THÜRINGER LANDTAG
4. Wahlperiode

Drucksache 4/1435
08.12.2005

U n t e r r i c h t u n g

durch die Präsidentin des Landtags

Sechster Bericht über die Tätigkeit der Thüringer Landesbeauftragten für den Datenschutz

Der Thüringer Landesbeauftragte für den Datenschutz hat den oben genannten Bericht mit folgendem Schreiben vom 8. Dezember 2005 zugeleitet:

"Anliegender Bericht wurde gemäß § 40 Abs. 4 des Thüringer Datenschutzgesetzes (ThürDSG) abschließend am 6. Dezember 2005 im Beirat vorberaten.
Ich übergebe Ihnen meinen 6. Tätigkeitsbericht mit der Bitte um Kenntnisnahme und zur weiteren Veranlassung.
Die öffentliche Vorstellung des 6. Tätigkeitsberichts findet am 19. Dezember 2005 statt."

Prof. Dr.-Ing. habil. Schipanski
Präsidentin des Landtags

Hinweis der Landtagsverwaltung:
Der Bericht ist als Anlage übernommen. Gemäß § 52 Abs. 5 GO wurde der Bericht sowie die gemäß § 40 Abs. 2 des Thüringer Datenschutzgesetzes zu erwartende Stellungnahme der Landesregierung zum Bericht an den Innenausschuss überwiesen.

Druck: Thüringer Landtag, 15. Dezember 2005

Vorwort

Der vorliegende 6. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz umfasst den Berichtszeitraum vom 1. Januar 2004 bis zum 31. Dezember 2005.

Dieser ist der letzte Tätigkeitsbericht in meiner 12-jährigen Amtszeit. Wie die vorangegangenen Berichte beinhaltet er Ergebnisse der Kontrolltätigkeit, so auch die gegenüber Daten verarbeitenden Stellen ausgesprochenen Beanstandungen wegen festgestellter Mängel beim Umgang mit personenbezogenen Daten.
Auch aktuelle datenschutzrechtliche Themen und Diskussionen werden angesprochen. Darüber hinaus werden Anregungen und Empfehlungen zu Verbesserungen des Datenschutzes und der Datensicherheit gegeben.
Der 6. Tätigkeitsbericht wurde gemäß § 40 Abs. 4 ThürDSG im Beirat vorberaten.
Er steht im Internet unter www.datenschutz.thueringen.de nicht nur den Behörden sondern auch interessierten Bürgerinnen und Bürgern zur Verfügung.

Erfurt, im Dezember 2005

Silvia Liebaug
Thüringer Landesbeauftragte für den Datenschutz

6. Tätigkeitsbericht des TLfD
Berichtszeitraum vom 01.01.2004 bis 31.12.2005

Inhaltsverzeichnis
Abkürzungsverzeichnis

Entschließungen der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Entschließungen zwischen den Konferenzen 2004/2005

Entschließungen der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10./11. März 2005 in Kiel

Entschließungen der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in Lübeck

Weitere Anlagen

Sachregister

Abkürzungsverzeichnis

Abkürz.	Bedeutung
AAÜG	Gesetz zur Überführung der Ansprüche und Anwartschaften aus Zusatz- und Sonderversorgungssystemen des Beitrittsgebiets (Anspruchs- und Anwartschaftsüberführungsgesetz)
Abs.	Absatz
AD	Active Directory
AEAO	Anwendungserlass zur Abgabenordnung
AES	Advanced Encryption Standard
AG	Arbeitsgruppe
AK	Arbeitskreis
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
ARGE	Arbeitsgemeinschaft
AsylbLG	Asylbewerberleistungsgesetz
BA	Bundesagentur für Arbeit
BAföG	Bundesausbildungsförderungsgesetz
BAT	Bundes-Angestelltentarif
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BfF	Bundesamt für Finanzen
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMF	Bundesministerium der Finanzen
BMGS	Bundesministerium für Gesundheit und Soziales
BMJ	Bundesministerium der Justiz
BOTNet	Robot Network
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BUK	Bundesverband der Unfallkassen e. V.
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
CN	Corporate Network
d. h.	das heißt
DA	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden
DIPF	Deutsches Institut für Internationale Pädagogische Forschung
DJI	Deutsches Jugendinstitut
DMP	Disease-Management-Programm
DMS	DokumentenManagementSysteme
DNA-Analyse	Genetischer Fingerabdruck
DSB	Datenschutzbeauftragte/Datenschutzbeauftragter
DT	Datenträger
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
E-Government/ eGovernment	Elektronische Verwaltung
EG-PassVO	EG-Passverordnung

EHUG	Gesetz über das elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister
EJTAnV	Eurojust-Anlaufstellen-Verordnung
ELSTER	Elektronische Steuererklärung
E-Mail	Elektronic-Mail (elektronische Post)
ePass	elektronischer Pass
EStG	Einkommenssteuergesetz
EU	Europäische Union
Eurojust	Gemeinsame Stelle zur justiziellen Zusammenarbeit
Europol	Europäisches Polizeiamt
FeV	Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaubnisverordnung)
G 10	Artikel-10-Gesetz
GBO	Grundbuchordnung
GBV	Grundbuchverfügung
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz
GKV	Gesetzliche Krankenversicherung
GMG	Gesundheitsmodernisierungsgesetz
GMS	Global Messaging Service
GO	Geschäftsordnung
GPRS	General Packet Ratio Service
GVBl.	Gesetz- und Verordnungsblatt
HAMASYS	HAushalts-MAnagement-SYStem
i. V. m.	in Verbindung mit
i. d. R.	in der Regel
IDS	Intrusion Detection System
IfS	Institut für Schulentwicklungsforschung
IGV-P	Integrationsverfahren Polizei
INPOL	Informationssystem der Polizei
InsO	Insolvenzordnung
IPSec	Internet Protocol Security
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
JKomG	Justizkommunikationsgesetz
JMBl.	Justiz-Ministerialblatt für Thüringen
JMStV	Jugendmedienschutz-Staatsvertrag
JVA	Justizvollzugsanstalt
Kfz	Kraftfahrzeug
KJM	Kommission für Jugendmedienschutz
LDAP	Lightweight Directory Access Protocol
LfD	Landesbeauftragter für den Datenschutz
MDK	Medizinischer Dienst der Krankenversicherung
MDStV	Mediendienstestaatsvertrag
MiZi	Mitteilungen in Zivilsachen
Nr.	Nummer
o. g.	oben genannt/oben genannte
OBG	Ordnungsbehördengesetz
OFD	Oberfinanzdirektion

OID	Oracle Internet Directory
OLG	Oberlandesgericht
PAG	Polizeiaufgabengesetz
PC	Personal Computer
PD	Polizeidirektion
PDA	Personal Digital Assistant
PERSOS-S	Personalverwaltungssystem
PIN	Persönliche Identifikationsnummer
PStG	Personenstandsgesetz
PTÜ	Präventive Telekommunikationsüberwachung
PZU	Postzustellungsurkunde
RFID	Radio Frequency Identification
RSAV	Risikostrukturausgleichsverordnung
RTCP	Realtime Control Protocol
RTP	Realtime Transmission Protocol
S.	Seite
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SIP	Session Initiation Protocol
SIS	Schengener Informationssystem
sog.	so genannte
Spit	Spam over Internettelephony
SRTP	Secure Realtime Transport Protocol
SSL	Secure Socket Layer
StARoV	Staatliches Amt zur Regelung offener Vermögensfragen
StBA	Staatsbauamt
StDAV	Steuerdaten-Abruf-Verordnung
StEG	Studie zur Entwicklung von Ganztagsschulen
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVollzG	Strafvollzugsgesetz
TB	Tätigkeitsbericht
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutzverordnung
TFM	Thüringer Finanzministerium
ThLARoV	Thüringer Landesamt zur Regelung offener Vermögensfragen
ThürAllgVwKostO	Thüringer Allgemeine Verwaltungskostenordnung
ThürBG	Thüringer Beamtengesetz
ThürDG	Thüringer Disziplinargesetz
ThürDSG	Thüringer Datenschutzgesetz
ThürDVOzGÖbVI	Thüringer Verordnung zur Durchführung des Gesetzes über die Öffentlich bestellten Vermessungsingenieure
ThürGÖbVI	Thüringer Gesetz über die Öffentlich bestellten Vermessungsingenieure
ThürKAG	Thüringer Kommunalabgabengesetz
ThürKO	Thüringer Kommunalordnung
ThürKWG	Thüringer Kommunalwahlgesetz
ThürKWO	Thüringer Kommunalwahlordnung
ThürMeldeG	Thüringer Meldegesetz
ThürPersVG	Thüringer Personalvertretungsgesetz

ThürSchulG	Thüringer Schulgesetz
ThürSchulO	Thüringer Schulordnung
ThürStanz	Thüringer Staatsanzeiger
ThürSÜG	Thüringer Sicherheitsüberprüfungsgesetz
ThürVSG	Thüringer Verfassungsschutzgesetz
ThürVWKostG	Thüringer Verwaltungskostengesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
ThürVwZVG	Thüringer Verwaltungszustellungs- und Vollstreckungsgesetz
TIM	Thüringer Innenministerium
TJM	Thüringer Justizministerium
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKM	Thüringer Kultusministerium
TKÜ	Telekommunikationsüberwachung
TLfD	Thüringer Landesbeauftragter für den Datenschutz
TLfV	Thüringer Landesamt für Verfassungsschutz
TLKA	Thüringer Landeskriminalamt
TLLV	Thüringer Landesamt für Lebensmittelsicherung und Verbraucherschutz
TLRZ	Thüringer Landesrechenzentrum
TLS	Thüringer Landesamt für Statistik
TLVwA	Thüringer Landesverwaltungsamt
TMBV	Thüringer Ministerium für Bau und Verkehr
TMG	Telemediengesetz
TMLNU	Thüringer Ministerium für Landwirtschaft, Naturschutz und Umwelt
TMSFG	Thüringer Ministerium für Soziales, Familie und Gesundheit
TMWAI	Thüringer Ministerium für Wirtschaft, Arbeit und Infrastruktur
TMWFK	Thüringer Ministerium für Wissenschaft, Forschung und Kunst
TPG	Thüringer Pressegesetz
u. a.	unter anderem
u. ä.	und ähnliches
u. U.	unter Umständen
UMTS	Universal Mobile Telecommunications System
USB-Stick	Mobiler Datenträger
UVT	Unfallversicherungsträger
UWG	Gesetz gegen den unlauteren Wettbewerb
vgl.	vergleiche
VISkompakt	Vorgangsinformationssystem
VoIP	Voice over IP
VOIPSA	VoIP Security Alliance
VPN	Virtual Private Network
VwVfG	Verwaltungsverfahrensgesetz
WaffG	Waffengesetz
WLAN	Wireless Local Area Network
z. T.	zum Teil
z. B.	zum Beispiel
ZBL	Zentrale Betriebsleitstelle
ZG	Zentrale Gehaltsstelle
ZIV	Zentrum für Informationsverarbeitung
ZSHG	Gesetz zur Harmonisierung des Schutzes gefährdeter Zeugen
ZSS	Zentrale Speicherstelle
ZustRG	Zustellungsreformgesetz

1. Technischer und organisatorischer Datenschutz

1.1 Die digitale Lebenswelt

1.1.1 Entwicklung der IuK

Telekommunikation, Informationstechnologie und Multimediaanwendungen wachsen zunehmend zusammen. Die heutigen Dienste jedoch zwingen Nutzer noch vielfach dazu, zwischen verschiedenen Netzen, Service-Providern, Zugangsgeräten und Abrechnungssystemen zu wechseln. Neue konvergente Dienste, die nahtlos miteinander verknüpft sind, einfach zu handhaben und überall verfügbar sind, stehen vor ihrer breiten Einführung. Ohne Medienbruch und grenzenlos für die Nutzer wird künftig über Festnetz, Kabel, Funk und Satellit kommuniziert. Die neue Architektur mit dem Namen Internet Protocol Multimedia Subsystem wird dies ermöglichen.
Der Trend zur Miniaturisierung von Prozessoren und Speichern, verbunden mit immer schnelleren Verarbeitungsgeschwindigkeiten und größeren Speicherkapazitäten, hält unvermindert an. Entsprechend flexibler und mobil sind die IuK-Geräte einsetzbar. Immer mehr greift die Digitalisierung gesellschaftlicher Prozesse um sich. Der Einsatz von RFID-Chips (1.12), die Einführung des elektronischen Passes (5.3.4), der Gesundheitskarte (11.4) und der JobCard (11.13) sind nur ein kleiner Ausschnitt der vielfältigen Möglichkeiten, die auch aus datenschutzrechtlicher Sicht relevant sind.
Die Digitalisierung der Sprachprozesse ermöglicht jetzt auch Sprache über das Internetprotokoll (Voice over IP 1.10) gemeinsam mit Daten zu übertragen. Kosten für teure Mietleitungen lassen sich somit einsparen. Ohne Ergreifung zusätzlicher Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit der übertragenen Gespräche und vor deren Manipulierbarkeit ergeben sich auch hier die allseits bekannten Schwachstellen, die bei der herkömmlichen Datenübertragung über das Internet zu bemängeln sind.
Der Einsatz moderner DokumentenManagementSysteme (DMS) schließt über die Verarbeitung der in digitaler Form vorliegenden Daten hinaus, auch deren elektronische Übertragung sowie Dokumentation und Archivierung ohne Medienbruch mit ein. Insbesondere eGovernment-Anwendungen (1.8) nutzen solche Technologien. In der Landesverwaltung ist hierfür als Basis das DMS „VISkompakt“ vorgesehen. Es ist somit absehbar, dass sowohl der elektronische Austausch von Schriftgut als auch dessen elektronische Dokumentation und Archivierung rasch zunehmen wird. Die elektronischen Datenprozesse müssen jedoch nicht nur effektiver sein als die bisherigen manuellen Prozesse, sondern auch sicher und datenschutzgerecht ablaufen. So muss nicht nur die Authentizität und Integrität der elektronischen Dokumente gewährleistet sein. Wichtige Aspekte für die Verarbeitung personenbezogener Daten sind u. a. Berechtigungskonzepte, in denen die Zugriffe auf die jeweiligen Dokumente nach Maßgabe der Erforderlichkeit und Zweckbindung zu regeln sind. Die Protokollierung der Verarbeitungsvorgänge und hiermit mögliche Leistungs- und Verhaltenskontrollen der Nutzer sind von hoher datenschutzrechtlicher Relevanz.
Für die Absicherung der Authentizität und Integrität der elektronischen Dokumente, aber auch um diesen in den erforderlichen Fällen Rechtsverbindlichkeit zu verleihen, bietet sich der Einsatz von elektronischen Signaturen (2. TB, 15.7.5; 4. TB, 15.4) an. Trotz der vielseitigen Einsatzmöglichkeiten hat sich die elektronische Signatur jedoch bisher noch nicht grundlegend durchgesetzt. Derzeit prägen Insellösungen das Bild, obwohl die gesetzliche Basis vorliegt, erforderliche Techniken hierzu auch vorhanden und einsatzfähig sind. Ein Grund ist sicher auch die fehlende systemübergreifende Hard- und Software, die selten interoperabel und zertifiziert ist. Anderseits fehlen für einen massenhaften Einsatz seitens der Bürger noch lohnenswerte Anwendungen. Die auf Landesebene vor einiger Zeit geplante Einführung einer zunächst fortgeschrittenen Signatur in der Landesverwaltung kam über ein Teststadium nicht hinaus

(4. TB, 15.8). Im Zuge der Umsetzung der vom Land geplanten eGovernment-Anwendungen ist jedoch der Einsatz der elektronischen Signatur erforderlich und zu realisieren. Über die herkömmlichen Maßnahmen zur Gewährleistung der Datensicherheit und Urheberschaft der digitalen Dokumente hinaus, ergeben sich insbesondere Anforderungen an die technische Verfügbarkeit der digital auf elektronischen Speichern vorgehaltenen Daten. Deren Langzeitverfügbarkeit hängt entscheidend von der technischen Entwicklung der Speichermedien ab. Diese schreitet sehr schnell voran, so dass im Ergebnis ständig neue Geräte und Datenformate zum Einsatz kommen werden, die ein permanentes Konvertieren der vorhandenen digitalen Archivbestände erfordern, um Datenverlusten vorzubeugen.
Schlüsseltechnologien, wie das Internet und die Mobiltelefonie, prägen unsere Zeit, welche von Mobilität gekennzeichnet ist und dem Einzelnen immer mehr Mobilität abverlangt. Die hohen Nutzerzahlen im Internet und im Mobilfunk sind ein sichtbares Zeichen für die Bedeutung von Information und Mobilität. Momentan wachsen Internet und Mobilfunk durch die dritte Mobilfunkgeneration (UMTS) zusammen. Dieses Wireless Computing, das mobile Internet, eröffnet eine neue Dimension der Informationsgesellschaft. Informationen können ortsunabhängig und zeitlich aktuell jederzeit bereitgestellt werden. Dazu werden rasant drahtlose Netzzugänge flächendeckend ausgebaut und qualitativ verbessert. Die Dienstleistungen des Internets sollen hierbei die entscheidende Rolle bei der Nutzung zukünftiger, insbesondere mobiler Funkdienste spielen. Schon jetzt ist die mobile Kommunikation (1.3) weit über die reine Sprachübertragung hinausgewachsen, wobei neue Techniken eine vielfach schnellere Datenübertragung ermöglichen. Kombinierte Lösungen aus Personal Digital Assistant (PDA) und Mobiltelefon, sog. Smart-Phones, bieten schon heute Funktionalitäten, über die bisher nur die stationäre Rechentechnik verfügte. Von unterwegs auf stationär vorgehaltene Daten zugreifen, E-Mails versenden und empfangen, im Internet surfen, Transaktionen online erledigen, alles ist laut Hersteller problemlos möglich. Spezielle Dienstleister können jederzeit die mobilen Nutzer mit Informationen versorgen, die konkret auf ihre Bedürfnisse abgestellt sind, wogegen nichts einzuwenden ist. Nicht nur mit der Einführung von personalisierten Diensten stehen aber auch datenschutzrechtliche Fragestellungen an. Wie ist es mit der Einhaltung datenschutzrechtlicher Grundprinzipien bestellt, wie mit der Sicherheit der gespeicherten und übertragenen Daten sowie der eingesetzten Systeme? Werden Nutzerprofile angelegt, wie wird einem möglichen Missbrauch von gespeicherten und übertragenen Nutzdaten sowie der Verbindungsdaten vorgebeugt? Welche Maßnahmen sind involviert, um die Vertraulichkeit, Integrität und Authentizität der Daten abzusichern? Hierzu gibt es seitens der Hersteller und Vertreiber im Gegensatz zu den von ihnen gepriesenen technischen Möglichkeiten solcher Systeme nicht selten keine oder unzureichende Aussagen. Die für den Nutzer gebotene Transparenz und Nachvollziehbarkeit zur Sicherheit der Daten bei den zum Einsatz kommenden Technologien und Verfahren weist noch einen erheblichen Nachholbedarf seitens der Hersteller und Anbieter auf.
Während die letzten Jahrzehnte durch eine Dezentralisierung der Datenverarbeitung geprägt waren und vorwiegend lokale Netze zum Einsatz kamen, ist sowohl im öffentlichen Bereich als auch in der Wirtschaft eine zunehmende Tendenz zu verzeichnen, die dezentralen IT-Systeme mit zentraler Rechentechnik zu ergänzen, um künftigen Anforderungen gerecht zu werden. Dazu werden sowohl leistungsstarke Server sowie vormals als Großrechner bezeichnete Rechner eingesetzt, um die zweifellos vorhandenen Vorteile einer zentralen Datenverarbeitung mit einer vor Ort vorgehaltenen flexiblen IuK-Infrastruktur zu verknüpfen. Mit dem Zentrum für Informationsverarbeitung (ZIV; 3. TB, 15.4) steht für die öffentlichen Stellen des Freistaates ein zentrales Rechenzentrum zur Verfügung, das von seiner Infrastruktur hohen Sicherheitsansprüchen genügt. Auf Dauer müssen eine gesicherte Datenübertragung zwischen den öffentlichen Stellen und dem ZIV sowie weiterhin eine wirksame Abschottung der auf der zentralen Rechentechnik zu verarbeitenden Daten der unterschiedlichen Stellen erfolgen. Auch hier wird der TLfD weiterhin auf eine datenschutzgerechte Gestaltung im Rahmen seiner Aufgaben hinwirken.

1.1.2 Aktuelle Sicherheitsaspekte

Sicherheitstechnische Aspekte rücken in der letzten Zeit in den Mittelpunkt der IuK und erfordern immer mehr personelle und finanzielle Aufwendungen. Im Vordergrund stehen derzeit Maßnahmen zur Bekämpfung von Viren oder Spam sowie wie bisher Maßnahmen zum Schutz der Daten vor unbefugtem Zugriff und Missbrauch. Die Mittel und Wege, IuK-Systeme anzugreifen, werden von Jahr zu Jahr komplexer. Bei den von schadensstiftender Software (Malware) wie Viren, Würmer und Trojaner (2. TB, 15.11; 4. TB, 15.5; 1.4) ausgehenden Bedrohungen spricht man schon heute von drei Generationen. Für das Auslösen von Bedrohungen der ersten Generation waren noch Handlungen der Nutzer notwendig, indem z. B. eine virenbehaftete Datei oder E-Mail geöffnet wurde. Bedrohungen der zweiten Generation ergaben sich vorwiegend durch aktive Würmer, die bekannte Sicherheitslücken in Applikationen ausnutzten, um sich automatisch massenhaft zu verbreiten. Schadensstiftende Software der dritten Generation zielt darauf ab, automatisiert, schnell und unerkannt für die Nutzer in so viele IT-Systeme wie möglich einzudringen, in dem vorwiegend bisher noch nicht bekannte oder veröffentlichte Sicherheitslücken genutzt werden. Während bei der ersten Generation dieser Bedrohungen zumeist kontinuierlich aktualisierte Antivirenprogramme hilfreich waren, sind jetzt darüber hinaus regelmäßige Schwachstellenanalysen zur Ermittlung und zum Schließen von Sicherheitslücken notwendig. Jede Schwachstelle ist zuallererst immer ein Zeichen für Programm- und Konfigurationsfehler. Das rasche Erkennen von Schwachstellen und das schnelle Reagieren zur Abwehr von Angriffen in Netzwerken wird zukünftig ein Wettlauf mit der Zeit. Die Zahl der hierfür auf dem Markt angebotenen speziellen Hard- und Softwarelösungen ist fast unüberschaubar, wobei ständig neue Produkte hinzukommen. Insbesondere auf dem Vormarsch sind Sicherheitslösungen für mobile Anwendungen, um Notebooks, PDAs und Smart-Phones von mobilen Mitarbeitern zu schützen. Da solche Produkte auf Grund der rasanten technischen Entwicklung kaum zertifiziert (5. TB, 15.11) werden, ist deren sicherheitstechnische Bewertung durch die Nutzer kaum möglich. Medienberichten zufolge wurde in der letzten Zeit weltweit ein hohes Aufkommen an neuen Würmern und Trojanern festgestellt. Dabei sind zunehmend Trojanerangriffe zu verzeichnen, bei denen eindeutig das Erreichen finanzieller Vorteile durch Datendiebstahl und Missbrauch fremder IT-Systeme im Mittelpunkt stehen. Insbesondere Phishing-Angriffe, bei denen mit gefälschten E-Mails und vorgetäuschten Web-Sites die Empfänger aus fingierten Gründen aufgefordert werden, ihre persönlichen Nutzerkennungen (PIN, Passwörter) einzugeben und somit Unbefugten zu offenbaren. Damit steigen die Folgeschäden sowohl bei Privatanwendern als auch bei öffentlichen Einrichtungen und Unternehmen. In der nächsten Zeit ist auch mit einer weiterhin steigenden Anzahl von Viren, Würmern, Trojanern und Spyware zu rechnen. Der Trend geht zu modularen Infektionsprogrammen die immer neue Befehle erhalten und somit ein höheres Potential an schädlichen Aktivitäten mit sich bringen können. Insbesondere passen sich diese Schädlinge innerhalb kürzester Zeit an die anzugreifenden Systeme an. Sie lassen gezielte Angriffe auf mehreren Ebenen und auf verschiedenen IT-Systemen zu. Dadurch, dass immer mehr IuK-Geräte bis hin zu Druckern internetfähig sind, werden auch diese direkt angreifbar, so dass sich über deren Schnittstellen auch häufiger Schadprogramme verbreiten können. So ermöglichen mobile Netze der dritten Generation wie GPRS oder UMTS Smartphones (1.3) die ständige Verbindung mit dem Internet, mit der Folge, dass diese damit auch leichter zu Zielen von Angriffen werden. Über ihren Zugang zu den lokalen Netzen können somit auch hier klassische Schadprogramme eindringen.
Besonders anfällig sind noch die auf neuen Technologien basierenden IuK-Systeme, wie Funknetze und Internettelefonie Voice over IP (VoIP; 1.10). Zurzeit werden durch Malware-Programmierer die technischen Möglichkeiten des Einsatzes für Mobiltelefone ausgelotet. Schon Anfang 2005 erfolgte mit der Verbreitung von PE_VLASCO, einem schadensstiftenden

Code mit einer ausgeklügelten Verbreitungsroutine, ein erster Einsatz. Auch für VoIP wird nach Ansicht von Sicherheitsexperten mit schadensstiftenden Programmen gerechnet, insbesondere wenn dieser Service in größerem Umfang genutzt wird. Dabei kann noch nicht abgeschätzt werden, welche Schäden durch einen erfolgreichen Angriff auf die telefonische Kommunikation entstehen können. Um ein möglichst breites Spektrum an Gefahrenquellen abzudecken, muss die künftige Sicherheitssoftware immer mehr integrierte und komplexe Lösungspakete anbieten.
Eine neue Bedrohungsform ist Robot Network (BotNet). Es handelt sich hierbei um große Gruppen von Computern, die über das Internet zu einem leistungsfähigen Rechnernetzwerk verknüpft werden und mit Hilfe spezieller schadensstiftender Programme ferngesteuert werden. Die infizierten Rechner können von den Angreifern für systematische Attacken auf andere Computer oder Netzwerke eingesetzt werden, um diese zum Absturz zu bringen oder zum Versenden von Spam bzw. zum Speichern von Raubkopien zu missbrauchen. Das Gefährliche daran ist, dass in der Regel die Zweckentfremdung der Rechner von den Benutzern nicht bemerkt wird.
Auch moderne mobile Speichermedien, wie USB-Sticks, können eine nicht unwesentliche Schwachstelle für die Sicherheit der IT und der Daten ergeben. Während die stationären IuK-Systeme mit Firewalls, Zugriffskontrollen usw. zum Teil aufwendig gesichert sind, können die Nutzer wichtige Daten und komplette Datenbanken in Aktentaschen bzw. Hosentaschen auf diesen mit sich herumtragen. Daher ist es wichtig, dass Sicherheitskonzepte nicht nur die herkömmlichen IuK-Geräte abdecken, sondern auch die mobile IuK (wie Laptop, PDA, Smart-Phone, USB-Stick) einbeziehen.
Eine große Verantwortung für die Sicherheit des Corporate Network (CN) der Landesverwaltung obliegt dem TLRZ. Als Basis hierfür liegt ein IT-Sicherheitskonzept vor, welches permanent dem Stand der Technik anzupassen ist. Alle sich dem CN anschließenden Stellen müssen über ein eigenes IT-Sicherheitskonzept verfügen. An der zentralen Schnittstelle zwischen CN und Internet sind gestaffelte Firewallsysteme, Viren- und Spamfilter (1.4) installiert. Neben Firewalls spielen zunehmend sog. Intrusion Detection Systeme (IDS; 5. TB, 15.1.2) eine wichtige sicherheitstechnische Rolle. Es handelt sich hierbei um speziell konfigurierte Sicherheitssysteme, die zwar üblicherweise keine Angriffe verhindern, solche jedoch erkennen oder aufspüren können. Ihr Nachteil ist allerdings derzeit noch, dass sie einen nicht unerheblichen Konfigurationsaufwand und spezialisiertes Wissen erfordern und auch nicht immer kompatibel zu eingesetzten Produkten der klassischen IT-Sicherheit sind. Der vom TLfD empfohlene Einsatz eines solchen IDS im CN wird auch seitens des TLRZ für erforderlich gehalten und ist vorgesehen, um innerhalb des CN schadensstiftende Aktivitäten und unberechtigte Zugriffe auf IT-Ressourcen rechtzeitig und möglichst beweisbar feststellen zu können. Mehrere Systeme wurden vom TLRZ bereits hierfür getestet. Zurzeit befindet sich das TLRZ in der Beschaffungsphase. Für das gemeinsame Active Directory (AD; 5. TB, 15.3) des Landes, es handelt sich hierbei um einen landesweiten Verzeichnisdienst, liegt inzwischen ebenfalls das vom TLfD geforderte Sicherheitskonzept im Entwurf vor. Auf Basis der darin definierten Richtlinien und Festlegungen werden dann die noch erforderlichen sicherheitstechnischen Maßnahmen umgesetzt.

Keine Fortschritte gibt es bisher bei der Einführung moderner kryptographischer Verfahren, insbesondere für eine sichere elektronische Übertragung personenbezogener Daten. Hier ist dringender Handlungsbedarf angezeigt, zumal auch das novellierte Thüringer Verwaltungsverfahrensgesetz zulässt, dass eine durch Rechtsvorschrift angeordnete Schriftform, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden kann, wobei das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen ist. Weiterhin erfordern zukünftige eGovernment-

Anwendungen öffentlicher Stellen des Landes über den Einsatz elektronischer Signaturen hinaus auch eine verschlüsselte Datenübertragung.
Die Praxis zeigt, dass eine nicht geringe Gefahr für die IuK-Sicherheit nach wie vor von den Nutzern ausgeht. Allerdings in der Regel nicht, weil sie absichtlich Schädigungen hervorrufen, sondern weil Sicherheitsrichtlinien bzw. Sicherheitskonzepte entweder nicht existieren, nicht deutlich genug kommuniziert, von den Nutzern unzureichend umgesetzt oder auch missachtet werden. Gemäß § 9 ThürDSG haben die öffentlichen Stellen die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage eines Sicherheitskonzeptes zu ergreifen. Kontrollen in öffentlichen Stellen des Landes ergaben, dass diese gesetzlichen Vorgaben nicht immer eingehalten werden. Fehlende, unzureichende oder veraltete Sicherheitskonzepte können grundsätzliche Fehler im Sicherheitsmanagement bewirken. So ist häufig nicht nachvollziehbar definiert, was, warum und wie zu schützen ist. Hieraus resultieren oftmals ad-hoc-Entscheidungen oder Sicherheitsinvestitionen aus der Intuition heraus. Oftmals wird auch nur an der bestehenden IT-Sicherheit geflickt und gebastelt und durchgreifende Konzepte fehlen.
Moderne Lösungen zur Zugangskontrolle wie bspw. dynamische Einmal-Passwörter, digitale Zertifikate oder biometrische Lösungen (3. TB, 15.4) setzen sich in der Praxis nur langsam durch. Zahlreiche neue Identifizierungsverfahren werden auf dem Markt angeboten, bspw. der Einsatz von Smart-Cards. Hiermit kann sich der Nutzer mit Wissen und Besitz relativ sicher in ein IT-System einloggen. Ungeachtet dessen dominiert noch immer das gute alte Passwort. Dies ist auch bei den öffentlichen Stellen des Landes der Fall. Die praktische Erfahrung zeigt, dass die Nutzer ein sehr ambivalentes Verhältnis zum Passwortschutz zeigen. Obwohl vielen Nutzern bewusst ist, dass ihre Passwörter vor Kenntnis anderer zu schützen sind, ist ein dementsprechend sorgfältiger Umgang mit ihren Kennwörtern nicht immer zu verzeichnen. So werden sie oftmals aufgeschrieben, nicht sicher aufbewahrt und mitunter auch anderen Mitarbeitern offenbart. Da aus Sicherheitsgründen immer komplexere und längere Passwörter gefordert werden, nimmt auch die Wahrscheinlichkeit zu, dass die Nutzer diese vermehrt aufschreiben bzw. vergessen.
Nicht befriedigend ist auch aus der Sicht des TLfD, dass zunehmend Anregungen für Maßnahmen zur Verbesserung der IT-Sicherheit von öffentlichen Stellen mit dem Hinweis auf fehlende finanzielle Mittel begegnet wird. Leider wird in Zeiten knapper Kassen IT-Sicherheit mehr als Kostenverursacher gesehen. Hier ist ein Paradigmenwechsel notwendig. Sicherheit kostet Geld und ist nicht zum Nulltarif zu bekommen. Eine fehlende angemessene Sicherheit kann nicht nur schwerwiegende Imageschäden zur Folge haben, sondern auch zu erheblichen zusätzlichen Kosten führen.

1.2 Technische und organisatorische Kontrolltätigkeit

Die IuK-Sicherheit hat sich in den öffentlichen Stellen Thüringens zunehmend zu einem festen Bestandteil beim Einsatz der EDV entwickelt. In den vorhergehenden Tätigkeitsberichten habe ich bereits immer wieder auf die Notwendigkeit zum Einsatz von Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten gemäß § 9 Abs. 2 ThürDSG hingewiesen. Im Mittelpunkt stand und steht die Umsetzung von Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Ebenso gilt es die Transparenz der eingesetzten Verfahren und die Nachvollziehbarkeit der Verarbeitungsvorgänge zu gewährleisten. Auch im Berichtszeitraum habe ich bei den durchgeführten Kontrollen diesen Sicherheitszielen große Aufmerksamkeit gewidmet und in diesem Zusammenhang nachfolgende Feststellungen gemacht sowie mit den betroffenen Stellen die notwendigen Schlussfolgerungen erörtert.

Bei Kontrollen musste teilweise immer noch festgestellt werden, dass mitunter Behörden entgegen § 10 ThürDSG für die von ihnen genutzten automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, keine Verfahrensverzeichnisse und schriftliche Freiga-

ben gemäß § 34 ThürDSG vorliegen haben, was mehrfach beanstandet wurde. Dies ist eine gesetzliche Pflicht, die eine Mitwirkung des behördlichen Datenschutzbeauftragten erfordert. Gemäß § 8 Abs. 1 ThürDSG ist der Auftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen und hieraus resultierender sicherheitstechnischer Maßnahmen verantwortlich. Um dieser gesetzlichen Forderung gerecht zu werden, bedarf es neben einem transparenten IT-Konzept und einem IT-Sicherheitskonzept zur Datenverarbeitung auch zumindest eines verantwortlichen fachkompetenten Mitarbeiters in der Behörde, der die ordnungsgemäße Umsetzung der Vorgaben durch den Auftragnehmer kontrolliert.
Die Daten verarbeitenden Stellen sind nach § 9 Abs. 2 ThürDSG zur Vorhaltung eines IT-Sicherheitskonzeptes verpflichtet. Nicht immer kann ein solches zur Kontrolle vorgelegt werden. Eine Nutzung des Internets mittels PCs, die im lokalen Netz angebunden sind, ist auch mit Gefährdungen für den Datenschutz und Datensicherheit verbunden. Um diesen zu begegnen, sind hierzu besondere Schutzmaßnahmen aber auch konkrete Regelungen notwendig. Aus datenschutzrechtlicher Sicht ist deshalb bei einem Anschluss an das Internet zu gewährleisten, dass zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und den Gefahren durch technische und organisatorische Maßnahmen hinreichend begegnet wird. Im Rahmen von Kontrollen hat der TLfD datenschutzrechtliche Forderungen und Empfehlungen aufgemacht.

Das ThürDSG verlangt nach § 9 ThürDSG von den Stellen solche technische und organisatorische Maßnahmen zu ergreifen, die notwendig sind, um einen unbefugten Zugang zu personenbezogenen Daten auszuschließen. Auch in größeren Behördenzentren, wo eine Hausverwaltung für alle Nutzer eingesetzt ist, obliegt die datenschutzrechtliche Verantwortlichkeit den betreffenden Daten verarbeitenden Stellen nach § 34 ThürDSG. Daher sind insbesondere bei der Vergabe von Reinigungs- und Bewachungsdiensten die jeweiligen Erfordernisse der einzelnen Behörden zu berücksichtigen. Wenn in einer Behörde keine ausreichende Anzahl verschließbarer Behältnisse für sensible personenbezogene Daten zur Verfügung stehen, können Reinigungsarbeiten nicht ohne Aufsicht der zuständigen Bediensteten, insbesondere außerhalb der Dienstzeiten erbracht werden. Das gilt auch für den Transport von zu vernichtendem Schriftgut, das nicht durch Reinigungskräfte aus den Papierkörben zu den für die Vernichtung bestimmten verschlossenen Containern verbracht werden kann, weil dann eine Kenntnis der enthaltenen personenbezogenen Daten durch Unbefugte, nicht ausgeschlossen werden kann.
Bei entsprechenden Feststellungen wurde deshalb von mir unverzüglich Abhilfe gefordert und empfohlen, dass die beteiligten Behörden bei der Vergabe von Dienstleistungen von der Haus verwaltenden Stelle einbezogen werden müssen, damit die jeweiligen Erfordernisse berücksichtigt werden können.

Sichere Aufbewahrung bedeutet aber nicht nur Schutz gegen unbefugte Zugriffe, sondern auch gegen sonstigen Verlust der Daten So werden häufig noch, wie Kontrollen ergeben, Sicherungskopien in einfachen Schränken in der Nähe der EDV-Technik aufbewahrt. Dies ist nicht akzeptabel, da im Brandfall nicht nur die Technik, sondern auch die Daten verloren gehen können. Aus diesem Grund sind Sicherungskopien stets in ausreichendem Maße räumlich getrennt von der IT-Technik in brandgeschützten Behältnissen aufzubewahren.

Mitunter gelangen Daten nur deshalb in unbefugte Hände, weil sie noch aufbewahrt werden, ohne dass hierfür eine Erforderlichkeit besteht. In einem Fall überprüfte ich nach einem Einbruch in einer öffentlichen Stelle die bisher dort getroffenen organisatorischen und technischen Maßnahmen zum Schutz der zu verarbeitenden personenbezogenen Daten. Es stellte sich heraus, dass auf der Festplatte eines gestohlenen PC noch Daten gespeichert waren, für die keine Erforderlichkeit mehr bestand. Unbeachtet geblieben war dabei, dass Daten in automatisierten Verfahren, die ausschließlich der Erstellung von Texten dienen, nur vorübergehend zu spei-

chern und danach unverzüglich zu löschen oder aber zu anonymisieren sind. Bei einer Löschung der automatisiert gespeicherten Texte nach dem Ausdruck in Papierform, wäre der Umfang der auf der entwendeten Festplatte gespeicherten personenbezogenen Daten wesentlich geringer gewesen. Besteht hingegen eine dienstliche Erforderlichkeit, die Texte zusätzlich automatisiert in einer vollständigen elektronischen Akte über einen längeren Zeitraum zu speichern sollte dies zweckmäßigerweise auf einem besonders gesicherten Server erfolgen. Im Ergebnis der Kontrolle wurde die betreffende Stelle aufgefordert, durch geeignete Maßnahmen, die diesbezüglichen geltenden Datenschutzbestimmungen einzuhalten bzw. durchzusetzen. Desweiteren wurden technische Hinweise gegeben, um der Gefahr von Einbrüchen vorzubeugen.

Fragen der Datensicherheit im Hinblick auf eine Gefährdung durch Einbrüche spielten auch bei einer anderen Kontrolle eine Rolle. Dort war der im Erdgeschoss untergebrachte Serverraum nicht ausreichend gegen unbefugten Zugriff und mögliche Elementarschäden gesichert. Da im Serverraum die zentralen Rechner vorgehalten werden und somit weitestgehend hier die Daten zentral gespeichert werden, kommt der Absicherung eines Serverraumes eine hohe Priorität zu. Insbesondere die Gewährleistung der Verfügbarkeit der hier vorgehaltenen Server und Daten sowie die Vertraulichkeit und Integrität der Daten sind von ausschlaggebender Bedeutung für die ordnungsgemäße Aufgabenerfüllung einer Behörde. Geeignete Maßnahmen zur Datensicherung sind daher zur Verhinderung des Zugangs Unbefugter z. B. auch der Einbau einer einbruchs- und feuerhemmenden Tür oder eine besondere Absicherung der Fensterbereiche.

