ohne aktives DRM möglich sein, die gewünschten Informationen zu bekommen. Z. B. könnten abhängig von einer Prüfung, ob ein DRM-System aktiv ist, unterschiedliche Anzeigen erfolgen. Ohne DRM-System könnten die Daten von maximal drei Einträgen angezeigt werden, umfangreiche Listen würden nur an Rechner gehen, bei denen ein DRM aktiv ist. Das DRM würde dann kontrollieren, dass keine Kopien erzeugt werden und nach Ablauf der Gültigkeitsdauer würde die Datei dem Zugriff entzogen.

Ob dieser Ansatz technisch realistisch ist und die rechtlichen Probleme löst, sollte untersucht werden. Derzeit wird zumindest versucht, die dem Trusted Computing zugrunde liegende Technik datenschutzfreundlich zu gestalten. Die Konsequenzen für den Einsatz eines DRM und den oben beschriebenen Ansatz sind zu klären.

8.7.3

Fazit

Es gibt derzeit keinen sicheren Kopierschutz im Internet. Lösungen müssen jedoch gefunden werden, damit sich für die Betroffenen keine gravierenden Nachteile durch die Veröffentlichung ihrer Daten im Internet ergeben.

9. Bilanz

9.1

Vorratsdatenspeicherung durch Telekommunikations-, Tele- und Mediendienstanbieter (33. Tätigkeitsbericht, Ziff. 4.2.1)

Auch im Jahr 2005 hat das Thema Vorratsspeicherung von Telefonverkehrs- und Internetnutzungsdaten die Datenschutzkontrollbehörden in Bund und Ländern beschäftigt. Die Strafverfolgungs- und Sicherheitsbehörden fordern seit langem, Anbieter von Telekommunikations- und Internetdiensten gesetzlich zu verpflichten, für Zwecke der Strafverfolgung und Gefahrenabwehr eine bestimmte Zeit lang Verkehrs- und Nutzungsdaten zu speichern.

Zu den Verkehrs- und Nutzungsdaten zählen u. a. Telefonnummern, Nummern von Telefonkarten, Standortdaten (Funkzelle, aus welcher der Anruf erfolgt), Beginn und Ende der Verbindung bzw. Nutzung nach Datum und Uhrzeit, Datenmengen, IP-Adressen, URL (Uniform Resource Locator – globale Adresse von Dokumenten und anderen Quellen im World Wide Web), Nutzerkennungen oder Passwörter. Anhand dieser Daten lässt sich feststellen, wer wann mit wem telefoniert oder wer von wem wann welche E-Mail oder SMS erhalten hat oder wer wann welche Internetseiten aufgerufen hat. Nach dem gegenwärtigen deutschen Telekommunikations-, Tele- und Mediendienstrecht müssen die Diensteanbieter die Daten nach Ende der Verbindung löschen, soweit sie nicht für Abrechnungs- oder Datensicherheitszwecke benötigt werden.

Der Deutsche Bundestag hat sich zuletzt im Januar 2005 in einer von allen Fraktionen gestützten Erklärung gegen die Vorratsdatenspeicherung ausgesprochen. Wie im letzten Tätigkeitsbericht prognostiziert (33. Tätigkeitsbericht, Ziff. 4.2.1) gerät der deutsche Gesetzgeber jedoch durch die EU unter Druck, den Strafverfolgungs- und Sicherheitsbehörden dieses Instrument zur Verfügung zu stellen. Die EU-Kommission hat am 21. September 2005 den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG vorgelegt (KOM [2005] 438 endgültig). Darin ist vorgesehen, dass Telekommunikationsverkehrsdaten ein Jahr und Internetnutzungsdaten sechs Monate zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten wie Terrorismus und organisierte Kriminalität gespeichert werden müssen. In einer

Entschließung vom 27./28. Oktober 2005 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an die Bundesregierung, den Bundestag und das Europäische Parlament appelliert, den Vorschlägen der EU-Kommission nicht zuzustimmen (vgl. Ziff. 10.6).