Ein Schwerpunkt bei den Kontrollen ist auch die Frage der Einrichtung von Zugriffsrechten auf automatisierte Verfahren, mit denen personenbezogene Daten verarbeitet werden. Hierzu wird stets darauf hingewiesen, dass die Erforderlichkeit sich aus der jeweiligen Arbeitsaufgabe des Mitarbeiters ergibt. Die eingerichteten Zugriffsrechte sind auf das zur Aufgabenerfüllung zwingend notwendige Maß zu beschränken und nachvollziehbar vorzuhalten. Insbesondere für die Administratoren stellt die Dokumentation der Rechteverwaltung einen wichtigen Beleg für den ordnungsgemäßen Vollzug der von den fachlichen Stellen gestellten datenschutzrechtlichen Anforderungen dar. Bei der Umsetzung von Stellvertreterregelungen sind für die Vertreter eigene Accounts einzurichten, um die Revisionsfähigkeit von Zugängen und Zugriffen zu gewährleisten.

Solange die Nutzung der IT-Technik nur für dienstliche Belange vorgesehen und erlaubt ist, bestehen aus datenschutzrechtlicher Sicht keine Bedenken, wenn der jeweilige Vertreter oder Vorgesetzte im Rahmen seiner Vertretung oder Aufsicht Einsicht in die Dokumente seiner Mitarbeiter erhält, da diese Dokumente im Auftrag der Behörde erstellt sind. Entsprechendes gilt auch für E-Mails die innerhalb eines internen Netzes oder über das Internet versandt wurden. Eine Einsichtnahme verstößt nicht gegen das Briefgeheimnis, da der Mitarbeiter als Beauftragter der Behörde und nicht als Privatperson handelt. Zu beachten sind dabei lediglich im Hinblick auf die sich damit ergebenden Möglichkeiten einer Verhaltens- und Leistungskontrolle die Mitbestimmungsrechte des Personalrats nach § 74 Abs. 2 ThürPersVG. Wird demgegenüber aber auch eine private Nutzung der IT erlaubt, was der TLfD ausdrücklich nicht empfiehlt, führt dies zwangsläufig zu einer Einschränkung der Zugriffsrechte durch Vertreter oder der Kontrollmöglichkeiten durch den Vorgesetzten und bedarf dann geeigneter organisatorischer oder technischer Regelungen, die eine Einsichtnahme in private Nachrichten ausschließen.

Wiederholt gab es Klärungsbedarf bei der Erhebung und Nutzung von Verbindungsdaten bei Telekommunikationseinrichtungen. Dies unterliegt nach § 74 Abs. 2 Nr. 11 ThürPersVG stets der Mitbestimmung des Personalrats, da sie als technische Einrichtung geeignet sind, das Ar-

beitsverhalten der Mitarbeiter zu kontrollieren. Zur Gewährleistung des informationellen Selbstbestimmungsrechts der Mitarbeiter und der Gesprächsteilnehmer sind deshalb in der jeweiligen Dienstvereinbarung zur Nutzung von Telekommunikationseinrichtungen, soweit dies für private Zwecke erlaubt wird, Regelungen aufzunehmen, die eine Kenntnisnahme und Nutzung der Verbindungsdaten durch den Arbeitgeber allein auf die ordnungsgemäße Gebührenabrechnung beschränken. In der Regel wird hierzu die angerufene Telefonnummer verkürzt gespeichert. Eine „Überwachung“ der Daten über Gesprächsteilnehmer/Telefonnummern verbietet sich in jedem Fall. Die Daten dienen lediglich zur Zuordnung der Gebühren bzw. dem Mitarbeiter zur Überprüfung der ihm gegenüber in Rechnung gestellten privaten Telefongespräche. Eine weitere Verarbeitung und Nutzung kommt nur dann in Betracht, wenn von einem Mitarbeiter die Führung eines ihm zugeordneten privaten Telefonats bestritten wird. Dementsprechend sind auch die privaten Einzelverbindungsdaten nach Zahlung durch die Mitarbeiter zu löschen.

1.3 Einsatz mobiler IuK

Im 5. TB (15.16) wurde über Sicherheitsaspekte beim Einsatz drahtloser Netze berichtet. Nunmehr liegt auch eine Orientierungshilfe des AK Technik der DSB des Bundes und der Länder zum Datenschutz in drahtlosen Netzen vor (www.datenschutz.thueringen.de).
Drahtlose Netze wie WLAN (Wireless Local Area Networks) sind inzwischen schon alltägliche Praxis und werden insbesondere mit mobilen IT-Geräten genutzt. Der mittelbare Einsatz von WLAN bspw. für entfernte Zugriffe auf lokale Datenbestände oder zur elektronischen Kommunikation stellt allerdings nur eine von mehreren Sicherheitsrisiken beim Einsatz mobiler IT dar. Denn naturgemäß sind schon mit dem Einsatz mobiler IuK-Geräte wie Laptop, PDA (Personal Digital Assistant), Mobiltelefon oder Smart-Phone (als Kombination von Mobiltelefon und PDA) Gefahren für die Vertraulichkeit, Integrität und Verfügbarkeit der zu verarbeitenden Daten und aber auch der IuK-Infrastruktur verbunden. Zu verzeichnen ist nicht nur eine ständig wachsende Anzahl an eingesetzten mobilen Kommunikationsgeräten, sondern auch eine zunehmende Funktions- und Einsatzvielfalt dieser Geräte. Auch für die öffentlichen Stellen des Landes ist dieser Trend zutreffend. So wurden auf Anfragen oberster Landesbehörden bereits vom TLRZ Tests für mobile Anwendungen durchgeführt.
Im Mittelpunkt stand hierbei die BlackBerry-Technologie, um Benutzern über drahtlose Verbindungen mit Wireless-Geräten Zugriffe auf im lokalen Netz der jeweiligen Stelle vorgehaltene Daten zu ermöglichen. Von großem Interesse ist die hierbei zur Anwendung kommende sog. Push-Technologie, die es ermöglicht, auf dem Behördenserver eingehende E-Mails diese bei Abwesenheit des Nutzers direkt auf sein mobiles IT-Gerät weiterzuleiten.
Aus datenschutzrechtlicher Sicht ist es somit wichtig, auf die mit dem Einsatz mobiler IuK verbundenen Gefährdungen und Sicherheitsanforderungen hinzuweisen.
Charakteristisch für mobile Geräte sind u. a. ihre netzunabhängige Stromversorgung, ihr zu vernachlässigendes Gewicht und ihre geringen Abmessungen. Sie lassen sich somit bequem und ständig mit sich führen, wobei der milieuwechselnde Einsatz solcher Geräte typisch ist. So werden sie auch an potentiell unsicheren Orten wie Hotelzimmer, Bahn, Mietwagen, Schwimmbädern etc. genutzt und ihre geringen Abmaße verleiten zu einer ungesicherten Aufbewahrung. Als Ausdruck einer modernen Lebensform werden sie zudem gern Außenstehenden als Statussymbole präsentiert. Somit ergibt sich beim Einsatz mobiler IuK eine nicht geringe Gefährdung durch einen Verlust (Diebstahl/Verlieren) der Geräte. Zumal herstellerseitig ohne zusätzliche Schutzmaßnahmen die Daten in der Regel unverschlüsselt auf den Geräten gespeichert werden und für die Zugangskontrolle häufig nur einfache, kurze numerische Passwörter eingesetzt werden. Soweit keine regelmäßigen Datensicherungen erfolgten, ist bei einem Verlust der Geräte neben der möglichen Offenbarung der Daten auch deren unwiederbringlicher Verlust verbunden. Eine fehlende Datensicherungsstrategie (Backup) stellt somit

eine Schwachstelle auch bei der Nutzung mobiler IuK dar. Ohne zusätzliche Sicherheitsmaßnahmen ist auch die drahtlose Kommunikation mit GMS, GPRS, UMTS, WLAN oder Bluetooth ein Unsicherheitsfaktor, da Luftschnittstellen leicht zugänglich und abhörbar sind. Abgesehen von Laptops gibt es für die meisten mobilen Gerätearten kein dominierendes Betriebs- und Applikationensystem. Insofern ist eine „standardisierte“ Sicherheitslösung zum Einhalten der gesetzlich vorgegebenen Sicherheitsziele gemäß § 9 Abs. 2 ThürDSG (Vertraulichkeit, Integrität, Verfügbarkeit) schwierig. Da auch jeder Nutzer umfassend von den neuen Funktionen des Mobile Computings partizipieren möchte, können sich schon durch eine unsachgemäße Handhabung der Geräte, bspw. infolge fehlender detaillierter Einweisung der Nutzer, auch Risiken für die Sicherheit gespeicherter und übertragener Daten ergeben und ohne verbindliche Richtlinien für den Betrieb und den Einsatz der mobilen Geräte ist der Umgang mit diesen Geräten und den hier zu verarbeitenden Daten allein in das Ermessen der Nutzer gestellt. Wie die Praxis zeigt, kann schon eine fehlende zentrale Administration der Geräte sicherheitstechnische Risiken bergen. Das Fehlen der zentralen Administration kann u. a. ermöglichen, Software von unsicheren Quellen zu installieren, schadenstiftende Programme zu laden und ohne Sicherheitskontrolle weiter zu transportieren. Insbesondere für Smart-Phones, die über GPRS oder UMTS ständig online sind, besteht diese Gefahr. So ist hier schon äußerste Vorsicht bei der Installation von Klingeltönen aus dem Internet geboten. Auch ein nicht geregelter Einsatz flexibler Speicherkarten kann zur intensiven Verbreitung schadenstiftender Programme beitragen. Soweit keine Verzeichnisse über die eingesetzten mobilen Geräte und eventuell eingerichtete Verbindungen bspw. in das lokale Netz geführt werden, ist zudem die für eine sichere Betriebsweise notwendige Transparenz nicht gegeben.

Um den mit dem Einsatz mobiler IuK verbundenen Risiken zielgerichtet begegnen zu können, ist es generell wichtig, die mobile Infrastruktur als einen Bestandteil der gesamten IT-Struktur aufzufassen und in diese einzugliedern. Und für die Nutzer gilt es zu beachten, die schon mit dem Einsatz der herkömmlichen IuK vertrauten Sicherheitsregeln zum Umgang mit Internet und E-Mail auf die neuen mobilen Szenarien zu übertragen. Die Sensibilisierung der Nutzer hierfür ist äußerst wichtig, um den hiermit verbundenen Gefährdungen bewusst zu begegnen, aber auch um die verfügbaren und eingerichteten Sicherheitsmaßnahmen zu nutzen.
Insbesondere mobile Mitarbeiter möchten die mit der mobilen IT verbundenen Möglichkeiten, wie den Zugriff auf ihre Daten im internen Netz, auf ihre E-Mail-Postfächer oder den Terminkalender nutzen. Auch über das drahtlose Umfeld hinaus sind hier Sicherheitsmechanismen zur Authentifizierung, Verschlüsselung und Zugriffskontrolle erforderlich. Hier bieten insbesondere Smart-Phones mit ihrem breiten Funktionsspektrum entsprechende Möglichkeiten. Je nach Anbieter werden auch schon Sicherheitslösungen zum Zugriffsschutz und zur Verschlüsselung der gespeicherten Daten angeboten. Auch für die Datenübertragung werden Sicherheitslösungen auf der Basis von IPSec-VPN-Client-Programmen (5. TB, 15.1.2, 15.7, 15.16) angeboten, die eine wirksame Authentifizierung der Benutzer bzw. Geräte sowie verschlüsselte Datenübertragungen ermöglichen. Eine Alternative zur IPSec-Technologie bietet die SSL-basierte VPN-Technik. SSL (Secure Socket Layer) ist ein Internet-Protokoll, das die Authentizität des angewählten Rechners (Server) überprüft und die Daten verschlüsselt überträgt. Die VPN-Tunnel werden hier über die SSL-Verschlüsselung des Webbrowsers aufgebaut. Da die meisten Mobilfunkgeräte heute mit Webbrowsern ausgerüstet sind, ergibt sich damit der Vorteil, dass die bisher üblichen VPN-Clients auf den Endgeräten nicht installiert werden müssen. Über jedes mobile Endgerät, welches über einen Internetbrowser verfügt, kann somit eine geschützte Zugriffsverbindung zum lokalen Netz aufgebaut werden.

Wie bei der herkömmlichen IT sind auch für den Einsatz von mobiler IuK gemäß § 9 Abs. 2 ThürDSG auf der Grundlage eines Sicherheitskonzeptes die zu treffenden technischen und organisatorischen Maßnahmen zu ermitteln. Die umgesetzten Maßnahmen müssen dem Schutz-

bedarf der Daten und dem Einsatzzweck der mobilen IuK angemessen sein. Nachfolgend sind beispielhaft technische und organisatorische Maßnahmen aufgezeigt, die seitens der Verantwortlichen für den Einsatz mobiler IuK zu beachten sind, wie

- Erfassen aller mobilen Geräte im IuK-Geräteverzeichnis und eventuelle Aktualisierung der Verfahrensverzeichnisse,
- Vergabe verbindlicher Regelungen für den Einsatz der mobilen Endgeräte,
  Hierzu gehören Vorgaben zum Umgang mit dem Gerät, zur Verfahrensweise bei Verlust des Gerätes, zur Weitergabe an Dritte, zur Zulässigkeit privater Nutzung, zum Datenumgang (was darf wo gespeichert werden), Backup-Strategie etc.
- Zentrale Administration der Geräte u. a.:
  - Einrichtung eines einheitlichen Grundzustandes vor der Auslieferung an den Benutzer. Dies umfasst u. a. die Installation geprüfter Anwendungen, berechtigter Kommunikationsprofile, Virenscanner, Personalfirewall, Verschlüsselungssoftware/ Sicherheitsprotokolle, das Aktivieren der Sicherheitsmechanismen sowie das Deaktivieren aller nicht erforderlichen Dienste (z. B. Bluetooth).
  - Aktualisieren von Software und Benutzerprofilen sowie zeitnahes Einspielen aktueller Sicherheitspatches und Updates.

Zu den Sicherheitsvorkehrungen gehören auch Hinweise an die Nutzer zum Umgang und Einsatz der mobilen IuK, um die hiermit verbundenen Risiken zu minimieren. U. a. sind die Nutzer aufgefordert:

- die Geräte sicher vor Verlust aufzubewahren, insbesondere bei Nutzung in unterschiedlichen Milieus,
- den Einsatz in der Öffentlichkeit möglichst zu unterlassen, wenn sensible Daten gespeichert sind,
- den Verlust des mobilen Gerätes sofort der verantwortlichen Stelle zu melden, damit der Account des Nutzers unmittelbar gesperrt werden kann,
- das Zugangspasswort zu aktivieren, herstellerseitig vordefinierte Passwörter zu ersetzen, vorgegebene Grundsätze zur Passwortgestaltung und Nutzung an der Hard- und Software einzuhalten,
- nur genehmigte Software einzusetzen und eigenmächtig keine Veränderungen vorzunehmen,
- regelmäßige Datensicherungen (Backups) durchzuführen, auch Adressbücher zu sichern, eventuelle Einbeziehung der Konfigurationsdaten vorzunehmen, zu beachten, dass auch ein leerer Akku zu Datenverlust führen kann,
- keine Parameter für die Zugriffskontrolle auf das interne lokale Netz (Nutzerkennung, Nutzerpasswort) auf dem Gerät zu speichern,
- schutzwürdige Daten (auch) auf den mobilen Speicherkarten verschlüsselt zu speichern und
- keine solche Daten zu übertragen, soweit kein dem Stand der Technik entsprechend sicheres Kommunikationsverfahren eingesetzt wird.

Gemäß dem konkreten Einsatzziel der eingesetzten IuK und der Sensibilität der zu verarbeitenden Daten müssen die ergriffenen technischen und organisatorischen Maßnahmen vor allem sicherstellen:

- die Sicherheit der Daten auf dem Endgerät selbst (Gerätesicherheit),
- das Verhindern von eigenmächtigen Eingriffen in die zentral implementierten Hard- und Softwareprofile und der unbefugten Installation von Applikationen auf dem Endgerät (Applikationssicherheit),
- eine sichere Übertragung zwischen dem mobilen Endgerät und dem Behördennetzwerk (Übertragungssicherheit).

1.4 Zentrale Spam- und Virenprüfung an der Kopfstelle des CN

Unerwünschte Werbe-E-Mails, sog. Spam und virenbehaftete E-Mails werden sowohl für private Nutzer als auch für Behörden und Unternehmen zu einem wachsenden Problem. Mittlerweile sind über 50 % aller Nachrichten, die deutsche E-Mail-Empfänger erreichen, Spam[1]. Spam stellt nicht nur eine Massenbelästigung dar, sie binden erhebliche finanzielle, zeitliche und personelle Ressourcen und verursachen somit enorme wirtschaftliche Schäden. Ein spezielles Gesetz, das grundsätzlich Spamming verbietet oder unter Strafe stellt, gibt es in Deutschland nicht. Nach der deutschen Rechtsprechung ist allerdings eine Zusendung von Spam ohne vorherige Zustimmung des Adressaten grundsätzlich rechtswidrig. Wegen Verletzung seines allgemeinen Persönlichkeitsrechts kann der Empfänger bei unerwünschten Werbe-Mails die Unterlassung verlangen (§§ 823 Abs. 1, 1004 BGB). In Umsetzung der EU-Richtlinie 2002/85 (Datenschutz in der elektronischen Kommunikation) vom 12.07.2002 findet die einschlägige Rechtsprechung insofern Berücksichtigung, als in § 7 des novellierten Gesetzes gegen den unlauteren Wettbewerb (UWG) vom 03.07.2004 eine ausdrückliche Regelung aufgenommen wurde, der zufolge unverlangte Werbesendungen wettbewerbswidrig sind, wenn der Empfänger nicht vorher zugestimmt hat oder im konkreten Fall ein Interesse am Erhalt derartiger Mails nicht angenommen werden kann. Gemäß § 7 Abs. 2 Nr. 3 UWG ist Werbung per E-Mail ohne Einwilligung des Betroffenen eine unzumutbare Belästigung und damit unlauter im Sinne des Gesetzes und zwar unabhängig davon, ob es sich bei dem Empfänger um eine Privatperson oder einen Gewerbetreibenden handelt. Das Gesetz lässt lediglich unter engen Voraussetzungen (§ 7 Abs. 3 UWG) die Versendung von Werbe-E-Mails im Rahmen einer bestehenden Kundenbeziehung ohne deren Einwilligung zu, wenn diese bereits bei der Erhebung ihrer Daten auf ihr Recht zum Widerspruch gegen solche Mails hingewiesen wurden.
Die Praxis zeigt allerdings, dass allein mit diesen gesetzlichen Regelungen das weltweite Aufkommen von Werbe-E-Mails nicht zu unterbinden ist. Insofern müssen auch seitens der empfangenden Stellen technische und organisatorische Maßnahmen zur Spam-Abwehr ergriffen werden. Hierbei sind allerdings auch datenschutzrechtliche Aspekte zu berücksichtigen. So stand auch bei der Konzeption und Einführung einer zentralen Spam- und Virenprüfung durch das TLRZ an der Kopfstelle des Corporate Network (CN) der Landesverwaltung die Klärung datenschutzrechtlicher Fragen an. In Umsetzung dieses Konzeptes wurde ein zentraler E-Mail-Gateway mit den Funktionalitäten Spam-Erkennung und Markierung sowie Virenfilterung zum Einsatz gebracht. Aus der Sicht des Datenschutzes war hierbei zu prüfen, inwieweit beim Umgang mit den eingehenden E-Mails die gesetzlichen Regelungen, insbesondere das Fernmeldegeheimnis, eingehalten werden. Die auf der zentral eingerichteten Kopfstelle des CN eingehenden Mails unterliegen dem Schutz des Fernmeldegeheimnisses nach § 88 Abs. 1 TKG. Hier stellt sich also nicht wie beim Dienstherrn des Empfängers die Frage, ob das Telekommunikationsgesetz Anwendung findet, da dieser dessen Regelungen nur zu beachten hat, wenn er die private E-Mail-Kommunikation erlaubt.
Die konkreten Hinweise des TLfD, die aus datenschutzrechtlicher Sicht bei einer solchen Prüfung zu beachten sind, wurden vom TLRZ umgesetzt. Jedes Ressort kann grundsätzlich eigenständig entscheiden, ob seine E-Mails dieser zentralen Prüfung auf Spam-Verdacht unterzogen werden soll. Das Scannen der eingehenden Mails läuft automatisiert ab. Entsprechend dem Verfahrensablauf der Prüfung, insbesondere unter Berücksichtigung der automatisierten Funktionsweise der eingesetzten Scanner, ist grundlegend davon auszugehen, dass hierbei keine visuelle Einsichtnahme in Kommunikationsinhalte und die näheren Umstände der Kommunikation erfolgt. Das Scannen auf Spam erfolgt durch ein Bewertungsprogramm, das anhand vorgegebener Kriterien eine Bewertung der Mail im Hinblick auf SPAM vornimmt. Je höher die hier vergebene Bewertungspunktzahl ausfällt, umso stärker ist der Verdachtsgrad des Vorliegens einer Spam-Mail. Die Auflistung der erkannten Kriterien wird im Header (Kopfzeilen)

[1] Zeitschrift Business & IT 5/2005; FAZ vom 04.05.2005

der Mail dargestellt. Ebenfalls wird hier die erreichte Wertung der Mail eingetragen sowie bei Verdacht auf Spam in einer weiteren Headerzeile das positive Resultat YES gesetzt. Durch Eintragen dieser Informationen in den Header, anstatt in der Betreffzeile, wird die Integrität der Mail nicht verletzt. Die diesbezügliche Auswertung der im Header eingetragenen zusätzlichen Informationen des Ergebnisses der Kontrolle auf Spam kann sich der lokale Empfänger anzeigen lassen. Im Ergebnis der Prüfung werden vom TLRZ keine Mails verworfen oder gelöscht. Alle gescannten Mails werden dem jeweiligen lokalen E-Mail-Server bzw. dem Empfänger zugesandt. Die endgültige Entscheidung, ob der festgestellte Verdacht auf Vorliegens einer Spam-Mail zutrifft, liegt somit beim Empfänger der Mail.

Nach Mitteilung des TLRZ sind auf dem E-Mail-Gateway weiterhin zwei Virenscanner aktiv. Wird bei der automatisierten Prüfung ein Virus entdeckt, so wird an die Empfängeradresse automatisch eine Nachricht generiert und in einer neuen E-Mail an den Empfänger versandt. Dem Adressaten wird in einer Information mitgeteilt, dass von einem bestimmten Absender an ihn eine virenverseuchte Mail gesendet wurde. Die virenbehaftete Mail wird für 30 Tage in Quarantäne gestellt. Obwohl in der Regel davon abzuraten ist, kann somit im Ausnahmefall der Empfänger unter Beachtung bestimmter Sicherheitskriterien diese E-Mail noch erhalten. Hierzu muss er Kontakt mit dem TLRZ aufnehmen. Ansonsten wird von einem fehlenden Interesse an der Bereitstellung dieser E-Mail ausgegangen und diese wird nach 30 Tagen automatisch gelöscht. Mit dieser Lösung obliegt dem Empfänger eine erhebliche Eigenverantwortung in Bezug auf die Sicherheit seines lokalen IT-Systems.
Vom TLRZ wurden alle am CN angeschlossenen Stellen detailliert über den Verfahrensablauf zur Prüfung eingehender E-Mails auf Spam-Verdacht und auf schadenstiftende Elemente sowie zum Umgang nicht zustellbarer E-Mails informiert. Mit dieser Information an die beteiligten Stellen kam das TLRZ auch der Forderung des TLfD gemäß § 9 Abs. 2 Nr. 6 ThürDSG nach, den diesbezüglichen Verfahrensablauf zu dokumentieren und somit nachvollziehbar für alle Beteiligten darzulegen. Dies ist eine Möglichkeit der Verfahrensweise zum jetzigen Zeitpunkt.

1.5 Datenschutzrechtliche Aspekte von Protokollierungen

Ein wesentliches Sicherheitsziel der Datenverarbeitung ist die Gewährleistung der Revisionsfähigkeit der durchgeführten Verarbeitungsprozesse. Insbesondere bei der Verarbeitung personenbezogener Daten geht es hierbei nicht nur darum die Daten verarbeitenden Stellen (Behörden, Unternehmen) vor Schäden zu bewahren, sondern auch den Einzelnen als Betroffenen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. In § 9 Abs. 2 Nr. 5 ThürDSG wird demzufolge auch für die Verarbeitung von personenbezogenen Daten u. a. gefordert, dass festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Sowohl bei der datenschutzrechtlichen/ sicherheitstechnischen Bewertung von Sicherheitskonzepten durch den TLfD als auch aufgrund von Anfragen von öffentlichen Stellen zeigte sich, dass für die datenschutzgerechte Umsetzung dieses Sicherheitszieles ein zunehmender Informationsbedarf besteht. Nachfolgend deshalb aus datenschutzrechtlicher Sicht einige grundsätzliche Hinweise zu aktuellen Fragen im Zusammenhang mit Protokollierungsvorgängen:
Sowohl Betriebssysteme als auch Anwendungsprogramme ermöglichen neben spezifischen Protokollierungsprogrammen das Aufzeichnen einer Vielzahl von benutzer-, prozess- und sicherheitstechnischen Ereignissen. Die Speicherung der protokollierten Daten erfolgt in sog. Log-Dateien. Solche Log-Dateien kamen historisch gesehen mit den Großrechnern verbreitet zum Einsatz. Sie kommen heutzutage nahezu auf allen IT-Systemen zum Einsatz und werden vorwiegend zur Beweissicherung des ordnungsgemäßen Ablaufes der Datenverarbeitungsprozesse geführt. Aufgrund ihrer möglichen Personenbeziehbarkeit stellen sie aber auch ein Instrument zur Kontrolle der Benutzer und Verwalter der IuK-Systeme dar. Gemäß § 20 Abs. 4

ThürDSG dürfen personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden. Demnach ist bspw. eine Nutzung zu Zwecken der Verhaltens- und Leistungskontrolle nicht erlaubt.
Auch für Protokollierungen ist das Prinzip der Erforderlichkeit und der Angemessenheit zu beachten. Der Grundsatz zur Zweckbindung erfordert konkrete Festlegungen an die Nutzung der Protokolldaten und somit schon im Vorfeld präzise Aussagen zur Zielstellung von Protokollierungen. Die hierzu in der Praxis häufig gebrauchte allgemeine Formulierung, dass die „durchgeführten Protokollierungen zu Sicherungszwecken und/oder zur Gewährleistung der Datensicherheit erfolgen“ ist somit unzureichend. Konkrete Zweckvorgaben für eine Protokollierung wären bspw. der Einsatz der Protokollierung zur Kontrolle der Einhaltung dienst- oder arbeitsrechtlicher Vorgaben, zur Aufrechterhaltung der Systemsicherheit, zur Prüfung/ Optimierung der Performance des IT-Systems und/oder zur Analyse und Behebung technischer Schwachstellen/ Fehler. Unter Beachtung einer solchen Zweckbindung ist es grundsätzlich zulässig, auch personenbezogene Daten zur Nachvollziehbarkeit von Nutzeraktivitäten zu erheben und auszuwerten, z. B. zur Aufdeckung von vorsätzlichen Datenmanipulationen oder unbefugten Zugriffsversuchen. Auch für das Erheben und Auswerten von Protokolldateien gelten die datenschutzrechtlichen Grundsätze der Datenvermeidung und der Datensparsamkeit. Das heißt, die Gestaltung der Protokolle hat sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten oder zu nutzen. Soweit es möglich ist, ist somit von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen.
In jedem Fall bedarf es genauer Festlegungen, wer diese Daten wie, mit welchen Hilfsmitteln, in welchen Abständen und zu welchem Zweck auswerten darf. Soweit personenbezogene Daten der Mitarbeiter protokolliert werden, ist der Personalrat bzw. Betriebsrat rechtzeitig zu informieren, damit er seine Beteiligungsrechte wahrnehmen kann. Enthalten die Protokolldaten auch personenbezogene Daten über Betroffene, z. B. wenn in deren zu verarbeitenden Datensätzen von den Nutzern (z. B. Sachbearbeiter) inhaltliche Ergänzungen oder Änderungen vorgenommen werden müssen und diese nachvollziehbar protokolliert werden, unterliegen auch diese Daten der Zweckbindung gemäß § 20 Abs. 4 ThürDSG. Im Übrigen haben die Betroffenen nach § 13 Abs. 1 Satz 2 ThürDSG kein Recht auf Auskunft zu diesen Daten.

Die gesetzlichen Regelungen enthalten keine ausdrücklichen zeitlichen Vorgaben für die Vorhaltung von Protokolldaten. Allein für die Nutzung von Telediensten sind anfallende personenbezogene Daten unmittelbar nach Beendigung der Nutzung zu löschen, soweit sie nicht für Zwecke der Abrechnung mit dem Nutzer erforderlich sind.
Gemäß den konkreten Gegebenheiten ist somit die Speicherungsdauer von der Daten verarbeitenden Stelle verbindlich festzulegen, wobei sie in der Regel ein Jahr nicht überschreiten sollte. Protokollierungen können je nach Erforderlichkeit in den unterschiedlichsten IuK-Prozessen durchgeführt werden. So auch bei der Nutzung des Internet sowie beim E-Mail-Verkehr (6.9). Zur Zulässigkeit solcher Protokollierungen wird auf die Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz des AK Medien verwiesen (www.datenschutz.thueringen.de).

Um Protokollierungen angemessen auszuführen und den protokollierten Datenumfang auch überschaubar zu gestalten, sind je nach Einsatzzweck die relevanten zu protokollierenden Ereignisse schon im Vorfeld sorgfältig auszuwählen. Insbesondere ist zu prüfen, in welchen Fällen es ausreichend ist, nur das fehlgeschlagene Ereignis festzuhalten. Häufig trifft dies für Regelübertretungen zu, z. B. beim Überschreiten der maximal zulässigen Zugangsversuche eines Logins oder bei der Feststellung unzulässiger Objekt- und Dateizugriffe. Andererseits sind auch erfolgreiche Ereignisse, wie durchgeführte Änderungen an den eingestellten Systemricht-

linien oder inhaltliche Änderungen an Datenobjekten aus Sicherheitsgründen nachvollziehbar festzuhalten. Als Nachweis unberechtigter Eingriffsversuche ist die Protokollierung vorwiegend fehlgeschlagener Ereignisse wichtig. Zur Nachvollziehbarkeit ausgeführter Aktionen von Berechtigten (Mitarbeiter, Administratoren) sind auch die erfolgreichen Ereignisse einzubeziehen.
In den Anwendungssystemen sind je nach Sensibilität der Daten Zugriffe auf und Veränderungen an Daten stichprobenweise oder vollständig zu protokollieren. Die mit einer lückenlosen Protokollierung entstehenden umfangreichen Datenmengen sind gemäß dem Stand der Technik beherrschbar. Eine effektive und gezielte Auswertung der zumeist massenhaft anfallenden Protokolldaten erfordert jedoch den Einsatz entsprechender automatisierter Auswertungsprogramme. Ohne solche werden Protokolldateien zu Datenfriedhöfen.

Mit Hilfe von Protokollierungen können i. d. R. Verstöße gegen vorgegebene Regelungen nur nachträglich festgestellt werden. Verhindert werden können sie damit nicht. In der Praxis zeigt sich allerdings, dass allein schon der Einsatz von angemessenen und notwendigen Protokollierungen einen vorbeugenden Sicherheitseffekt bewirkt. Durch die Auswertung protokollierter Verstöße können weiterhin die getroffenen technischen und organisatorischen Maßnahmen gezielt aktualisiert bzw. ergänzt werden, um mögliche Sicherheitsverletzungen zukünftig schon präventiv auszuschließen.
Protokollierungen erfordern ein planmäßiges Vorgehen, um letztendlich auch ihren Einsatz verbindlich in Dienst-/Betriebsvereinbarungen zu regeln. So sind schon im Vorfeld u. a. folgende Festlegungen zu treffen:

- welche Ereignisse/Aktionen auf welchen IT-Systemen und in welchen Programmsystemen aufzuzeichnen sind,
- welche Datenobjekte zu erfassen sind,
- Stichproben- oder Vollprotokollierung,
- auf welchen IT-Systemen/Datenträgern die Protokolldateien physisch vorgehalten werden,
- zum Speicherumfang der Protokolldateien,
- zur Archivierung/Auslagerung der Aufzeichnungen,
- zur Auswertung der Protokolle,
  - wer darf die Protokolle wann und wie auswerten,
  - welche Auswertungssoftware wird eingesetzt,
- Fristen zum Löschen der gespeicherten Datensätze,
- zur Unterrichtung der Mitarbeiter über die durchzuführenden Protokollierungen,
- Maßnahmen zum Schutz der protokollierten Daten vor unbefugten Zugriff sowie zur Verhinderung und zur Aufdeckung von Manipulationsversuchen,
- zur Vorgehensweise bei Feststellung von Verstößen,
- zur Einbeziehung des DSB und des Personal-/Betriebsrates.

1.6 Sicherheitstechnische Anforderungen beim Löschen elektronischer Datenträger

Seitens des TLfD wurde bereits in vergangenen Tätigkeitsberichten (1. TB, 15.9; 5. TB, 15.8) auf die datenschutzgerechte Löschung von auf elektronischen Datenträgern (DT) vorgehaltenen personenbezogenen Daten bei PCs, Druckern und Kopierern hingewiesen.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten (DSB) des Bundes und der Länder hat nun eine Orientierungshilfe zum Löschen magnetischer Datenträger erarbeitet. Die hier aufgeführten Empfehlungen sind für ein datenschutzgerechtes Löschen von Daten, die auf magnetischen Datenträgern gespeichert sind, zu beachten. Die Orientierungshilfe definiert auch Anforderungen an Softwarewerkzeuge zum

sicheren Löschen, die als Auswahlkriterien bei deren Beschaffung/Einsatz herangezogen werden können.
Diese Orientierungshilfe ist im Internet abgelegt unter www.datenschutz.thueringen.de.

Auch in der Thüringer Landesverwaltung steigt die Anzahl an auszusondernder oder defekter IT-Technik stetig an, sodass eine zentrale datenschutzgerechte Entsorgung für die öffentlichen Stellen des Landes aus datenschutzrechtlicher Sicht durchaus von Interesse wäre.

Bei der datenschutzgerechten Löschung personenbezogener Daten auf DT sind auch IT-Bürogeräte, die ebenfalls über elektronische DT verfügen, mit einzubeziehen. Bisher zumeist als separate Geräte eingesetzt, werden deren Funktionen zunehmend durch sog. Multifunktionsgeräte übernommen, die zentral und eingebunden in das lokale Netz somit einer Vielzahl von Nutzern zur Verfügung stehen.
Diese Geräte verfügen über elektronische DT mit einer hohen Speicherkapazität, auf denen eine Vielzahl unterschiedlicher Daten infolge der hier ausgeführten Kopier-, Druck- und Scan-Vorgänge vorgehalten werden. Eine endgültige Löschung dieser Daten gemäß § 16 ThürDSG erfolgt hier, wie auch bei den herkömmlichen IT-Geräten in der Regel nicht (5. TB, 15.8). Verschiedene Hersteller bieten deshalb für ihre Geräte, neben der Möglichkeit einer personenbezogenen Zugriffskontrolle auf die hier gespeicherten Daten und deren Verschlüsselung, auch Sicherheitstools zur physischen Löschung der Daten an. Die öffentlichen Stellen des Landes sind daher angehalten, schon bei der Beschaffung der Geräte auf die Bereitstellung solcher Sicherheitsfunktionalitäten zu achten.

1.7 Datenschutz bei Auktionen von Handys und Computern

Laut einer Mitteilung im Internet werden von Thüringer Finanzämtern gepfändete Gegenstände sowie ausgesondertes Inventar der Verwaltung bei Internetauktionen angeboten.
In diesem Zusammenhang habe ich gegenüber der OFD auf die datenschutzrechtliche Verpflichtung hingewiesen, dass insbesondere bei Handys und Computern, personenbezogene Daten der bisherigen Nutzer vor Übergabe an den neuen Eigentümer zuverlässig zu löschen sind. Meiner Forderung, auf der entsprechenden Internetseite auf die zur Verhinderung einer Offenbarung personenbezogener Daten gegenüber unbefugten Dritten vorgesehenen Maßnahmen gem. § 9 ThürDSG hinzuweisen, wurde nachgekommen. Es wurde zugesichert, dass der Verpflichtung zur Datenlöschung nachgekommen wird, wobei die ordnungsgemäße Löschung durch ein Protokoll zu dokumentieren ist.
Ebenso habe ich die Obersten Landesbehörden, den Thüringer Landtag, den Thüringer Rechnungshof, die kommunalen Spitzenverbände sowie die Städte und Landkreise mit der Bitte um Rückäußerung über die Problematik in Kenntnis gesetzt und auf das erforderliche Löschen und Vernichten von Daten und Datenträgern hingewiesen (5. TB, 15.8). Nach Auskunft der befragten Stellen wird die Zollauktion nur vereinzelt genutzt. Dabei sind Handys, Computer, Kopierer und Drucker nicht veräußert worden.

1.8 E-Government in der Thüringer Landesverwaltung

In meinem letzten Tätigkeitsbericht (5. TB, 15.4) wies ich bereits darauf hin, dass im Freistaat Thüringen eine Arbeitsgruppe "Electronic Government" gebildet wurde, um die Bestrebungen zur Verwaltungsmodernisierung auf allen Ebenen der Verwaltung auf der Basis einer einheitlichen Technologie zu unterstützen und zu koordinieren.

Per Kabinettsbeschluss wurden am 19. Oktober 2004 dem neu eingerichteten Steuerkreis Verwaltungsreform, IT und eGovernment im Thüringer Finanzministerium die Aufgaben der res-

sortübergreifenden Umsetzung des eGovernment-Konzeptes des Freistaates und die verstärkte Abstimmung zwischen diesen Aktivitäten und den Verwaltungsstrukturmaßnahmen übertragen.

Derzeit wird im Rahmen von eGovernment ein Service Portal für die Bürger und die interne Verwaltung aufgebaut.
Für die Nutzung des Service Portals wird ein zentraler Verzeichnisdienst, auf der Basis von Oracle eingerichtet (OID). Zur Authentifizierung der Landesbediensteten sollen dazu die bereits im Active Directory (AD) der Thüringer Landesverwaltung gespeicherten personenbezogenen Daten (wie bspw. Name, Vorname, Behörde, Telefonnummer) übernommen werden. Vom TFM wurde auf Nachfrage zur Erforderlichkeit einer solchen Datenübernahme mitgeteilt, dass auch bspw. Vorschriftensammlungen oder Mitteilungen in das Service Portal eingestellt werden sollen, so dass voraussichtlich alle Beschäftigten im OID vorhanden sein werden, um die umfassenden Anwendungen nutzen zu können. Darüber hinaus werden nach dem derzeitigen Stand keine Daten außerhalb des Landesnetzes zugänglich gemacht. Damit ist in der Regel keine weitergehende Persönlichkeitsbeeinträchtigung als mit der bereits jetzt möglichen Einsichtnahme in Daten des AD durch die Beschäftigten des Landes gegeben. Somit bestehen gegen diese Datenübernahme aus datenschutzrechtlicher Sicht keine Bedenken.
Der Auffassung des TFM, die Fachanwendungen zukünftig in Form von zwei Fachanwendungsinstanzen im internen und externen Portalsegment aus architektonischer, sicherheitstechnischer Sicht bereitzustellen, wird auch seitens des TLfD aus datenschutzrechtlicher Sicht zugestimmt.
Sowohl zur Bereitstellung des Formularservers (1.8.2) als auch zur Fachanwendung HAMASYS (1.8.1) wird bspw. der neu aufzubauende Verzeichnisdienst des Service Portals benötigt.
Im Übrigen sei darauf hingewiesen, dass bei den Fachanwendungen § 3 a Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) - elektronische Kommunikation - zu beachten ist (5.1).

Zur Absicherung des Service Portals Thüringen werden aus datenschutzrechtlicher Sicht hohe Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen gestellt. Gemäß § 9 Abs. 2 ThürDSG sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage eines Sicherheitskonzepts zu ermitteln und haben je nach der Art der zu schützenden Daten deren Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, die Revisionsfähigkeit der Verarbeitung und die Transparenz des Verfahrens zu gewährleisten.
Dem TLfD liegt die Strukturierung des IT-Sicherheitskonzeptes für das Service Portal mit den entsprechenden Zielen vor. Die Grundlage hierfür bilden neben dem ThürDSG das IT-Sicherheitshandbuch des BSI, herstellerspezifische Sicherheitshinweise, sowie im Land Thüringen geltende Sicherheitsrichtlinien und Sicherheitskonzepte. Das Sicherheitskonzept soll dabei direkt auf die im Rahmen des Gesamtprojektes zu erstellenden Feinkonzepte aufbauen.
In einer Stellungnahme des TLfD wurden hierzu entsprechende Hinweise und Anregungen zur weiteren Verfahrensweise gegeben, welche Berücksichtigung finden sollen.

Das zentrale eGovernment-Projekt "thegov" hat als Projektziel die Bereitstellung einer Serviceplattform für die Landes- und Kommunalverwaltung in Thüringen. Mit der Plattform ist künftig die Nutzung von zentralen Serverdiensten wie z. B. E-Mail, LDAP und Zertifikatsverzeichnisdienst sowie die Gewährleistung der Vertraulichkeit der hier vorgehaltenen Daten u. a. durch eine Verschlüsselung möglich.

Durch die zentrale Bereitstellung eines Dokumentenmanagement- und Vorgangsmanagementsystems (DMS) VISkompakt (5.1.3) soll landesweit eine schrittweise Ablösung der bisher papierorientierten Schriftgutverwaltung eingeleitet werden. Dieses DMS stellt neben der elektronischen Vorgangs- und Dokumentenverwaltung weitere Werkzeuge zur Registratur, zum Um-

gang mit Aktenplänen und elektronischen Akten, zur Volltextrecherche, zur Verwaltung von Adressen und Postbüchern zur Verfügung. Bei der Umstellung der Aktenführung von Papier auf EDV gibt es allerdings eine Reihe datenschutzrechtliche Aspekte zu beachten. So sind neben einem Sicherheitskonzept, vorab auch Fragen zur gesetzlichen Zulässigkeit der automatisierten Verarbeitung von Daten aus datenschutzrechtlicher Sicht, zum Schutzniveau der Daten, zu Zugriffsberechtigungen, zur Protokollierung von Vorgängen und Ereignissen, zur Löschung/Sperrung von Daten und zur Archivierung zu klären.

1.8.1 Das HAushalts-MAnagement-SYStem (HAMASYS) in der Thüringer Landesverwaltung

Bei HAMASYS handelt es sich um ein HAushalts-MAnagement-SYStem.
HAMASYS gliedert sich in folgende Teilprojekte:

1. Landesweite Einführung eines einheitlichen IT-Verfahrens für die Mittelbewirtschaftung, Kasse und Vermögensnachweisführung/ Inventarisierung
2. Einführung eines modernen Verfahrens für die Haushaltsaufstellung
3. Einführung der Kosten- und Leistungsrechnung in geeigneten Bereichen
4. Controlling des gesamten Landeshaushaltes.

Ziel des Vorhabens sind genauere und aktuellere Aussagen zum Haushaltsmitteleinsatz sowie einen Verzicht auf Doppelerfassungen, wodurch Verwaltungsabläufe beschleunigt, Kostenstrukturen dargestellt sowie Wirtschaftlichkeitsbetrachtungen, Prognosen zur Kostenentwicklung und Vergleiche zwischen gleichartigen Behörden ermöglicht werden sollen. Daraus verspricht man sich Ansatzpunkte für eine Optimierung der Steuerung des Landeshaushaltes und eine Kostenreduzierung. Die Transparenz der Kosten soll durch die Abrechnung nach Produkten (dem liegt ein von der Finanzministerkonferenz des Bundes und der Länder 2004 beschlossener bundeseinheitlicher Produktrahmenplan zu Grunde), Kostenstellen, Kostenarten und Kostenträger erhöht werden. Unter Kostenstelle ist der Ort der Kostenentstehung - bspw. ein Referat - zu verstehen. Die Kostenstelle sollte mindestens drei Personen umfassen, damit ein Personenbezug weitestgehend ausgeschlossen werden kann. Das Gesamtprojekt soll ca. 350 Behörden mit 5000 bis 6000 Nutzern umfassen.
Dem Verfahren liegt der Verzeichnisdienst „Active Directory“ und das Protokoll für Verzeichnisdienste „LDAP“ zu Grunde.
Jeder Nutzer (bspw. HH-Sachbearbeiter, zur Auszahlungsanordnung Befugte, Kassenmitarbeiter, Inventarisierer, Controller) soll mittels Web-Client über das Corporate Network mit der Datenbank verbunden werden. Dabei muss sich der Nutzer nur einmal anmelden und kann das ganze System entsprechend seinen zugewiesenen Zugriffsrechten nutzen (Single Sign On- Fähigkeit). Bei der Nutzung von HAMASYS wird die vom Land bereitgestellte PKI-Infrastruktur genutzt. Es ist vorgesehen, dass Auszahlungsanordnungen mittels einer fortgeschrittenen Signatur gezeichnet werden.
Das erste Teilprojekt umfasst die Mittelbewirtschaftung, die Kasse und die Vermögensnachweisführung / Inventarisierung. Pilotbehörden sind die OFD Erfurt und das Thüringer Landesamt für Lebensmittelsicherheit und Verbraucherschutz (TLLV). Die Phase des „Costumizing“, die die Einstellung der Anfangsdaten und Abbildung der Projektstrukturen beinhaltet wurde mittlerweile innerhalb der Pilotbehörden abgeschlossen. Die Freigabe des Projektes in den Pilotbehörden wurde für Dezember 2005 angekündigt. Gleichzeitig soll das Verfahrensverzeichnis, eine Vereinbarung zur Auftragsdatenverarbeitung gemäß § 8 ThürDSG mit dem ZIV sowie das Sicherheitskonzept vorliegen. In den Jahren 2006 und 2007 soll die Einführungsphase abgeschlossen sein und das Projekt in den Produktivbetrieb gehen.
In diesem Teilprojekt fallen folgende Daten an:

1. Die auf den Auszahlungsanordnungen angegebenen Daten wie z. B. Name, Vorname, Adresse, Bankverbindung von Mitarbeitern der Landesverwaltung, Bürgern und Firmen werden vom Client der einzelnen Dienststellen in die Datenbank HAMASYS im ZIV übertragen. Beim Datenbankzugriff ist die Mandantenfähigkeit gewährleistetet, d. h. jede Dienststelle hat nur Zugriff auf ihre eigenen Daten.
2. Im Rahmen des Controlling des gesamten Landeshaushaltes werden aus dem Datenbestand Statistiken, ohne unmittelbaren Personenbezug, erstellt.

1.8.2 Formularserver

Als eine zentrale Anwendung im Service Portal der Thüringer Landesregierung wird der Formularserver fungieren.
Die Landesregierung strebt die Ablösung von Papierformularen durch elektronische Formulare in großem Umfang an. Ein wesentlicher Schritt in diese Richtung war deshalb im Rahmen des eGovernment-Konzeptes der Landesregierung auch die Bereitstellung eines Formularservers, um die teilweise noch dezentral vorgehaltenen Formulare zu bündeln und, soweit erforderlich und sachgerecht, auch ressortübergreifend zur Verfügung zu stellen, um diese in die elektronische Vorgangsbearbeitung integrieren zu können.

Die Landesregierung hält es darüber hinaus für geboten, künftig die Formulare nicht nur elektronisch zum Ausdruck bereitzustellen, sondern schrittweise deren elektronische Übertragung auszubauen. Angefangen mit der Möglichkeit, Formulare elektronisch auszufüllen, über automatische Plausibilitätsprüfungen bis hin zur elektronischen Übersendung an die Verwaltung und elektronischen Bearbeitung in der Verwaltung sollen nicht nur die Formularbereitstellung, sondern auch die Geschäftsprozesse der Verwaltung optimiert werden[2].

Mit dem Formularservice für Thüringen möchte das Land die technologischen, administrativen und organisatorischen Voraussetzungen zur Effektivierung der formularbasierten Verwaltungsprozesse schaffen:
- Angebot eines umfangreichen, qualitativ hochwertigen und sachgebietsbezogenen Formularpools zur Unterstützung der formularbasierten Geschäftsprozesse in Verwaltungen,
- Schaffung eines gemeinsamen, einheitlichen Zugangspunktes zu unterschiedlichen Bearbeitungssystemen und -vorgängen,
- Bereitstellung einer Plattform zur medienbruchfreien Erstellung und Bearbeitung von formularbasierten Vorgängen

Soweit mit diesen Formularen auch personenbezogene Daten elektronisch übertragen werden, spielen datenschutzrechtliche Aspekte eine wesentliche Rolle. Hier wird der TLfD auch künftig beratend tätig werden.

1.9 Datenschutzgerechter Anschluss an Internet und Online-Banking bei Gerichtsvollziehern

Im 5. TB (15.9) berichtete ich über Sicherheitsaspekte beim Online-Banking von Gerichtsvollziehern. Anlass war die Entscheidung des TJM, den Gerichtsvollziehern seines Geschäftsbereiches die Teilnahme am Online-Banking-Verfahren zu gestatten. In Absprache mit dem TLfD wurde der Einsatz dieses Verfahrens allerdings an die Einhaltung erforderlicher sicherheitstechnischer Vorgaben gebunden. Die hierfür vorgegebenen technischen und organisatorischen Sicherheitsmaßnahmen sollten sich zunächst im praktischen Einsatz bewähren und wurden deshalb zunächst als ergänzende Bestimmungen zu der Verwaltungsvorschrift „Einsatz von EDV-Technik im Gerichtsvollzieherbüro“ erlassen. U. a. werden hier die für die Gerichtsvoll-

[2] Drucksache 4/275 vom 27.10.2004

zieher zuständigen Prüfungsbeamten verpflichtet, die Sicherheitsstandards der eingesetzten EDV regelmäßig zu überprüfen. Nach der Erprobung sollen die Regelungen in die bestehende Verwaltungsvorschrift aufgenommen werden. Das Thüringer Oberlandesgericht wird hierzu einen Erfahrungsbericht erstellen, anhand dessen die Wirksamkeit und Praktikabilität der erfolgten Vorschrift/ Regelungen zur Teilnahme am Online-Banking geprüft werden. Zwischenzeitlich teilte mir das TJM mit, dass dem Thüringer Oberlandesgericht der Kontrollumfang für die Prüfungsbeamten der Gerichtsvollzieher zu hoch erschien. Die Prüfungsbeamten hätten nicht die erforderlichen EDV-Kenntnisse, den wirksamen Einsatz der Sicherheitsapplikationen zu prüfen. Da insoweit unklar war, welchen Umfang die Prüfungstätigkeit bei den Gerichtsvollziehern haben soll, überarbeitete das TJM vorab diese ergänzende Vorschrift zum Online-Banking. In der Neufassung wird nun deutlicher geregelt, dass in erster Linie der Gerichtsvollzieher für die Sicherheit beim Online-Banking und den Schutz seines PC verantwortlich ist. Daneben wurde die Kontrolle der Prüfungsbeauftragten auf den Einsatz der Sicherheitsapplikationen und ihrer testweisen Nutzung beschränkt. Desweiteren wurde der Vorschlag des TLfD aufgegriffen, ausschließlich nur Chipkartenlesegeräte der Klasse 3 zum Einsatz zuzulassen. Diese verkörpern derzeit den höchsten sicherheitstechnischen Stand. Insbesondere wird hier die Eingabe der PIN direkt auf die Chipkarte übermittelt, ohne im Rechner zwischengespeichert zu werden. Damit wäre ein Auslesen der PIN durch bösartige Softwareprogramme (Trojaner) nicht möglich.

Aufgrund der bundesweiten Bedeutung dieser Thematik hat zwischenzeitlich auch eine Arbeitsgruppe des AK Technik der DSB, an dem sich auch der TLfD beteiligte, eine Orientierungshilfe zum datenschutzgerechten Anschluss an Internet und Online-Banking bei Gerichtsvollzieherinnen und Gerichtsvollziehern erarbeitet. Die Orientierungshilfe enthält u. a. sicherheitstechnische Hinweise zur Trennung von lokalen Rechnern und externen Systemen, zum Anschluss an das Internet, zum E-Mail-Dienst, zum Virenschutz und zum Online-Banking. Maßgebende Sicherheitsvorkehrungen, die schon in den oben genanten ergänzenden Regelungen des TJM bestimmt sind, werden hier bundesweit empfohlen. Die Orientierungshilfe steht zur Einsicht und zum Abruf unter der Web-Adresse www.datenschutz.thueringen.de zur Verfügung.

1.10 Sicherheitsfragen bei der Internettelefonie Voice over IP (VoIP)

Unter Voice over IP versteht man die Übertragung von Sprache über IP (Internet Protocol)-basierte Netze. Stellt das IP-Netz ein Intranet bzw. das Internet dar, so spricht man auch von Intranet- bzw. Internet-Telefonie. Grundsätzlich sind folgende Arten der Sprachkommunikation mit VoIP zu unterscheiden:

- Kommunikation PC-zu-PC,
- Kommunikation PC-zu-Telefon,
- Kommunikation Telefon-zu-Telefon.

Sowohl im privaten Bereich als auch in Unternehmen und Behörden kommt zunehmend VoIP zum Einsatz. Anfang des Jahres 2005 verzeichneten die Voice over IP-Anbieter bereits rund eine halbe Million Anschlüsse in Deutschland.[3] Ein neues Einsatzgebiet für VoIP ist die Übertragung der Sprachdaten über drahtlose Netze (Voice over WLAN).
Eine technische Herausforderung der Sprachübertragung über IP-Netze ist die Absicherung der gewohnten Sprachqualität. Die Hauptprobleme bei der Übertragung von Echtzeitdaten über IP-Netze sind mögliche Verzögerungen und Verluste der Sprachpakete. Nach Angaben der Hersteller sind diese im Wesentlichen gelöst worden, sodass Gespräche in guter Sprachqualität geführt werden können. Zunächst wird die Sprache mit einem Mikrophon (z. B. Telefonhörer)

[3] Zeitschrift c't 2005, Heft 12

erfasst. Die aufgenommenen analogen Signale werden vor der Übertragung digitalisiert, codiert und zusätzlich noch komprimiert, um die Übertragungsmenge zu reduzieren.

Zwischen den kommunizierenden Geräten wird eine TCP (Transmission Control Protocol) - Verbindung aufgebaut. Diese Verbindung dient der Signalisierung, d. h. der Übermittlung der Steuerung, um eine Nutzerverbindung für die Sprachübermittlung aufzubauen. Standardisierte Protokolle (H.323, SIP) regeln die Signalisierung. Damit der Verbindungsaufbau gesteuert werden kann, müssen die gewählten Rufnummern in IP-Adressen umgesetzt werden. Über die mit der Signalisierung aufgebaute virtuelle Verbindung wird die Sprache in einzelnen IP-Paketen mit dem RTP (Realtime Transmission Protocol) übertragen. Dabei wird die Übermittlung der Sprache mit dem Protokoll RTCP (Realtime Control Protocol) kontrolliert.

Alle genannten Protokolle weisen eine Gemeinsamkeit auf, nämlich die Datenübertragung erfolgt unverschlüsselt. Dies trifft sowohl für die Signalisierungsdaten als auch für die Gesprächsdaten zu. Darüber hinaus treffen für die Datenübertragung mittels VoIP die gleichen Gefährdungen zu, die mit der herkömmlichen Nutzung des Internets verbunden sind. Mit verfügbaren Tools und den Informationen über diese Schwachstellen stehen Angreifern entsprechende Angriffspunkte zur Verfügung. Hat ein Angreifer Zugriff auf die ausgetauschten Sprachdatenpakete (Sniffing), hat er die Möglichkeit, das geführte Telefonat mitzuhören und aufzuzeichnen. Aber auch Denial of Service (DoS)-Angriffe auf die eingesetzten Server und IP-Spoofing, also das Vortäuschen einer fremden IP-Adresse, sind von der herkömmlichen Internetnutzung bekannte Angriffsvarianten. Selbst die beim E-Mail-Dienst bekannten Spam (1.4) treten bei Voice over IP als „Spit“ (Spam over Internettelephony) auf. Auch Administratoren sehen sich durch den Übergang der Sprache auf Datennetze mit ganz neuen Gefahren und Herausforderungen konfrontiert. Bisher waren TK-Anlagen zumeist eigenständige Einheiten mit zugehöriger Verkabelung und Endgeräten. Diese werden jetzt zunehmend in komplexe Datennetze integriert, welche zunehmend mit dem Internet gekoppelt sind. Im Vergleich zu den bisher leitungsvermittelnden Telekommunikationsnetzen ist bei einer Übertragung der Sprachdaten über das für alle zugängliche Internet bzw. drahtlose Netz der Einsatz von Sicherheitsprotokollen für die IP-Telefonie dringend anzuraten. So wird eine verbesserte Sicherheit bei der Kommunikation mit VoIP durch eine verschlüsselte Übertragung der Sprachdaten erzielt. Hierfür bietet sich der Einsatz von Sicherheitsprotokollen an, wie das Secure Realtime Transport Protocol (SRTP). Die zu übertragenden Sprachpakete werden hier mit dem symmetrischen Verschlüsselungsverfahren AES (Advanced Encryption Standard) unter Einsatz eines 128-Bit-Schlüssels kryptiert. VoIP-Telefone einiger Hersteller nutzen schon SRTP und können damit abhörsichere Verbindungen (ENDE-zu-ENDE-Verschlüsselung) aufbauen.

Derzeit arbeiten Hersteller, Provider und Lösungsanbieter an gemeinsamen Konzepten für eine sichere IP-Telefonie. Dazu wurde Anfang des Jahres 2005 die VoIP Security Alliance (VOIPSA) von weltweit führenden Unternehmen auf dem Gebiet der Telekommunikation gegründet.

Die DSB des Bundes und der Länder haben auf ihrer 70. Konferenz im Oktober 2005 in einer Entschließung (Anlage 19) Hersteller, Anbieter und Anwender von VoIP-Lösungen aufgefordert, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren. Dazu sind angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere datenschutzgerechte Nutzung in Netzwerken zu ermöglichen, entsprechende Verschlüsselungsverfahren anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen, vorhandene Sicherheitslücken schnellstmöglich zu beseitigen sowie eingesetzte Protokolle und Algorithmen offen zu legen. Der AK Technik der DSB des Bundes und der Länder erarbeitet derzeit eine Orientierungshilfe zum Einsatz von VoIP.

1.11 Initiative „Deutschland sicher im Netz“

Die Initiative „Deutschland sicher im Netz“ ist eine Gemeinschaftsinitiative großer Unternehmen und Institutionen unter der Schirmherrschaft des Bundesministers für Wirtschaft und Arbeit. Ziel ist eine verstärkte Online-Sicherheit, insbesondere bei der Nutzung des Internet. Zielgruppe sind vor allem kleine und mittelständische Unternehmen, Institutionen sowie Privatnutzer. Ihnen allen ist gemeinsam, dass sie zumeist weder über finanzielle, zeitliche oder personelle Ressourcen verfügen, um sich wirksam vor aktuellen Gefährdungen im Internet zu schützen. Oftmals fehlt es an Wissen und aktuellen Informationen für entsprechende Schutzmaßnahmen. Die Initiative setzt auf eine aktive Mitwirkung der betreffenden Nutzer und möchte diese zu einem bewussten Umgang mit der Informationstechnologie motivieren. Dies setzt voraus, dass die Nutzer die Bedrohungen und Gefahren beim Nutzen des Internet kennen und ihr Verhalten hierauf einstellen, indem sie u. a. aktuelle Sicherheitsfunktionen und -technologien richtig nutzen und durch diszipliniertes Verhalten Fehler und Nachlässigkeiten vermeiden. Die Initiative hat in diesem Sinne ein Handlungsversprechen zur Sicherheit in der Informationsgesellschaft entwickelt, mit dem sie sich zu einem nachhaltigen und kontinuierlichen Engagement im Bereich IT-Sicherheit verpflichtet.
Dazu wurden mehrere Themengebiete definiert. So ist kostenlos ein Sicherheitscheck zur Verfügung zu stellen, mit dem Internetnutzer ihre PC umfassend auf Sicherheitsmängel überprüfen können. Zugleich wird bei der Einstellung und Installation von notwendigen Schutzmechanismen Hilfestellung geboten. Ein weiteres Themengebiet ist die Entwicklung sicherer Software. Schon bei der Programmierung von Software und Web-Applikationen sollen bekannte Angriffsmöglichkeiten ausgeschlossen werden. Dazu werden Konzepte zur sicheren Softwareentwicklung und zum Umgang mit Sicherheitsschwachstellen in Form von Veranstaltungen an Universitäten und Entwicklertreffen vermittelt und die Ergebnisse publiziert. Ein weiteres Handlungsversprechen ist, kleinen und mittelständischen Unternehmen ein Paket zur Informationssicherheit zur Verfügung zu stellen. Dieses beinhaltet Sicherheitsrichtlinien, Verfahrensanweisungen, Checklisten und Notfallpläne. Weiterhin soll es dieser Zielgruppe ermöglicht werden, über Systemhäuser Informationen für eine effektive Anwendung von zertifikationsbasierenden Sicherheitsmechanismen zum Zweck der Authentifizierung, Verschlüsselung und elektronischen Signatur zu erhalten. Durch diese Schutzmaßnahmen soll insbesondere das Vertrauen in eBusiness-Anwendungen und eGovernment-Anwendungen gefördert werden. Mit einem Lernpaket sollen Internetnutzer über einen sicheren Online-Handel und den Schutz ihrer persönlichen Daten aufgeklärt werden. Dieses Paket soll insbesondere in allgemeinen Bildungseinrichtungen zum Einsatz kommen. Auch ein Sicherheitsbarometer wird entwickelt, welches auf einen Blick erkennen lässt, ob eine weit reichende Bedrohung im Internet besteht. Die Meldungen dieses Sicherheitsbarometers sollen verständlich für die Nutzer aufbereitet und über verschiedene Kommunikationskanäle zur Verfügung gestellt werden. Nicht zuletzt wird ein Portal für Kinder im Alter von 8 - 13 Jahre entwickelt, das über die Möglichkeiten und Risiken der neuen Medien aufklärt und sie befähigt, diese aktiv, kompetent und selbstbestimmt zu nutzen. Hierzu werden auch für Eltern und Lehrer Materialien und Unterrichtseinheiten zur Verfügung gestellt.
Die Initiative wird sich auch dafür einsetzen, dass der Gesetzgeber die immer noch ausstehenden Rechtsvorschriften für ein Datenschutzaudit nach § 9 a Bundesdatenschutzgesetz erlässt. Mit einem Datenschutzaudit können die Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen.
Die Initiative wird von DSB des Bundes und der Länder begrüßt und im Rahmen ihrer Möglichkeiten auch unterstützt. So wurden u. a. auf einer Sondersitzung des AK Technik mit den

Initiatoren der Sicherheitsinitiative die o. g. Themengebiete diskutiert und auch diesbezügliche Erfahrungen seitens der DSB vorgetragen.
Auf ihrer 70. Konferenz sprachen sich die DSB des Bundes und der Länder dafür aus, die Zusammenarbeit mit der Initiative fortzusetzen.

1.12 Datenschutzrechtliche Aspekte beim Einsatz von Funkchips (RFID) zur Identifikation

Das Kürzel RFID steht für Radio Frequency Identification und stellt ein kontaktloses automatisiertes Verfahren zur Identifikation unterschiedlicher Objekte und Waren dar.
Die kontaktlosen RFID-Systeme gewinnen neben anderen automatischen Identifikationsverfahren wie dem Barcode-System, Klarschriftlesern, biometrischen Verfahren und konktaktbehafteten Chipkarten seit einigen Jahren zunehmend an Bedeutung. Ein RFID-System arbeitet heute mit einem winzigen Mikrochip (Transponder), der an dem zu identifizierenden Objekt angebracht ist und dessen gespeicherte Informationen per Funk an mit einer Antenne versehene fest installierte oder mobile Erfassungsgeräte (Leseeinheit bzw. auch Schreibeinheit) übermittelt werden. Diese auf Abruf des Erfassungsgerätes erfolgte Übertragung ist äußerlich für die Betroffenen i. d. R. nicht bemerkbar. Die Erfassungsgeräte verfügen zumeist über zusätzliche Schnittstellen, an die IT-Systeme zum Speichern und Auswerten der erhobenen Daten angeschlossen werden.
Die bereits eingesetzten oder in Entwicklung befindlichen RFID-Techniken unterscheiden sich erheblich was sowohl die Reichweite der kontaktlosen Datenübermittlung als auch die Größe und technische Leistungsfähigkeit der eingesetzten Speicherchips betrifft. Neben einer weltweit eindeutigen geschützten Identifikationsnummer verfügen moderne RFID-Chips auch über einen frei beschreibbaren Bereich, der mit unterschiedlichen Informationen belegt werden kann. Die hier gespeicherten Daten können nach dem derzeitigen Stand noch bis zu zehn Jahren abgerufen werden, soweit der Chip nicht zerstört oder sein Dateninhalt überschrieben wird. Es gibt Transponder mit nur lesendem als auch mit schreibendem Zugriff. Sie verfügen über eine eigene Energiequelle oder werden durch das Erfassungsgerät über Funk versorgt. Je nach eingesetzter Frequenz können solche Transponder von einigen Zentimetern bis zu mehreren Metern (in Einzelfällen bis zu 1 Kilometer) von den Erfassungsgeräten ausgelesen werden. Die eingesetzten Transponder sind so klein, dass sie visuell kaum bemerkbar auf Transport- oder Produktverpackungen angebracht, in Textilien oder amtlichen Dokumenten (wie z. B. Pass) eingearbeitet und sogar schon in den menschlichen Körper implantiert werden können.
Mit einem Transponder versehene Objekte sind schnell und berührungslos lokalisierbar und ersparen Zeit- und Arbeitsaufwand. Veröffentlichungen belegen, dass derzeit solche automatisierte kontaktlose Datenübermittlungen schon in Verfahren der Industrieautomatisation, des Warenmanagements, der Tieridentifikation sowie bei Zutrittssystemen und elektronischen Wegfahrsperren eingesetzt werden.
Die RFID-Technologie bietet auch im Endkundenbereich des Einzelhandels vielfältige potenzielle Anwendungsfelder. Beim Einkaufen ist uns vertraut, dass für jedes ausgewählte Produkt an der Kasse nachvollziehbar der Barcode-Streifen eingescannt und ein entsprechender Kaufbeleg ausgestellt wird. Es handelt sich hierbei um eine Datenerhebung, die im Augenschein des Kunden erfolgt. Die Tage dieser Verfahrensweise sind jedoch gezählt. In Zukunft wird auch hier die RFID-Technologie breiten Einzug halten. Im Gegensatz zum Barcode, bei dem in der Regel nur die Registrierung der Artikelart des betroffenen Objektes erfolgt, wird jetzt durch den Einsatz von RFID-Chips jeder Artikel für sich eindeutig identifiziert. Da weiterhin jeder RFID-Chip mehr Informationen speichern kann, als der heute übliche Barcode, kann somit jeder Artikel exakter erfasst werden. Auch das automatische Überwachen von Verkaufsregalen, durch welches das Ladenpersonal zum Nachfüllen aufgefordert wird, ist in der Erprobung. Wie

auch der Einsatz der RFID-Markierung als Diebstahlsicherung oder als Äquivalent zum bisherigen Kassenzettel für Gewährleistungsansprüche.
In der Praxis großer Handels-Konzerne wurde erprobt und wird nunmehr demonstriert wie an den Verkaufsprodukten angebrachte Chips zukünftig den Barcode im Einzelhandel ersetzen können. Fährt der Kunde mit seinem Warenkorb an der Kasse vorbei, werden alle RFID-Chips ohne Berührung ausgelesen und dem Kunden sofort die Rechnung präsentiert. Aus der Sicht des Kunden wird man dies als Fortschritt ansehen. Wo überall die RFID-Chips ausgelesen werden können, kann allerdings der Kunde nicht feststellen, denn die Funkwellen mit denen die gespeicherten Daten zum Erfassungsgerät übertragen werden breiten sich räumlich aus. So könnte schon bei der Entnahme eines Produktes aus dem Regal, um es lediglich in Augenschein zu nehmen, diese Aktion registriert werden. Betritt ein Kunde mit RFID-Chips gekennzeichneten Artikeln ein anderes Geschäft, könnten diese eventuell wieder registriert werden. Obwohl bei den hier geschilderten Szenarien noch keine personenbezogenen Daten erhoben werden, ergibt sich schon hier die Frage, inwieweit die Privatsphäre des Kunden tangiert wird. Nicht jedem wird es recht sein, wenn der rechtmäßig erworbene Inhalt seiner Einkaufstasche unbemerkt ausgelesen werden kann. Dies wird besonders deutlich, wenn diese bspw. Medikamente enthält, deren Packungen mit RFID-Chips gekennzeichnet sind. Pressemeldungen zufolge werden auch Überlegungen seitens der europäischen Zentralbank angestellt, Geldscheine aus Sicherheitsgründen mit RFID-Chips zu versehen. Hiermit würde sich automatisch die Frage nach dem gläsernen Portemonnaie stellen. Die möglichen Anwendungen für den Einsatz von RFID-Chips scheinen fast unbegrenzt zu sein. Neben den vielen positiven Auswirkungen dieser Technologie sind, wie aufgezeigt, auch negative Folgen für die Privatsphäre denkbar.
Funk-Etiketten, die nach dem Verkauf - ohne weitere Schutzmaßnahmen - aktiv bleiben, können im Alltagsgebrauch jederzeit elektronische Spuren hinterlassen. Werden ihre Daten mit bereits bestehenden personenbezogenen Datenbeständen verknüpft, bietet sich die Möglichkeit, Bewegungs-, Konsum- und Kontaktprofile über die Betroffenen zu erstellen. So besteht insbesondere durch den Einsatz von EDV-Hintergrundsystemen beim Bezahlen der Ware bspw. mit einer Kundenkarte die Möglichkeit, seitens des Verkäufers die Daten aus den RFID-Chips mit den personenbezogenen Daten des Käufers zu verknüpfen und somit dessen Kaufverhalten detaillierter als bisher beim Einsatz von Barcode zu analysieren.
Bei der Entwicklung der RFID-Technologie spielten bisher Fragen der Informationssicherheit und des Datenschutzes eine noch untergeordnete Rolle. Die DSB des Bundes und der Länder schlossen sich deshalb auf ihrer 67. Konferenz voll inhaltlich einer Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre zu RFID an (www.datenschutz.thueringen.de). In dieser wird u. a. die Notwendigkeit hervorgehoben, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen.
Aus sicherheitstechnischer Sicht können sich Gefahren ergeben durch den Verlust der Vertraulichkeit der zu verarbeitenden Daten, z. B. durch Abhören der Kommunikation zwischen dem Transponder und dem Erfassungsgerät oder dem Auslesen auf dem Transponder gespeicherten Daten durch Vortäuschen eines autorisierten Erfassungsgerätes. Denkbar wäre auch ein Verlust der Integrität der Daten z. B. durch unautorisierte Schreibzugriffe auf den Transponder. Ebenso sind Täuschungen durch Entfernen des Transponders und dessen Anbringen an ein anderes Objekt möglich. Weiterhin sind durch ein unbefugtes Deaktivieren des Transponders, durch Blocken des Lesegerätes oder durch Stören des Datenaustausches über die Luftschnittstelle Gefahren für den Verlust der Verfügbarkeit von RFID-Systemen gegeben.
Somit sind seitens des RFID-Betreibers gemäß der möglichen Bedrohungen und der Schutzwürdigkeit der zu verarbeitenden Daten angemessene Sicherheitsmaßnahmen zu ergreifen. Bedrohungsszenarien für den Einsatz von RFID-Systemen und mögliche Abwehrmaßnahmen dagegen sind in der BSI-Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“ aufgezeigt.

Grundsätzlich muss auch bei der Nutzung von RFID-Systemen das Recht auf informationelle Selbstbestimmung gewährleistet sein. Nur durch einen transparenten Umgang mit dieser Technologie können die in den Datenschutzgesetzen geforderte Zweckbindung, Datensparsamkeit und Vertraulichkeit bei der Verarbeitung personenbezogener Daten sichergestellt werden. Hier sind zunächst die Hersteller und Nutzer von RFID-Systemen aufgefordert, solche Systeme zu entwickeln und einzusetzen, die dem gesetzlich normierten Prinzip der Datensparsamkeit genügen und weitgehend ohne Personenbezug auskommen. So sollte ein Auslesen der auf dem RFID-Chips gespeicherten Daten prinzipiell nur mit Wissen des Besitzers (Käufers) erfolgen. Kann auf die Verarbeitung personenbezogener Daten nicht verzichtet werden, so sind

- die Betroffenen umfassend über Einsatz, Verwendungszweck und Inhalt von RFID-Chips zu informieren,
- Kommunikationsvorgänge mit RFID-Chips für die Betroffenen eindeutig erkennbar zu machen,
- Daten auf RFID-Chips nur solange zu speichern, wie es zur Erreichung des Zwecks erforderlich ist,
- die Möglichkeiten zur Deaktivierung, Löschung von RFID-Chips zu schaffen und
- die Vertraulichkeit der gespeicherten und der übertragenen Daten durch wirksame Authentisierung der beteiligten Geräte und durch Verschlüsselung sicherzustellen.

Die Entwicklungen im Bereich der RFID-Technologie haben Auswirkungen auf weite Teile des privaten und öffentlichen Lebens. Auf welche gesellschaftliche Akzeptanz ihr Einsatz stößt, hängt nicht zuletzt vom Ergebnis der Abwägung der mit dem jeweiligen Anwendungsfall verbundenen Chancen und Risiken ab. Da die RFID-Technologie momentan noch vor ihrer breiten Einführung steht, hat nicht nur der Handel bereits jetzt in der Planungsphase die Möglichkeit, in Zusammenarbeit mit DSB und Verbraucherschutzinitiativen Regeln für einen datenschutzgerechten Umgang mit RFID zu gestalten.
Eine Arbeitsgruppe des AK Technik der DSB des Bundes und der Länder erstellt in diesem Sinne derzeit eine datenschutzrechtliche Orientierungshilfe zum Einsatz von RFID.

2. Europäischer und Internationaler Datenschutz

2.1 Europol

Zu Europol ist aktuell zu berichten, dass am 27. November 2003 von den Mitgliedstaaten der Europäischen Union ein Protokoll zur Änderung bestehender und Einführung neuer Artikel jenes Übereinkommens unterzeichnet worden ist, mit dem die Anwendung des Europol-Übereinkommens wirksamer gestaltet werden soll. Das Protokoll aufgrund von Artikel 43 Satz 1 des Übereinkommens über die Errichtung eines europäischen Polizeiamtes (Europol-Übereinkommen) sieht eine Erweiterung der Zuständigkeit bei der Terrorismusbekämpfung in Fällen schwerer internationaler Kriminalität vor. Der von der Bundesregierung am 12. August 2005 dem Bundesrat vorgelegte Entwurf eines Vertragsgesetzes zur Ratifizierung des Änderungs-Protokolls wird derzeit beraten. Für die gemeinsame Kontrollinstanz von Europol (GKI) wurde als Vertreter der Länder der Hessische Datenschutzbeauftragte als Nachfolger des aus dem Dienste ausgeschiedenen Landesbeauftragten für den Datenschutz in Sachsen-Anhalt benannt.

2.2 Eurojust

Das im 5. TB (2.3) angesprochene Gesetz zur Umsetzung des Beschlusses (2002/187/JI) des Rates vom 28. Februar 2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität (Eurojust-Gesetz - EJG) ist am Tag nach der Verkündung vom

17. Mai 2004 in Kraft getreten (BGBl. I 2004, S. 902). Der Gesetzentwurf hat dabei keine wesentlichen Änderungen im datenschutzrechtlichen Bereich erfahren.
Mit der Verordnung über die Benennung und Einrichtung der nationalen Eurojust-Anlaufstelle für Terrorismusfragen (Eurojust-Anlaufstellen-Verordnung - EJTAnV) vom 17. Dezember 2004 (BGBl. I 2004, S. 3520) wurde als nationale Eurojust-Anlaufstelle für Terrorismusfragen der Generalbundesanwalt beim Bundesgerichtshof bestimmt. Datenschutzrechtliche Regelungen enthalten auch die Bestimmungen der Geschäftsordnung betreffend die Verarbeitung und den Schutz personenbezogener Daten bei Eurojust vom 21. Oktober 2004 (ABl. EU 2005 Nr. C 68, S. 1), die die interne Verarbeitung personenbezogener Daten durch Eurojust regeln. Dabei ist auch vorgesehen, dass Eurojust erforderlichenfalls weitere Regelungen für die Verarbeitung personenbezogener Daten bei nicht fallbezogenen Tätigkeiten ausarbeitet. Derartige Regelungen werden der gemeinsamen Kontrollinstanz mitgeteilt und in gesonderten internen Handbüchern veröffentlicht. Auch die vorliegenden Bestimmungen werden nach den Schlussbestimmungen regelmäßig im Hinblick auf erforderliche Änderungen überprüft.

3. Datenschutz im Parlament

Regelungen in der Geschäftsordnung des Thüringer Landtags zum Datenschutzbeauftragten

Zu den Regelungen in § 112 der Geschäftsordnung (GO) des Thüringer Landtags - Datenschutzbeauftragter - fand im Berichtszeitraum mit der Landtagsverwaltung eine Diskussion zur Teilnahmemöglichkeit des TLfD an vertraulichen Sitzungen statt.

Im Ergebnis ist festzustellen, dass die Landtagspräsidentin eine Auslegung, entsprechend der bisherigen Übung nach § 112 Abs. 2 GO dahingehend vornimmt, dass der Datenschutzbeauftragte an den Sitzungen der Ausschüsse teilnehmen kann, soweit es sich nicht um vertrauliche Sitzungen handelt. Bezogen auf die Regelung im § 112 Abs. 3 GO, dass die Ausschüsse die Anwesenheit des DSB verlangen können, erscheint es nach Ansicht der Landtagspräsidentin als fraglich, ob dieses Verlangen auch in den Fällen des § 112 Abs. 2 Satz 1 GO überhaupt möglich wäre. Gegebenenfalls bedürfte diese Thematik einer grundsätzlichen Klärung.

Ich bin der Auffassung, dass nach dem Wortlaut der geltenden GO im § 112 Abs. 3 die Teilnahme des TLfD auch an vertraulichen Sitzungen möglich ist und zwar dann, wenn es der Landtag als auch seine Ausschüsse verlangen. Das Zitierrecht des Parlaments bezogen auf den TLfD halte ich, ungeachtet der unabhängigen Stellung des DSB, im Hinblick auf Artikel 69 der Verfassung des Freistaats Thüringen für legitim, da es Aufgabe des TLfD beim Landtag ist, sich für die Wahrung des Rechts auf Schutz der personenbezogenen Daten und zur Unterstützung bei der Ausübung der parlamentarischen Kontrolle einzusetzen.

4. Neue Medien - Rundfunk - Telekommunikation

4.1 Telemediengesetz (TMG)

Im November 2004 haben sich Bund und Länder auf Eckpunkte zur Fortentwicklung der neuen Medienordnung verständigt. Ziel der Überlegung ist es, materiellrechtliche Datenschutzregelungen für Teledienste und Mediendienste in einem Bundesgesetz zusammen zu fassen, wobei beide Dienste in dem neuen Begriff Telemedien zusammengefasst werden sollen. Sowohl das Teledienstegesetz (TDG) als auch das Teledienstedatenschutzgesetz (TDDSG) sowie der Mediendienstestaatsvertrag (MDStV) sollen durch dieses Gesetz, das derzeit auf Arbeitsebene erarbeitet wird, abgelöst werden. Vorgesehen ist auch, den Rundfunkstaatsvertrag entsprechend

zu ändern. In einer Bund/Länderarbeitsgruppe, an der auch Datenschutzbeauftragte der Länder teilnehmen, wird derzeit versucht, die hier notwendigen Klärungen herbeizuführen. Über den Fortgang wird der TLfD berichten.