Am 14. Dezember 2005 hat sich das Europäische Parlament in einer Legislativen Entschließung zu dem Kommissionsvorschlag dafür ausgesprochen, Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste anfallen, ab dem Zeitpunkt der Kommunikation für einen Zeitraum von mindestens sechs bis höchstens 24 Monaten auf Vorrat zu speichern (P6_TA-PROV [2005]12-14, Vorläufige Ausgabe PE 336.126). Die Mitgliedstaaten können nach der in erster Lesung vom Europäischen Parlament verabschiedeten Richtlinie den Diensteanbietern allerdings auch längere Aufbewahrungsfristen vorschreiben (Abänderung 56 – Erwägung 12 a – neu). Damit soll Ländern wie Polen, die eine 15-jährige Speicherdauer anstreben oder Irland, das eine dreijährige Aufbewahrungszeit vorgesehen hat, entgegengekommen werden. Die Bundesrepublik Deutschland ist gehalten, die durch die Richtlinie eröffneten Spielräume nach Maßgabe der nationalen datenschutzrechtlichen Standards auszufüllen.

9.2

Datenübermittlungen an Parteien zu Wahlwerbezwecken aus dem Einwohnermelderegister (32. Tätigkeitsbericht, Ziff. 8.3)

Der Umfang der Adressdaten von Wahlberechtigten, die die Meldebehörden sechs Monate vor Wahlen an Parteien zu Werbezwecken übermitteln dürfen, war immer wieder Gegenstand von Beschwerden und bereits mehrfach Thema in meinen Tätigkeitsberichten, zuletzt im 32. Tätigkeitsbericht 2003.

Da der Gesetzestext des § 35 Abs. 1 HMG nicht eindeutig den Umfang der zu übermittelnden Adressdaten von Wahlberechtigten begrenzt, sondern von „Gruppen“ spricht, die nach dem Lebensalter zusammengesetzt sind, bestand zwischen Parteien und Meldebehörden oft Dissens, ob z. B. auch die Daten aller Wahlberechtigten übermittelt werden durften. In meinen Beiträgen hatte ich deshalb das Hessische Ministerium des Innern (HMdI) um eine Klarstellung gebeten, die den Umfang der Datenübermittlung sinnvoll begrenzt.

Der Hessische Verwaltungsgerichtshof hatte mit Beschluss vom 21. Oktober 2001 klargestellt, dass nicht alle Altersgruppen gemeint seien und daher die Adressdaten aller Wahlberechtigten nicht übermittelt werden dürfen. Die Melderegisterauskünfte an die Parteien sollen dort nicht zu einer 100%igen Erfassung der Adressdaten aller Wahlberechtigten führen. Unklar blieb aber weiterhin, welche Gruppenbildung in der Summe zulässig ist.

Nunmehr hat das HMdI in einem Erlass an alle hessischen Gemeinden vom 3. Mai 2005 klargestellt, dass nicht über die Daten aller Wahlberechtigten verfügt werden darf. Die Kommune hat bei der Beurteilung der Rechtmäßigkeit eines Auskunftsbeglehrens einer Partei zu beachten, dass im Einzelfall die Summe der übermittelten Daten nicht mehr als 75 % der Daten aller Wahlberechtigten ausmacht. Soweit alle Wahlberechtigten angesprochen werden sollen, ist auf andere Möglichkeiten (z. B. Postwurfsendungen) zu verweisen.

Anlässlich der Bundestagswahl 2005 kam es zu keiner Datenschutzbeschwerde aus diesem Themenkreis, was ich u. a. auf die Klarstellung im genannten Erlass zurückführe.

9.3

Videüberwachung in öffentlichen Verkehrsmitteln

(31. Tätigkeitsbericht, Ziff. 3.1.3)

Im 31. Tätigkeitsbericht hatte ich unter Ziff. 3.1.3 über die Videüberwachung in den neuen Bussen der Hanauer Straßenbahn AG berichtet. Inzwischen setzen immer mehr öffentliche Verkehrsbetriebe die Videüberwachung in Bussen und Bahnen ein, um die Sicherheit für Fahrer und Fahrgäste zu erhöhen und um Vandalismusschäden vorzubeugen. So gibt es beispielsweise in den Straßenbahnbeiwagen der Verkehrsbetriebe Darmstadt (HEAG) Videokameras und seit kurzem auch einen Testversuch in Bussen der Stadtwerke Wiesbaden (ESWE).

In beiden Fällen wurde die Installierung der Kameras mit erheblichen Beschädigungen der Fahrzeuge in der Vergangenheit begründet. Diese Argumentation erschien gerade für die Installierung der Kameras in den Beiwagen der HEAG plausibel, da die Beiwagen vom Fahrer nicht eingesehen werden können.

In Wiesbaden dienen die Kameras, neben der Abwehr von Beschädigungen, dem Fahrer allerdings auch zur Türsteuerung im hinteren Busteil. Dieser Fahrzeugteil lässt sich durch die Kameras am Monitor sehr viel besser einsehen als durch Rückspiegel.

In beiden Fällen werden die Bilder in so genannten „Blackboxes“ aufgezeichnet und nach 48 Stunden überschrieben, wenn kein Vorfall gemeldet wurde. Zugang zu diesen Daten hat nur ein kleiner autorisierter Personenkreis. Die Festplatten dürfen nur im Fall eines Zwischenfalls ausgewertet werden.

Die Fahrgäste werden durch Aufkleber bzw. Plakate auf die Videoüberwachung hingewiesen. Auf den Hinweisschildern findet sich auch eine Telefonnummer, unter der die Fahrgäste nähere Informationen zur Videoüberwachung erhalten können. Für Wiesbaden hatte ich bemängelt, dass Fahrgäste, die im hinteren Busteil einsteigen, den Hinweis auf die stattfindende Videoüberwachung kaum wahrnehmen können. Die ESWE hat insoweit Nachbesserung zugesagt.

9.4

Datenbankprotokolle im Einwohnerwesen

(33. Tätigkeitsbericht, Ziff. 6.4)

Im 33. Tätigkeitsbericht hatte ich die zweckwidrige Nutzung eines an sich rechtmäßigen Zugriffs auf Meldedaten anderer Kommunen durch Meldeamtsmitarbeiter moniert. Die unzulässigen Zugriffe erfolgten durch Manipulation einer zulässigen Transaktion und konnten durch Auswertungen von Datenbankprotokollen nachgewiesen werden. Die Auswertungen zeigten seinerzeit, dass die Vorgehensweise bei den Meldeämtern sehr verbreitet war; eine Stichprobenkontrolle vor Ort bei besonders auffälligen Kommunen ergab, dass die Nutzer meist von der Absicht geleitet wurden, möglichst schnell und unbürokratisch ansonsten rechtmäßige Auskünfte zu geben, ohne dass den Mitarbeitern und Mitarbeiterinnen die Unzulässigkeit ihrer Vorgehensweise ausreichend bewusst war.

Nach der Veröffentlichung der Vorkommnisse in meinem 33. Tätigkeitsbericht und einem aufklärenden Anschreiben des Unternehmensverbundes KGRZ/ekom21 an die Kommunen, habe ich die angekündigte Kontrollauswertungen durchgeführt. Ich konnte feststellen, dass die

Maßnahmen guten Erfolg zeigten: Statt der 16 besonders auffälligen Kommunen waren es nur noch zwei andere Kommunen, die eine überdurchschnittliche Anzahl von „verdächtigen“ Transaktionen aufwies. Deren Meldebehörden und behördliche Datenschutzbeauftragten habe ich entsprechend angeschrieben. Die übrigen Zahlen der Auswertung ließen nicht mehr auf unzulässige Zugriffe schließen. Zur weiteren Sicherstellung einer zulässigen Verfahrensweise werde ich auch künftig in unregelmäßigen Abständen derartige Überprüfungen veranlassen. Die Angelegenheit zeigt deutlich, dass Protokollierungsverpflichtungen und Datenbankauswertungen zu Kontrollzwecken nach wie vor sinnvolle und wichtige Maßnahmen für einen effektiven Datenschutz darstellen.

9.5

Neue Rechtsgrundlagen zur DNA-Analyse im Strafverfahren

(32. Tätigkeitsbericht, Ziff. 5.2, 5.3, 20.10)

Schon mehrmals – zuletzt ausführlich im 32. Tätigkeitsbericht, Ziff. 5.2 – hatte ich über Debatten zur Ausweitung des Anwendungsbereiches der DNA-Analyse im Strafverfahren sowie die Notwendigkeit einer Rechtsgrundlage für die so genannten Massenscreenings berichtet. Auch dieses Jahr hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erneut mit diesem Komplex beschäftigt und in einer Entschließung vom 15. Februar 2005 nochmals auf die besondere Qualität des mit einer DNA-Analyse verbundenen Grundrechtseingriffs hingewiesen (vgl. Ziff. 10.1).