4.2 Jugendmedienschutz-Staatsvertrag (JMStV)

Der Jugendmedienschutz-Staatsvertrag (JMStV) vom 1. April 2003 sieht nach § 14 Abs. 2 zur Einhaltung der für die Anbieter geltenden Bestimmungen nach diesem Staatsvertrag die Bildung der Kommission für Jugendmedienschutz (KJM) vor, die der jeweils zuständigen Landesmedienanstalt als Organ bei der Erfüllung ihrer Aufgaben dient. Der Sitz der KJM wird danach einvernehmlich durch Beschluss der Ministerpräsidenten bestimmt. Diese haben Erfurt als Sitz der KJM festgelegt, die Geschäftsstelle der KJM hat ihren Sitz bei der Thüringer Landesmedienanstalt, die als öffentliche Stelle der Kontrolle des TLfD unterliegt. In diesem Zusammenhang stellte sich die Frage, wer für die Kontrolle der Verarbeitung personenbezogener Daten durch die KJM für eigene Zwecke zuständig ist. Der TLfD hat hierzu die Auffassung vertreten, dass nach dem Sitzlandprinzip die Zuständigkeit beim TLfD liegt. Diese Auffassung wird sowohl vom Thüringer Innenministerium als auch von den DSB des Bundes und der Länder geteilt.

4.3 Novellierung des Telekommunikationsgesetzes

Am 26. Juni 2004 trat nach langwierigen Beratungen die Neufassung des Telekommunikationsgesetzes (TKG) in Kraft, zu dessen Entwurf schon zuvor (4. TB, 4.2) berichtet worden war. Eingang fand in dieses Gesetz die Telekommunikations-Datenschutzverordnung (TDSV) (4. TB, 4.4), was zu einer Vereinfachung beim Datenschutz im Telekommunikationsbereich führt. Während bisher eine Auskunft über Name und Anschrift eines Teilnehmers, von dem nur die Rufnummer bekannt war, nach § 14 Abs. 4 TDSV verboten war, ist nunmehr gemäß § 105 Abs. 3 TKG die sog. Inverssuche möglich. Aus Datenschutzsicht wäre eine Lösung vorzuziehen gewesen, die die Inverssuche nur bei einer ausdrücklichen Einwilligung des Kunden zugelassen hätte. Eine solche Inverssuche ist allerdings nur erlaubt, wenn der Kunde im Telefonbuch oder einem öffentlichen elektronischen Verzeichnis eingetragen ist und gegen die Inverssuche keinen Widerspruch eingelegt hat. Der Diensteanbieter hat ihn auf dieses Widerspruchsrecht hinzuweisen. Neu ist die Vorschrift zu Standortdaten in § 98 TKG. Diese Daten dürfen nur in dem für die Bereitstellung dieser Dienste erforderlichen Maß innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat. Den Teilnehmern muss die Möglichkeit gegeben werden, ihre Einwilligung zur Verarbeitung von Standortdaten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise oder unentgeltlich zeitweise zu untersagen. § 111 TKG schreibt nunmehr für alle Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen und dabei Rufnummern vergeben oder für von anderen vergebene Rufnummern Telekommunikationsanschlüsse bereitstellen, vor, Daten für Auskunftsersuchen von Sicherheitsbehörden vorzuhalten. Problematisch ist hierbei, worauf schon zuvor (5. TB, 4.2) hingewiesen wurde, dass die Verpflichtung auch für Prepaid-Mobilfunkkarten gilt und damit im Ergebnis eine anonyme Nutzungsmöglichkeit im Bereich der Telekommunikation nicht mehr möglich ist.

4.4 Vorratsdatenspeicherung von TK-Daten

Die Europäische Kommission hat im Berichtszeitraum den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten für die elektronische Kommunikation vorgelegt, nach der alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden sollen, systematisch

eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über 1 Jahr bei Telefonaten und 6 Monaten bei Internet-Nutzung für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke wie z. B. Abrechnung gar nicht benötigen. Darüber hinaus hat der EU-Ministerrat über einen noch weitergehenden Vorschlag beraten, der ebenfalls der Zusammenarbeit im Bereich der Strafverfolgung und der Terrorismusbekämpfung dienen sollte. Die DSB des Bundes und der Länder haben, nachdem sie zunächst im Rahmen einer Presseinformation auf die Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen hingewiesen hatten, mit Entschließung der 70. Konferenz am 27./28. Oktober 2005 (Anlage 20) ihre bereits seit 2002 geäußerte grundsätzliche Kritik an der Pflicht zur anlassunabhängigen Vorratsdatenspeicherung nochmals bekräftigt. Mit der beabsichtigten Vorratsspeicherung ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen. Dies widerspricht dem grundgesetzlich geschützten Fernmeldegeheimnis ebenso wie auch dem durch die Europäische Menschenrechtskonvention garantierten Schutz der Privatsphäre. Beides droht unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden. Für die Vorratsspeicherung zu Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Strafverfolgung kann der Grundrechtseingriff nicht gerechtfertigt werden, zumal weniger intensive Eingriffsmöglichkeiten wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) bisher nicht ernsthaft erwogen wurden. Die Konferenz hat an die Bundesregierung, den Bundestag und das Europäische Parlament appelliert, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen und darauf hingewiesen, dass eine anlasslose Vorratsdatenspeicherung auf der Grundlage des Grundgesetzes verfassungswidrig wäre.

4.5 Zulässigkeit des Mithörens von Telefongesprächen

Ein Petent bat um datenschutzrechtliche Prüfung, ob und unter welchen Voraussetzungen das Mithören von Telefongesprächen durch weitere Mitarbeiter zulässig ist. Im vorliegenden Fall hatte ein Mitarbeiter einer öffentlichen Stelle in Thüringen im Verlauf des Gesprächs mit dem Petenten durch Einschalten des Lautsprechers dem im gleichen Raum arbeitenden weiteren Mitarbeiter das Mithören des Telefongespräches ermöglicht. Im Verlauf der Klärung der Sachlage, stellte sich heraus, dass das betreffende Telefongespräch aufgrund unterschiedlicher Auffassungen eskaliert war und der Betroffene in diesem Zusammenhang erklärte hatte, sich über den Mitarbeiter sowie das Telefonat beschweren zu wollen. Aufgrund des sich daran anschließenden Gesprächsverlaufs erschien es dem Mitarbeiter ab einem bestimmten Zeitpunkt zweckmäßig, eine weitere Person durch das Mithören zu beteiligen. Hierüber wurde der Betroffene im Gespräch ausdrücklich hingewiesen, sodass er die Möglichkeit hatte, bei Nichtzustimmung das Gespräch sofort zu beenden.
Diese Verfahrensweise des Mitarbeiters wurde vom TLfD als rechtskonform und zulässig bewertet, auch wenn unzweifelhaft beim Mithören von Gesprächen mit Privatpersonen das informationelle Selbstbestimmungsrecht der Betroffenen berührt wird. Das Bundesverfassungsgericht hat dazu festgestellt, dass das Mithören von Telefongesprächen über eine Freisprechanlage das Persönlichkeitsrecht des Betroffenen verletzen kann (1 BvR 1611/96 und 805/98). Es bedarf deshalb aus der Sicht des Datenschutzes zwingend bei einer Nutzung der technischen Möglichkeiten der modernen Telekommunikationstechnik beim Einschalten des Lautsprechers eines expliziten Hinweises an den Gesprächspartner, damit dieser unmittelbar entscheiden kann, ob er mit der Vorgehensweise einverstanden ist oder nicht. Im letzteren Fall kann er dann, wenn kein Einvernehmen besteht, das Gespräch unverzüglich beenden. Auch im vorliegenden Fall erfolgte das Mithören nicht ohne Wissen des Betroffenen und er hatte auch zu jeder Zeit die Möglichkeit, das Gespräch bei Nichtzustimmung zu beenden. Durch die Fortset-

zung des Gesprächs in Kenntnis dessen, dass eine weitere Person mithört, konnte der Mitarbeiter von einer konkludenten Einwilligung zu dessen Mithören ausgehen.

5. Innenverwaltung - Statistik - Kommunales - Sparkassen

5.1 Innenverwaltung

5.1.1 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG)

Mit dem Thüringer Gesetz zur Änderung verwaltungsverfahrensrechtlicher und anderer Vorschriften vom 25. November 2004 (GVBl. S. 853) sind die im 5. TB (5.1.1) angesprochenen Änderungen am 3. Dezember 2004 in Kraft getreten. Somit wurde in Thüringen die Grundlage für die elektronische Kommunikation zwischen den Bürgern und der Verwaltung des Landes geschaffen.
Ein noch im Entwurf zur Änderung des Thüringer Verwaltungsverfahrensgesetzes enthaltener § 37 a, wonach es Gemeinden und Landkreisen künftig gestattet werden sollte, ihnen bekannte, auf Grund § 15 Abs. 1 Nr. 1 c ThürKAG nach § 30 AO geschützte Daten, die sie bei der Verwaltung kommunaler Abgaben verwenden dürfen, auch bei der Vollstreckung wegen anderer öffentlich-rechtlicher Geldforderungen verwenden zu können, hat keinen Eingang in das Gesetz gefunden. Die vorgesehene Regelung begegnete erheblichen datenschutzrechtlichen Bedenken, da damit jegliche Zweckbindung entfallen wäre und sich die Frage nach der Verhältnismäßigkeit einer derartigen Regelung zwingend stellte. Im Rahmen der Beteiligung des TLfD war angeregt worden, hier vorzugsweise eine Änderung der Abgabenordnung zu betreiben.
Zur praktischen Handhabung hat das TIM die Landesverwaltung per Erlass insbesondere auf Fragen des Zugangs, der in § 3 a Thüringer Verwaltungsverfahrensgesetz für die Übermittlung elektronischer Dokumente nicht näher ausgeführt ist und einen weiten Ermessensspielraum gestattet, hingewiesen. Aus Gründen der Rechtssicherheit sollen die Adressaten darauf hingewiesen werden, dass die genannte E-Mail-Adresse entweder nur für den Empfang einfacher Mitteilungen ohne Signatur und/oder Verschlüsselungen dient oder dass durch die Nennung der E-Mail-Adresse nicht der Zugang zur Übermittlung von elektronischen Dokumenten, die mit einer (qualifizierten) elektronischen Signatur verbunden sind, eröffnet wird. In den Fällen, in denen das Gesetz bspw. handschriftliche Dokumente oder eine Aushändigung vorschreibt oder in sonstiger Weise deutlich macht, dass sich die elektronische Form der Kommunikation aus der Natur der Sache heraus verbietet, sind die jeweiligen Vorschriften weiterhin einzuhalten. Sind die verwendeten Kommunikationsmethoden zueinander nicht kompatibel, kann von den Kommunikationspartnern erwartet werden, dass sie sich gegenseitig darüber unterrichten.
Durch dieses Artikelgesetz hat auch § 4 Abs. 3 Satz 2 ThürDSG eine Änderung erfahren. In Bezug auf die elektronische Kommunikation bedarf die Einwilligung der Schriftform oder der elektronischen Form mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 Signaturgesetz, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Beim Anspruch auf Schadensersatz nach § 18 Abs. 3 ThürDSG ist die entsprechende Anwendung des BGB konkretisiert worden.

5.1.2 Informationsfreiheitsgesetz (IFG) des Bundes

Nach einem länger andauernden Gesetzgebungsverfahren wird zum 1. Januar 2006 das Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz - IFG) vom 5. September 2005 in Kraft treten. Darin wird das voraussetzungslose Zugangsrecht der Bürger zu Informationen bei Behörden des Bundes geregelt. Der Schutz personenbezogener Daten wird durch § 5 IFG gewährleistet, indem Zugang zu personenbezogenen Daten nur ge-

währt werden kann, soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat. Es hat also eine Abwägung im Einzelfall zu erfolgen, ob Zugang zu personenbezogenen Daten Dritter gewährt wird. Die Einhaltung der Vorschriften des Informationsfreiheitsgesetzes und insbesondere die Überprüfung von Abwägungsentscheidungen zwischen Informationsinteresse und Datenschutz sind in § 12 IFG dem Bundesbeauftragten für den Datenschutz zugewiesen. Da bereits in einigen anderen Bundesländern ähnliche Regelungen existieren, habe ich mich an das TIM mit der Bitte gewandt, mich rechtzeitig an einem etwaigen Gesetzesvorhaben zu beteiligen.

5.1.3 Vorgangsinformationssystem (VISkompakt)

Der TLfD wurde vom TIM über den geplanten Einsatz eines elektronischen Schriftgutverwaltungssystems (VISkompakt) informiert, mit dem neben einer IT-gestützten Registratur auch der Aufbau eines elektronischen Aktenbestandes in Form elektronisch gespeicherter Dokumente sowie eine IT-gestützte Vorgangsbearbeitung ermöglicht werden soll. Es bestand Einvernehmen, dass es hierzu neben den zu treffenden technisch organisatorischen Maßnahmen gemäß § 9 ThürDSG auch einer Freigabe nach § 34 Abs. 2 ThürDSG sowie eines Verfahrensverzeichnisses nach § 10 ThürDSG bedarf. Im Rahmen der Kontrolltätigkeit habe ich auch bei anderen Stellen den Einsatz dieses Vorgangsverwaltungssystems festgestellt und ebenfalls auf diese datenschutzrechtlichen Anforderungen hingewiesen. Seitens des TFM wurde nunmehr mitgeteilt, dass eine erweiterte Version dieses Vorgangsverwaltungs- und Dokumentenmanagementsystems eingeführt werden soll, zu der eine ressortübergreifende Arbeitsgruppe gebildet wurde. Zu dem im Geschäftsbereich des TIM bereits eingesetzten Verfahren VISkompakt hat das TIM thematisiert, ob es sich bei diesen Vorgangsverwaltungssystemen um allgemeine Verfahren handelt, für die nach § 34 Abs. 3 Nr. 1 ThürDSG eine Freigabe nicht erforderlich ist, weil sie ausschließlich dem internen Verwaltungsablauf dienen. Nach Auffassung des TLfD handelt es sich bei dem Einsatz des Dokumentenmanagementsystems/ Vorgangsmanagementsystem „VISkompakt“ um ein Verfahren, bei dem die Möglichkeiten der Verarbeitung personenbezogener Daten über die eines Registraturverwaltungssystems hinausgehen. Dies betrifft sowohl die Verarbeitung personenbezogener Daten der jeweiligen Mitarbeiter und damit möglicher Leistungskontrollen als auch die Verarbeitung von Metadaten der Dokumente bis hin zur Erstellung elektronischer Akten, die personenbezogene Daten der Verfahrensbeteiligten enthalten und auf die auch automatisiert zugegriffen werden kann. Diese Verfahren können nicht mit solchen verglichen werden, die nur einen beschränkten Anwendungsbereich haben (z. B. Organisation des internen Verwaltungsablaufs) oder nur konkrete Datensammlungen zu ganz konkreten Zwecken (Kommunikations- und Anschriftenverzeichnis zur Versendung von Informationen an den Betroffenen) enthalten. Das Potential des Dokumentenmanagementsystems reicht weit über die Organisation des internen Verwaltungsablaufs hinaus bis hin zur Erstellung und Arbeit mit einer elektronischen Akte. Im Hinblick darauf, dass dieses System landesweit eingesetzt werden soll, habe ich den Vorschlag des TIM aufgegriffen die datenschutzrechtlichen Fragen hierzu in der zuständigen Arbeitsgruppe zu erörtern. Hier sind insbesondere die Fragen nach einem Sicherheitskonzept, zur Zulässigkeit der automatisierten Verarbeitung von Daten, zum Schutzniveau der Daten, zu Zugriffsberechtigungen, zur Protokollierung von Vorgängen und Ereignissen sowie zur Löschung/Sperrung von Daten und zur Archivierung zu erörtern. Gleichzeitig befasst sich auch eine Arbeitsgruppe der DSB des Bundes und der Länder mit den datenschutzrechtlichen Anforderungen an derartige Dokumentenmanagementsysteme.

5.1.4 Zulässigkeit der Einsichtnahme in Wahlniederschriften

Im Nachgang zu den Kommunalwahlen wurde aus dem Kreis der Wahlleiter die Frage gestellt, ob und in welchem Umfang nach Abschluss der Wahlen Einsichtnahmen in Wahlniederschriften und sonstige Wahlunterlagen zulässig sind. Hierzu wurde in Abstimmung mit dem TIM die nachfolgende Auffassung vertreten.
Auch wenn die Wahlniederschriften personenbezogene Daten enthalten, finden auf sie nur bedingt die datenschutzrechtlichen Bestimmungen Anwendung. Dies ergibt sich daraus, dass es sich um Daten von Personen handelt, die deren amtliche Handlung dokumentieren (z. B. Namen des Wahlvorstandes) oder die öffentlich bekannt gemacht wurden (z. B. Ergebnisse der einzelnen Wahlbewerber im Rahmen der öffentlichen Auszählung). Da es sich bei den Wahlniederschriften um Schriftgut der öffentlichen Verwaltung handelt, das gemäß § 51 ThürKWO bis 3 Monate vor der nächsten Wahl aufzubewahren ist, gelten hierfür auch die allgemeinen Regeln zum Umgang mit dienstlichem Schriftgut. Dies erfordert eine vor unbefugtem Zugriff geschützte Aufbewahrung. Ziel der Aufbewahrung ist es, der Rechtsaufsichtsbehörde die Prüfung einer Wahlanfechtung bzw. die Durchführung einer Wahlprüfung von Amtswegen zu ermöglichen sowie im Falle einer gerichtlichen Überprüfung der betreffenden Entscheidung der Rechtsaufsichtsbehörde die Niederschriften dem Gericht vorlegen zu können. Darüber hinaus dient die Aufbewahrung von Niederschriften dazu, gemäß § 23 i. V. m. § 27 ThürKWG nach dem Ausscheiden eines Gemeinderats- bzw. Kreistagsmitglieds dem Wahlleiter bzw. Bürgermeister oder Landrat die Feststellung des Nachrückers zu ermöglichen. Eine Einsichtnahme für andere Zwecke ist nicht vorgesehen. Die übrigen Wahlunterlagen, wie Wählerverzeichnisse, Wahlscheinanträge u. a. sind entsprechend § 51 ThürKWO spätestens mit Ablauf von 6 Monaten nach der Wahl zu vernichten. Eine Einsichtnahme ist nur im Rahmen der Wahlprüfung oder bei Wahlanfechtungen erlaubt.

5.1.5 Nicht datenschutzgerechte Entsorgung fehlerhafter Wahlbenachrichtigungskarten

Im Vorfeld der letzten Bundestagswahl informierte ein Bürger den TLfD darüber, dass in seinem Wohngebiet in einem Wertstoffsammelbehälter für Papier eine Vielzahl bedruckter Wahlbenachrichtigungskarten liegen würden. Bei der sofort vorgenommenen Prüfung vor Ort bestätigte sich die Richtigkeit der Meldung dahingehend, dass sich in dem Container ca. 500 Wahlbenachrichtigungskarten überwiegend als perforierte Endlosdrucke befanden, die entweder nicht oder unvollständig oder fehlerhaft bedruckt waren. Weitere Recherchen ergaben, dass es sich dabei ausschließlich um Fehldrucke eines Unternehmens handelte, welches von Gemeinden im Freistaat Thüringen mit dem Druck und Versand der Wahlbenachrichtigungskarten beauftragt worden war. Durch eine Verkettung mehrerer Umstände waren die Fehldrucke nicht wie vorgesehen ordnungsgemäß vernichtet, sondern fahrlässig in dem betreffenden Wertstoffbehälter entsorgt worden. Diese nicht ordnungsgemäße Vernichtung der personenbezogenen Daten wurde gemäß § 39 Abs. 1 ThürDSG beanstandet.
Da der Wertstoffcontainer zum Zeitpunkt der Kontrolle durch den TLfD bereits gut gefüllt war und nicht ausgeschlossen werden konnte, dass einige der Wahlbenachrichtigungskarten auch zwischen das Altpapier gerutscht waren, wurde mit Unterstützung der Kommunalverwaltung Kontakt mit dem zuständigen Entsorgungsbetrieb aufgenommen. Dieser erklärte sich auch sogleich bereit, den Wertstoffcontainer abzuholen und den Inhalt datenschutzgerecht zu vernichten, so dass damit jeder weitere Zugriff auf die Unterlagen durch Unbefugte ausgeschlossen werden konnte. Darüber hinaus wurden die betroffenen Gemeinden vorsorglich über den Landeswahlleiter ausdrücklich darauf hingewiesen, bei der Stimmabgabe auf die nach § 56 Bundeswahlordnung vorgesehene Legitimationspflicht der Wähler zu achten.

Bei der Kontrolle in dem öffentlich-rechtlichen Wettbewerbsunternehmen wurde festgestellt, dass dort die notwendigen materiellen Voraussetzungen für eine datenschutzgerechte Vernichtung der Unterlagen in Form eines geeigneten und funktionstüchtigen Aktenvernichters durchaus zur Verfügung standen. Organisatorischen Regelungen zum Umgang mit Fehldrucken gab es aber bisher noch nicht, was aber in Auswertung des Vorfalls unverzüglich nachgeholt wurde. Im Zuge der Kontrolle wurde auch gefordert, dass die Vereinbarungen mit den Gemeinden für Datenverarbeitungen im Auftrag gemäß § 8 ThürDSG zu überarbeiten sind. Das Unternehmen hat dies zugesagt.

5.1.6 Übermittlung von Unterlagen aus Verwaltungsakten an Dritte

Eine Kommune hatte vor Jahren ein Grundstück an eine Privatperson verkauft. Die damit verbundenen Erwartungen zur Nutzung hatten sich für die Kommune nicht erfüllt, sodass man den Weiterverkauf an ein an diesem Grundstück interessiertes Kreditinstitut nachdrücklich unterstützte. Im Rahmen späterer Verhandlungen zwischen dem Grundstückseigentümer und dem kaufinteressierten Kreditinstitut stellte der Eigentümer fest, dass dem potentiellen Käufer der vollständige Inhalt des Kaufvertrags bekannt war, den er damals mit der Kommune abgeschlossen hatte. Die weiteren Ermittlungen ergaben, dass die Kommune diesen Vertrag dem Kreditinstitut als Fax übermittelt hatte, ohne dass dies in irgendeiner Weise (z. B. in der Grundstücksakte oder im Postausgang) dokumentiert worden war. Dadurch ließ sich nicht mehr recherchieren, welcher Bereich oder Mitarbeiter zu welchem Zweck und auf welcher Rechtsgrundlage den Kaufvertrag an das Kreditinstitut gesandt hatte. Die Übermittlung des Kaufvertrags ohne entsprechende Befugnisse, wie auch die fehlende Revisionsfähigkeit der Datenverarbeitung wurden deshalb gemäß § 39 Abs. 1 ThürDSG beanstandet. Um künftige Wiederholungen auszuschließen, wurde unverzüglich von der betreffenden Kommune eine Dienstanweisung in Kraft gesetzt, die die Dokumentationspflicht für aus- und eingehende Unterlagen sowie die Verfahrensweise bei der Übermittlung personenbezogener Daten künftig regelt.

5.1.7 Umgang der Verwaltung mit personenbezogenen Daten aus Petitionen

Gemäß § 11 ThürDSG gehört es zu den Schutzrechten der Betroffenen, sich unbeschadet des allgemeinen Petitionsrechts oder anderer Rechte unmittelbar an den TLfD zu wenden, wenn ihre schutzwürdigen Belange durch die Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch eine öffentliche Stelle beeinträchtigt werden. Sie dürfen nicht benachteiligt oder gemaßregelt werden, weil sie von diesem Recht Gebrauch machen. Eine Befugnis des TLfD zur Kontrolle des Umgangs mit personenbezogenen Daten im Petitionsausschuss des Thüringer Landtags ist nach dem ThürDSG nicht vorgesehen. Sofern aber Beschwerden beim TLfD auch Fragen zum Umgang mit Daten aus Petitionen in den öffentlichen Stellen, die diese zur Erarbeitung von Stellungnahmen zur Kenntnis erhalten haben, aufwerfen, kontrolliert auch dort der TLfD die Einhaltung der Bestimmungen zum Datenschutz. In diesem Zusammenhang habe ich festgestellt, dass es eine gängige Praxis ist, den jeweils betroffenen Stellen zur Erarbeitung einer angeforderten Stellungnahme zum Sachverhalt über ihre Aufsichtsbehörden die vollständigen Petitionen mit Anlagen als Kopien zu übergeben. Eine Prüfung, ob alle in der Petition enthaltenen Informationen zur Sachverhaltsklärung der betreffenden Stelle mitgeteilt werden müssen oder auch Teile davon ausreichen würden, erfolgt dabei, wie festzustellen war, nicht. Dadurch kann nicht ausgeschlossen werden, dass die Stellen teilweise auch Kenntnis von Daten erhalten (wie z. B. die Namen der Petenten bei allgemeinen Fragenstellungen oder Sachverhalte, soweit der Petent mehrere voneinander unabhängige Probleme in seiner Petition anspricht), die sie zur sachlichen Prüfung des Inhaltes der Petition und zur Erarbeitung der Stellungnahme und somit zur Aufgabenerfüllung von der betreffenden Stelle nicht benötigen. Eine

Notwendigkeit der Beschränkung der Informationen auf den erforderlichen Umfang ergibt sich aber nicht nur aus der fehlenden Übermittlungsbefugnis für diesen „Datenüberschuss“, sondern insbesondere auch, weil ansonsten die Gefahr besteht, dass diese über das erforderliche Maß hinausgehenden Daten von den Stellen mitunter auch zweckwidrig und damit unzulässig verwendet werden können. Dass dies nicht lediglich theoretische Überlegungen sind, machten im letzten Berichtszeitraum wiederum Beschwerden deutlich, wo z. B. in einem Fall auf diesem Weg der Name eines Petenten an das „Schwarze Brett“ einer öffentlichen Einrichtung gelangte, der sich zu allgemeinen Problemen geäußert hatte. Um dies auszuschließen, sind daher die Aufsichtsbehörden verpflichtet, bei der Bearbeitung von Petitionen zu prüfen, welche Informationen für den nachgeordneten Bereich zur sachlichen Klärung der Beschwerde und die Beantwortung der Fragen notwendig sind, da bei einer undifferenzierten „Durchleitung“ der Petition u. U. gegen datenschutzrechtliche Bestimmungen verstoßen wird. Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist nach § 21 Abs. 4 ThürDSG die Übermittlung auch dieser Daten nur dann zulässig, wenn eine Trennung nicht oder nur mit einem unvertretbarem Aufwand möglich ist und keine berechtigten Interessen des Betroffenen oder eines Dritten an der Geheimhaltung überwiegen. In jedem Fall ist aber jede weitere Verarbeitung oder Nutzung der über das erforderliche Maß hinausgehenden Daten nicht zulässig.

5.1.8 Kontrolle von Ausschreibungen zur Einreiseverweigerung nach Artikel 96 Schengener Durchführungsübereinkommen (SDÜ)

Wenn die Voraussetzungen vorliegen, können abgeschobene Ausländer aus Drittstaaten zur Einreiseverweigerung nach Art. 96 Schengener Durchführungsübereinkommen (SDÜ) im Schengener Informationssystem (SIS) ausgeschrieben werden. Das bedeutet, dass ihnen im Schengener Geltungsbereich an den Außengrenzen die Einreise verweigert wird.
Im Rahmen einer bundesweit koordinierten Kontrolle des Ausschreibungsverfahrens nach Art. 96 SDÜ wurden in diesem Berichtszeitraum auch in Thüringen datenschutzrechtliche Kontrollen in einzelnen Ausländerbehörden anhand von nach dem Zufälligkeitsprinzip ausgewählten Akten/Fällen durchgeführt. Kontrolliert wurden die Ausschreibungsvoraussetzungen: Ob es sich bei den zur Einreiseverweigerung um sog. Drittausländer handelte, ob der Ausschreibungsgrund Abschiebung vorlag und ob die Frist zur Ausschreibung jeweils kontrolliert wurde. Auch ging es darum, inwiefern die Löschungen der Ausschreibungen im angemessenen Zeitraum erfolgten und ob die Löschung oder die Gründe für eine Verlängerung der Ausschreibungsfrist dokumentiert waren. Dabei war festzustellen, dass in der Regel die Gründe für eine Fristverlängerung nicht dokumentiert, durchaus aber differenzierte Fristen festgelegt worden waren. Die Löschverfügungen wurden teilweise zu Dokumentationszwecken aufbewahrt, obwohl eine Vernichtung der Unterlagen im Fall der Löschung im SIS vorgesehen war. Den Forderungen des TLfD wurde im Ergebnis der Kontrollen nachgekommen.
Bundesweit musste insgesamt festgestellt werden, dass bezüglich der Ausschreibungsfristen und der Dokumentation Probleme bestehen. Die Fristen für die Ausschreibung in den einzelnen Ländern wurden unterschiedlich vergeben, eine Speicherung der Ausschreibung für 3 Jahre stellt allerdings die Regel dar, längere Speicherungsfristen bilden eher die Ausnahme.

5.1.9 Kontrolle des Einsatzes eines Chipkartensystems zur Gewährung von Asylbewerberleistungen

Die Leistungsgewährung in den kommunalen Gebietskörperschaften entsprechend § 3 Abs. 2 des Asylbewerberleistungsgesetzes (AsylbLG) erfolgt regelmäßig in Form von Sachleistungen und Wertgutscheinen. Zu diesem Zweck kommen in verschiedenen kreisfreien Städten und

Landkreisen Chipkartensysteme zum Einsatz. Mit einer Chipkarte können somit Asylbewerber bargeldlos in Vertragsgeschäften einkaufen. Kommunale Gebietskörperschaften wurden um Auskunft darüber gebeten, ob der Einsatz des Chipkartensystems durch sie selbst oder in Auftragsdatenverarbeitung durch eine beauftragte Firma erfolgt. Den übersandten Vereinbarungen war teilweise nicht zu entnehmen, welche personenbezogenen Daten durch die kommunalen Gebietskörperschaften selbst und welche durch die Firma verarbeitet werden. Besonders wichtig war in diesem Zusammenhang auch, dass die Betroffenen gemäß § 5 Abs. 4 ThürDSG über ihre zustehenden Rechte sowie über die von ihnen bei Verlust des Datenträgers zu treffenden Maßnahmen und über die Folgen aufzuklären sind. Die Hinweise des TLfD zu den Verträgen wurden insgesamt aufgenommen bzw. umgesetzt.

Im Rahmen einer datenschutzrechtlichen Kontrolle in einem Landratsamt zum praktischen Umgang mit personenbezogenen Daten beim Einsatz des Chipkartensystems war festzustellen: Das vorliegende Verfahrensverzeichnis nach § 10 ThürDSG zu dem eingesetzten Verfahren ließ nicht erkennen, dass es sich um Auftragsdatenverarbeitung nach § 8 ThürDSG handelte. Zu überarbeiten war auch die Darstellung der Art der gespeicherten Daten und die Speicherungsdauer. Sowohl auf der den Betroffenen ausgehändigten Chipkarte als auch bei der beauftragten Firma werden personenbezogene Daten verarbeitet. Zur Aufgabe der Firma gehört es, die Bezahlung der Einkäufe der Asylbewerber abzuwickeln. Ein Vergleich der der Datenverarbeitung im Auftrag zu Grunde liegenden Vereinbarung mit den Feststellungen vor Ort ergaben hier Unterschiede. Hier war zunächst zu klären, welche Daten hierfür vom Auftragnehmer benötigt und dort verarbeitet werden. Insbesondere war auch zu berücksichtigen, dass es sich bei der Übermittlung der personenbezogenen Daten zwischen dem Auftraggeber und dem Auftragnehmer nicht um eine Datenübermittlung im Sinne des § 22 ThürDSG handelt. Festzustellen war vor Ort, dass die personenbezogenen Daten auf dem Kommunikationsserver lediglich durchgeleitet werden. Eine Speicherung im Zusammenhang mit getätigten Einkäufen durch die Betroffenen im Landratsamt erfolgte demnach nicht. Die Überarbeitung des Verfahrensverzeichnisses ist zwischenzeitlich erfolgt. Das Sicherheitskonzept nach § 9 ThürDSG zu den zu treffenden organisatorischen und technischen Maßnahmen steht noch aus.

5.1.10 Generelle Schweigepflichtentbindung von Asylsuchenden

Zu der an den TLfD gerichteten Anfrage, ob ein Sozialamt im Zusammenhang mit anderen Anträgen auf Sozialhilfe von Asylsuchenden eine generelle Schweigepflichtentbindung verlangen kann, ergab die datenschutzrechtliche Prüfung Folgendes: Unter der Überschrift „Schweigepflichtentbindungserklärung, datenschutzrechtliche Einwilligung“ sollte der asylsuchende Patient oder dessen gesetzlicher Vertreter den jeweils behandelnden Arzt oder Therapeuten von der ärztlichen Schweigepflicht gegenüber den Mitarbeitern des Sozialamts über Art und Umfang seiner für seine Person vorgesehenen oder ausgeführten medizinisch notwendigen Behandlungen und Leistungen entbinden. Als Grundlage hierfür wurde die Aufgabenerfüllung der Behörde nach § 4 Abs. 1 Asylbewerberleistungsgesetz zur Gewährung der erforderlichen Leistungen für ambulante und stationäre ärztliche und zahnärztliche Behandlungen einschließlich der Versorgung mit Arznei und Verbandsmitteln genannt. Eine Schweigepflichtentbindung kann sich aber nur auf den jeweiligen behandelnden Arzt beziehen, dessen Behandlungskosten zur Übernahme anstehen. Eine solche pauschale Erklärung ist aus datenschutzrechtlicher Sicht unwirksam. Darüber hinaus dürften Mitarbeiter des Sozialamtes auch nicht über die erforderlichen fachlichen Grundlagen verfügen, um beurteilen zu können, ob eine Behandlung erforderlich und nach dem Asylbewerberleistungsgesetz zu übernehmen ist. Dies obliegt einer ärztlichen Einschätzung, wozu das betreffende Sozialamt ohnehin in Amtshilfe das Gesundheitsamt in Anspruch nahm.

Auf die Hinweise des TLfD wurde die Erklärung über die Entbindung von der ärztlichen Schweigepflicht für den Einzelfall unter Bezeichnung des konkret zu entbindenden Arztes und der Angabe des Zwecks konkretisiert. Gegenüber dem betroffenen Sozialamt wurde nochmals bekräftigt, dass Schweigepflichtentbindungen auch nur in den Fällen einzuholen sind, in denen die zur Bestimmung von Art und Umfang der eingereichten Rechnungen zu ärztlichen Leistungen für die Prüfung der Kostenerstattung nicht ausreichen.

5.2 Statistik

5.2.1 Umsetzung der Thüringer Verordnung über die statistische Erhebung personenbezogener Daten im Kultusbereich

Mit der dritten Verordnung über die statistische Erhebung von personenbezogenen Daten im Kultusbereich vom 17. November 2004 wird aus datenschutzrechtlicher Sicht bei den künftigen Erhebungen zur Schulstatistik eine neue Qualität der Datenverarbeitung in Thüringen erreicht, indem für Längsschnittuntersuchungen alle Daten eines Schülers während seiner gesamten Schullaufbahn mit einem unveränderlichen Schülermerkmal versehen werden. Um dennoch zu verhindern, dass für die zunächst personenbezogen erhobenen Schülerdaten die Zuordnung über Jahre erhalten bleibt, erfolgt die Pseudonymisierung nach Abschluss der Plausibilitätsprüfungen automatisiert durch eine Einwegverschlüsselung.
Im Zusammenhang mit dieser Änderung der Verordnung über die statistische Erhebung von personenbezogenen Daten im Kultusbereich wurde das Verfahren bei der Durchführung der Schulstatistik in einer Schule und im TKM kontrolliert. Hierbei wurde festgestellt, dass mit der Erhebung der Schülerdaten seit dem Jahr 1994 das Thüringer Landesamt für Statistik (TLS) beauftragt ist, welches zu diesem Zweck auch die notwendigen Erhebungsunterlagen und Programme erarbeitet und den Schulen zur Verfügung stellt. Die von den Schulen durch das TLS erhobenen und hinsichtlich ihrer Plausibilität geprüften Daten werden dann als Einzeldatensätze der Statistikstelle des TKM zur weiteren Verarbeitung und Auswertung übergeben, die nach den verschiedenen Aspekten aggregiert und in Form von Tabellen den Nutzern zur Verfügung stellt. Ein Zugriff auf Einzeldaten der Schüler durch Dritte wird dabei ausgeschlossen. Darüber hinaus speichert auch das TLS eine Kopie des Datenbestandes zur Erstellung von Tabellen für Ländervergleiche der Kultusministerkonferenz sowie in Abstimmung mit dem TKM für eigene Veröffentlichungen. Eine entsprechende Auftragsdatenverarbeitung ist nach dem geltenden Recht durchaus zulässig. Im Hinblick darauf, dass künftig die Erhebung der Daten der Schüler bis zur Generierung des Schülermerkmals personenbezogen erfolgen soll, wurde deshalb das TKM aufgefordert, die Vereinbarung mit dem TLS den aktuellen Bedingungen und Vorgaben anzupassen. Ein Vertragsentwurf liegt zwischenzeitlich vor.
Bezüglich der Bereitstellung von Daten aus dem Personalverwaltungssystem PERSOS-S für statistische Zwecke befindet sich der TLfD mit dem TKM noch im Gespräch.

5.2.2 Gewährleistung des Datenschutzes bei Telearbeitsplätzen im Thüringer Landesamt für Statistik (TLS)

Im Rahmen der Kontrolltätigkeit wurde im Berichtszeitraum auch die Einhaltung datenschutzrechtlicher Bestimmungen bei der Nutzung von Telearbeitsplätzen im Thüringer Landesamt für Statistik (TLS) überprüft. Hierbei wurde festgestellt, dass derzeit im TLS Telearbeitsplätze, mit denen personenbezogene Daten verarbeitet werden, ausschließlich zur Durchführung der amtlichen Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt (Mikrozensus) genutzt werden. Bei dieser Statistik erfolgen mit der Novellierung des Mikrozensusgesetzes ab dem Jahr 2005 über das ganze Jahr verteilt Befragungen in Privathaushalten. Während hierzu früher ausschließlich Vordrucke verwendet wurden, werden nun für die Datenerhebungen von den

Interviewern mobile Erfassungsgeräte (Laptop) eingesetzt. Nach Abschluss erfolgt dann eine Datenfernübertragung an das TLS. Durch die direkte Datenerfassung beim Auskunftspflichtigen in automatisierter Form wird das Erhebungsverfahren dahingehend vereinfacht, als auf die bisherige „Vorarbeit“ der Eintragung der Daten in Fragebögen verzichtet und durch gleichzeitige automatische Plausibilitätsprüfung bei der Eingabe auch die Notwendigkeit späterer Rückfragen vermieden werden kann. Selbstverständlich sind hierfür den besonderen Risiken des Verfahrens entsprechende, besondere technische und organisatorische Maßnahmen zu treffen, um den Forderungen des Datenschutzes und der Datensicherheit gerecht zu werden (5. TB, 15.6.2). Die besondere Aufmerksamkeit gilt dabei der Sicherung der Vertraulichkeit der Daten, um jeden unbefugten Zugang zu Daten durch Dritte z. B. im Haushalt des Interviewers oder bei Verlust oder Diebstahl, wie auch im Rahmen der Fernübertragung auszuschließen. Dies wird im vorliegenden Fall durch eine Vielzahl technischer und organisatorischer Mittel (wie Einrichtung eines Mehrfach-Passwortschutzes, Nutzung von hard- und softwareseitiger Verschlüsselungen, Einrichtung automatisierter Löschungen sowie Sperrung einzelner Ein- und Ausgangsfunktionen) gelöst. Darüber hinaus werden selbstverständlich die Erhebungsbeauftragten entsprechend den gesetzlichen Vorgaben sorgfältig ausgewählt und nachdrücklich auf die Einhaltung der geltenden Geheimhaltungsvorschriften verpflichtet, sodass aus datenschutzrechtlicher Sicht keine Bedenken gegen eine Nutzung der betreffenden Telearbeitsplätze beim Thüringer Landesamt für Statistik erhoben wurden.