Durch das Gesetz zur Novellierung der forensischen DNA-Analyse vom 12. August 2005 (BGBl. I S. 2360), das am 1. November 2005 in Kraft getreten ist, haben die Diskussionen zumindest vorläufig ein Ende gefunden.

Ob der Gesetzgeber die datenschutzrechtlichen Belange gebührend berücksichtigt hat, erscheint zumindest fraglich. Eine wesentliche Änderung ergibt sich durch die Einführung einer Einwilligung als mögliche Voraussetzungen anstelle der richterlichen Anordnung. Dabei kann sich die Einwilligung auf die Entnahme des Untersuchungsmaterials, auf die Auswertung durch das Labor und auch auf die Speicherung in der DNA-Datei beim BKA beziehen. Zwar ist es zu begrüßen, dass nunmehr durch den Gesetzgeber eine Klarstellung erfolgt ist, doch bleibt die Problematik der Freiwilligkeit einer solchen Einwilligung im Bereich des Strafverfahrens

bestehen. Problematisch ist erst recht die Einwilligung in die Speicherung beim BKA. Diese Speicherung erfolgt für Zwecke zukünftiger Ermittlungsverfahren, über deren Tragweite im Zeitpunkt der Einwilligung keinerlei konkrete Vorstellungen bestehen. Gleichzeitig ist auch der Anwendungsbereich der DNA-Identitätsfeststellung in künftigen Strafverfahren ausgeweitet worden. Ausreichend ist nunmehr der Verdacht einer Straftat von erheblicher Bedeutung oder gegen die sexuelle Selbstbestimmung. Zudem kann es auch ausreichen, wenn wiederholt sonstige Straftaten begangen worden sind und dies im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichsteht.

Mit der Einführung der Grundlage für Reihengentests kommt der Gesetzgeber im Prinzip einer lange geäußerten Forderung nach. Dabei ist zu begrüßen, dass die Rahmenbedingungen für diese Verfahren genau beschrieben sind. Im Gesetz ist auch festgelegt, dass Daten aus diesen Massentests nicht zur Identitätsfeststellung in künftigen Strafverfahren beim Bundeskriminalamt gespeichert werden dürfen.

Nicht berücksichtigt hat der Gesetzgeber die Forderung der Datenschutzbeauftragten, dieses Verfahren nur als Ultima Ratio einzusetzen, wenn andere Ermittlungsansätze nicht zum Erfolg geführt haben. Einschränkende Voraussetzung ist freilich der Deliktsbereich, zu dessen Aufklärung solche Tests eingesetzt werden dürfen. Es muss sich um ein Verbrechen gegen das Leben, die körperliche Unversehrtheit, die persönliche Freiheit oder die sexuelle Selbstbestimmung handeln.

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

10.1

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17. Februar 2005

Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

Die strafprozessuale DNA-Analyse ist – insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten – ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z. B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber – auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung – in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den so genannten nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich,

welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im Übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

10.2

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10./11. März 2005

Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und -interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe

berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepaxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

10.3

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 10./11. März 2005

Einführung der elektronischen Gesundheitskarte

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend auf Grund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen – technischen wie organisatorischen – Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss

technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschlüssen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungsstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzerfordernissen Abstriche gemacht werden.

10.4

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 1. Juni 2005

Einführung biometrischer Ausweisdokumente

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützter Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische

Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben. Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

- dass die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,
- dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,

- dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,
- dass vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,
- dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

10.5

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005

Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische **Informationsgesellschaft** unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden **Modernisierung des Datenschutzrechtes**. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der **Ausforschung ihrer Lebensgewohnheiten** und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig. Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen **Evaluierung durch unabhängige Stellen** unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der **Leistungs- und Finanzkontrolle** die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im **Gesundheitswesen**, gentechnische Verfahren und eine intensiviertere Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u. a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte **Arbeitnehmerdatenschutzgesetz** muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

Die **Datenschutzkontrolle** hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher **Datenschutz in der Europäischen Union** gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

10.6

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005

Keine Vorratsdatenspeicherung in der Telekommunikation

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internet-Nutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z. B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dambruch zulasten des Datenschutzes unverdächtigter Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis

als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner und -partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzelnen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z. B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden. Mit einem Quick-freeze-Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommunikation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt.

Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnte. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen. Dieselben – unzutreffenden – Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

10.7

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005

Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Datenerhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.

Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern

in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und -empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z. B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Lösungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS beachtet werden.

Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisherigen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung“).

Es handelt sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für Datenschutz unterliegen. Dies haben die Bundesanstalt und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems A2LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein

klar definiertes Zugriffsberechtigungs- und Lösungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

10.8

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005

Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privater Callcenter durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

10.9

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005

Telefonieren mit Internet-Technologie (Voice over IP - VoIP)

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internet-Technologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internet-Telefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

- angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,
- Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,
- Sicherheits- und Datenschutzängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,
- auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offen zu legen,
- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und
- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

10.10

Entscheidung der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005

Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen

aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit.

Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber auf Grund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes – insbesondere die Angemessenheit der Datenerhebung – und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der – zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten – Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u. a. bei der Novellierung der §§ 100a und 100b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

10.11

Entscheidung der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005

Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.

10.12

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 15. Dezember 2005

Sicherheit bei eGovernment durch Nutzung des Standards OSCI

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheitsstandard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von so genannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem

gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

Organisationsplan des Hessischen Datenschutzbeauftragten

Hessischer Datenschutzbeauftragter

Prof. Dr. Michael Ronellenfitsch Tel. (06 11) 14 08 20

Vorzimmer:

Ursula Gegner Tel. (06 11) 14 08 21

Vertretung des Hessischen Datenschutzbeauftragten und Dienststellenleitung

Ute Arlt Tel. (06 11) 14 08 22

Gruppe A

Referat A1

Gruppenleitung, Koordinierung und Grundsatzfragen, interne Verwaltung Redaktion des Tätigkeitsberichts

Ute Arlt Tel. (06 11) 14 08 22

Mitarbeiterinnen:

Christel Friedmann-Baradel Tel. (06 11) 14 08 14

Karin Nitsche Tel. (06 11) 14 08 34

Referat A2

Bildung, Verwaltung von Hochschulen und anderen Wissenschaftseinrichtungen, Schulverwaltung, Schulen einschl. Forschung, Archive

Manfred Weitz Tel. (06 11) 14 08 45

Mitarbeiterin:

Karin Nitsche Tel. (06 11) 14 08 34

Referat A3

Finanzwesen, Einwohnerwesen, Verkehr

Cornelia Topp Tel. (06 11) 14 08 38

Mitarbeiterinnen:

Christa Kreis Tel. (06 11) 14 08 43

Helga Schaller Tel. (06 11) 14 08 41

Referat A4

Neue Verwaltungssteuerung, automatisierte Personaldatenverarbeitung, insbes. SAP R/3 HR

Bernd Groh Tel. (06 11) 14 08 35

Mitarbeiter:

Josef Hiegl (abgeordnet vom RP Darmstadt)

Tel. (06 11) 14 08 48

Gruppe B

Referat B1

Gruppenleitung, Informatik I

Rüdiger Wehrmann

Tel. (06 11) 14 08 37

Mitarbeiter:

Karl-Heinz Raub

Tel. (06 11) 14 08 15

Günter Soukup

Tel. (06 11) 14 08 18

Holger Weigel

Tel. (06 11) 14 08 28

Referat B2

Informatik II

Dr. Gisela Quiring-Kock

Tel. (06 11) 14 08 50

Mitarbeiter:

Karl-Heinz Raub

Tel. (06 11) 14 08 15

Holger Weigel

Tel. (06 11) 14 08 28

Referat B3

Informatik III

Maren Thiermann

Tel. (06 11) 14 08 31

Mitarbeiter:

Karl-Heinz Raub

Tel. (06 11) 14 08 15

Holger Weigel

Tel. (06 11) 14 08 28

Gruppe C

Referat C1

Gruppenleitung, Rechtsfragen der Informations- und Kommunikationstechnik, Rundfunk, Statistik, Versicherungen, Kreditinstitute, Kammern, Umwelt, Landwirtschaft, Forsten und Naturschutz, internationaler Datenschutz

Wilhelm Rydzy

Tel. (06 11) 14 08 24

Mitarbeiter:

Michael Sobota

Tel. (06 11) 14 08 27

Rainer Banse

Tel. (06 11) 14 08 33

Referat C2

Verfassungsschutz, Ausländerrecht, Europarecht, Schengener Informationssystem

Angelika Schriever-Steinberg Tel. (06 11) 14 08 25

Mitarbeiter:
Alfons Schranz Tel. (06 11) 14 08 32

Referat C3

Justiz, Staatsanwaltschaften, Vollzugsanstalten, Polizei, Ordnungswidrigkeiten

Barbara Dembowski Tel. (06 11) 14 08 26

Mitarbeiter:
Alfons Schranz Tel. (06 11) 14 08 32
Rainer Banse Tel. (06 11) 14 08 33