5.3 Kommunales

5.3.1 Entwurf einer Neufassung des Thüringer Meldegesetzes (ThürMeldeG)

Mit den erfolgten Änderungen im Melderechtsrahmengesetz vom 25.08.2004 ergibt sich auch die Notwendigkeit der Novellierung des Thüringer Meldegesetzes. Diese sowie weitere Forderungen zur Überarbeitung und Ergänzung des Thüringer Meldegesetzes sollen in einer Neufassung umgesetzt werden. Dazu erfolgten in den letzten Monaten bereits unter dem Aspekt des Datenschutzes Gespräche zwischen dem TIM und dem TLfD. Im Rahmen der Anhörung habe ich auch zum zwischenzeitlich vorliegenden Gesetzentwurf Stellung genommen. Neben einer Reihe von Hinweisen und Anregungen für Änderungen wurde insbesondere zu der Absicht, künftig den vollständigen Meldedatenbestand in sog. Spiegelregistern beim Landesrechenzentrum zu führen und dort im Rahmen regelmäßiger Datenübermittlungen oder durch Abrufverfahren anderen Stellen zu übermitteln, Stellung bezogen. Kritikpunkt ist dabei insbesondere, dass die vorgesehene Regelung nicht mit den bestehenden datenschutzrechtlichen Bestimmungen im Einklang steht, weil die vom Gesetzgeber bestimmte dauerhafte Vorhaltung aller Meldedaten im Landesrechenzentrum und deren Übermittlung an öffentliche und private Stellen ohne Mitwirkung der Gemeinden den Grundsätzen der Datenverarbeitung im Auftrag der Gemeinden widerspricht. Es handelt sich hierbei unzweifelhaft um eine Aufgabenübertragung auf das TLRZ, da die Gemeinden in dieser Verarbeitungsphase faktisch über keinerlei Weisungsbefugnisse oder Kontrollrechte verfügen und insoweit ihrer datenschutzrechtlichen Verantwortung nicht gerecht werden können. Dies bedarf einer gesetzlichen Klarstellung. Darüber hinaus sollte aber auch die vorgesehene „Doppelführung“ des Melderegisters sowohl in der Gemeinde wie auch im Landesrechenzentrum nochmals einer kritischen Prüfung unterzogen werden, da die Erforderlichkeit und Zweckmäßigkeit hierfür nicht nachvollzogen werden kann. Denkbar wäre z. B. statt dessen die Einrichtung einer sog. „Verbunddatei“, an der sich alle Meldebehörden in Thüringen beteiligen würden. Dadurch könnte auch der Gefahr begegnet werden, dass u. U. zur gleichen Anfrage verschiedene Auskünfte aufgrund der späteren Aktualisierungen des Registers im TLRZ erteilt werden.

5.3.2 Unzulässige Übermittlung von Meldedaten für Zwecke der Wahlwerbung

Im Berichtszeitraum musste das Verfahren zur Nutzung von Meldedaten für Zwecke der Wahlwerbung in einer Kommune beanstandet werden. Im vorliegenden Fall hatte der Bürgermeister die Anschriften aller Erstwähler vom Meldeamt mit der Begründung angefordert, in diesen Personenkreis zu einem Erstwählerforum einladen zu wollen. Gleichzeitig hatte er die Daten einer Partei unter Hinweis auf die Möglichkeiten einer Übermittlung nach § 33 ThürMeldeG für Zwecke der Wahlwerbung übergeben. Hierzu habe ich im Ergebnis meiner Prüfung der Kommune mitgeteilt, dass die zuständige Stelle innerhalb einer Kommune für die Verarbeitung und Nutzung von Meldedaten allein die Meldebehörde ist. Eine Weitergabe von Meldedaten innerhalb einer Gemeindeverwaltung ist der Meldebehörde nach § 29 ThürMeldeG erlaubt, soweit die betreffenden Daten zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich sind. Dies trifft selbstverständlich ebenso auf den Bürgermeister zu, auch wenn dieser oberste Dienstbehörde und Dienstvorgesetzter der Gemeindebediensteten ist. Eine Aufgabenstellung des Bürgermeisters zur Kenntnis von Erstwählern lässt sich weder aus der Kommunalordnung noch aus anderen Rechtsvorschriften ableiten. Insoweit war die Übergabe der Meldedaten an den Bürgermeister aufgrund der fehlenden Erforderlichkeit und rechtlichen Befugnis unzulässig.
Auch wenn in § 33 ThürMeldeG die Erteilung von Auskünften über Meldedaten an Parteien und Wählergruppen im Zusammenhang mit allgemeinen Wahlen unter bestimmten Voraussetzungen erlaubt ist, so entscheidet hierüber gemäß § 33 ThürMeldeG allein die Meldebehörde im pflichtgemäßen Ermessen. Voraussetzung für die Übermittlung von Namen und Anschriften der Wahlberechtigten ist eine vorherige Information der Betroffenen über ihr Recht, der Übermittlung in allgemeiner Form zu widersprechen sowie die Tatsache, dass sie von diesem Recht keinen Gebrauch gemacht haben. Da im Rahmen der weiteren Prüfung festgestellt wurde, dass die betreffende Gemeinde ihren Informationspflichten über das Widerspruchsrecht bisher nicht nachgekommen war und deshalb die Meldebehörde im konkreten Fall auch nicht befugt gewesen wäre, die Daten an die auskunftsersuchende Partei zu übermitteln, wurde die gesamte Verfahrensweise gemäß § 39 Abs. 1 ThürDSG beanstandet. Die Gemeinde wurde aufgefordert, die Einwohner auf ihr Widerspruchsrecht hinzuweisen sowie vom Empfänger der Daten deren unverzügliche Löschung zu fordern, welche schriftlich bestätigt wurde.

5.3.3 Veröffentlichung von Einwohnerdaten im Zusammenhang mit der Umbenennung von Straßen

Im Zuge der Zusammenlegung und Eingliederung von Gemeinden müssen häufig auch Umbenennungen von Straßen und Hausnummern vorgenommen werden. Gemäß § 5 Abs. 3 ThürKO ist dies dann die Angelegenheit der jeweiligen Gemeinde, über die gemäß § 15 Abs. 1 ThürKO alle Einwohner zu unterrichten sind. Dass hierbei mitunter das gebotene und zulässige Maß überschritten wird, zeigte sich im letzten Berichtszeitraum in zwei Fällen.
So nahm eine Stadtverwaltung die Umbenennung von Straßen und Hausnummern in einem Ortsteil zum Anlass, alle aus ihrer Sicht wichtigen öffentlichen und privaten Versorgungsträger und Institutionen der Stadt bzw. des Kreises nicht nur über die alten/ neuen Anschriften zu informieren sondern in diesem Zusammenhang auch die jeweiligen Grundstückseigentümer zu benennen. Begründet wurde dies mit einer vermeintlichen Erleichterung der Umschlüsselungsarbeiten in den betreffenden Einrichtungen. In einer anderen Gemeinde wurden nicht nur einzelne Stellen sondern gleich Jedermann im Rahmen der öffentlichen Bekanntmachung des Gemeinderatsbeschlusses über die Umbenennung in einem Anhang zum Amtsblatt über die Namen der jeweiligen Grundstückseigentümer bzw. Bewohner in Kenntnis gesetzt. Mit diesem Service glaubte man, besonders bürgerfreundlich zu sein, ohne das informationelle Selbstbestimmungsrecht der einzelnen Betroffenen zu beachten.

Zu den geschilderten Verfahrensweisen habe ich den betroffenen Kommunen mitgeteilt, dass es weder eine gesetzliche Vorgabe noch eine Erforderlichkeit dafür gibt, im Zusammenhang mit der Umbenennung von Straßen und Hausnummern die Namen der jeweiligen Bewohner oder Grundstückseigentümer zu erheben bzw. anderen Personen oder Stellen zu übermitteln. Nach den betreffenden Beschlüssen handelte es sich lediglich um die Neubenennung bzw. den Austausch von Straßennamen und Hausnummern, für die es keiner Kenntnis personenbezogener Daten der jeweiligen Bewohner oder Eigentümer durch den Bürgermeister, die Gemeinderatsmitglieder oder sonstiger Personen oder Stellen bedurfte. Zur eindeutigen Darstellung des zu regelnden Sachverhaltes war nach dem Beschluss lediglich die Kenntnis der Straßennamen bzw. Hausnummern alt bzw. neu in Form einer Übersicht erforderlich. Es bestand im Zusammenhang mit der Umbenennung auch für die Gemeindeverwaltung selbst keine Notwendigkeit für eine gesonderte Erhebung personenbezogener Daten, da in allen Dateien der Verwaltung mit Anschriften (z. B. im Melderegister, Grundsteuerdatei) nur die bisherigen durch die neuen ersetzt werden mussten, was in der Regel in automatisierter Form möglich ist. Mit der Veröffentlichung des Beschlusses war in der Folge ebenso Jedermann (einschließlich aller Versorgungsträger und Institutionen) eigenständig und ohne weitere Informationen in der Lage, alle bei ihm bekannten bzw. gespeicherten grundstücksbezogenen Daten mit den neuen Anschriften zu aktualisieren bzw. umzuschlüsseln. Selbstverständlich bestehen keine datenschutzrechtlichen Bedenken gegen eine zusätzliche Zuleitung des Beschlusses an einen aus kommunaler Sicht wichtigen Empfängerkreis. Mit der Übermittlung der personenbezogenen Daten wurde jedoch gegen geltendes Datenschutzrecht verstoßen, zumal die Namen der jeweiligen Grundstückseigentümer zweckwidrig aus anderen Gemeindeunterlagen genutzt wurden.
Im Ergebnis meiner Feststellungen wurden die Betriebe und Einrichtungen, die die Grundstückslisten empfangen hatten, aufgefordert, die betreffenden Listen nicht zu nutzen, nicht zu kopieren und an die Gemeinde zurückzusenden, was auch erfüllt wurde. Des weiteren wurden die Vorgänge in den Gemeinderäten und Verwaltungen ausgewertet und die betreffenden Übersichten vernichtet.

5.3.4 Biometrische Merkmale in Pässen und Personalausweisen

Bereits mit Artikel 7 des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002 sind gleich lautende Änderungen des Passgesetzes (§ 4 Abs. 3) und des Personalausweisgesetzes (§ 1 Abs. 4) erfolgt, wonach in den Pass bzw. den Personalausweis neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers auch in mit Sicherheitsverfahren verschlüsselter Form in den Personalausweis bzw. den Pass eingebracht werden dürfen. Die Arten der Merkmale sowie die technischen Einzelheiten hierzu wurden jeweils einem gesonderten Bundesgesetz vorbehalten. Was die Personalausweise betrifft, so gibt es außer der Ankündigung der Bundesregierung, einen neuen Personalausweis mit biometrischen Daten und einer Bürgercardfunktion einschließlich elektronischer Unterschrift zur Verwendung im elektronischen Geschäftsverkehr ab 2007 einzuführen, noch keinen Gesetzentwurf.

Weiter fortgeschritten ist demgegenüber die Einführung eines elektronischen Passes (ePass) mit biometrischen Merkmalen. Die Bestimmung der biometrischen Merkmale in den Pässen hat zwischenzeitlich die Europäische Union vorgenommen und mit der am 18. Januar 2005 in Kraft getretenen „Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“ (ABl. EU Nr. L 385 S. 1) die Aufnahme biometrischer Merkmale in die Reisepässe der Unionsbürger verbindlich geregelt. Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß Artikel 249 des Vertrages zur Gründung der Europäischen Gemeinschaft unmittelbar in allen Mitgliedstaaten. Art. 1 Abs. 2 Satz 1 EG-PassVO

sieht vor, dass die Pässe und Reisedokumente mit einem Speichermedium zu versehen sind, das ein Gesichtsbild enthält. Die Mitgliedstaaten haben nach Art. 1 Abs. 2 Satz 2 EG-PassVO auch Fingerabdrücke in interoperablen Formaten hinzu zu fügen. Schließlich ist in Art. 1 Abs. 2 Satz 3 EG-PassVO vorgesehen, dass die Daten zu sichern sind und das Speichermedium eine ausreichende Kapazität aufweisen und geeignet sein muss, die Integrität, die Authentizität und die Vertraulichkeit der Daten sicherzustellen. Mit der Festlegung der weiteren technischen Spezifikationen wurde nach Art. 2 EG-PassVO die Kommission in Form von Durchführungsbestimmungen im sog. „Komitologieverfahren“ ermächtigt. Die Kommission hat in ihrer „Entscheidung über die technischen Spezifikationen zu Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“ vom 28. Februar 2005 [K(2005) 409 endg] u. a. verbindliche Vorgaben zu den technischen Anforderungen an die im Pass gespeicherten biometrischen Merkmale sowie zu den Vorkehrungen zum Schutz dieser Daten vor Verfälschung und unbefugtem Zugriff gemacht, die ihrerseits größtenteils auf technische Standards und Normen u. a. der Internationalen Zivilluftfahrtorganisation (ICAO) der Vereinten Nationen verweisen. Mit dem Erlass dieser Durchführungsbestimmungen beginnen die Fristen des Art. 6 EG-PassVO zu laufen, die eine Anwendung der Verordnung in Bezug auf das Gesichtsbild spätestens nach 18 Monaten (also am 1. September 2006) sowie in Bezug auf Fingerabdrücke nach 36 Monaten (also am 1. März 2008) vorschreiben.

Wegen der unmittelbaren Geltung der Regelungen der EG-PassVO sind in den Mitgliedstaaten grundsätzlich keine Änderungen der nationalen Gesetze erforderlich. Mit der Ausgabe von Pässen, die den Anforderungen der EG-PassVO entsprechen wurde zum 1. November 2005 begonnen. Hierzu wurde vom Bundesministerium des Innern mit Zustimmung des Bundesrates die Zweite Verordnung zur Änderung passrechtlicher Vorschriften vom 8. August 2005 (BGBl. I S. 2306) erlassen. Darin wurden die Passmusterverordnung, die Verordnung zur Durchführung des Passgesetzes und die Passgebührenverordnung den Vorgaben der EG-PassVO angepasst. In letzterer ist u. a. die Gebühr für die Ausstellung eines ePasses von bislang 26 € auf 59 € erhöht worden. Obwohl der Bundesrat der Verordnung zugestimmt hat, bedauerte er in einer gleichzeitig verabschiedeten Entschließung, dass die Länder bei der Entwicklung der Sicherheitsverfahren von der Bundesregierung nicht eingebunden wurden und daher auch deren technischen Reife nicht verifizieren konnten.

Die neuen ePässe sollen mit einem RFID-Chip ausgestellt werden, auf dem das Gesichtsbild sowie die anderen bereits jetzt aus dem Pass maschinenlesbaren Daten (Name, Vorname, Geburtstag, Geschlecht, Seriennummer und Gültigkeitsdauer) elektronisch gespeichert werden. Die Unverfälschtheit und Richtigkeit der im ePass gespeicherten Daten soll durch eine digitale Signatur sichergestellt werden. Der Schutz vor unbefugtem Zugriff, der bei einem kontaktlosen RFID-Chip durch Abhören der Funkkommunikation zwischen dem Pass und dem Lesegerät möglich ist, soll durch ein Zugriffskontrollsystem (Basic Access Control) realisiert werden, das durch das optische Einlesen der maschinenlesbaren Datenzone des Passes aktiviert wird und die Kommunikation mit dem Lesegerät kryptographisch verschlüsselt (Sitzungsschlüssel). Für die ab 2007 vorgesehene zusätzlich aufzunehmenden Fingerabdrücke ist wegen der Sensibilität der Daten vom Bundesministerium des Innern ein erweitertes Zugriffskontrollsystem (Extendend Access Control) vorgesehen, bei dem durch ein zusätzliches kryptographisches Protokoll der Zugriff nur von dafür speziell autorisierten Lesesystemen erfolgen kann.

Mit dem ePass soll die eindeutige Identifizierung aller Passinhaber durch biometrische Merkmale ermöglicht werden. Dies kann einerseits einen Sicherheitsgewinn bei der Vorbeugung und Bekämpfung von Verbrechen ermöglichen. Damit verbunden sind aber auch Risiken für die Persönlichkeitsrechte der Passinhaber, die insbesondere darin zu sehen sind, dass diese Identifizierungsdaten neben dem Zweck der eindeutigen Identifizierung des Passinhabers

durchaus geeignet sind, als Schlüssel zur Verknüpfung von Daten des Betroffenen aus den unterschiedlichsten Verwendungszusammenhängen zu dienen und damit umfassende Persönlichkeits- und Bewegungsprofile zu erstellen. Dies auch gerade deshalb, weil die vorgesehenen biometrischen Merkmale durchaus auch von Dritten ohne Kenntnis des Betroffenen erhoben werden könnten (z. B. Fingerabdrücke an Gegenständen). Aus diesem Grund bedarf es aus datenschutzrechtlicher Sicht einer strengen Zweckbindung der im Pass gespeicherten personenbezogenen Daten sowie eines Schutzes gegen unbefugtes Auslesen dieser Daten aus dem Pass. In einer Entschließung der Datenschutzkonferenz des Bundes und der Länder vom 8. März 2002 wurde in diesem Zusammenhang gefordert, dass die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt bleiben soll, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber übereinstimmen. Eine Verwendung der Daten für andere öffentliche oder private Zwecke sollte ausgeschlossen werden und insbesondere keine Einrichtung zentraler Dateien erfolgen. Hierauf hat im Rahmen des EU-Rechtsetzungsverfahrens der Bundesbeauftragte für den Datenschutz in seiner Funktion als Vorsitzender der Datenschutzgruppe nach Art. 29 der EG-Datenschutzrichtlinie in gleich lautenden Schreiben an das Europäische Parlament, den Rat und die Kommission hingewiesen. Mit Unterstützung des Europäischen Parlaments wurde daraufhin durch das zuständige Ratsgremium der ursprüngliche Kommissionsvorschlag um eine strenge Zweckbindungsregel in Art. 4 Abs. 3 EG-PassVO ergänzt sowie die Anforderung an das Speichermedium in Art. 1 Abs. 2 EG-PassVO aufgenommen, Integrität, Authentizität und Vertraulichkeit der Daten sicherzustellen und die Vorgabe für die technischen Spezifikationen nach Art. 2 Buchstabe b EG-PassVO formuliert, einen unbefugten Zugriff auf die Daten im Pass zu verhindern. Die Zweckbindungsregel in Art. 4 Abs. 3 EG-PassVO, bestimmt eindeutig, dass die Daten des ePasses ausschließlich zur Identitätskontrolle vor Ort durch Vergleich der Merkmale des Passinhabers mit den auf dem Pass gespeicherten Daten ohne Rückgriff auf zentrale Datenbanken verwendet werden dürfen. Dies entspricht der geltenden Rechtslage des deutschen Passgesetzes. Bundesminister Schily hat bei der Vorstellung des ePasses am 1. Juni 2005 hierzu ausdrücklich erklärt, dass eine zentrale Speicherung der Passdaten nicht geplant sei. Damit erscheinen die derzeitigen Regelungen zur Zweckbindung der Passdaten vom Ansatz her ausreichend.

Nicht abschließend beurteilt werden kann die Frage, ob mit der vorgesehenen technischen Lösung die Vorgaben der EG-PassVO zur Sicherstellung von Integrität, Authentizität und der Vertraulichkeit der auf dem Chip gespeicherten Daten durch entsprechende rechtliche, organisatorische und technische Maßnahmen erfüllt werden. Daher hat die Konferenz der DSB des Bundes und der Länder in einer Entschließung vom 1. Juni 2005 (Anlage 12) davor gewarnt, ohne die Festlegung von technischen und organisatorischen Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung auf der Grundlage eines umfassendes Datenschutz- und IT-Sicherheitskonzeptes bereits in diesem Jahr mit der Ausgabe der ePässe zu beginnen. Denn eine europarechtliche Verpflichtung hierzu besteht erst ab Mitte nächsten Jahres. Auch der Europäische Datenschutzbeauftragte hat Anfang Juni 2005 auf Anfrage des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments u. a. darauf hingewiesen, dass eine Datensicherheitsanalyse des Verfahrens gerade deshalb erschwert wird, weil ein großer Teil der technischen Standards, auf die die Durchführungsbestimmungen der Kommission verweisen, noch in der Entwicklung sind. Am 1. November 2005 wurde mit der Einführung der ePässe ohne Vorliegen eines umfassenden Datenschutz- und IT-Sicherheitskonzepts begonnen. Vertreter der DSB des Bundes und der Länder wurden zuvor lediglich im Rahmen einer Informationsveranstaltung vom BMI über Einzelheiten des Verfahrens unterrichtet. Zudem sind einige Informationen auf der Homepage des BMI zum Abruf bereitgestellt. Im Zusammenhang mit der Einführung der ePässe wurde in den regionalen Medien berichtet, dass in den Passbehörden des Landes noch keine Anzeigegeräte vorhanden sind,

an denen die Bürgerinnen und Bürger ihre auf dem Chip gespeicherten persönlichen Daten einsehen können. Aus datenschutzrechtlicher Sicht halte ich jedoch eine Möglichkeit zur Überprüfung der tatsächlich auf dem Chip gespeicherten Daten durch den Bürger für zwingend erforderlich, zumal nach Artikel 4 Abs. 1 EG-PassVO den Betroffenen dieses Recht ausdrücklich eingeräumt ist. Daher habe ich das TIM aufgefordert, für die Umsetzung des Auskunftsrechts bei den Thüringer Passbehörden zu sorgen.

5.3.5 Einsatz von Videotechnik durch kommunale Einrichtungen

Wie bereits in vorangegangenen Tätigkeitsberichten (4. TB, 4.8; 5. TB, 5.2.19) thematisiert wurde, ist auch im vorliegenden Berichtszeitraum festzustellen, dass in den Kommunen immer häufiger die Videotechnik zum Einsatz kommt. Aufgrund der technischen Weiterentwicklung sinken die Anschaffungskosten für diese Anlagen. Außerdem können die Kameras problemlos installiert werden und ermöglichen eine akzeptable Bildqualität. Man erhofft sich von der Videoüberwachung im Allgemeinen eine Abschreckungswirkung zur Verhinderung von Straftaten und Ordnungswidrigkeiten sowie im Falle eines Rechtsverstoßes dessen Aufklärung und die Verfolgung des Täters. Darüber hinaus soll das Sicherheitsgefühl der Bevölkerung gestärkt werden.
Im Thüringer Datenschutzgesetz ist allerdings nach wie vor keine spezifische Rechtsgrundlage hinsichtlich der Voraussetzungen für eine zulässige Videobeobachtung zur Wahrnehmung des Hausrechts für Thüringer Behörden, geschaffen worden, die dem für Bundesbehörden, private Stellen und öffentliche Wettbewerbsunternehmen geltenden § 6 b BDSG vergleichbar wäre. Eine Videoüberwachung durch öffentliche Stellen ist landesgesetzlich nur für die Polizei im PAG und für die Ordnungsbehörden im OBG geregelt, wobei für § 26 OBG anzumerken ist, dass die „Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen“ eher auf dort genannte Ereignisse im Einzelfall, so z. B. öffentliche Veranstaltungen und Ansammlungen, die nicht dem Versammlungsrecht unterliegen, als auf eine stationäre, also auf Dauer eingerichtete Videoüberwachung zielt.
Soweit die nachfolgenden Voraussetzungen erfüllt sind, hält es der TLfD unter Berücksichtigung der Bestimmungen des § 19 ThürDSG für vertretbar, bestehende Bedenken bezüglich der fehlenden ausdrücklichen Erhebungsbefugnis für die Videoüberwachung zur Durchsetzung des Hausrechts im Hinblick auf die insoweit gebotene Gleichbehandlung aller öffentlichen und privaten Stellen zur Prävention, Gefahrenabwehr und den Schutz des öffentliche Eigentums für einen gewissen Zeitraum zurückzustellen. Prüfmaßstab des TLfD, u. a. bei Beratungsersuchen, zum Einsatz einer Videoüberwachung durch eine Kommune, ist zunächst die Beurteilung der Frage, ob die Maßnahme zur Erfüllung des damit angestrebten Zwecks geeignet erscheint, keine anderen „milderen Mittel“, die der Gemeinde zumutbar sind, durch diese ergriffen werden können und die von der Videoüberwachung ausgehende Grundrechtsbeeinträchtigung letztlich als angemessen zu beurteilen ist.
Des Weiteren ist es erforderlich, auf eine Videoüberwachung sowie auf die verantwortliche Stelle hinzuweisen. Dies geschieht zweckmäßigerweise auf Schildern, die in dem Video überwachten Bereich angebracht werden. Dadurch wird Transparenz für die Betroffenen geschaffen, um sicherzustellen, dass sie ihre Datenschutzrechte auch wahrnehmen können.
Für die gesamte Videoüberwachungsanlage sind gemäß § 9 ThürDSG die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Bestimmungen des ThürDSG zu gewährleisten. Dies geschieht i. d. R. in Form einer Dienstanweisung. Zunächst ist dabei festzulegen, dass die Kommune ihren bDSB in die Planung, Durchführung und Kontrolle des Videoeinsatzes einbezieht. Ebenfalls sind der Zweck, das Ziel und der Umfang der Überwachung zu beschreiben und festzulegen. Weiterhin ist aufzuführen, in welchen Fällen Aufzeichnungen stattfinden, wer hierzu Zugang hat, wie lange diese aufbewahrt werden und zu welchem Zeitpunkt diese wieder gelöscht werden. Die Videoüberwa-

chung ist in regelmäßigen Abständen daraufhin zu überprüfen, ob die Maßnahme weiterhin für erforderlich erachtet wird.
Da moderne Anlagen die Bilder digital aufzeichnen und diese durch ein automatisiertes Verfahren ausgewertet werden können, ist es erforderlich, die Videoüberwachung gemäß § 34 Abs. 2 ThürDSG schriftlich freizugeben und in das nach § 10 ThürDSG zu führende Verfahrensverzeichnis aufzunehmen.

5.3.6 Unzulässige Datenübermittlungen im Zusammenhang mit Fördermaßnahmen

Aufgrund einer Presseveröffentlichung, in welcher über Einzelheiten aus Förderanträgen berichtet wurde, die eine politische Jugendorganisation beim zuständigen Landratsamt eingereicht hatte, erreichte den TLfD eine Anfrage zur datenschutzrechtlichen Bewertung der Übermittlungsbefugnisse des Landratsamtes an die Presse.
Im Ergebnis des diesbezüglichen Schriftverkehrs mit dem betreffenden Landratsamt und einer durchgeführten Kontrolle wurde gegenüber dem Landratsamt eine Beanstandung gemäß § 39 ThürDSG ausgesprochen. Grund hierfür war die mangelnde Sorgfalt des Landrats beim Umgang mit personenbezogenen und personenbeziehbaren Daten insbesondere deren Übermittlung außerhalb des öffentlichen Bereichs, hier an die Presse, ohne dass es dafür eine Rechtsgrundlage in § 22 ThürDSG gab.
Dem Auskunftsanspruch der Presse ist ein hoher Stellenwert im Thüringer Pressegesetz (TPG) eingeräumt. In § 4 Abs. 2 TPG ist allerdings auch festgelegt, dass Auskünfte zu verweigern sind, soweit Vorschriften über die Geheimhaltung und den Datenschutz entgegenstehen. Aus Sicht des TLfD bestand keinerlei Erforderlichkeit, personenbezogene Angaben aus einzelnen Belegen der Presse gegenüber zugänglich zu machen. Vom Landrat wurde die ausgesprochene Beanstandung dahingehend behoben, dass zugesagt wurde, die datenschutzrechtlichen Aspekte bei der zukünftigen Arbeit umzusetzen.

5.3.7 Einsichtsrechte von Vorgesetzten in dienstliche Unterlagen

Im Berichtszeitraum wurde die Frage an den TLfD herangetragen, unter welchen Voraussetzungen und in welchem Umfang die Dienstvorgesetzten der Standesbeamten befugt sind, in Personenstandsunterlagen Einsicht zu nehmen. Grundsätzlich können sich Dienstvorgesetzte jederzeit im Rahmen ihrer Aufsicht alle dienstlichen Unterlagen vorlegen lassen und darin Einsicht nehmen. Problematisch wird dies aber, wenn die Dienst- und die Fachaufsicht wie bspw. bei einem Standesamt nicht zusammenfällt. Insoweit nimmt das Standesamt innerhalb einer Gemeinde eine Sonderstellung dahingehend ein, als die Dienstaufsicht über die Standesbeamten, nicht jedoch die Fachaufsicht von der Gemeinde ausgeübt wird. In § 22 Abs. 2 der DA für Standesbeamte und ihre Aufsichtsbehörden heißt es dazu: „Die Aufsicht über die persönliche Dienstführung übt der Dienstvorgesetzte aus. Er ist nicht befugt, die dem Standesbeamten obliegenden Amtshandlungen wahrzunehmen, einen Dritten mit der Wahrnehmung zu beauftragten oder die Post des Standesamtes zu öffnen.“ Entsprechend dieser gesetzlichen Vorgaben im Personenstandsrecht sind ausschließlich Standesbeamte zum Umgang mit Personenstandsakten befugt (§ 61 PStG i. V. m. § 86 DA für Standesbeamte, § 70 a PStG i. V. m. §§ 12, 22 DA für Standesbeamte). Zur Durchsetzung dieses Trennungsgebots zwischen dem Standesamt und der übrigen Kommunalverwaltung bedarf es selbstverständlich auch entsprechender technischer und organisatorischer Maßnahmen, die u. a. in Vertretungsregelungen, der Schlüsselordnung oder beim Postlauf ihren Niederschlag finden müssen. Dies wurde im letzten Berichtszeitraum auch in einem Standesamt überprüft.
Dennoch ist die Kenntnisnahme von Personenstandsdaten durch den Dienstvorgesetzten nicht gänzlich ausgeschlossen, da die Vorgabe zur Abschottung des Standesamtes nicht vorrangig zur Gewährleistung der Vertraulichkeit der Daten auch gegenüber dem Dienstvorgesetzten

sondern insbesondere zur Sicherung der Integrität, Verfügbarkeit, Authentizität und Revisionsfähigkeit der Daten besteht. Dies ergibt sich insbesondere auch aus den Bestimmungen des § 61 Abs. 1 PStG, wonach Behörden Einsicht in und Auskunft aus Personenstandsunterlagen im Rahmen ihrer Zuständigkeit verlangen können. Eine Befugnis zur Einsichtnahme in Personenstandsunterlagen kann sich daher für den Bürgermeister einer Gemeinde in seiner Funktion als Dienstvorgesetzter der Standesbeamten bzw. für den von ihm beauftragten Untersuchungsführer bei der Durchführung eines Disziplinarverfahrens nach § 27 ThürDG im Rahmen der Ermittlungen gegen einen Standesbeamten ergeben, da der Untersuchungsführer nach § 30 Abs. 1 ThürDG verpflichtet ist, die erforderlichen Beweise zu erheben sind und hierzu insbesondere Urkunden und Akten beizuziehen sowie in Augenschein zu nehmen. Maßgebliche Voraussetzung ist hierbei die Erforderlichkeit der Kenntnisnahme der Daten für den Untersuchungsführer zur Durchführung des Disziplinarverfahrens. Dies ist sicher unzweifelhaft für diejenigen Unterlagen gegeben, die sich durch den Untersuchungsauftrag aufgrund vorliegender konkreter Hinweise für ein Fehlverhalten des betreffenden Mitarbeiters eindeutig bestimmen lassen. In diesem Fall kann auch eine Prüfung der Akten ohne Beteiligung der Fachaufsichtsbehörde vorgenommen werden, soweit deren Einbeziehung nicht als Sachverständige geboten ist. Zu berücksichtigen sind dabei aber ggf. Spezialvorschriften, die einer uneingeschränkten Einsichtnahme in Standesamtsunterlagen und deren Verwendung durch den Untersuchungsführer entgegenstehen können. So sollte insbesondere bei einem eingetragenen Sperrvermerk nach § 4 Abs. 2 ZSHG Kontakt mit der Zeugenschutzstelle aufgenommen werden, um insbesondere das weitere Verfahren bei einer Nutzung der Unterlagen zu klären. Ebenso sollten bei einer Einsichtnahme und Verwendung von Daten über Adoptionen oder Transsexuelle besonders strenge Maßstäbe angelegt werden.

5.3.8 Nutzung automatisierter Abrufverfahren durch das Rechnungsprüfungsamt

Von einer Kommune wurde im Berichtszeitraum die Frage nach der Zulässigkeit der Einrichtung von Zugriffsrechten auf die in den Verwaltungseinheiten genutzten automatisierten Verfahren aufgeworfen. Hierzu wird folgende Auffassung vertreten: Rechnungsprüfungsämter nehmen innerhalb einer Gemeinde eine Sonderstellung ein, indem sie zur Erfüllung ihrer Aufgaben in alle prüfungsrelevanten Unterlagen ungeachtet der ansonsten geltenden Zweckbindungsregelungen für personenbezogene Daten Einsicht nehmen können. Entscheidende Voraussetzung für die Zulässigkeit der Kenntnisnahme ist lediglich, dass die jeweiligen Unterlagen und Daten für das konkrete Prüfungsvorhaben bzw. den Prüfungsauftrag prüfungsrelevant sind. Insoweit verfügt das Rechnungsprüfungsamt über uneingeschränkte Auskunfts- und Einsichtsrechte im Hinblick auf Unterlagen und Daten, deren Kenntnis zur Aufgabenerfüllung erforderlich ist, aber nicht auf ausnahmslos alle in der Verwaltung vorliegenden Daten und Unterlagen. Zu beachten ist dabei, dass auch wenn in Thüringen der funktionale Behördenbegriff gilt und die jeweilige Kommune als speichernde Stelle die Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen für alle in der Verwaltung gespeicherten personenbezogenen Daten trägt, grundsätzlich nur die mit der konkreten Wahrnehmung der jeweiligen Verwaltungsaufgabe betraute Stelle zum Umgang mit den betreffenden Daten befugt ist und die ordnungsgemäße Verarbeitung und Nutzung zu sichern hat. Eine Regelung, wonach das Rechnungsprüfungsamt im eigenen Ermessen die Einrichtung eines Zugriffs auf automatisiert gespeicherte Daten bestimmen könnte, ist somit weder mit dem allgemeinen Datenschutzrecht noch mit der jeweiligen kommunalen Rechnungsprüfungsordnung vereinbar. Ebenso wenig wie ohne Beteiligung des sachlich zuständigen Fachbereichs das Rechnungsprüfungsamt vom Hauptamt einen Generalschlüssel für alle Räume und Behältnisse einer beliebigen Verwaltungseinheit verlangen oder eine zentrale Registratur dem Rechnungsprüfungsamt jede gewünschte Unterlage zur Einsichtnahme übergeben kann, ist z. B. auch der Administrator einer Kommune nicht befugt, allein auf Weisung des Rechnungsprüfungsamtes beliebige Zugriffs-

rechte auf automatisierte Verwaltungsverfahren einzurichten. Dies ergibt sich daraus, dass weder das Hauptamt, eine Registratur oder ein EDV-Administrator „Herr“ des jeweiligen Datenverarbeitungsverfahrens und der Daten ist, sondern diese Bereiche lediglich intern bestimmte Dienstleistungsfunktionen wahrnehmen. Die Bereitstellung von Daten bzw. die Einrichtung lesender Zugriffsrechte ist für das Rechnungsprüfungsamt ausschließlich von der zu prüfenden Stelle zu veranlassen. Dabei muss zur Einhaltung des Datenschutzes im Vorfeld jedes einzelnen Prüfungsverfahrens auf der Grundlage des konkreten Prüfungsziels und -auftrags unter Berücksichtigung der datenschutzrechtlichen Grundsätze der Erforderlichkeit und Verhältnismäßigkeit entschieden werden, ob, für welchen Zeitraum und für welche Daten ein Vollzugriff oder ein Teilzugriff auf die Unterlagen oder das automatisierte Verfahren für den jeweiligen konkreten Prüfungszweck zu ermöglichen ist. Die Verantwortung für die Zulässigkeit der Kenntnisnahme der Daten trägt hierbei als Empfänger das Rechnungsprüfungsamt, sodass es einer detaillierten Begründung der Erforderlichkeit nicht bedarf, soweit dies anhand der Prüfungsaufgabe plausibel ist. Dies trifft in gleicher Weise auf die in automatisierten Verfahren oder die in Schrift oder sonstiger Form gespeicherten Daten zu. Eine unterschiedliche Verfahrensweise ist insoweit weder geboten noch aus datenschutzrechtlicher Sicht gerechtfertigt. In welchem Umfang die für den Prüfungszweck bereitgestellten prüfrelevanten Daten tatsächlich vom Rechnungsprüfungsamt genutzt werden, entscheidet dieses dann nach eigenem Ermessen. Es bestehen daher auch keine Bedenken, soweit erforderlich, einem Rechnungsprüfungsamt zeitlich befristete Zugriffsrechte auf automatisierte Abrufverfahren einzurichten. Ein Erfordernis für die Einrichtung gesonderter automatisierter Abrufverfahren allein für das Rechnungsprüfungsamt dürfte demgegenüber aufgrund der zeitlichen Begrenzung von Prüfungen sowohl aus datenschutzrechtlicher als auch aus wirtschaftlicher Sicht in der Regel nicht gerechtfertigt sein. In jedem Fall bedürfte dies insbesondere hinsichtlich der Erforderlichkeit und Verhältnismäßigkeit einer umfassenden Prüfung und Begründung.

5.3.9 Datenschutz beim Rettungswesen

In meinem 5. TB (5.2.9) hatte ich darüber berichtet, dass im Rahmen einer Kontrolle in einem Rettungsdienstbereich dem TLfD vom Aufgabenträger die geforderte Einsicht in alle vorhandenen Unterlagen gemäß § 37 Abs. 1 ThürDSG nicht gewährt wurde. Weder die Beanstandung durch den TLfD nach § 39 ThürDSG noch die eindeutige Unterstützung des TLfD durch die Kommunalaufsicht konnten daran etwas ändern. Da die von der Kommune gewollte gerichtliche Klärung bislang noch nicht erfolgte, konnte der Vorgang auch in diesem Berichtszeitraum noch nicht abgeschlossen werden.
Die vorgenannte Problematik hatte sich im Rahmen der Bearbeitung einer Beschwerde ergeben, bei der bei dem besagten Aufgabenträger die Dokumentation der Notarzteinsätze nicht den gesetzlichen Anforderungen entsprach. Dies war in der Folge Anlass für weitere Prüfungen in anderen Rettungsdienstbereichen. Die hierbei festgestellten unterschiedlichsten Verfahrensweisen zur Dokumentation von Rettungsdiensteinsätzen wurden anschließend mit der zuständigen Aufsichtsbehörde ausgewertet, mit der Zielstellung, eine allen Anforderungen gerecht werdende gesetzeskonforme und einheitliche Vorgabe für den Inhalt, die Form und die Verwendung der Notarzteinsatzprotokolle zu finden. Obwohl auch die sich anschließenden Beratungen mit dem Rettungsdienstausschuss der Landesärztekammer aus der Sicht des TLfD durchaus konstruktiv waren, wurde bisher vom zuständigen Ministerium noch keine abschließende Festlegung getroffen.
Unbefriedigend ist auch, dass bei der Prüfung, wie die Verbindlichkeit von Festlegungen zum Umgang mit Einsatzdokumentationen bei den Notärzten durchgesetzt werden kann, in dem kontrollierten Rettungsdienstzweckverband keine konkreten schriftlichen Vereinbarungen mit medizinischen Einrichtungen oder Ärzten zur Sicherung des Notarzteinsatzes vorgelegt werden konnten. Da dies auch aus datenschutzrechtlicher Sicht nicht hinnehmbar ist, habe ich entspre-

chende Regelungen angemahnt. Hierüber wurde auch die zuständige Fachaufsicht informiert, die den Hinweis aufgegriffen und von dem Aufgabenträger gleichfalls die zur Sicherung des Notarzteinsatz erforderlichen Vereinbarungen eingefordert hat.