Gruppe D

Referat D1

Gruppenleitung, Gesundheitswesen, Wissenschaft und Forschung, Betreuungsrecht,

Dr. Rita Wellbrock Tel. (06 11) 14 08 23

Mitarbeiter:
Michael Sobota Tel. (06 11) 14 08 27

Referat D2

Personalwesen, Sozialwesen

Dr. Robert Piendl Tel. (06 11) 14 08 36

Referat D3

Kommunen, Vermessungswesen, Gewerberecht, Öffentlichkeitsarbeit

Ulrike Müller Tel. (06 11) 14 08 42

Mitarbeiterin:
Helga Schaller Tel. (06 11) 14 08 41

Sachwortverzeichnis

Access Point	8.5.2.1
Adressdaten	9.2
Adressierung von Finanzamtspost	5.11.1
Akkreditierung	4.3, 4.3.3
Altersteilzeit	
- Personalrat	5.10.3
Arbeitnehmerdatenschutzgesetz	10.5
Arbeitsgemeinschaft (ARGE)	5.8.4.1
Arbeitslosengeld II	5.9.1, 10.7
Auftragsdatenverarbeitung	5.8.1.1, 5.8.4.2, 5.8.7
- im Gesundheitswesen	5.8.1.1, 5.8.4.2, 5.8.7
- im Ausland	5.8.4
Automatische Löschung	3.3.3
Automatisierter Abruf	6.2
- Dokumentationsverpflichtung	6.2
- Liegenschaftskataster berechtigtes Interesse	6.2
Bankverbindungsdaten	5.5.2
Behördliche Datenschutzbeauftragte	2.2, 5.1.1
- Aufgaben	2.2.1
- bei Fraktionen	5.1.1
- Rechtsstellung	2.2.1
Berechtigungskonzept	8.2.4.2
Berufsheimlichkeitsgeheimnisträger	5.4.1
Betriebsmanagement	3.3.1
Bibliothek	5.7.1
Bild-, Tonaufnahmen	5.6.1.2
Biobanken	5.8.2
Biometrische Ausweisdokumente	4.2, 10.4
Bluetooth	8.5.1
Blut- und Gewebeproben	5.8.2
Buchtitel	5.7.1

Bundesamt für Sicherheit in der Informationstechnik (BSI)	8.6
Bundeskriminalamt	3.3.3
Bundesnetzagentur	8.6
Datenbankprotokolle	9.3
Datenschutz-Audit	10.5
Datenschutzkontrolle, unabhängige	10.5, 10.11
Datenverarbeitung im Auftrag	5.8.1.1, 5.8.4.2, 5.8.7
- im Gesundheitswesen	5.8.1.1, 5.8.4.2, 5.8.7
- im Ausland	5.8.4
Dienstanweisung	5.4.2
Digital Rights Management (DRM)	
- Kopierschutz	8.7.2.2
Disease-Management-Programme	5.8.4
DNA-Analyse	9.5, 10.1
DNA-Identitätsfeststellung	9.5
Dokumentenmanagementsystem	5.10.1, 8.1.4, 8.2
- Recherche	8.2.4.2
- Sachbearbeitung	8.2.4.2
DOMEA	8.2
Dritte Säule	3.2
Drittstaaten	3.4.4
Einscannen	8.2.4.1
Eintrittskarten WM 2006	4.3.2
Eintrittskarten	10.2
Einwilligung	4.3.3, 9.5
Einwohnermelderegister	9.2
- Datenübermittlung an Parteien	9.2
Elektronische Gesundheitskarte	10.3
Elektronische Signatur	5.8.1
Telefonieren mit Internet-Technologie	10.9
Erhebungsverbot	4.1.1, 10.10
Errichtungsanordnungen	3.4.2
EURODAC	3.1