5.4 Sparkassen

5.4.1 Verlust von Kundendaten in einer Sparkasse

Wie ich aus Presseberichten entnommen hatte, waren vertrauliche Kundendaten einer Sparkasse in Form von Listen mit Namen von Schuldnern und die Höhe ihrer jeweiligen Verbindlichkeiten in der Öffentlichkeit aufgetaucht. Ich forderte daraufhin die Sparkasse zu einer schriftlichen Stellungnahme auf und führte eine datenschutzrechtliche Kontrolle in der betroffenen Sparkassenfiliale durch.
Wie sich herausstellte, gelangten die Kundendaten im Zusammenhang mit einem dort ehemalig beschäftigten Mitarbeiter in die Öffentlichkeit, der unter anderem als Kundenbetreuer tätig war. Die näheren Umstände, auf welche Weise und durch wen die Listen an die Öffentlichkeit gelangten, waren Gegenstand staatsanwaltschaftlicher Ermittlungen.
Die aus datenschutzrechtlicher Sicht zu klärende Frage war, ob die Sparkasse alle erforderlichen technischen und organisatorischen Maßnahmen getroffen hatte, um die Ausführung der Vorschriften über den Datenschutz zu gewährleisten. Die Sparkasse übergab die vorhandenen Unterlagen über Regelungen zum Datenschutz. Es handelte sich hierbei um eine allgemeine Dienstanweisung zu Datenschutzbestimmungen sowie um eine spezielle Organisationsanweisung für die Mitarbeiter der Sparkasse, deren Empfang durch jeden einzelnen Beschäftigten bestätigt werden muss, der zugleich auf die gewissenhafte Beachtung der Regelungen verpflichtet wird. Darüber hinaus konnte die Sparkasse sowohl eine Verpflichtung des ausgeschiedenen Mitarbeiters auf das Datengeheimnis sowie dessen Verpflichtung nach dem Verpflichtungsgesetz als auch eine Niederschrift über dessen Gelöbnis nach § 6 BAT vorlegen.
Nach Prüfung aller Unterlagen und unter Berücksichtigung des geschilderten Sachverhalts war festzustellen, dass seitens der Sparkasse keine Versäumnisse im Umgang mit Kundendaten vorlagen, da diese ausweislich der übergebenen Organisations- und Dienstanweisungen sowie der verschiedenen Verpflichtungen die gemäß § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen getroffen hatte.
Ich hatte der Sparkasse abschließend dringend empfohlen, ausscheidenden Mitarbeitern eine Erklärung darüber abzuverlangen, dass sie keine dienstlichen Unterlagen mit personenbezogenen Kundendaten beim Ausscheiden mitnehmen dürfen. Dieser Hinweis wurde von der Sparkasse aufgenommen.

5.4.2 Kopien des Personalausweises

Das Kopieren von Dokumenten bei der Sparkasse veranlasst immer wieder Kunden, sich an den TLfD zu wenden und dort die Zulässigkeit der Maßnahme anzuzweifeln. Dies betrifft insbesondere die Aufforderung der Sparkasse gegenüber dem Kunden, den Personalausweis zum Zwecke der Erstellung einer Kopie vorzulegen.
War in der Vergangenheit der Kunde aufgrund der gesetzlichen Regelung des § 154 Abs. 2 AO bei der Eröffnung eines Girokontos nicht verpflichtet, die Kopie seines Personalausweises zu dulden, erfolgte im Jahre 2003 im Geldwäschegesetz eine Klarstellung. Gemäß § 2 Abs. 1 GwG hat ein Kreditinstitut bei Abschluss eines Vertrages zur Begründung einer auf Dauer angelegten Geschäftsbeziehung, insbesondere bei der Führung eines Kontos und bei den sonstigen in § 154 Abs. 2 Satz 1 der AO genannten Geschäften den Vertragspartner zu identifizieren. Dem Institut wird die Möglichkeit eingeräumt, die auf dem Ausweispapier genannten Angaben

aufzunehmen oder durch Anfertigung einer Kopie der Seiten des zur Feststellung der Identität vorgelegten Ausweises, die diese Angaben enthalten, aufzuzeichnen und aufzubewahren.
Der TLfD hat die anfragenden Sparkassenkunden über die gegebene Rechtslage informiert.

6. Personal

6.1 Thüringer Gesetz zur Änderung besoldungs- und anderer dienstrechtlicher Vorschriften

In den vergangenen Tätigkeitsberichten hatte ich schon mehrfach eine gesetzliche Regelung für die in der Praxis bereits durchgeführte Beihilfebearbeitung durch private Versicherungsunternehmen für die Kommunen angemahnt. Unter Berücksichtigung der datenschutzrechtlichen Hinweise des TLfD wurde im letzten Berichtszeitraum eine Regelung in das Thüringer Beamtengesetz aufgenommen, wonach es den Gemeinden, Verwaltungsgemeinschaften, Zweckverbänden und Landkreisen und sonstigen der Aufsicht des Freistaats Thüringen unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts erlaubt ist, zur Berechnung und Gewährung von Beihilfen nach dem Thüringer Beamtengesetz geeignete Unternehmen nach Maßgabe der Vorschriften des Thüringer Datenschutzgesetzes zu beauftragen. Eine Aufgabenübertragung ist nicht zulässig.

6.2 Einrichtung einer Personalentwicklungsstelle

Mit der Richtlinie zur Vermittlung von Personal sowie zur Besetzung von Stellen/Planstellen in der Thüringer Landesverwaltung (Personalentwicklungsrichtlinie) vom 5. Oktober 2005 (ThürStanz 2005, S. 2056 ff.) wurde mit Wirkung vom 1. November 2005 das Verfahren für die Besetzung von Stellen/Planstellen in der Thüringer Landesverwaltung geregelt. Die Richtlinie enthält auch die Aufgaben der Personalentwicklungsstelle sowie der Ressorts. Die Ressorts melden der Personalentwicklungsstelle die Beschäftigten, deren Aufgaben infolge Modernisierungsmaßnahmen entfallen und die in anderen Bereichen der Landesverwaltung eingesetzt werden sollen. Zur Vereinfachung des Meldeverfahrens wurde ein Fragebogen unter Beteiligung des TLfD erarbeitet, der als Grundlage der Abfrage der Beschäftigtendaten dienen soll. Dieser enthält Angaben zum Beschäftigtenprofil (zur Person, zum derzeitigen Dienstposten und zur Ausbildung) die von der Dienststelle auszufüllen sind, aber auch Angaben, die die Beschäftigten freiwillig machen können. Dies betrifft besondere Kenntnisse, Befähigungen und insbesondere auch den Verwendungswunsch. Die Daten zum Beschäftigtenprofil, die nicht freiwillig abgegeben werden, werden auf der Grundlage des § 101 Abs. 1 Satz 2 ThürBG ohne dass es einer besonderen Einwilligung des Betroffenen bedarf an die Personalentwicklungsstelle weitergeleitet. Die freiwilligen Angaben können nur mit einer Einwilligung übermittelt werden. Sollen die freiwilligen Angaben auch in der personalführenden Stelle verarbeitet werden, so bedarf dies ebenfalls der Einwilligung. Das zuständige Thüringer Finanzministerium hat meine gegebenen Hinweise zu dem Fragebogen sowie zu der Form der Einwilligungserklärung jeweils eingearbeitet. Daher bestehen gegen den Fragebogen keine datenschutzrechtlichen Bedenken.

6.3 Einhaltung des Dienstwegs in Personalangelegenheiten/Bewerbungen auf dem Dienstweg

In Stellenausschreibungen verschiedener Geschäftsbereiche der Thüringer Ministerien war immer wieder zu lesen, dass die Bewerber aufgefordert sind, ihre Bewerbung auf dem Dienstweg an die näher bezeichnete Stelle zu richten. Darüber hinaus wurden im Rahmen der Bearbeitung von Anrufungen des TLfD nach § 11 ThürDSG und durchgeführten datenschutzrecht-

lichen Kontrollen in Personalakten von Bediensteten des Landes Bewerbungsunterlagen aufgefunden, obwohl die Bewerbungen nicht erfolgreich und damit auch nicht im unmittelbaren Zusammenhang mit dem Dienstverhältnis standen. Dies bedurfte einer grundsätzlichen Klärung.
Die DSB des Bundes und der Länder haben sich bereits vor geraumer Zeit mit der Zulässigkeit, Bewerbungen auf Stellenausschreibungen auf dem Dienstweg an die ausschreibende Stelle zu richten, beschäftigt und sind einhellig zu der Auffassung gelangt, dass für Bedienstete weder eine auf die beamtenrechtlichen Vorschriften noch auf andere Rechtsvorschriften zu stützende Verpflichtung besteht, eine Bewerbung auf dem Dienstweg an die ausschreibende Personalstelle zu leiten. Soweit ein Informationsbedürfnis des Dienstherrn besteht, wird ihm durch die Verpflichtung des Beamten, seinen Vorgesetzten rechtzeitig über einen angestrebten Wechsel zu unterrichten, Rechnung getragen. Lediglich wenn ein Betroffener dies selbst wünscht, wäre einer Bewerbung auf dem Dienstweg nichts entgegen zu setzen. Insbesondere eine Stellungnahme zu einer Bewerbung bspw. des unmittelbaren Vorgesetzten, wie verschiedenen Stellenausschreibungen zu entnehmen war, ist nach dem Beamtenrecht nicht vorgesehen. Dasselbe gilt auch für Angestellte, die nicht anders behandelt werden können.
Das TIM hat die Auffassung der DSB des Bundes und der Länder mitgetragen und sieht ebenfalls dem Informationsbedürfnis des Dienstherrn durch die Verpflichtung des Beamten, den Vorgesetzten rechtzeitig über einen angestrebten Wechsel zu unterrichten, in ausreichendem Maße Rechnung getragen. Auch zur Problematik der Aufnahme von Unterlagen erfolgloser Bewerbungsunterlagen in die Personalakte hat das TIM der Auffassung des TLfD zugestimmt, dass nach § 97 Abs. 1 ThürBG nur solche Unterlagen zur Personalakte gehören, die in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehen. Dies trifft auf Bewerbungsunterlagen insbesondere bei erfolgloser Bewerbung nicht zu, da sich am bestehenden Dienstverhältnis nichts ändert. Bei der Abheftung von Bewerbungsunterlagen darf auch nicht im Einvernehmen mit dem betroffenen Beamten von der eindeutigen Regelung des § 97 Abs. 1 Satz 2 ThürBG, nach dem andere Unterlagen, die nicht im unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehen, nicht aufgenommen werden dürfen, abgewichen werden.
Der TLfD hat zur Bekräftigung seiner Forderungen sich auf die eindeutige Äußerung des TIM bezogen und die betroffenen Geschäftsbereiche nochmals darauf hingewiesen. Die Ressorts haben angekündigt, ihre Praxis zu ändern.

Aus dem Geschäftsbereich des TFM wurde an mich die Anfrage gerichtet, ob eine Weisung zur Einhaltung des Dienstwegs in Personalangelegenheiten rechtmäßig ist. Die konkrete Weisung war nach Auffassung des TLfD für die Betroffenen zu undifferenziert und barg damit die Gefahr, dass Personalvorgänge bei unzuständigen Stellen oder ohne konkrete Erforderlichkeit zur Aufgabenerfüllung bei verschiedenen Teilen der Dienststelle zur Kenntnis gelangen. Aus Gründen der Transparenz müsste angegeben werden, welche Stelle für welche konkreten Aufgaben der Personalverwaltung zuständig ist. Selbstverständlich können bei manchen Anträgen die Kenntnis oder die Befürwortung des unmittelbaren Vorgesetzten und des zur Genehmigung Bestimmten erforderlich sein, bspw. bei Sonderurlaub, Urlaubsübertragung, Teilzeit und Altersteilzeit, Arbeitszeit/Kernzeit und Freistellungen, dies darf jedoch nicht dazu führen, dass diese Unterlagen nicht nur bei der letztendlich zuständigen Stelle zur Personalakte, sondern auch bei den zu durchlaufenden Stellen zu Personalunterlagen genommen werden. Auf die Bedenken des TLfD hin wurde die Weisung außer Kraft gesetzt.

6.4 Personalaktenführung

Die ordnungsgemäße und datenschutzgerechte Personalaktenführung war im Berichtszeitraum mehrfach Gegenstand durchgeführter Kontrollen:

Aufgrund einer Eingabe einer Bediensteten in einer Justizvollzugsanstalt des Landes wurde im Rahmen einer datenschutzrechtlichen Kontrolle in die Personalakte nebst Nebenakten Einsicht genommen und diese hinsichtlich der allgemein gültigen Anforderungen überprüft. Nach § 97 Abs. 1 Satz 2 ThürBG gehören zur Personalakte alle Unterlagen, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten); andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden. Nebenakten dürfen nur unter der Voraussetzung des § 97 Abs. 2 Satz 3 ThürBG geführt werden. In diesen dürfen Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden, abgeheftet werden. Dabei ist zu beachten, dass auch diese Unterlagen nur dann abgeheftet werden dürfen, wenn sie für die Aufgabe der nebenaktenführenden Stelle erforderlich sind.
Die Einsichtnahme der im TJM geführten Personalakte der Betroffenen ergab, dass im allgemeinen Teil bspw. Arbeitsgemeinschaftszeugnisse und Studienbescheinigungen abgeheftet waren, die bei der seinerzeitigen Bewerberauswahlentscheidung von der Betroffenen freiwillig übersandt wurden. Da sie mit dem späteren Dienstverhältnis nicht im unmittelbaren inneren Zusammenhang stehen, wurden sie zwischenzeitlich entfernt. In einer Teilakte war die Kopie eines Teils des Mutterpasses abgeheftet, aus der nur die im Fall einer Schwangerschaft mitzuteilenden Daten zu entnehmen waren. Dagegen ist nichts einzuwenden, wenn anstatt einer konkreten Bescheinigung über die maßgeblichen Umstände, die kostenpflichtig ist, von Betroffenen eine Kopie des Mutterpasses gefertigt wird, aus dem sich auch nur die erforderlichen Angaben ergeben. Eine Vorlage des Mutterpasses dürfte allerdings von einer Personalverwaltung nicht verlangt werden. Darüber hinaus ist darauf zu achten, dass sich in der Personalakte nicht mehrere Kopien einer Unterlage befinden, wie dies im Fall des Mutterpasses vorzufinden war. Die bisher durchgeführte Praxis, Kopien der an die für die Zahlbarmachung der Bezüge zuständige Zentrale Gehaltsstelle übersandten Unterlagen zum Nachweis der Übersendung ebenfalls in der Personalakte vorzuhalten, war aufzugeben, da eine weitere Aufgabenerfüllung zu den in den Unterlagen enthaltenen personenbezogenen Daten entfällt. Zum Nachweis der Weiterleitung an die für die Führung der Besoldungsakte zuständigen Zentralen Gehaltsstelle reicht insoweit aus datenschutzrechtlicher Sicht das Übersendungsschreiben aus. Soweit Krankheitsblätter in Personalakten aufbewahrt werden, sind diese nach Ablauf einer Aufbewahrungsfrist von 5 Jahren zu löschen. Dies kann jedoch zu praktischen Hindernissen führen, wenn fortlaufend Erkrankungen auf einem Blatt vermerkt werden. Die Anregung des TLfD, das Krankheitsblatt jeweils nur für ein Jahr anzulegen, um es mit den entsprechenden beizufügenden Unterlagen nach Ablauf der Aufbewahrungsfrist problemlos löschen zu können, wurde aufgegriffen.
In der von der Justizvollzugsanstalt geführten Personalnebenakte waren umfangreiche Einstellungsunterlagen vorhanden, für die aus datenschutzrechtlicher Sicht keine Erforderlichkeit bestand, da sich der Werdegang aus dem Personalblatt ergibt. Die Justizvollzugsanstalten werden daher auf Veranlassung des TJM künftig nach Abschluss eines jeden Bewerberausleseverfahrens in die Personalnebenakten nur noch die Bewerbungsunterlagen der eingestellten Anwärter aufnehmen, die zur Aufgabenerfüllung der Vollzugseinrichtung unbedingt erforderlich sind.
Die Frage, weshalb die Kopie eines Versetzungsgesuchs, das letztendlich nicht erfolgreich war, in der Personalnebenakte abgeheftet war, führte zu einer grundsätzlichen Diskussion. Versetzungsgesuche weisen Parallelen zu Bewerbungen auf andere Dienstposten auf. Bewerbungen, die letztendlich nicht erfolgreich sind, können nicht zur Personalakte genommen werden, da sie nicht im unmittelbaren Zusammenhang mit dem Dienstverhältnis stehen (6.1). Eine Abheftung eines Versetzungsgesuchs, das letztendlich nicht erfolgreich war, ist auch für die aufgabenerfüllende personalnebenaktenführende Stelle nicht erforderlich, sodass es zu entfernen war. Anders gestaltet es sich allerdings mit der Personalakte. Nach § 134 Abs. 1 ThürBG, der sowohl das Petitionsrecht des Beamten als auch die davon zu unterscheidenden Anträge nennt, gehört es zur Verpflichtung des Beamten, seine Anträge auf dem Dienstweg vorzulegen. Aufgrund

des daraus resultierenden unmittelbaren Zusammenhangs mit dem Dienstverhältnis können damit solche Unterlagen auch zur Personalakte genommen werden.
Im Ergebnis der Feststellungen aus der datenschutzrechtlichen Kontrolle wurden aus der Personalakte und Personalnebenakte die als unzulässig festgestellten Unterlagen entfernt.
Ein weiterer Kritikpunkt im Rahmen der durchgeführten datenschutzrechtlichen Kontrolle war die Praxis des Justizbereichs im Zusammenhang mit dem Recht der Betroffenen auf Widerspruch gegen die Einsichtnahme des TLfD in die Personalakten nach § 37 Abs. 2 ThürDSG. Die Ausübung des Widerspruchsrechts steht jedem Betroffenen zu. § 37 Abs. 2 Satz 3 ThürDSG sieht eine Unterrichtung der Betroffenen in allgemeiner Form vor. Im Bereich der Justiz war jedoch für den auszuhändigenden Hinweis auf das Widerspruchsrecht ein Empfangsbekenntnis vorgesehen. Darüber hinaus musste festgestellt werden, dass zumindest in einer Justizvollzugsanstalt die Aushändigung des Hinweises auf das Widerspruchsrecht zum Anlass genommen wurde, sich darum zu bemühen, dass die Bediensteten von ihrem Recht Gebrauch machen. Diese Vorgehensweise verkannte, dass die Ausübung des Rechts der Betroffenen nur auf freiwilliger Basis erfolgen kann. Bemühungen einer Dienststelle, dass die Betroffenen von ihrem Widerspruchsrecht Gebrauch machen, müssen daher ausscheiden. Es wurde dem TLfD jedoch versichert, dass die Bemühungen tatsächlich nicht sehr groß gewesen sein dürften, da der Anteil der widersprechenden Bediensteten prozentual vergleichbar mit anderen Anstalten war.

Ebenfalls aus Anlass einer Petition gemäß § 11 ThürDSG wurde die Personal- sowie Personalnebenaktenführung für Angestellte des Staatsbauamtes Gera (StBA), seinerzeit im Ressort des TFM, kontrolliert.
Hierbei wurde festgestellt, dass die Personalakte nicht der Vorgabe der Personalaktenführungsrichtlinie des TIM vom 21.09.1998 (ThürStanz 1998, S. 1812 f.) entsprach, da sie keine Gliederungsgesichtspunkte erkennen ließ und auch nicht ersichtlich war, dass das TFM gemäß der in Nr. 11 der Personalaktenführungsrichtlinie gegebenen Öffnungsklausel eine eigene Gliederung vorgenommen hatte. Die dort vertretene Auffassung, dass die Personalaktenführungsrichtlinie im Tarifbereich zweckmäßigerweise nicht anwendbar ist, trifft nicht zu, zumal sie mangels anderweitiger Regelungen in anderen Behörden problemlos entsprechend angewendet wird. Weiterhin bemängelt wurde, dass die Personalakte eine Protokollnotiz zu einer Einsichtnahme des Betroffenen in seine Personalakte, Arbeitsaufzeichnungen des Mitarbeiters, die der Eingruppierung zu Grunde gelegt wurden und Unterlagen zu einer erfolglosen Bewerbung enthielt. Da diese Unterlagen nicht im direkten Zusammenhang zur Personalverwaltung und -bewirtschaftung stehen, sind sie nicht als Bestandteil der Personalakte zu betrachten (§ 97 Abs. 1 ThürBG). Eine Einsicht des Betroffenen in seine Personalakte ist nicht zu dokumentieren, da aus der Wahrnehmung des Einsichtsrechts keine personalrechtlichen Konsequenzen abgeleitet werden können. Unterlagen zur Dienstunfähigkeit sollten nicht, wie festgestellt, in der Personalakte selbst, sondern gesondert geführt werden. Der Forderung, die Personalakte vollständig zu überarbeiten, wurde nachgekommen.
Nach Wechsel der Ressortzugehörigkeit des StBA habe ich die Angelegenheit in Zusammenarbeit mit dem TMBV weitergeführt. Vom TMBV wurde zunächst die Aufnahme von Unterlagen zu erfolglosen Bewerbungen und zu Bewerbungen auf dem Dienstweg in die Personalakte für erforderlich gehalten. Nach Auffassung des für das Beamtenrecht federführende TIM ist sowohl die Aufnahme von Unterlagen zu erfolglosen Bewerbungen in die Personalakte als auch zu Bewerbungen auf dem Dienstweg als unzulässig anzusehen (6.3). Daher waren die entsprechenden Schriftstücke aus den Personalakten zu entfernen. Unterlagen zu erfolglosen Bewerbungen sind nach Nr. 9 Personalaktenführungsrichtlinie nach Abschluss des Auswahlverfahrens bzw. entsprechender Folgeprozesse dem Bewerber zurückzugeben. Eine weitere Aufbewahrung dieser Unterlagen kommt nur mit Zustimmung des Bewerbers in einem Zeit-

raum von 1- 2 Jahren in Frage. Das TMBV hat zugesagt, die im Ministerium geführten Personalakten der Thüringer Staatsbauämter entsprechend zu überarbeiten.
Zu der im StBA geführten Personalnebenakte wurde gefordert, alle Unterlagen und Doppel zu entfernen, die nicht zwingend beim StBA benötigt werden, da nach § 97 Abs. 2 Satz 3 ThürBG Nebenakten nur Unterlagen enthalten dürfen, deren Kenntnis zur rechtmäßigen Aufgabenerfüllung der betreffenden Behörde erforderlich ist. Daher waren Unterlagen, die an die ZG weiterzuleiten sind, nicht in Kopie vorzuhalten, da dem StBA hierzu keine weiteren Aufgaben zukommen. Zur Aufgabenerfüllung des StBA sind lediglich der Personalbogen, sowie Unterlagen zu Urlaub und zur Schwerbehinderteneigenschaft (Kopie des Ausweises) erforderlich. Die Mängel in der Führung der Personalnebenakten wurden gemäß § 39 Abs. 1 Satz 1 ThürDSG beanstandet. Ebenfalls wurde beanstandet, dass in der Geschäftsstelle des StBA neben einer Niederschrift eines Personalgesprächs mit dem Betroffenen, als ausschließlicher Bestandteil der Personalakte, Doppel von Schriftstücken aus der Personal- bzw. Nebenakte des Betroffenen geführt wurden, da die Führung von personenbezogenen Akten außerhalb der Personalakten unzulässig ist. Meiner Forderung, die Nebenakten und die Unterlagen der Geschäftsstelle daraufhin zu überprüfen, ob sich vergleichbare Mängel auch in Bezug zu anderen Beschäftigten zeigen und alle Akten kurzfristig zu überarbeiten, wurde entsprochen.

6.5 Einsichtnahme in Personalakten kostenpflichtig?

Ein Landesbediensteter wandte sich an den TLfD mit der Frage, ob es zulässig sei, dass die für ihn zuständige personalaktenführende Stelle seine dortige Akteneinsicht in seine Personalakte in Rechnung gestellt hat.
Der TLfD vertrat hierzu gegenüber der personalaktenführenden Stelle die Auffassung, dass eine solche Einsicht kostenfrei zu erteilen ist. In ihrem Antwortschreiben bestand die Stelle aber weiterhin darauf, dass die In-Rechnung-Stellung der Einsichtnahme rechtmäßig sei.
Daraufhin wandte sich der TLfD an die zuständige oberste Landesbehörde und bat dort um eine Stellungnahme zum Sachverhalt. Nachdem zunächst die Rechtsauffassung der personalaktenführenden Stelle bestätigt wurde, hat der TLfD in einem weiteren Schreiben auf Nr. 1.1 ThürAllgVwKostO verwiesen, wonach „Amtshandlungen im Rahmen eines bestehenden oder früheren öffentlich-rechtlichen Dienst- oder Amtsverhältnisses einschließlich eines Widerspruchsverfahrens“ gebührenfrei sind. Nach Auffassung des TLfD ist die Gewährung der Einsichtnahme in Personalakten durch den Bediensteten zweifelsohne eine solche Amtshandlung. Unstrittig hingegen ist die Kostenerhebung von Auslagen, etwa für Kopien oder Abschriften. Sowohl die Regelung des § 90 c BBG als auch die fast wortgleiche Regelung des § 100 ThürBG setzt das jederzeitige rechtliche Interesse des Beamten an der Einsicht in seine vollständige Personalakte als gegeben voraus. Dies gilt in entsprechender Anwendung auch für Bedienstete im Angestelltenverhältnis.
Die oberste Landesbehörde hat in einer nochmaligen Stellungnahme dem TLfD bestätigt, dass die Ermöglichung der Einsichtnahme eines Bediensteten in seine Personalakte zu den gebührenfreien Amtshandlungen im Sinne der Thüringer Allgemeinen Verwaltungskostenordnung zählt. Dies wurde auch der personalaktenführenden Stelle zur Kenntnis gegeben. Die Stelle hat daraufhin von einer weiteren Verfolgung der strittigen Kosten abgesehen.

6.6 Auskunftserteilung aus alten Personalakten

Aufgrund einer Anfrage beschäftigte sich der TLfD erneut mit der Frage der Aufbewahrungsdauer und der Zulässigkeit der Benutzung von Personalakten in öffentlichen Stellen des Freistaats Thüringen, die vor 1990 abgeschlossen wurden und für die Aufgabenerfüllung der betreffenden Stelle nicht mehr benötigt werden. Eine Löschung bzw. Vernichtung dieser Unterlagen unterblieb bisher weitgehend, weil bei den Lohn- und Gehaltsunterlagen gesetzliche

Aufbewahrungsfristen entgegenstehen und bei den übrigen Personalunterlagen zum Teil auch nicht ausgeschlossen werden kann, dass ansonsten schutzwürdige Interessen der Betroffenen bei der Nachweisführung von Beschäftigungszeiten gegenüber den Rentenversicherungsträgern beeinträchtigt werden könnten. Entsprechend der Vorgaben des § 15 ThürDSG dürfen diese Unterlagen nur noch mit Einwilligung des Betroffenen übermittelt und genutzt werden. Ausgenommen davon sind Lohnunterlagen zu deren Aufbewahrung die Arbeitgeber im Beitrittsgebiet nach § 28 f SGB IV verpflichtet sind. Entsprechend der vorgenannten Regelung sind diese mindestens bis zum 31. Dezember 2006 aufzubewahren, soweit sie nicht dem Betroffenen ausgehändigt oder die für die Rentenversicherung erforderlichen Daten bescheinigt wurden. Sie dürfen frühestens mit Ablauf der auf die letzte Prüfung der Träger der Rentenversicherung bei dem Arbeitgeber folgenden Kalenderjahres vernichtet werden. Diese Vorschrift betrifft nicht die Personalakten in ihrer Gesamtheit sondern ausschließlich diejenigen Teile, die die für die Rentenberechnung notwendigen Angaben nach § 98 Abs. 1 SGB X über die tatsächlich geleisteten Lohn- bzw. Gehaltszahlungen einschließlich der Zu- und Abschläge, Krankentage u. a. enthalten. Durch die Vorgaben des § 98 Abs. 1 SGB X und § 8 AAÜG sind die früheren Arbeitgeber zur Erteilung von Auskünften über die Beschäftigungsverhältnisse insbesondere zur Art, Dauer und dem Entgelt verpflichtet. Nach Wegfall der obigen Gründe für eine weitere Aufbewahrung der „alten“ Personalakten sind diese, entsprechend den Bestimmungen des § 16 ThürDSG dem zuständigen Archiv zur Übernahme anzubieten und soweit eine Archivwürdigkeit nicht festgestellt wird, zu vernichten.

6.7 Nutzung von Personaldaten zur Kosten- und Leistungsrechnung

Im Rahmen des Aufbaus einer Kosten- und Leistungsrechnung in einem Landratsamt wurde die Frage an den TLfD herangetragen, ob der Fachdienst Finanzen vom Personalamt eine Übersicht über die Namen der Mitarbeiter und deren Vergütungsgruppe erhalten kann und inwieweit der Personalrat daran zu beteiligen ist. Hierzu habe ich dem betreffenden Landratsamt mitgeteilt, dass Kosten- und Leistungsrechnungen als innerbetriebliches Informations- und Steuerinstrument zur Effektivierung des Mitteleinsatzes mit der Folge möglicher Veränderungen beim Personaleinsatz sowie anderen Maßnahmen im Bereich der Personalwirtschaft dienen. Die Kosten- und Leistungsrechnungen sind insoweit eine spezielle Form von Organisationsuntersuchungen, für die nach § 20 Abs. 3 ThürDSG auch Daten der jeweiligen Stelle genutzt werden, die für andere Zwecke erhoben und gespeichert sind. Berücksichtigt man, dass die Aufgabenzuweisung für die Kosten- und Leistungsrechnung der Organisationshoheit der betreffenden Stelle unterfällt, dass die Kenntnis der Vergütungs- und Lohngruppen für die einzelnen Mitarbeiter zur Kosten- und Leistungsrechnung erforderlich ist, dass die Ergebnisse der Untersuchung für die Personalwirtschaft benötigt werden und bei Beamten ohnehin die Besoldungsgruppe aufgrund ihrer Amtsbezeichnung bekannt ist, bestehen keine datenschutzrechtlichen Bedenken gegen eine Weitergabe der Lohn- und Gehaltsgruppen durch das Personalamt an die mit der Kosten- und Leistungsrechung betrauten Mitarbeiter. Da die Einführung und Anwendung der Kosten- und Leistungsrechnung als eine Maßnahme zur Einführung neuer und grundlegender Änderungen oder Ausweitungen bestehender Arbeitsmethoden zu bewerten ist, besteht nach § 75 Abs. 3 ThürPersVG ein eingeschränktes Mitbestimmungsrecht des Personalrats. Inwieweit der Landkreis der Empfehlung des Gesetzgebers folgt, eine entsprechende Dienstvereinbarung zum Verfahren mit dem Personalrat abzuschließen oder diesen nur im Rahmen der Beteiligung umfassend über das konkrete Verfahren auch im Hinblick auf die Verarbeitung und Nutzung der Mitarbeiterdaten vorab informiert und ggf. dessen Hinweise berücksichtigt, sollte zwischen den Parteien einvernehmlich festgelegt werden.

6.8 Unzulässige Datenerhebung zur Überprüfung des gewöhnlichen Aufenthaltsortes von Mitarbeitern

Es ist durchaus nicht unüblich, von den Angehörigen der Berufsfeuerwehr die Wohnsitznahme in der jeweiligen Kommune zu fordern, um auf sie im Notfall ggf. auch außerhalb ihrer Dienst- und Bereitschaftsdienstzeiten zurückgreifen zu können. In einer Kommune hatte man deshalb bei der Ausschreibung der Stellen für die Berufsfeuerwehr, im Rahmen der Einstellungsgespräche und in den Arbeitsverträgen die Notwendigkeit der Wohnsitznahme bzw. die Verlegung des Lebensmittelpunktes in die betreffende Kommune als eine zwingende Voraussetzung für die Aufnahme des Arbeitsverhältnisses vorgegeben. Bei Gesprächen mit den Bediensteten sowie bei Zufallsalarmierungen stellte die Kommune fest, dass ein bestimmter Teil der Bediensteten außerhalb der Dienst- oder Bereitschaftszeit nur schwer oder nicht erreichbar war. Dies führte in der Folge zu der Vermutung, dass in einigen Fällen lediglich eine formale Änderung der Anschriften aber kein tatsächlicher Wohnortwechsel bzw. die geforderte Verlegung des Lebensmittelspunktes in die Kommune bei den betreffenden Bediensteten erfolgt sei. Aus diesem Grund wurde der in der Verwaltung tätige Ermittlungsdienst mit einer entsprechenden Prüfung beauftragt, der hierzu in einem Zeitraum von 6 bis 14 Wochen die angegebene Wohnung des jeweiligen Angehörigen der Berufsfeuerwehr zu unterschiedlichen Zeiten außerhalb der Dienst- und Bereitschaftszeit aufsuchte, um dessen Anwesenheit oder zumindest die seines Privatfahrzeugs festzustellen. Bei dieser Gelegenheit wurde auch der Briefkasten im Hinblick auf seine regelmäßige Leerung in Augenschein genommen, und, falls es sich zufällig ergab, wurden auch Hausbewohner angesprochen. Darüber hinaus verfolgte der Ermittlungsdienst auch einige der Bediensteten nach Dienstschluss mit einem Fahrzeug bis zur Stadtgrenze, um zu prüfen, ob und wann die Betreffenden das Stadtgebiet verließen. Die Intensität der Beobachtungen war dabei sehr unterschiedlich und umfasste je Mitarbeiter bis zu 26 Beobachtungen bzw. Einzeldokumentationen.

Diese Datensammlungen über das Verhalten von Bediensteten der Berufsfeuerwehr außerhalb ihrer Arbeits- und Bereitschaftszeit wurden vom TLfD, da sie im besonderen Maße den Bereich der privaten Lebensgestaltung berührten, als unrechtmäßig beurteilt und gemäß § 39 ThürDSG beanstandet. In ihrer Stellungnahme verteidigte die Kommune ihr Handeln, indem nicht nur die Anwendbarkeit des Thüringer Datenschutzgesetzes für die Erhebung und Verarbeitung der betreffenden Daten sondern auch die Zuständigkeit des TLfD bestritten wurde. Begründet wurde dies damit, dass nach Meinung der Kommune das Thüringer Datenschutzgesetz nur für den hoheitlichen Bereich der öffentlichen Verwaltung, nicht jedoch bei privatrechtlichen Verträgen (wie z. B. bei Arbeitsverträgen) gelte. Dieser Auffassung habe ich nachdrücklich widersprochen, in dem ich darauf hingewiesen habe, dass für die Anwendbarkeit des ThürDSG nicht maßgeblich ist, in welchem Zusammenhang oder für welchen Zweck die Daten verarbeitet werden, sondern ausschließlich, ob es sich bei der Daten verarbeitenden Stelle um eine öffentliche Stelle im Sinne des ThürDSG handelt. Für die Zulässigkeit und das Verfahren der Datenerhebung bei dem in Rede stehenden Fall gelten daher die Bestimmungen der §§ 4 und 19 ThürDSG. Aufgrund der fehlenden spezialgesetzlichen Erhebungsbefugnis waren die Datenerhebungen ohne Einwilligung und „hinter dem Rücken“ der Betroffenen unrechtmäßig. Dieser Auffassung schlossen sich die Rechtsaufsichtsbehörden ausdrücklich an. Da sich in der Folge auch das Arbeitsgericht mit der Angelegenheit befasste, war aber die Löschung der unzulässig erhobenen Daten erst nach Abschluss des Verfahrens möglich.

Im Nachgang zu der o. g. Prüfung wurde vom TLfD auch die Arbeitsweise des Zentralen Ermittlungsdienstes der betreffenden Kommune einer datenschutzrechtlichen Kontrolle unterzogen. Dabei wurde festgestellt, dass die für die Tätigkeit des Ermittlungsdiensts getroffenen Regelungen nicht geeignet waren, um z. B. vorgenannte Verstöße gegen datenschutzrechtliche Bestimmungen auszuschließen. Dies betraf insbesondere die Form der Beauftragung, bei der nicht deutlich wurde, dass die jeweils auftragserteilende Stelle innerhalb der Stadtverwaltung

bei der Ermittlungstätigkeit die Verantwortung für die Datenverarbeitung trägt und der Ermittler dementsprechend umfassend über die geltenden Rechtsvorschriften informiert werden muss. Darüber hinaus wurde der Ermittlungsdienst auch gegenüber Dritten (z. B. den befragten Nachbarn) wie ein Privatdetektiv tätig, ohne dass erkennbar war, in wessen konkretem Auftrag er handelt. Um künftig Verstöße gegen datenschutzrechtliche Bestimmungen durch den Ermittlungsdienst auszuschließen, wurde im Ergebnis der Prüfung von der Kommune eine Dienstordnung für den Zentralen Ermittlungsdienst erarbeitet, in der die Rechte und Pflichten der „Auftraggeber“ und der Ermittler bei einer Beauftragung geregelt sind.

6.9 Dienstliche und Private Nutzung von E-Mail und Internet am Arbeitsplatz

Die zunehmende Nutzung von Internet und E-Mail am Arbeitsplatz wirft eine Reihe rechtlicher Fragen auf, die für Dienststellenbeschäftigte und Personalvertretungen gleichermaßen bedeutsam sind. Aus Datensicherheitsgründen muss zwingend die Nutzung des Internets protokolliert werden, damit eine Kontrollmöglichkeit gegeben ist. Dabei müssen transparente interne Regelungen für Klarheit bei allen Beteiligten sorgen.
Wenn öffentliche Stellen ihren Beschäftigten die Nutzung von Internetdiensten ausschließlich zu dienstlichen Zwecken gestatten, wie dies auch seitens des TLfD empfohlen wird, sind Kontrollen nur stichprobenweise und bei konkretem Missbrauchsverdacht zulässig. Die technischen und organisatorischen Maßnahmen der Protokollierung und Auswertung bedürfen der eindeutigen Regelung in einer Dienstvereinbarung. Die entsprechende Protokollierung unter der Beachtung der Datenvermeidung und Datensparsamkeit unterliegt der Zweckbindung nach § 20 Abs. 4 ThürDSG.
Vorab ist darauf hinzuweisen, dass es keinen Anspruch der Bediensteten gibt, das Internet privat am Arbeitsplatz nutzen zu können. Ist die private Nutzung des Internets jedoch gestattet oder zumindest geduldet, kann dies an einschränkende Voraussetzungen anknüpfen und muss auch in angemessener Weise kontrolliert werden. Dabei ist das Fernmeldegeheimnis zu beachten. Eine Protokollierung darf ohne Einwilligung nur dann erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs oder zu Abrechnungszwecken erforderlich ist. Die Verwendung der Protokolldaten zu anderen Zwecken ist aber auch bei begründetem Verdacht auf möglichen Missbrauch oder strafbare Handlungen sowohl im dienstlichen Bereich als auch bei der privaten Nutzung des dienstlichen Internetzugangs dadurch grundsätzlich nicht ausgeschlossen. Da dies jedoch in der Praxis erfahrungsgemäß zu Schwierigkeiten führt, empfiehlt es sich, grundsätzlich keine private Nutzung des Internets und E-Mail zuzulassen. Sollte eine private Nutzung dennoch zugelassen werden, sind die Vorschriften des Telekommunikationsgesetzes und der Telekommunikations-Datenschutzverordnung bzw. des Teledienstedatenschutzgesetzes anzuwenden, da der Dienstherr in diesem Fall seinen Beschäftigten gegenüber die Funktion eines Telekommunikations- bzw. Telediensteanbieters wahrnimmt. Dies setzt aus Sicht des TLfD zwingend eine entsprechende klare Dienstvereinbarung zur Protokollierung der Aktivitäten voraus.

7. Polizei

7.1 Auswirkungen von Urteilen des BVerfG auf das Thüringer Polizeiaufgabengesetz

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 hat festgestellt, dass die Regelungen in der Strafprozessordnung zur Durchführung der akustischen Wohnraumüberwachung zu Zwecken der Strafverfolgung verfassungswidrig sind (10.1). Das Bundesverfassungsgericht hat ausgeführt, dass ein aus Artikel 1 Abs. 1 GG herzuleitender unantastbarer Kernbereich privater Lebensgestaltung besteht, der dem staatlichen Zugriff entzogen ist. Für die Praxis bedeutet dies, dass die akustische Wohnraumüberwachung, sobald dabei Daten aus dem absolut ge-

schützten Kernbereich privater Lebensgestaltung erhoben werden, abgebrochen und Aufzeichnungen gelöscht werden müssen. Auch wenn sich diese Entscheidung nur auf strafprozessuale Befugnisse bezieht, kann dieser Rechtsgedanke, wie zwischenzeitlich allgemein anerkannt ist, auch im Bereich präventiver polizeilicher Eingriffsbefugnisse nicht unberücksichtigt bleiben. Die DSB haben dies in ihrer Entschließung zur Entscheidung des Bundesverfassungsgerichts in der 67. Konferenz der DSB des Bundes und der Länder und in der 68. Konferenz deutlich gemacht (Anlagen 2 und 7). Dass Änderungsbedarf angesichts dieses Urteils auch für das PAG besteht hat der TLfD gegenüber dem TIM dargelegt.
§ 35 PAG ist um eine Regelung zu ergänzen, die beschreibt, wie zu verfahren ist, wenn der absolute Kernbereich privater Lebensgestaltung im Rahmen eines Lauschangriffs im polizeilichen Bereich berührt wird. Auch wird zu berücksichtigen sein, dass das Bundesverfassungsgericht von einer Zulässigkeit eines Lauschangriffs nur bei schwerer Kriminalität ausgeht, sodass Gefahrensituationen für Sachen oder Tiere, wie sie in § 35 Abs. 1 Satz 1 Ziffer 1 PAG aufgeführt sind oder Vergehen nach § 35 Abs. 1 Satz 1 Ziffer 2 PAG nicht zu einem Lauschangriff berechtigen können. § 35 Abs. 5 PAG sieht eine Unterrichtung des Landtags vor, nicht aber die des Betroffenen. Berücksichtigt man jedoch, dass nach der Entscheidung des Bundesverfassungsgerichts zum repressiven Bereich eine Unterrichtung des Betroffenen unerlässlich ist, kann dies angesichts der Eingriffsintensität auch im präventiven Bereich nicht anders sein. Bei den besonderen Mitteln der Datenerhebung nach § 34 PAG besteht ebenfalls Handlungsbedarf, da der in Bezug genommene Straftatenkatalog auch Vergehen umfasst. Seitens des Innenministers ist erklärt worden, dass eine Änderung in Angriff genommen werden sollte, wobei man das Urteil des Bundesverfassungsgerichts zum Niedersächsischen Polizeirecht abwarten wollte. Mit Urteil vom 27. Juli 2005 hat das Bundesverfassungsgericht die § 34 a PAG vergleichbare Regelung des Niedersächsischen Gesetzes für die Sicherheit und Ordnung weitgehend für verfassungswidrig erklärt. Auch wenn sich § 34 a PAG in einigen Bereichen von dieser Regelung unterscheidet, gebietet diese Entscheidung gleichwohl, dass § 34 a PAG zu überarbeiten ist. So sind auch hier Vorkehrungen zum Schutz der individuellen Entfaltung im Kernbereich privater Lebensgestaltung zu treffen. Dies hat die 70. Konferenz der DSB des Bundes und der Länder am 27./28. Oktober 2005 in einer Entschließung (Anlage 15) nochmals bekräftigt.
Für die für das Frühjahr 2006 angekündigte Novelle zum PAG wurde dem TLfD eine frühestmögliche Beteiligung zugesichert.

7.2 Präventiv-polizeiliche Telekommunikationsüberwachung in der Praxis

Mit dem Thüringer Gesetz zur Änderung des Polizei- und Sicherheitsrechts vom 20. Juni 2002 wurde § 34 a PAG eingeführt, wonach unter den dort genannten Voraussetzungen die Polizei von einem Betreiber, der geschäftsmäßig Telekommunikationsdienste erbringt, Auskunft über den Inhalt einschließlich der innerhalb des Kommunikationsnetzes in Datenspeichern abgelegten Inhalte und die näheren Umstände der Telekommunikation einschließlich der Daten über den Standort nicht ortsfester Telekommunikationsanlagen verlangen kann. Gesetzlich festgeschrieben ist eine jährliche Unterrichtungspflicht gegenüber dem Landtag. Nach dem Bericht der Landesregierung über die durchgeführten präventiv-polizeilichen Telekommunikationsüberwachungen im Jahr 2002 (Thüringer Landtag, Drucksache 3/3566 vom 4. September 2003) war eine Maßnahme berichtet worden. Für 2003 (Thüringer Landtag, Drucksache 4/249 vom 18. Oktober 2004) waren insgesamt 38 Maßnahmen gemeldet worden. Dabei handelt es sich fast ausschließlich um Positionsdatenermittlungen von Mobiltelefonen zur Gefahrenabwehr mit geringer Zeitdauer.
Da es sich bei der präventiv-polizeilichen Telekommunikationsüberwachung (PTÜ) nach § 34 a PAG um ein neues Eingriffsinstrument handelt, habe ich vor Ort in den Polizeidienststellen zu den durchgeführten PTÜ seit Inkrafttreten der gesetzlichen Regelung datenschutzrechtliche Kontrollen durchgeführt (5. TB, 7.1). Bei den Kontrollen vor Ort waren in der An-

fangszeit nach Inkrafttreten der gesetzlichen Änderungen verschiedene Defizite festzustellen. In einigen Fällen erfolgte die Anordnung der PTÜ bei Gefahr im Verzug nicht durch den Leiter der PD oder dessen Vertreter, sondern durch nachgeordnete Polizeibedienstete. Teilweise fehlte die Bestimmung der Dauer der Maßnahme, obwohl dies nach § 34 a Abs. 2 Satz 8 PAG zwingend vorgeschrieben ist. Richterliche Bestätigungen nach der Anordnung der Maßnahme bei Gefahr im Verzug waren nur in wenigen Fällen eingeholt worden. Dies wurde anfangs nicht für notwendig angesehen, da davon ausgegangen wurde, dass die Maßnahme mit einer einmaligen Ortung zum Erfolg führte und damit abgeschlossen war, sodass für eine richterliche Bestätigung kein Raum war. In weiteren Fällen erfolgte die erforderliche Benachrichtigung der Betroffenen mit erheblicher zeitlicher Verzögerung.

Für den Berichtszeitraum ist festzustellen, dass diese Defizite mit einer unter Beteiligung des TLfD erarbeiteten Dienstanweisung des TIM zwischenzeitlich behoben wurden. Diese Dienstanweisung bestimmt, dass künftig bei Gefahr im Verzug zeitgleich mit der Anfrage an den Provider dem zuständigen Amtsrichter der Antrag auf richterliche Bestätigung zugeleitet werden soll. Bei der Dauer der Maßnahme muss der Zeitraum angegeben werden. Auch die Benachrichtigung der Anschlussinhaber und Nutzer, soweit diese nicht identisch sind, darf nur in Ausnahmefällen unterbleiben. Die im Rahmen der durchgeführten Kontrollen festgestellten Mängel wurden durch die zuständigen Polizeidienststellen behoben.
Mit Bericht der Landesregierung über die präventiv-polizeiliche Telekommunikationsüberwachung im Jahr 2004 (Thüringer Landtag, Drucksache 4/1078 vom 26. Juli 2005) wurden insgesamt 45 Maßnahmen gemeldet, wobei es sich auch hier in der Mehrzahl um Positionsdatenermittlungen von Mobiltelefonen zur Gefahrenabwehr mit geringer Zeitdauer handelte. Inhaltliche Überwachungen erfolgten in fünf Fällen. Lediglich in einem Fall erfolgte keine nachträgliche Vorlage bei Gericht.
Dass insbesondere durch die Anwendung der Dienstanweisung die datenschutzrechtlichen Regelungen in diesem Zusammenhang eingehalten werden können, haben datenschutzrechtliche Kontrollen zu durchgeführten Maßnahmen im Jahre 2004 ergeben. Nach dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 (7.1) hat das TIM unverzüglich durch Erlass an alle in Betracht kommenden Polizeidienststellen ausgeführt, dass die Anwendung von § 34 a Abs. 1 Satz 1 Nr. 1 und 3 PAG aufgrund der Ausführungen des Bundesverfassungsgerichts zur PTÜ in Niedersachsen nicht mehr in Betracht komme und angeordnet, dass bis auf weiteres PTÜ-Maßnahmen nur noch auf § 34 a Abs. 1 Satz 1 Nr. 2 PAG gestützt erfolgen können. Dies betrifft Fälle, in denen u. a. Leben, Gesundheit und Freiheit einer Person betroffen sind. Es wurde festgelegt, dass von der Beantragung von Verlängerungsanordnungen abzusehen sei, sofern nicht gleichzeitig auch die Voraussetzungen nach § 34 a Abs. 1 Satz 1 Nr. 2 PAG vorliegen. Dies kann jedoch nur eine Zwischenlösung darstellen, da aufgrund der Entscheidung des Bundesverfassungsgerichts auch ein Novellierungsbedarf für § 34 a PAG besteht, den jetzt auch die Landesregierung sieht (7.1). Durch das Urteil sehe ich mich insoweit bestätigt, als ich bereits im Gesetzgebungsverfahren für die Streichung von § 34 a Abs. 1 Satz 1 Nr. 1 und 3 PAG eingetreten bin, ohne dass dies vom Gesetzgeber aufgegriffen worden ist.

7.3 Polizeiliche Informationssysteme

Nach längerer Vorbereitungszeit war im August 2003 das Verfahren INPOL-neu in Betrieb gegangen. In der Folgezeit wurden unter den DSB des Bundes und der Länder noch offene datenschutzrechtliche Fragen zum Verfahren INPOL-neu (sowohl bund- als auch länderseitig) in einem Fragenkatalog zusammengefasst. Darin sind im Wesentlichen datenschutzrechtliche Fragen bei der praktischen Umsetzung des Verfahrens wie bspw. Einrichtung der Zugriffsrechte, Abfragemöglichkeiten oder Protokollierung von Zugriffen sowie zu erstellende Sicherheitskonzepte angesprochen. Auf der Grundlage dieses Katalogs habe ich mich auch mit dem TIM

in Verbindung gesetzt. Neben der Beantwortung von Fragen wurde im Berichtszeitraum auch stichprobenartig im Thüringer Landeskriminalamt (TLKA) Einblick in die Verbunddateien von INPOL genommen. Ein Vergleich mit den diesen Datenspeicherungen zugrunde liegenden Akten hat ergeben, dass gegen die Aufnahme der Daten in die Verbunddatei keine datenschutzrechtlichen Bedenken bestanden. Lediglich in einem Fall war ein zur Löschung markierter Datensatz trotz Überschreiten der Frist noch nicht gelöscht worden. Dies war darauf zurückzuführen, dass aufgrund eines Systemfehlers im Bundeskriminalamt (BKA), das die Datensätze der Verbunddateien führt, eine Löschung vorübergehend technisch nicht möglich war. Nach Behebung des Fehlers teilte das TLKA die Löschung des Datensatzes mit. Im Rahmen der Kontrolle sowie der Stellungnahme zum Fragenkatalog konnte erreicht werden, dass bei Zugriffen auf INPOL-neu neben der Protokollierung aller lesenden und schreibenden Zugriffe künftig auch unberechtigte Zugriffsversuche beim Login vollständig durch das TLKA protokolliert sowie die Protokolle stichprobenartig ausgewertet werden. Dies halte ich für einen wesentlichen Fortschritt im Vergleich zu der nach § 11 Abs. 6 BKAG vorgesehenen zehnprozentigen Stichprobenprotokollierung durch das BKA, da es sich hier regelmäßig um sehr sensible Daten handelt. Selbstverständlich dürfen diese Daten nach § 20 Abs. 4 ThürDSG nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage verwendet werden. Mit dieser Datensicherheitsmaßnahme werden nicht alle Polizeibediensteten unter Generalverdacht eines unbefugten Datenzugriffs gestellt, vielmehr kann die Tatsache der lückenlosen Protokollierung die Beamten im Zweifelsfall von einem möglichen Verdacht entlasten. Noch nicht abschließend geklärt sind die Fragen im Zusammenhang mit einem nach § 9 Abs. 2 ThürDSG zu erarbeitenden Sicherheitskonzept. Hier liegen erste Entwürfe vor, die jedoch insbesondere hinsichtlich der konkret zu treffenden Maßnahmen überarbeitungsbedürftig sind. Ich bin diesbezüglich mit dem TIM weiter im Gespräch.

Ein anderes Problem zur Speicherung von und zum Zugriff auf sensible personenbezogene Daten in polizeilichen Informationsverfahren wurde durch eine Anfrage an mich herangetragen. Danach soll es im Integrationsverfahren Polizei (IGV-P), einem Vorgangsverwaltungsprogramm der Thüringer Polizei über die Schlüsselnummer 901 (Angaben zum Aufenthalt von Homosexuellen) möglich sein, gezielt eine Auswertung des Datenbestandes nach diesem Merkmal durchzuführen und damit Listen über Personen mit einem Bezug zur Homosexualität herzustellen. Eine Überprüfung hat dabei ergeben, dass die Schlüsselnummer 901 im IGV-P eines von 388 Eingabemöglichkeiten darstellt, um die Tatörtlichkeit näher zu bezeichnen. Im aktuellen Bestand der gespeicherten Vorgänge war kein Vorgang, bei dem dieser Schlüssel vergeben worden war. Das TIM hat in der Folge den Schlüssel 901 aus dem Katalog der Tatörtlichkeiten gelöscht. Zusätzlich wurden nach einer weiteren Prüfung die Schlüssel „Homosexueller“ und „Lesbierin“ aus dem Katalog „Täterrolle“ gelöscht, da diese ebenfalls einen Bezug zur sexuellen Orientierung enthalten. Da diese Angaben in der Vergangenheit offenbar nicht zur Arbeit der Polizei erforderlich gewesen sind und es sich dabei um besonders sensible Daten nach § 3 Abs. 9 ThürDSG handelt, erscheint die Löschung der Merkmale angemessen.

7.4 Erkennungsdienstliche Behandlung

Durch eine Eingabe erhielt der TLfD Kenntnis davon, dass das TLKA den Antrag eines Petenten auf Löschung seiner erkennungsdienstlichen Unterlagen abgelehnt hatte. Nachdem er Klage erhoben hatte, war ihm mitgeteilt worden, dass die erkennungsdienstlichen Unterlagen zwischenzeitlich gelöscht und der Zeitpunkt nicht mehr feststellbar war. In der Verwaltungsakte gab es keine Löschungsvermerke und auch kein Protokoll hierzu. Da der Petent in der Wahrnehmung seiner Datenschutzrechte erheblich beeinträchtigt worden war, weil ihm trotz mehrmaliger Anfrage zur Datenlöschung eine falsche Auskunft gegeben worden war, wurde dies

vom TLfD beanstandet. Das TLKA hat durch organisatorische Maßnahmen sichergestellt, dass derartige Vorfälle ausgeschlossen werden können.

Ein anderer Petent wandte sich an den TLfD, weil die zuständige Polizeidienststelle seinen Antrag auf Vernichtung/Löschung erkennungsdienstlicher Unterlagen ebenfalls abgelehnt hatte. Parallel zu der Beschwerde war jedoch bereits ein verwaltungsgerichtliches Verfahren anhängig. Dessen ungeachtet lagen aus datenschutzrechtlicher Sicht die Voraussetzungen für eine Löschung nach § 45 Abs. 2 Satz 1 PAG nicht vor, da, wie aus dem Bescheid bereits hervorging, in den vergangenen Jahren immer wieder Ermittlungsverfahren gegen den Betroffenen eingeleitet worden sind, sodass eine Erforderlichkeit für ein weiteres Vorhalten der Datenspeicherungen begründet werden konnte.

7.5 Videoaufzeichnungen der Polizei im Zusammenhang mit einer Demonstration

Aufgrund von Presseberichten begehrte der TLfD Auskunft vom TIM zu polizeilichen Videoaufzeichnungen im Zusammenhang mit einer Demonstration.
Hierzu bedurfte es zunächst der Klärung, auf welcher Rechtsgrundlage die besagten Videoaufzeichnungen durch die Polizei erfolgten, welche Regelungen/Festlegungen zur Löschung der Aufnahmen bestanden und insbesondere ob auch Löschprotokolle vorliegen. Ich habe mich vor Ort in der zuständigen Polizeidienststelle über den Bestand, den Umfang sowie den Umgang mit den auf der Rechtsgrundlage der §§ 12 a Versammlungsgesetz und 33 PAG gefertigten Videoaufnahmen informiert. Beim praktischen Umgang ließen sich keine datenschutzrechtlichen Mängel feststellen. Der Weg der Bänder von den aufnehmenden Einheiten bis zur zuständigen Dienststelle zwecks Auswertung im strafrechtlichen Ermittlungsverfahren war nachvollziehbar. Die Aufnahmen waren auch aufgrund ihrer Erforderlichkeit zu Beweiszwecken in entsprechenden Strafverfahren nicht gelöscht. In diesem Zusammenhang habe ich dem TIM empfohlen, ergänzend zu den gesetzlichen Vorschriften gesonderte Regelungen zum praktischen Umgang mit der Videotechnik, den Aufzeichnungen, der Fertigung von Kopien und deren Verbleib sowie zum Löschen der Bänder zu treffen.
Bei der anderen Frage, ob datenschutzrechtliche Gründe einer Vorführung der Bänder im Innenausschuss des Thüringer Landtags entgegenstehen, war zu berücksichtigen, dass es sich bei den Aufnahmen um personenbezogene Daten handelt. Dass die Landesregierung dem Informationsersuchen des Innenausschusses nachgekommen ist, hatte somit auch datenschutzrechtlichen Bezug. Da im Ausschuss eine vertrauliche Sitzung zu diesem Beratungsgegenstand beschlossen wurde, habe ich keine Bedenken geäußert, zumal darüber hinaus angemessene technische und organisatorische Maßnahmen getroffen waren, um den Datenschutz sicherzustellen. Dies beinhaltete, dass die Videokassetten dem Ausschuss zur Präsentation vom zuständigen Mitarbeiter direkt zur Verfügung übergeben und nach Abschluss auch wieder mitgenommen wurden.

7.6 Mitteilung des Verfahrensausgangs von der Staatsanwaltschaft an die Polizei

Bei der Verlängerung eines Jagdscheins wurde ein Bürger mit der Frage konfrontiert, wie ein staatsanwaltschaftliches Ermittlungsverfahren wegen eines Verkehrsdelikts gegen ihn ausgegangen sei. Da dieses Verfahren sowohl längst eingestellt worden war aber auch vom Tatvorwurf her für den Betroffenen als eine Bagatellangelegenheit erschien, vermutete der Betroffene einen datenschutzrechtlichen Verstoß und wandte sich an den TLfD. Eine Überprüfung des Vorgangs beim zuständigen Ordnungsamt ergab, dass im Rahmen der waffenrechtlichen Zuverlässigkeitsüberprüfung das Ordnungsamt die zuständige Polizeibehörde nach § 5 Abs. 5 Nr. 3 WaffG um Auskunft über anhängige Strafverfahren ersuchte. Von der Polizei wurde daraufhin das staatsanwaltschaftliche Aktenzeichen sowie das den Ermittlungen zu Grunde lie-

gende Delikt mitgeteilt. Eine Überprüfung bei der Polizei sowie der zuständigen Staatsanwaltschaft hat ergeben, dass die Staatsanwaltschaft das Verfahren zu einem Verkehrsdelikt zwar längst eingestellt, davon aber der Polizei nichts mitgeteilt hatte. Aufgrund von § 482 Abs. 3 StPO und Nr. 11 Abs. 4 MiStra ist die Staatsanwaltschaft nicht verpflichtet, von Amts wegen den Ausgang des Ermittlungsverfahrens an die Polizeibehörde zu übermitteln. Nach einer direkten Anfrage bei der Staatsanwaltschaft wurden die Angaben über den Verfahrensausgang im Ordnungsamt in den Akten ergänzt. Die Polizei hat den Verfahrensausgang jedoch erst im Rahmen meiner Überprüfung erfahren und in ihren Unterlagen berichtigt. Durch diesen Fall wird deutlich, dass es auch bei der Verfolgung von geringfügigen Verkehrsdelikten zu Beeinträchtigungen der Betroffenen kommen kann, wenn nicht aktuelle Daten von der Polizei an weitere Behörden beauskunftet werden. Ich habe mich daher an das Thüringer Justizministerium mit der Bitte gewandt, sich auf Bundesebene für eine Streichung des § 482 Abs. 3 StPO und Nr. 11 Abs. 4 MiStra einzusetzen, da angesichts des vermehrten Einsatzes der EDV im Verkehr zwischen Staatsanwaltschaften und der Polizei eine solche Regelung, die offenbar der Entlastung der Staatsanwaltschaften dienen soll, nicht mehr erforderlich erscheint. Da erfahrungsgemäß derartige Gesetzgebungsverfahren einen längeren Zeitraum in Anspruch nehmen, habe ich das TIM gebeten, zwischenzeitlich durch organisatorische Maßnahmen bei der Thüringer Polizei sicherzustellen, dass in Fällen der Beauskunftung keine unvollständigen Daten übermittelt werden. Wenn der Ausgang des Verfahrens bei einem Verkehrsdelikt nicht bekannt ist, sollte sich die Polizeibehörde vor der Beantwortung des jeweiligen Auskunftsersuchens bei der zuständigen Staatsanwaltschaft über den aktuellen Verfahrensstand erkundigen. Darüber, ob dies künftig landesweit in dieser Weise gehandhabt wird, bin ich mit dem TIM noch im Gespräch.

7.7 Datenverarbeitung im Zusammenhang mit der Fußball-Weltmeisterschaft 2006

Um einen reibungslosen Ablauf der Fußballweltmeisterschaft 2006 in Deutschland zu gewährleisten, bedarf es von Seiten der Organisatoren enormer Anstrengungen, die u. a. die Verarbeitung personenbezogener Daten von Zuschauern aber auch von sonstigen Mitwirkenden umfassen. In einer Entschließung der 69. Konferenz der DSB des Bundes und der Länder am 10./11. März 2005 in Kiel (Anlage 14) haben sich die DSB mit Blick auf die Personalisierung von Eintrittskarten dafür ausgesprochen, personenbezogene Daten der Zuschauer nur im unbedingt erforderlichen Umfang zu erheben und zu verarbeiten.

Ein anderes Problem stellt das sog. Akkreditierungsverfahren dar, dem alle Personen unterzogen werden sollen, die während der Weltmeisterschaft Zugang zu besonders geschützten Bereichen in Stadien haben (z. B. Pressevertreter, Ordner, Caterer, private Sicherheitsdienste). Diese Personengruppe soll mit ihrem Einverständnis bestimmte personenbezogene Daten wie Name, Anschrift, Geburtsdatum etc., an den Deutschen Fußballbund melden, der nach einer Überprüfung entscheidet, ob und in welche Sicherheitsbereiche die jeweiligen Mitarbeiter zugelassen (akkreditiert) werden. Maßgebliches Kriterium für diese Entscheidung ist eine Empfehlung der Sicherheitsbehörden, ob Bedenken gegen den Bewerber vorliegen. Hierzu übermittelt der DFB diese Daten dem Bundeskriminalamt (BKA), der Bundespolizei sowie dem für den Wohnort des Bewerbers zuständigen Landeskriminalamt. Insoweit ist diese Problematik auch für Thüringen als nicht Spielort-Land relevant. Von dort werden jeweils Abfragen der polizeilichen Datenbanken durchgeführt. Das BKA übermittelt die Daten auch dem Bundesamt für Verfassungsschutz (BfV), das für eine Überprüfung bei den Landesämtern für Verfassungsschutz sorgt und das Ergebnis der Überprüfung dem BKA mitteilt. Vom BKA, bei dem die Ergebnisse zusammenlaufen, wird dem DFB eine abschließende sicherheitsbehördliche Empfehlung für Akkreditierung oder Nichtakkreditierung abgegeben. Der DFB macht diese Empfehlung zur Grundlage seiner Entscheidung.

Problematisch ist an diesem Verfahren, dass die Erhebung und Verarbeitung der Daten der Betroffenen durch die Sicherheitsbehörden ausschließlich auf der Grundlage einer Einwilligung des Betroffenen erfolgt. In anderen Bereichen (z. B. Luftverkehrssicherheit) existieren hierzu spezielle Rechtsgrundlagen für eine „Sicherheitsüberprüfung". Angesichts der nicht unerheblichen Gefahren, die mit der Durchführung dieser Großveranstaltung verbunden sind, halte ich dies nur dann für vertretbar, wenn das Verfahren für die Betroffenen mit größtmöglichster Transparenz durchgeführt wird. Hierzu gehört insbesondere, dass in der Information zur Einwilligung der Betroffene umfassend über die Verarbeitung seiner Daten durch die Sicherheitsbehörden informiert wird. Hinsichtlich der Beteiligung des Verfassungsschutzes ist dies jedoch bislang noch nicht ausreichend erfolgt. Darüber hinaus bedarf es einer klaren Aufklärung, bei welcher Stelle der Betroffene im Falle der Ablehnung einer Akkreditierung Auskunft zu den Gründen hierfür erhalten kann. Zudem sind die nach den bislang vorliegenden Unterlagen vorgesehenen Kriterien zur Einbeziehung des Verfassungsschutzes zu weitgehend, da eine Ablehnung einer Akkreditierung bereits dann empfohlen werden soll, wenn Erkenntnisse über nicht gewaltbereiten Extremismus vorliegen. Eine solche Praxis erscheint jedoch im Hinblick auf die Wahrung des rechtsstaatlichen Verhältnismäßigkeitsgebots als bedenklich, da durch ein solches negatives Votum in die von Art. 12 Grundgesetz geschützte Berufsausübungsfreiheit der Betroffenen eingegriffen würde. Gemeinsam mit den Kollegen von Bund und Ländern werde ich das Verfahren weiter begleiten, um eine möglichst datenschutzgerechte Lösung zu erreichen.

7.8 Vorbeugende Verkehrsüberwachung

Im Rahmen der Diskussion des Projektes „Automatische Kennzeichenerfassung" (5. TB, 7.5) wurde bekannt, dass ein Pilotprojekt zur automatischen Abstands- und Geschwindigkeitsmessung von Fahrzeugen in Rede stand. Vom TLfD wurde dies zum Anlass genommen, mit dem TIM Kontakt aufzunehmen und eine Vor-Ort-Kontrolle durchzuführen. Dabei konnten keine hinreichenden Auskünfte zu bereits erfolgten Datenverarbeitungen im Zuge der Installation der Anlage gegeben werden und auch auf ein entsprechendes Schreiben des TLfD an das TIM erfolgte keine nähere Erläuterung hierzu, da nicht klar war, auf welche Weise im vorliegenden Fall nach § 34 Abs. 1 ThürDSG die Einhaltung der Vorschriften zum Datenschutz sichergestellt war, wozu insbesondere auch die Organisation des verwaltungsinternen Handelns zum Vollzug der §§ 9, 10, 10 a ThürDSG zählte. Zwar war die Abnahme der installierten Anlage noch nicht erfolgt, doch bedurfte es angesichts des Umstandes, dass die Anlage einsetzbar war, konkreter Regelungen und Vorgaben für die mit der Installation beauftragte Firma, um zu gewährleisten, dass den schutzwürdigen Belangen Betroffener angemessen Rechnung getragen wurde. Der TLfD hat das Fehlen entsprechender Regelungen und vertraglicher Vorgaben als einen wesentlichen Mangel im Hinblick auf § 34 ThürDSG angesehen und nach § 39 Abs. 1 Satz 1 ThürDSG beanstandet. Im Anschluss daran erfolgten die erforderlichen Klärungen, sodass die Beanstandung als behoben betrachtet werden konnte. Das Vorhaben wurde danach intensiv durch den TLfD begleitet, bis dann zur Jahresmitte 2005 die Inbetriebnahme erfolgte. Datenschutzrechtliche Bedenken lagen nicht vor. Der TLfD ist zu den bisher gemachten Erfahrungen mit dem TIM auch weiterhin im Gespräch.

7.9 Verkehrsüberwachung und Zählung im Autobahntunnel

Aufgrund von Pressemeldungen, wonach in der Tunnelkette der A 71 regelmäßig Verkehrszählungen durchgeführt werden, habe ich mich mit dem Thüringer Ministerium für Wirtschaft, Arbeit und Infrastruktur (TMWAI) in Verbindung gesetzt und um Auskunft gebeten, welche technischen Mittel hierzu zum Einsatz kommen sowie ob dabei auch personenbezogene Daten

verarbeitet werden. Das TMWAI hat hierzu mitgeteilt, dass in den Tunneln der Kammquerung ca. 250 Zählstellen vorwiegend mit Induktionsschleifen eingerichtet sind, die der Erfassung der Verkehrsbewegung und Steuerung der Verkehrsströme dienen, wobei keine personenbezogenen Daten erfasst werden. Daneben sind in den Tunneln bzw. in den Vorfeldern der Tunnel 280 Kameras installiert, die schwenkbar sind, jedoch keine Zoomfunktion besitzen. Diese dienen ausschließlich der Überwachung des Verkehrsflusses bzw. der betriebstechnischen Anlagen. Insbesondere zu der Frage, ob es sich bei den erfassten Videobildern auch um die Erhebung personenbezogener Daten handelt, habe ich in der vom Thüringer Landesamt für Straßenbau betriebenen Zentralen Betriebsleitstelle (ZBL) einen Kontrollbesuch durchgeführt. Dort laufen die Signale der Videokameras zusammen und können in Monitorreihen durch die diensthabenden Mitarbeiter beobachtet werden, wobei das Videobild alle 30 Sekunden auf die nächste Kamera umschaltet. Damit soll der Verkehrsfluss beobachtet und gegebenenfalls Steuerungsmaßnahmen veranlasst werden. Diese Signale werden jeweils 24 Stunden aufgezeichnet und dann überschrieben. Daneben gibt es Bildwiedergabeaufzeichnungen, die ergebnisgesteuert gestartet werden. Bei einem besonderen Ereignis, z. B. Befahren einer Standspur, startet die Aufzeichnung automatisch und wird im Betriebsraum auf einem Monitor abgebildet. Die Einsatzkraft in der Leitstelle kann den Fahrer bspw. mit Lautsprecher ansprechen. Diese Aufzeichnungen werden für 7 Tage gespeichert. Die Qualität der Aufnahmen sowie die fehlende Zoomfunktion ermöglichen keine Identifizierung des Autokennzeichens oder von Personen, sodass von einer nicht personenbezogenen Datenverarbeitung auszugehen ist. Ein Personenbezug lässt sich nur in solchen Fällen herstellen, in denen Zusatzinformationen zu dem aufgezeichneten Geschehen vorliegen. Dies kann bspw. die Aussage eines Zeugen zum amtlichen Kennzeichen im Fall einer Anzeige wegen zu dichten Auffahrens sein. Bei einer entsprechenden Anforderung werden diese Daten gesichert und 90 Tage aufbewahrt. Die Verarbeitung dieser Daten erfolgt dann nicht bei der ZBL, sondern bei der hierfür zuständigen Polizei. Obwohl es sich im Ergebnis um keine Erhebung personenbezogener Daten handelt, habe ich dem Landesamt für Straßenbau empfohlen, die existierende Arbeitsanweisung zur Videoüberwachung zu ergänzen, um sicherzustellen, dass ein Personenbezug der Videoaufnahmen nur durch berechtigte Stellen hergestellt werden kann. Diesen Anregungen ist das Thüringer Landesamt für Straßenbau im Wesentlichen nachgekommen, indem Aufbewahrungs- und Löschfristen entsprechend der Erforderlichkeit festgelegt und insbesondere das Verfahren für die Auskunftserteilung an Polizei und andere berechtigte Stellen revisionssicher ausgestaltet wurde. Meiner zusätzlichen Anregung, auf die Videoüberwachung im Tunnelbereich durch besondere Beschilderung hinzuweisen, ist das Landesamt für Straßenbau letztlich aus Gründen der Straßenverkehrssicherheit nicht gefolgt, da einerseits die Tatsache der Videoüberwachung in der ZBL durch die Medien und durch die Verteilung entsprechender Flyer hinreichend bekannt sei und andererseits im Vorfeld der Tunnel bereits eine Vielzahl von nicht amtlichen Informationen erfolgten und mit einer weiteren Information die Grenzen der visuellen Informationserfassungskapazität überschritten würde.

Im weiteren Verlauf hat mich das Thüringer Innenministerium um eine Stellungnahme dazu gebeten, ob diese Live-Bilder bei besonderen Ereignissen sowohl an die Verkehrspolizeiinspektion Suhl als auch das Gefahrenabwehrzentrum der Tunnelfeuerwehr übertragen werden können. Dabei soll keine Daueraufschaltung auf die Monitore dieser Behörden erfolgen sondern vielmehr eine klar definierte Verfahrensanweisung zugrunde gelegt werden, nach der nur in besonderen Gefahrensituationen (z. B. Gegenstände auf der Fahrbahn, Geisterfahrer, Ölspur, Brand, Verkehrsunfall etc.) eine Übermittlung der Bilder erfolgen soll. Gegen eine solche Verfahrensweise habe ich keine datenschutzrechtlichen Bedenken erhoben, da ein Personenbezug allein aus den Videobildern nicht herstellbar ist. Soweit die Polizei oder die Feuerwehr im Zuge des weiteren Einsatzes personenbeziehbare Erkenntnis erhalten, erfolgt die Datenverarbeitung nach den für diese Stelle geltenden Grundsätzen. Ich habe allerdings gegenüber dem TIM

gefordert, dass die Verfahrensweise mit dem Landesamt für Straßenbau abgestimmt und konkretisiert wird, welche Stellen zum Kreis der potentiellen Empfänger der Aufnahmen gehören sollen. Eine abschließende Stellungnahme hierzu liegt noch nicht vor.

7.10 Kontrolle der Zentralen Bußgeldstelle

Im Zusammenhang mit der Einführung des Pilotverfahrens „Vorbeugende Verkehrsüberwachung“ (7.8) wurde in der Zentralen Bußgeldstelle das Verfahren zur Verfolgung von Verkehrsverstößen einer datenschutzrechtlichen Prüfung unterzogen. Hierbei wurde festgestellt, dass dort ausschließlich Daten über festgestellte Verkehrsverstöße verarbeitet werden und insoweit die erhobenen Daten auf das für die Aufgabenerfüllung zwingend notwendige Maß reduziert sind. In einer zentralen Filmauswertestelle wird lediglich anhand der Bildqualität geprüft, ob die jeweiligen Bilder auch gerichtsfest verwendbar sind, ansonsten werden diese gelöscht. Bei den derzeit in Thüringen vorgenommenen Abstandsmessungen wird die Bußgeldstelle nur über die Verkehrsordnungswidrigkeit schriftlich informiert, während die dazugehörigen Videoaufnahmen bei den jeweiligen Verkehrspolizeiinspektionen verbleiben. Bei gerichtlichen Verfahren werden ggf. Kopien dieser Aufnahmen von den betreffenden Verkehrspolizeiinspektionen direkt den Gerichten zugesandt.
Eine weitere Kontrolle im Berichtszeitraum bezog sich auf die technischen und organisatorischen Maßnahmen. Eingehend wurden die Verfahrensabläufe der Datenfernübertragung der aufgezeichneten Geschwindigkeitsverstöße aus dem Rennsteigtunnel an die ZBS in Artern erörtert. Die bei der Kontrolle noch nicht vorhandenen Verfahrensverzeichnisse und Errichtungsanordnungen liegen zwischenzeitlich im Entwurf dem TIM zur Bestätigung vor. Das Sicherheitskonzept und die verfahrensspezifischen Sicherheitskonzepte liegen noch nicht vor, sodass diese Kontrolle noch nicht abgeschlossen werden konnte.

8. Verfassungsschutz

8.1 Auswirkungen der Urteile des BVerfG auf das Thüringer Verfassungsschutzgesetz

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 (7.1) hat auch Auswirkungen auf Maßnahmen nach dem Thüringer Verfassungsschutzgesetz (ThürVSG). Wenn die Entscheidung auch nur Maßnahmen betrifft, die auf die StPO gestützt werden, sind diese Gesichtspunkte angesichts der Eingriffsintensität auch auf den Bereich der präventiven Maßnahmen zu übertragen, zu denen solche nach § 7 Abs. 2 ThürVSG zählen. Im Anhörungsverfahren zur Änderung des Gesetzes (5. TB, 8.2) war vom TLfD Kritik u. a. zu der Aufnahme weniger gravierender Delikte wie Urkundenfälschung und Untreue geäußert worden. Nach § 7 Abs. 2 Nr. 1 ThürVSG ist der sog. Lauschangriff dann möglich, wenn die materiellen Voraussetzungen beim Eingriff in das Brief-, Post- oder Fernmeldegeheimnis nach § 1 Abs. 1 und § 3 Abs. 1 des Artikel 10-Gesetzes (G 10) vom 26. Juni 2001 gegeben sind. Nach § 3 Abs. 1 Nr. 1 - 5 sowie 7 G 10 stehen hier Straftaten in Rede, die die Gefährdung des demokratischen Rechtsstaates, Landesverrat und Gefährdung der äußeren Sicherheit und Vergehen nach dem Ausländergesetz betreffen. Dieser Strafrahmen liegt unterhalb der Grenzen von 5 Jahren, die nach dem Urteil des Bundesverfassungsgerichts im repressiven Bereich zu einem entsprechenden Eingriff berechtigt. Auch ist nach § 7 Abs. 2 Nr. 1 und 2 eine Bezugnahme auf Bestrebungen nach § 2 Abs. 1 Satz 2 Nr. 1, 3 oder 4 durch Planung oder Begehung von Straftaten nach §§ 129, 130, 131 StGB für einen verdeckten Lauschangriff nicht mehr möglich, da diese Straftaten ebenfalls Vergehen darstellen, bei denen der Strafrahmen unterhalb der nach dem Bundesverfassungsgericht vorgegebenen Grenze liegt. Daher können auch die nach § 7 Abs. 2 Satz 1 Nr. 3 aufgeführten Straftaten nach §§ 261, 263 - 265, 265 b, 331 - 334 StGB sowie § 92 Abs. 2 AuslG

nicht mehr möglich sein, sodass im Gesetz auch hier bei der in Aussicht gestellten Novellierung des ThürVSG Änderungen erforderlich sind.

8.2 Verwaltungsvorschrift zum Sicherheitsüberprüfungsgesetz

Das am 4. April 2003 in Kraft getretene Thüringer Sicherheitsüberprüfungsgesetz (ThürSÜG; 5. TB, 8.1) sieht in § 34 vor, dass das für den Geheimschutz zuständige Ministerium die zur Ausführung des Gesetzes erforderlichen Verwaltungsvorschriften und das für die Wirtschaft zuständige Ministerium im Einvernehmen mit dem vorgenannten Ministerium die Verwaltungsvorschriften für den Bereich der nicht öffentlichen Stellen erlässt. In der Begründung hierzu heißt es, dass der Erlass allgemeiner Verwaltungsvorschriften erforderlich ist, um die Verwaltungsabläufe innerhalb der zuständigen Stelle zu regeln. Auf meine Anfrage hat mir das hier federführende TIM mitgeteilt, dass es im Hinblick auf den von der Landesregierung vorgesehenen Abbau von Verwaltungsvorschriften keine Verwaltungsvorschrift sondern eine Handlungsempfehlung geben will. Unabhängig davon, welche Form für die ergänzenden Regelungen vorgesehen sei, hat der Gesetzgeber den entsprechenden Auftrag erteilt, der nach mehr als zwei Jahren nach Inkrafttreten des ThürSÜG umgesetzt werden sollte. Der TLfD sieht hier Handlungsbedarf.

8.3 Kontrollen im Landesamt für Verfassungsschutz

Das Thüringer Landesamt für Verfassungsschutz (TLfV) wurde auch im Berichtszeitraum kontrolliert. Ausgangspunkt dafür waren Vorwürfe gegen das TLfV, rechtswidrig Daten erhoben zu haben. Im Rahmen der durchgeführten Kontrolle bestätigte sich dieser Vorwurf nicht.