EUROJUST	3.1
Europäischer Datenschutzbeauftragter	3.1, 3.2, 3.3.1
EUROPOL	3.1
Evaluierung	5.6.1.1
E-Beihilfe	5.10.1
E-Government	8.1, 8.1.2, 10.12
- Clearingstellen	10.12
- OSCI-Standard	10.12
- Probleme zentrale IT-Verfahren, Sachstand	8.1
- Sachstand Signatur	8.1.2
- Sachstand Verschlüsselung	8.1.2
E-Mail	
- Übermittlung von medizinischen Gutachten	5.8.6.2
E-Pass	4.2, 10.4
- biometrische Merkmale	4.2, 10.4
- Fingerabdruck	4.2
- RFID-Chip	4.2
Fachaufsicht	5.4.2
Fahrerlaubnisregister	5.5.1
- Karteikartenabschriften	5.5.1
- Tilgungsfristen	5.5.1
Finanzkontrolle	10.5
Fingerabdrücke	3.1, 3.3
Fraktionen im Hessischen Landtag	5.1.1
- Status	5.1.1.3
Führerscheindaten	5.5.1
Fußballweltmeisterschaft	4.3, 10.2
Gemeinsame Kontrollinstanz	3.3
Gesundheitsämter	5.8.5
Großer Lauschangriff	5.4.1
Harmonisierung	3.3.2
Hartz IV	5.9.1, 10.7, 10.8
- Kontoauszüge	5.9.1
- Telefonbefragung	10.8

Hessischer Datenschutzbeauftragter	2.1
- Aufgaben	2.1.1.2, 2.1.2.1
- Kontrollzuständigkeit	2.1.1, 2.1.2.3
- Rechtsstellung	2.1.1.2
- Unabhängigkeit	2.1.3
- Zuständigkeit	2.1.1, 2.1.2.3
Hochschulverwaltung	7.1.2
Hot Spots	8.5.2.1
Inaktive User	5.10.2
Informationsfreiheit	2.1.2, 2.1.2.2
Infrarotschnittstelle	8.5.1
Inkassobüro	6.1, 6.1.1
Insolvenzbekanntmachung	5.2.2
Internet	5.2.2
Internet	8.7, 10.9
- Kopierschutz	8.7
- VoIP	10.9
IT-Sicherheitsbeauftragte	7.1.2, 5.6.2
IT-Sicherheitsleitlinie	7.1.2, 5.6.2
Jugendgerichtshilfe	5.9.3
Justiz	
- Auskunftsrecht	5.3.3
-Verfahrensausgang	5.3.4
Kernbereich privater Lebensgestaltung	4.1, 10.10
Kfz-Steuer	5.5.2
Kopierschutz	
- Internet	8.7
Krankenakten	5.8.1
Krankenhäuser	
- Biobanken	5.8.3
- digitale Datenspeicherung	5.8.1
- Krankenakten	5.8.1
- Langzeitarchivierung	5.8.1
Langzeitarchivierung von Krankenakten	5.8.1

Laptops	5.8.6.1
Lauschangriff	4.1
Liegenschaftskataster	6.2
- Online-Abruf	6.2
MDK Sachsen-Anhalt	5.8.7.1
Medizinischer Dienst der Krankenversicherung	5.8.6, 5.8.7
Melderegisterauskunft	9.2
Mikroverfilmung	5.8.1
Mitwirkungspflichten	5.9.1, 5.9.2
Neue Verwaltungssteuerung	5.10.2
Neugeborenen-Screening	5.8.2
Organisierte Kriminalität	5.4.1, 3.1, 3.2
Orientierungshilfe Mobile Netze	8.5
- Rechtliche Aspekte	8.5.2
- Technische Aspekte	8.5.1
Passwort	8.3
- Probleme in Rechenzentren	8.3
Personal Digital Assistant	8.5.1
Personalakten	8.2.4.1
Personalaktenrecht	5.10.1
Personalausweisnummer	4.3.2, 10.2
Personenakten	5.4.1
Polizei	5.3.2, 5.3.4
- Löschung von Daten	5.3.2
- POLAS-HE	5.3.2
- Verfahrensausgang	5.3.4
Polizeiärztlicher Dienst	5.10.4
Polizeiverwaltung	5.10.4
Private IT-Geräte	5.6.1.3
Privatisierung der Universitätskliniken Gießen und Marburg	7.1.1
Produkthaushalt	2.1.3
Programme	
- KQP I	5.8.6.4
- KQP II	5.8.6.4

- OCR	5.8.6.4
Protokollierung	
- Nutzungsdaten	8.5.2.1.3
- Verkehrsdaten	8.5.2.1.3
Prümer Vertrag	3.3
Pseudonymisierung	5.8.7, 5.8.7.3, 5.8.7.4
Radio Frequency Identification (RFID)	
- WM-Eintrittskarten	4.3
Reihengentest	9.5
RFID-Chips	4.3
Rückführung	3.3.3
Sachakten beim Verfassungsschutz	5.4.1
SAP R/3 HR	5.10.2
Scannen	8.2.4.1
Schengener Informationssystem	3.3, 3.3.1
- SIS II	3.3.1
- Teilnahme der Schweiz	3.3
SCHUFA-Adressdatenermittlung	6.1, 6.1.2
Schuleingangsuntersuchung	5.8.5
Schulgesundheitspflege	5.8.5
Sicherheitsbehörden	4.3.3, 10.10
Sicherheitskonzept	4.3, 5.6.2, 5.10.1.2, 7.1.2, 8.2.3, 8.5.2.1.1, 10.4, 10.9
- Access-Point-Betreiber	8.5.2.1.1
- biometrische Ausweisdokumente	10.4
- Dokumentenmanagementsystem	8.2.3
- E-Beihilfe	5.10.1.2
- Fußball-Weltmeisterschaft	4.3
- Hochschulen	7.1.2
- Schulen	5.6.2
- Voice over IP - VoIP	10.9
Sicherheitsmaßnahmen	
- Funknetze	8.5.1
Software	

- Lotus Notes	5.8.6.2, 5.8.7.1
- OpenPGP	5.8.6.3
- SafeGuard Easy	5.8.6.1
- sicherer Verkehr	5.8.6.3
Sozialdaten	5.8.4.2
Sozialdatenschutz	5.9
Speicherfrist	3.3.1
Standardsuchhilfe SAP R/3 HR	5.10.2.3
Steuergeheimnis	5.5.2
Stimmzettel	6.3
Straftaten von erheblicher Bedeutung	4.1.1.2
Telearbeit	8.4
- DSL-Anschluss	8.4
- ISDN-Anschluss	8.4
- Laptop	8.4
- Papierkorb	8.4
Telefonüberwachung	4.1
- Kennzeichnung von Daten	4.1
- von Stimmzetteln bei Wahlen	6.3
Telekommunikationsgeheimnis	4.1
Telekommunikationsgesetz	8.6.3
Telekommunikationsüberwachung	
- präventive	4.1, 10.10
Terrorismus	3.1, 3.2, 3.3
Transparenz	3.4.1
Trennungsgebot	5.4.1, 5.4.2
Unabhängigkeit	2.1.3, 5.2.1, 10.5, 10.11
- Datenschutzkontrolle	10.5, 10.11
- Hessischer Datenschutzbeauftragter	2.1.3
- richterliche	5.2.1
Verbindungsdaten	4.1
Verfassungsschutz	4.3.3, 5.4.1
- Sachakten	5.4.1
Verschlusssachen	8.2.4.1

Verwertungsverbot	4.1.1.1
Videüberwachung	4.3.1, 5.3.1, 5.3.1.2
Videüberwachung	4.3.1, 5.3.1.2, 5.3.3.1, 9.3, 10.5
- Fußball-Weltmeisterschaft	4.3.1
- in Frankfurt	5.3.1.2
- öffentliche Verkehrsmittel	9.3
- Trends in Hessen	5.3.3.1
- Vandalismus	9.3
- Zunahme	10.5
Voice over IP - VoIP	8.6, 10.9
Vorabkontrolle	8.2.3
Vorratsdatenspeicherung	9.1
- Entschließungen DSB-Konferenz	10.6
- EU-Kommission	9.1
- Europäisches Parlament	9.1
- Internetdienste	9.1, 10.6
- Mediendienste	9.1, 10.6
- Teledienste	9.1, 10.6
- Telekommunikationsdienste	9.1, 10.6
Wahlstatistik	6.3
Wahlwerbung	9.2
WLAN	8.5.1, 8.5.2
- dienstliche Nutzung	8.5.2.1.1
- geschlossene Benutzergruppe	8.5.2.2
- private Nutzung	8.5.2.2.1
Wohngeld	5.9.2
- Antragsformular	5.9.2
Wohnraumüberwachung	5.4.1
Zugriffsberechtigung SAP R/3 HR	5.10.2.4
Zulassungsstellen	5.5.2
Zuverlässigkeitsüberprüfung	4.3.3