8.4 Kontrolle von G 10-Maßnahmen

Über die Änderungen in § 15 Abs. 5 G 10, durch den die Kontrollbefugnis für die gesamte Erhebung, Verarbeitung und Nutzung der nach diesem Gesetz erlangten personenbezogenen Daten der G 10-Kommission des Bundes übertragen wurde, hatte ich schon berichtet (5. TB, 8.2). Auch in diesem Berichtszeitraum wurde die aufgrund eines Urteils des Bundesverfassungsgerichts eingeführte Regelung nicht in Thüringer Landesrecht umgesetzt. Berücksichtigt man, dass nach § 16 Abs. 2 G 10 personenbezogene Daten des BfV nur dann an Landesbehörden übermittelt werden dürfen, wenn die Kontrolle ihrer Verarbeitung und Nutzung durch den Landesgesetzgeber geregelt ist, ist hier dringender Änderungsbedarf gegeben, wenngleich sich an meiner Rechtsauffassung, dass dann eine Kontrollzuständigkeit beim TLfD besteht, nichts geändert hat.

9. Finanzen - Steuern

9.1 Gesetz zur Förderung der Steuerehrlichkeit oder der gläserne Bankkunde

Am 01.04.2005 ist das Gesetz zur Förderung der Steuerehrlichkeit (BGBl. I 2003 S. 2928), über dessen Entwurf ich bereits in meinem 5. TB (9.3) berichtet hatte, in Kraft getreten. Hierzu hat die Konferenz der DSB des Bundes und der Länder in ihrer Entschließung „Staatliche Kontenabfrage muss auf den Prüfstand!“ (Anlage 10) vom 26.11.2004 gefordert, das Gesetz mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere sollte das Gebot der Normenklarheit beachtet werden. Nach § 93 Abs. 8 AO erhält eine Behörde Auskunft zu Kontenstammdaten wie bspw. Name, Geburtsdatum und Kontonummer, wenn sie ein Gesetz anwendet, das an „Begriffe des Einkommenssteuergesetzes“ anknüpft. Welche Behörden dies sein sollen, geht jedoch aus dem Gesetz nicht hervor. Ein

Widerspruch zum verfassungsrechtlichen Transparenzgebot liegt darin, dass Bankkunden erst bei einer Diskrepanz zwischen ihren Angaben und den Ergebnissen der Kontenabfrage von der erfolgten Abfrage in Kenntnis gesetzt werden. In diesem Sinne äußerte sich auch der BfD in seiner Stellungnahme an das Bundesverfassungsgericht anlässlich einer Verfassungsbeschwerde und eines Antrags auf Erlass einer einstweiligen Anordnung. In seinem Beschluss vom 22.03.2005 hat das Bundesverfassungsgericht die beantragte einstweilige Anordnung gegen den automatisierten Abruf von Kontenstammdaten abgelehnt. Ein Grund dafür war der zuvor durch das BMF verfügte Anwendungserlass zur Abgabenordnung (AEAO), der u. a. vorsieht, dass ein Abruf der Kontenstammdaten zum Zwecke der Steuererhebung nur anlassbezogen und zielgerichtet sowie unter Bezugnahme auf eindeutig bestimmte Personen zulässig ist. Darüber hinaus wurde die Benachrichtigung der Betroffenen in verschiedenen Verfahrensstadien geregelt. Für den Kontenabruf nach § 93 Abs. 8 AO wurde eine Konkretisierung der abrufberechtigten Behörden der Sozialverwaltung vorgenommen.

Im noch nicht abgeschlossenen Hauptsacheverfahren gegen die gesetzlichen Neuregelungen haben verschiedene LfD und der BfD in einer weiteren Stellungnahme, der ich mich angeschlossen habe, gegenüber dem Bundesverfassungsgericht u. a. kritisiert, dass der Wortlaut des § 93 Abs. 8 AO keine Aussage darüber enthält, zu welchem Zweck eine Abfrage erfolgen darf und nicht konkret bezeichnet, um welche Begriffe des Einkommenssteuergesetzes es sich handelt. Da eine Vielzahl von Begriffen aus dem Einkommenssteuerrecht in Frage kommen, ist der Anwendungsrahmen der Vorschrift nicht exakt einzugrenzen. Daraus ergibt sich auch, dass es für die Betroffenen nicht ersichtlich ist, welche Behörden zur Abfrage berechtigt sein können. Auch wenn im AEAO sieben Gesetze benannt wurden, deren Anwendung gemäß § 93 Abs. 8 AO zur Abfrage berechtigen, ist dennoch nicht erkennbar welche Behörden zu welchem Zweck Zugriffsbefugnisse erhalten können. Daher sind die Berechtigung zur Abfrage, die konkreten Verwendungszwecke und die Zulässigkeit der Datennutzung gesetzlich zu regeln. Im Hinblick auf den Grundsatz der Verhältnismäßigkeit sollte, um der Gefahr von Routineabfragen zu begegnen, bereits im Gesetz geregelt werden, wer in den berechtigten Stellen eine Kontenabfrage anordnen darf. Ein Schritt in die richtige Richtung ist es, dass die für die Kontenabfrage genutzten Formulare die Prüfung und Zeichnung durch Vorgesetzte vorsehen. Unzureichend sind auch die Regelungen des § 93 Abs. 7 und 8 AO in Bezug auf das verfassungsrechtliche Transparenzgebot. Demgegenüber wäre es erforderlich, dass der Betroffene bereits vor einer Kontenabfrage über die Möglichkeit der Abfrage und deren Voraussetzung informiert wird. Schließlich wurde kritisiert, dass im Gesetz keine Dokumentation der Zugriffe vorgesehen ist, welche den Betroffenen neben der Information über den Abruf in die Lage versetzen könnte, den Kontenabruf auch gerichtlich überprüfen zu lassen. Hierzu wäre zu fixieren, wer in der ersuchenden Behörde oder beim Gericht aus welchen Gründen eine Kontenabfrage veranlasst hat und warum dies erforderlich war. Besonders wichtig ist es hierbei, die Abfragen beim Bundesamt für Finanzen (BfF) zu protokollieren. Es bleibt abzuwarten, ob das Bundesverfassungsgericht die datenschutzrechtlichen Kritikpunkte aufgreift.

Nach Medienberichten seien in den ersten 8 Wochen seit dem Inkrafttreten der Neuregelung bundesweit 804 Kontenabfragen durch das BfF durchgeführt worden. In 674 Fällen seien detaillierte Prüfungen z. B. des Kontostandes und der Kontenbewegungen vorgenommen worden.

Auf meine Anfrage zum Vollzug in Thüringen hat das TFM mitgeteilt, dass in Thüringen zwischen dem 01.04.2005 und dem 30.06.2005 insgesamt 21 Anfragen nach § 93 Abs. 7 AO durch sechs Finanzämter und gemäß § 93 Abs. 8 AO durch ein BAföG-Amt eines Studentenwerks veranlasst worden waren. Die beispielhaft bei einem Finanzamt durchgeführte Recherche ergab, dass letztlich erfolglos versucht wurde bei langjährigen Vollsteckungsschuldnern mittels der Abfrage von Konten bisher unbekannte Vollsteckungsmöglichkeiten zu ermitteln. Das BAföG-Amt teilte mit, dass im Rahmen der Überprüfung nach § 45 EStG i. V. m. § 41 BAföG in drei Fällen bei Studenten Zinseinkünfte vermutet wurden, die in deren BAföG-Anträgen nicht angegeben waren. Dies hatte sich jedoch nicht bestätigt.

9.2 Verordnung über den automatisierten Abruf von Steuerdaten des Bundesamtes für Finanzen, der Finanzämter und Gemeinden (StDAV)

Auch im Berichtszeitraum wurde die datenschutzrechtliche Begleitung der Neuregelung der StDAV, über die ich schon im 5. TB (9.5) berichtet hatte, fortgesetzt. So ist im Verordnungsentwurf vom Januar 2004 die Formulierung, die AO sei eine Datenschutzvorschrift mit abschließendem Charakter und lasse für andere Datenschutzvorschriften keinen Raum, auf die Forderung der DSB des Bundes und der Länder hin, gestrichen worden. Ebenso berücksichtigt wurde die geäußerte Kritik an der Formulierung, wonach Amtsträger auch „... zur Bearbeitung sonst zugewiesener Aufgaben des Besteuerungsverfahrens ...“ berechtigt sind, Daten eines Finanzamts abzurufen.
Zur Regelung in § 2 Abs. 2 des Entwurfs vom Januar 2004, wonach, auch wenn ein Gesetz dies nicht ausdrücklich vorsieht, Abrufverfahren eingerichtet werden sollen, wenn es wegen des Umfangs der Daten oder ihrer häufigen oder besonders eilbedürftigen Nutzung angemessen ist, wurde gefordert, diese Formulierung zu streichen, da damit die Ermächtigung zur Einrichtung von Abrufverfahren vom Gesetzgeber zur Verwaltung vorschoben wird. Diese Forderung blieb unberücksichtigt.
§ 6 Abs. 1 des Verordnungsentwurfs von Mai 2005 bestimmt die im Zusammenhang mit Datenabrufen aufzuzeichnenden Daten. Dies sind neben der Benutzerkennung, Datum, Uhrzeit die „ … sonstigen zur Prüfung der Zulässigkeit der Abrufe erforderlichen Daten.“, worunter insbesondere die Begründung für den Abruf zu verstehen ist. Nachdem ich davon Kenntnis erlangte, dass im Hinblick auf den damit verbundenen Aufwand vorgesehen ist, die in § 6 Abs. 1 normierte Verpflichtung zur Aufzeichnung von Abrufbegründungen zu streichen, habe ich gegenüber dem TFM ausgeführt, dass nach § 9 Abs. 2 Nr. 5 ThürDSG öffentliche Stellen je nach der Art der zu schützenden Daten jederzeit zu gewährleisten haben, dass festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit). Daher würde ein Verzicht auf die Aufzeichnung aussagekräftiger Begründungen von Datenabrufen die Revisionsfähigkeit in Frage stellen, was angesichts der hohen Sensibilität von Steuerdaten datenschutzrechtlich bedenklich wäre. Um die Aussagefähigkeit der Aufzeichnung zu erhöhen, wurde angeregt, zu dokumentieren, für welchen Vorgang (Aktenzeichen oder Steuernummer) die abrufende Stelle die Daten benötigt. Damit würde mit geringem Aufwand die Grundlage für eine erfolgreiche Prüfung der Zulässigkeit der Abrufe geschaffen, wodurch die Protokollierung als ein Mittel der dienst- und datenschutzrechtlichen Aufsicht wirksam sein kann. Bei der nachfolgenden Beratung des Entwurfs der StDAV im Bundesrat wurden die Bedenken gegen eine Streichung der Verpflichtung zur Aufzeichnung der Abrufbegründung berücksichtigt.

9.3 Einführung von Telearbeit in der Thüringer Steuerverwaltung

Nachdem im Kreise der DSB des Bundes und der Länder bekannt wurde, dass in einigen Bundesländern Telearbeit in der Steuerverwaltung praktiziert wird, habe ich das TFM um Auskunft zu entsprechenden Vorhaben in Thüringen und um datenschutzrechtliche Beteiligung gebeten.
Nach Mitteilung des TFM war beabsichtigt, für den Außendienst in den Bereichen Betriebsprüfung, Lohn- und Umsatzsteueraußenprüfung und nachfolgend ggf. für Teilbereiche des Innendienstes probeweise Telearbeit einzuführen.
Daraufhin habe ich mitgeteilt, welche Anforderungen an die Errichtung von Telearbeitsplätzen aus datenschutzrechtlicher Sicht zu stellen sind. Insbesondere sollten die gemäß § 9 ThürDSG zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage eines IT-Sicherheitskonzeptes ermittelt werden und in das Konzept des Vorhabens einfließen. Zu den Anforderungen an die Einrichtung von Telearbeitsplätzen sowie die Umsetzung eines solchen

Pilotvorhabens im TIM hatte ich in der Vergangenheit mehrfach berichtet (3. TB, 15.13; 5. TB, 15.6).
Derzeit wird nach Mitteilung des TFM im Hinblick auf die bevorstehende Behördenstrukturreform von der Pilotierung des Vorhabens abgesehen.

9.4 Datenschutzprobleme mit der elektronischen Steuererklärung (ELSTER)

Seit April 2005 sind Unternehmen gesetzlich verpflichtet, die Lohnsteueranmeldungen und Umsatzsteuervoranmeldungen elektronisch an die Finanzämter zu übermitteln. Wie Meldungen aus der Presse und einer Mitteilung des BfD zu entnehmen war, wird bei der Übermittlung dieser Steuerdaten an die Finanzämter mittels der ELSTER-Software der Steuerverwaltung keine Authentifizierung des Absenders vorgenommen. Da hierdurch nicht auszuschließen ist, dass Unberechtigte Steuerdaten manipulieren können, habe ich das TFM auf die Sicherheitslücken hingewiesen. Nach übereinstimmender Auffassung der Finanzverwaltung bestehe kein Handlungsbedarf, da gegenüber dem papiergebundenen Verfahren keine erhöhten Risiken bestehen würden, Plausibilitätskontrollen durchgeführt würden und ab Anfang 2006 ein Authentifizierungsverfahren eingeführt werde.
Nach wie vor unerledigt ist der anlässlich einer datenschutzrechtlichen Kontrolle geforderte Abschluss einer Verwaltungsvereinbarung zur Nutzung der für das Verfahren ELSTER erforderlichen Clearingstellen durch die Bundesländer (5. TB, 9.6). Derzeit liegt lediglich ein Entwurf eines Abkommens zur Regelung des zentralen und einheitlichen Betriebs der Kommunikationsplattform für das Verfahren ELSTER vor. Da es sich beim Betreiben der Clearingstellen um eine Datenverarbeitung im Auftrag handelt, habe ich das TFM auf die gemäß § 8 Abs. 2 ThürDSG erforderlichen Regelungen zu Unterauftragsverhältnissen und die nach § 9 ThürDSG notwendigen technisch-organisatorischen Maßnahmen hingewiesen und gefordert, entsprechende Bestimmungen in die Verhandlungen über das Abkommen einzubringen. Diese Verpflichtungen, die das Kontrollrecht des Auftraggebers gewährleisten sollen und die auch in §§ 9 und 11 BDSG sowie in den Datenschutzgesetzen der anderen Bundesländer zu finden sind, sind unabdingbarer Bestandteil eines Vertrages zur Datenverarbeitung im Auftrag.

9.5 Auftragsdatenverarbeitung beim Druck und Versand von Lohnsteuerkarten

Eine datenschutzrechtliche Kontrolle hatte den im Auftrag einer Stadtverwaltung durch eine Firma außerhalb Thüringens durchgeführten Druck und Versand von Lohnsteuerkarten zum Gegenstand. Im Verfahren werden seitens der Stadtverwaltung aus der Meldedatei die für die Ausstellung von Lohnsteuerkarten erforderlichen Daten extrahiert, mittels PGP verschlüsselt und online zum Auftragnehmer geleitet. Nach dem Druck der Lohnsteuerkarten im Rechenzentrum des Unternehmens werden diese durch die Deutsche Post AG mittels „Infopost“ an die Adressaten versandt, die übermittelten Daten gelöscht und etwaige Fehldrucke vernichtet.
Es wurde Einvernehmen darüber erzielt, dass die Auftragserteilung zum Druck und Versand der Lohnsteuerkarten künftig unter Bezugnahme auf den bestehenden Rahmenvertrag zur Auftragsdatenverarbeitung zwischen den Vertragspartnern zu ergänzen ist. Darüber hinaus waren Festlegungen zur Löschung der personenbezogenen Daten und zur Vernichtung von Fehldrucken zu treffen, da hierzu keine schriftlichen Regelungen ersichtlich waren. Ebenso wurde gefordert, das zur verschlüsselten Online-Datenübermittlung angewandte Verfahren zu bezeichnen und ein Verfahrensverzeichnis nach § 10 ThürDSG zu erstellen. Zur Versandart „Infopost“, bei der übergebene Postsendungen durch einen Mitarbeiter der Post stichprobenweise zur Prüfung der vereinbarten äußeren Beschaffenheit geöffnet werden, bestehen, wie bereits im 4. TB (9.6) dargelegt, keine Bedenken, wenn dies in Anwesenheit eines Mitarbeiters des Kunden geschieht (Vieraugenprinzip) und in den Auftragsunterlagen fixiert wird. Weiterhin wurde die Stadtverwaltung darauf hingewiesen, die für den Auftragnehmer im anderen Bundesland

zuständige Kontrollstelle gemäß § 8 Abs. 6 ThürDSG über die Auftragsdatenverarbeitung zu unterrichten (5. TB, Anlage 23). Die Forderungen und Hinweise wurden erfüllt.

9.6 Fehlerhafte Zustellung von Steuerunterlagen

Ein Bürger beschwerte sich gemäß § 11 ThürDSG darüber, dass ein Jahressteuerbescheid in einer offenen Zeitungsröhre anstatt im daneben befindlichen Briefkasten zugestellt worden sei. Das mit Hinweis auf eine Gefährdung des Steuergeheimnisses gemäß § 30 Abgabenordnung um Stellungnahme ersuchte zuständige Finanzamt bestätigte das Vorkommnis. Hierbei habe ein Zusteller des beauftragten Postunternehmens entgegen der dienstlichen Weisung gehandelt und sei dafür abgemahnt worden. Nach Auskunft des Unternehmens werden dessen Mitarbeiter regelmäßig auf die ordnungsgemäße Zustellung und die Einhaltung des Datenschutzes hingewiesen.

9.7 Verfolgung von Postsendungen

Von der OFD Erfurt wurde ich gemäß § 40 Abs. 7 i. V. m. § 2 Abs. 1 ThürDSG um datenschutzrechtliche Beratung gebeten. Zu beurteilen war das Verfahren eines von einem Thüringer Finanzamt beauftragten Unternehmens zur Verfolgung von Postzustellungsurkunden (PZU) des Amtes.
Bei diesem Verfahren wird die auf der PZU eingetragene Adresse des Empfängers und dessen Steuernummer gescannt und elektronisch gespeichert. Gleichfalls gespeichert werden das Datum und die laufende Nummer der PZU. Daneben wird die laufende Nummer auch als Strichcode verschlüsselt auf ein Etikett gedruckt, das auf die PZU geklebt wird. Danach werden die PZU auf die Kurierfahrer verteilt und an die Adressaten zugestellt. Nach dem Rücklauf der PZU werden die Strichcodelabel der PZU gescannt und mit den gespeicherten Daten abgeglichen. Sind PZU nach 5 Tagen noch nicht zurück, werden die hierzu gespeicherten Daten durch die Software angezeigt, sodass nach dem Verbleib der PZU geforscht werden kann. Die Löschung der gespeicherten Daten erfolgt vierteljährlich.
Das beschriebene Verfahren habe ich in datenschutzrechtlicher Hinsicht als unbedenklich angesehen. Die Löschung der zum Zwecke der Sendeverfolgung gespeicherten Adressen und Steuernummern der Empfänger nach Ablauf eines Vierteljahres war in datenschutzrechtlicher Hinsicht nicht zu kritisieren.

9.8 Vollstreckung von Steuerschulden durch die Parkkralle

Laut Pressemeldungen, hat das TFM seit Mai 2005 begonnen, die Parkkralle zur Vollstreckung von Steuerschulden bei einem Pilotversuch in zwei Finanzämtern einzusetzen. Auch wurde darüber berichtet, dass verschiedene Thüringer Kommunen dieses Mittel nutzen. Die Parkkralle war bereits vor Jahren Gegenstand meiner datenschutzrechtlichen Bewertung (2. TB, 14.10). Die Presseveröffentlichungen waren Anlass, bei Stellen, die dieses Pfändungsverfahren nutzen, sich über die konkrete Vorgehensweise und die hierzu erlassenen Anweisungen berichten zu lassen. In zwei Kommunen wurde kontrolliert, wie in konkreten Fällen verfahren wurde.
Allen Vollstreckungsmaßnahmen ist gemeinsam, dass die Pfändung durch die Festsetzung eines Fahrzeugs mittels der Parkkralle als letztes Mittel erfolgt. Wird auf einen Bußgeldbescheid nicht reagiert, so wird zunächst unter Fristsetzung gemahnt. Nachdem die Frist erfolglos verstrichen ist, wird eine Vollstreckung vorbereitet. Dabei wird als erstes geprüft, ob eine Innenvollstreckung, etwa durch eine Konten- oder Gehaltspfändung, möglich ist. Anschließend wird der Schuldner in seiner Wohnung aufgesucht und dort nach Barmitteln oder Wertgegenständen gesucht, die sich für eine Pfändung eignen. Führt auch dies nicht zu einem Erfolg, wird bei der Zulassungsstelle angefragt, ob der Schuldner als Halter eines Fahrzeugs gespeichert ist. Ist dies

der Fall, geht die Vollstreckungsbehörde zunächst von der Eigentumsvermutung des Schuldners am Fahrzeug aus. Danach wird der Standort des Fahrzeugs ermittelt, die Parkkralle angebracht und der Schuldner schriftlich über die erfolgte Pfändung informiert.
Eine mir vom TFM übersandte Dienstanweisung legt die Voraussetzungen des Einsatzes, das Vorgehen beim Anbringen der Parkkralle und die Informations- und Dokumentationspflichten fest. Danach ist das Fahrzeug vor Anbringen der Parkkralle zu Beweiszwecken digital zu fotografieren. Die so erstellten Fotos sind unter dem Aktenzeichen des Vollstreckungsschuldners (bzw. Dritteigentümers) „ … zu speichern und nach Ablauf einer angemessenen Zeit zu löschen“. Nach Mitteilung des TFM, das ich hierzu befragt hatte, erfolgt die Löschung je nach Einzelfall, spätestens jedoch nach Ablauf der Verjährungsfrist für die Geltendmachung etwaiger Schadensersatzansprüche. Desweiteren haben die Vollstreckungsbeamten des Finanzamtes - unter Angabe des Fahrzeughalters, des Standorts des Fahrzeugs und anderer Daten - unverzüglich dem Ordnungsamt und dem örtlich zuständigen Polizeirevier anzuzeigen, dass ein Fahrzeug im öffentlichen Verkehrsraum blockiert wurde. Nach Auffassung des TIM, die von mir unterstützt wird, ist eine derartige Datenübermittlung entbehrlich, wenn das gepfändete Fahrzeug an beiden Seitenscheiben mit Warnhinweisen versehen ist und die verkehrsrechtlichen Erfordernisse eingehalten wurden. Eine abschließende Stellungnahme des TFM hierzu steht noch aus.
Nach Mitteilung des TFM wurde die Parkkralle innerhalb von anderthalb Monaten fünf mal wegen Rückständen bei der Umsatz-, Lohn- sowie der Kfz-Steuer eingesetzt. In vier Fällen wurde die Parkkralle am darauf folgenden Tag wieder entfernt, da die Schulden beglichen worden waren. In einem Fall wurden von der das Fahrzeug finanzierenden Bank eigene Rechte geltend gemacht. Da der Wert des Fahrzeugs den noch offenen Kreditbetrag übersteigt, beabsichtigte das Finanzamt, den Pkw bei der Bank auszulösen und zu verwerten. Hierzu wurde das Fahrzeug dem Schuldner weggenommen.
Aus datenschutzrechtlicher Sicht stellt das Verfahren einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar. Die Blockierung eines Rades am Fahrzeug und das an die Seitenscheibe geklebte Pfandsiegel zeigen die erfolgte Pfändung für jeden Passanten an. Wer das Auto kennt, kann die Pfändung personenbezogen zuordnen. Eine solche Maßnahme ist jedoch dann zulässig, wenn sie auf einer geeigneten gesetzlichen Grundlage beruht (§ 268 Abs. 2 AO i. V. m. § 38 ThürVwZVG) und verhältnismäßig ist. Der Grundsatz der Verhältnismäßigkeit verbietet eine Überpfändung, bei der der Wert des Fahrzeugs den der Forderung erheblich übersteigt. Zugleich darf ein solches bloßstellendes Mittel nur angewandt werden, wenn keine anderen Pfändungsmöglichkeiten genutzt werden können. In den mir bislang bekannt gewordenen Fällen ist der Einsatz der Parkkralle als gerechtfertigt anzusehen.

9.9 Weitergabe von personenbezogenen Daten durch ein Landratsamt zum Test von Software

Von einem Landratsamt wurde ich mit der Bitte um datenschutzrechtliche Bewertung darüber unterrichtet, dass personenbezogene Daten des Landratsamtes aus den Bereichen Mahnung und Vollsteckung zum Test von Software an ein Unternehmen außerhalb Thüringens übermittelt wurden.
Nach Prüfung der Angelegenheit teilte ich mit, dass auf die Übergabe von personenbezogenen Daten des Landratsamtes an die Softwarefirma zu Testzwecken § 8 ThürDSG Anwendung findet. Ein hierfür schriftlich erteilter Auftrag entsprach hinsichtlich des Verwendungszwecks der übergebenen Daten, der Verpflichtung zur Löschung nach Auftragserfüllung sowie der Unterwerfung unter das Datenschutzgesetz den Vorgaben nach § 8 Abs. 2 ThürDSG. Nicht enthalten war hingegen die Verpflichtung des Auftragnehmers, vom Auftraggeber veranlasste Kontrollen jederzeit zu ermöglichen. Mit Hinweis auf den Mustervertrag des TLfD zur Auftragsdatenver-

arbeitung (5. TB, Anlage 23) habe ich die Überarbeitung der Auftragserteilung gefordert. Dass künftig in diesem Sinne verfahren werden soll, wurde vom Landratsamt bestätigt.
Nach § 8 Abs. 6 ThürDSG hat der Auftraggeber die für die Einhaltung des Datenschutzes beim Auftragnehmer zuständige Kontrollestelle über die Beauftragung zu unterrichten, falls die Bestimmungen des ThürDSG auf den Auftragnehmer nicht anwendbar sind. Da der Auftragnehmer außerhalb Thüringens gelegen ist und die zuständige Kontrollstelle noch nicht informiert worden war, habe ich das Landratsamt um Abhilfe gebeten. Der Forderung wurde nachgekommen.

9.10 Gewährung des Auskunftsrechts bei der Bearbeitung vermögensrechtlicher Ansprüche

Von einem Antragsteller in einem vermögensrechtlichen Verfahren wurde ich um Prüfung gebeten, ob das Auskunftsrecht im Zusammenhang mit entscheidungserheblichem Beweismaterial hinreichend gewährt wurde. Insbesondere vermutete der Petent, dass sich im Thüringer Landesamt zur Regelung offener Vermögensfragen (ThLARoV) und dem Staatlichen Amt zur Regelung offener Vermögensfragen (StARoV) Unterlagen zu einem Strafverfahren und zur Aufhebung einer Enteignungsmaßnahme aus dem Jahr 1948 befinden.
In der hierzu durchgeführten datenschutzrechtlichen Kontrolle wurden die im ThLARoV und StARoV zu den vom Antragsteller beanspruchten Vermögenswerten geführten Verwaltungs- und Prozessakten überprüft. Die Kontrolle ergab, dass die vom Petenten genannten Unterlagen nicht im Aktenbestand enthalten waren. Es war nicht feststellbar, dass den Rechten des Betroffenen auf Auskunft nicht ausreichend nachgekommen wurde, da sich dieses Recht immer nur auf solche Daten erstrecken kann, die von der Stelle gespeichert sind.

10. Justiz

10.1 Akustische Wohnraumüberwachung - Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004

Mit dem Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (Akustische Wohnraumüberwachung) vom 24. Juni 2005 (BGBl. I S. 1841), das am 1. Juli 2005 in Kraft getreten ist, wurde auf die Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff vom 3. März 2004 (1 BvR 2378/98 und 1 BvR 1084/99) gesetzgeberisch reagiert. In seiner Entscheidung hatte das Bundesverfassungsgericht die gesetzlichen Grundlagen in großen Teilen für verfassungswidrig erklärt. Richtungweisend wurde festgestellt, dass die Vorschriften der Strafprozessordnung (StPO) zur Durchführung der akustischen Wohnraumüberwachung zu Zwecken der Strafverfolgung den verfassungsrechtlichen Anforderungen im Hinblick auf den Schutz der Menschenwürde (Artikel 1 Abs. 1 GG), den vom Rechtsstaatsprinzip umfassten Grundsatz der Verhältnismäßigkeit, der Gewährung effektiven Rechtsschutzes (Artikel 19 Abs. 4 GG) und dem Anspruch auf rechtliches Gehör (Artikel 103 Abs. 1 GG) nicht in vollem Umfang genüge. Aus der durch Artikel 1 Abs. 1 GG geschützten Menschenwürde ist danach ein unantastbarer Kernbereich privater Lebensgestaltung herzuleiten, der jedem staatlichen Zugriff entzogen ist. Praktisch bedeutet dies, dass eine akustische Wohnraumüberwachung abgebrochen und Aufzeichnungen gelöscht werden müssen, sobald sie die Erhebung von Informationen aus dem absolut geschützten Kernbereich privater Lebensgestaltung betrifft. Die vertrauliche Kommunikation, wozu im Regelfall die Privatwohnung dient, benötigt einen Schutz. Zwar ist nicht ein absoluter Schutz der Räume der Privatwohnung verlangt, wohl aber der Schutz des Verhaltens in diesen Räumen, soweit es sich um die individuelle Entfaltung im Kernbereich privater Lebensgestaltung handelt. Dieser Schutz darf auch nicht durch Abwägung mit Strafverfolgungsinteressen im Hinblick auf den Grundsatz der Verhältnismä-

ßigkeit relativiert werden. Artikel 13 Abs. 3 Satz 1 GG fordert, dass die aufgezählten Katalogstraftaten, die eine akustische Wohnraumüberwachung ermöglichen, als solche und nicht nur im Einzelfall besonders schwer sind. Ein Anhaltspunkt für die Schwere sind die Folgen der Tat für betroffene Rechtsgüter. Dies sieht das Bundesverfassungsgericht beim Straftatenkatalog des § 100 c Abs. 1 Nr. 3 StPO bei Vergehenstatbeständen, deren Strafrahmen keinen überdurchschnittlichen Unrechtsgehalt zum Ausdruck bringen und die ausweislich ihrer Strafandrohung nur dem mittleren Kriminalitätsbereich zugeordnet werden können, nicht für gegeben an. § 100 c Abs. 3 StPO besagt zwar, dass Maßnahmen auch durchgeführt werden dürfen, wenn Dritte unvermeidbar betroffen sind, im Umkehrschluss folgt daraus jedoch, dass die akustische Wohnraumüberwachung unzulässig ist, wenn diese zu einer vermeidbaren Beeinträchtigung führt.
Wie das Bundesverfassungsgericht weiterhin festgestellt hat, gebietet die Rechtsschutzgarantie des Artikel 19 Abs. 4 GG die Benachrichtigung der Betroffenen. Diese Benachrichtigungspflicht besteht auch gegenüber solchen Personen, die sich als Gast oder sonst zufällig in einer überwachten Wohnung aufgehalten haben und die in ihrem durch Artikel 3 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG geschützten Recht am gesprochenen Wort und in ihrem informationellen Selbstbestimmungsrecht betroffen sind. Jedoch kann durch die Nachforschung zur Feststellung der Identität sonstiger Beteiligter auch ein Grundrechtseingriff entstehen. Zielpersonen einer akustischen Wohnraumüberwachung sind ausschließlich Beschuldigte. Dritte im Sinne des § 100 c Abs. 3 StPO sind alle anderen Betroffenen, ungeachtet dessen, ob diese sich in der Wohnung des Beschuldigten oder in der überwachten Wohnung eines Dritten aufhalten. Die Anforderungen, die an die Unvermeidbarkeit der Betroffenheit Dritter zu stellen sind, hängen damit maßgeblich von den tatsächlichen Gegebenheiten und Möglichkeiten des Ausschlusses Dritter im Einzelfall ab.
Das Bundesverfassungsgericht hatte den Bundesgesetzgeber für verpflichtet angesehen, einen verfassungsmäßigen Rechtszustand bis spätestens zum 30. Juni 2005 herzustellen.
Die DSB des Bundes und der Länder haben in ihrer Entschließung in der 67. Konferenz vom 25./26. März 2004 (Anlage 2) zur Entscheidung des Bundesverfassungsgerichts Stellung genommen. Sie haben dabei die Auffassung vertreten, dass die Ausführungen des Bundesverfassungsgerichts nicht nur für die Vorschriften für die akustische Wohnraumüberwachung in der StPO von Bedeutung sind, sondern auch andere Eingriffsbefugnisse, wie die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung, auf den Prüfstand gestellt werden müssen.
Das Bundesjustizministerium hat am 1. November 2004 die Ergebnisse eines Gutachtens des Max-Planck-Instituts für ausländisches und internationales Strafrecht zur Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung veröffentlicht. Das Gutachten kommt unter anderem zu dem Ergebnis, dass in der Praxis zurückhaltend mit diesem Instrument umgegangen wird. Allerdings wurde auch Regelungsbedarf aufgezeigt.

10.2 DNA-Analyse

Auch in diesem Berichtszeitraum setzte sich die Diskussion zur Absenkung der rechtlichen Schranken für die DNA-Analyse nach § 81 g StPO fort. Mit einem Gesetzesantrag einiger Länder „Entwurf eines Gesetzes zur Neuregelung der DNA-Analyse zu Zwecken des Strafverfahrens“ (Bundesratsdrucksache 99/05 vom 3. Februar 2005) wurde gefordert, den genetischen Fingerabdruck zur Identitätsfeststellung im künftigen Strafverfahren mit dem gewöhnlichen Fingerabdruck gleichzusetzen. Die Konferenz der DSB des Bundes und der Länder hat zu dieser Bundesratsinitiative eine Entschließung gefasst (Anlage 11), in der sie die Gleichsetzung der DNA-Analyse mit dem gewöhnlichen Fingerabdruck ablehnt und darauf hingewiesen hat, dass mit der DNA-Analyse weitergehende Erkenntnisse über den Menschen gewonnen werden können, als dies mit dem gewöhnlichen Fingerabdruck möglich ist. Sie hat die Beachtung der

Rechtsprechung des Bundesverfassungsgerichts gefordert, mit der die Verfassungsmäßigkeit der DNA-Analyse wegen ihres Eingriffscharakters mit der Begründung, dass sie eine Straftat von erheblicher Bedeutung, die Prognose, dass künftig gegen den Beschuldigten Strafverfahren von dieser Bedeutung zu führen und die richterliche Kontrolle dieser Umstände zu gewährleisten sind, voraussetzt, bejaht wird. Darüber hinaus müssen diese Voraussetzungen auch im jeweiligen Einzelfall vorliegen. Die besondere Qualität des Grundrechtseingriffs durch eine DNA-Analyse muss nach Auffassung der DSB des Bundes und der Länder bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden. Dies schließe eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus. Dabei wird auch seitens der DSB die Bedeutung der DNA-Analyse als erfolgreiches Ermittlungsinstrument nicht verkannt.
Die Gesetzesinitiative des Bundesrats wurde nicht weiter verfolgt, dafür lag bereits im Mai 2005 ein Referentenentwurf für ein Gesetz zur Novellierung der forensischen DNA-Analyse vor. Mit dem am 1. November 2005 in Kraft getretenen Gesetz zur Novellierung der forensischen DNA-Analyse vom 12. August 2005 (BGBl. I S. 2360) ist unter Ersetzung des DNA-Identitätsfeststellungsgesetzes die DNA-Analyse nunmehr auch mit der Einwilligung des Betroffenen möglich, was eine entsprechende differenzierte Belehrung – wie von den DSB immer wieder betont - voraussetzt. Der Straftatenkatalog in § 81 g StPO ist durch den Begriff „Straftaten von erheblicher Bedeutung“ und Straftatenkategorien ersetzt worden. Es reicht nunmehr auch die wiederholte Begehung anderer ggf. auch leichterer Straftaten für die Durchführung von DNA-Analysen aus, was allerdings nicht bedeuten darf, dass der mehrfache „Hühnerdiebstahl“ jetzt ohne weiteres dazu zählt. Auch die Schwelle zur Speicherung in der DNA-Datei wurde gesenkt.
Darüber hinaus wurde ein neuer § 81 h eingefügt, der das sog. DNA-Massenscreening regelt. Wenn bestimmte Tatsachen den Verdacht begründen, dass ein Verbrechen gegen das Leben, die körperliche Unversehrtheit, die persönliche Freiheit oder die sexuelle Selbstbestimmung begangen worden ist, können Personen, die bestimmte, auf den Täter vermutlich zutreffenden Prüfungsmerkmale erfüllen, mit ihrer schriftlichen Einwilligung einer DNA-Analyse unterzogen werden. Voraussetzung für eine solche DNA-Reihenuntersuchung ist allerdings ein grundsätzlicher richterlicher Beschluss. In der Vergangenheit wurden auch ohne eine solche konkrete Rechtsgrundlage DNA-Massenscreenings durchgeführt, die aber auf unterschiedliche Rechtsgrundlagen gestützt waren. Dies hatte die DSB des Bundes und der Länder auf ihrer 69. Konferenz im März 2005 veranlasst, in einem Brief des Vorsitzenden an die Bundesjustizministerin über datenschutzrechtlich relevante Gesichtspunkte in diesem Zusammenhang zu informieren. Kernpunkte dabei waren, dass von einer DNA-Massenscreeningmaßnahme regelmäßig ganz überwiegend Unverdächtige betroffen sind, so dass die Anzahl der unterzogenen Personen einzugrenzen ist, von diesem Instrument jedoch nur bei ganz erheblichen Straftaten und nur dann Gebrauch gemacht werden darf, wenn andere Möglichkeiten zur Aufklärung der konkreten Tat nicht mehr bestehen. Sie darf nur auf der Grundlage eines richterlichen Beschlusses mit Einwilligung der Betroffenen erfolgen. Die Nichteinwilligung allein darf nicht einen Tatverdacht begründen. Zudem müssen angemessene Löschungsregelungen festgelegt werden. Es ist zu begrüßen, dass eine eindeutige gesetzliche Grundlage geschaffen wurde.

10.3 Telekommunikationsüberwachung

Nach vorliegenden Statistiken war für das Jahr 2004 zu bemerken, dass die Telefonüberwachungen nach §§ 100 a, 100 b StPO bundesweit weiter angestiegen sind. Für Thüringen bewegt sich die Anzahl in der Größenordnung der Vorjahre.
Im Berichtszeitraum war Gegenstand datenschutzrechtlicher Kontrollen der Umgang mit personenbezogenen Daten im Zusammenhang mit der Durchführung von Telekommunikations-

überwachungsmaßnahmen nach § 100 a StPO und insbesondere die Benachrichtigungen Betroffener nach § 101 StPO bei den Staatsanwaltschaften des Landes. Der Benachrichtigung Betroffener kommt erhebliche Bedeutung zu, da erst die Benachrichtigung über eine durchgeführte Maßnahme die Betroffenen in die Lage versetzt, ihre Rechte wahrzunehmen. Als Betroffene werden von den Strafverfolgungsbehörden zunächst die Beschuldigten, ggf. aber auch der Nachrichtenmittler oder der Inhaber der vom Beschuldigten benutzten Telekommunikationsanschlüsse angesehen. Darüber hinaus ist die Praxis angehalten, weitere Personen zumindest dann zu benachrichtigen, wenn ihre Identität feststeht und aufgrund weiterer Umstände des Einzelfalls von einem erheblichen Eingriff in die Grundrechte des Dritten auszugehen ist. Eine umfangreiche Ermittlung der Identität eines Dritten wäre demgegenüber mit einem weitergehenden Eingriff in das informationelle Selbstbestimmungsrecht verbunden, sodass davon abgesehen wird.
Bei den durchgeführten Kontrollen in den Staatsanwaltschaften war anhand der Unterlagen festzustellen, dass soweit Beschuldigte als Anschlussinhaber betroffen waren, diese in der Mehrzahl in der verantwortlichen Vernehmung bzw. durch Akteneinsicht der Verteidiger teilweise auch in der Hauptverhandlung über die stattgefundenen Überwachungsmaßnahmen informiert wurden. Unterbliebene Benachrichtigungen von Beschuldigungen waren mit der Gefährdung weiterer Ermittlungen begründet. Soweit andere Anschlussinhaber betroffen waren, wurden diese teilweise nicht oder erst geraume Zeit später benachrichtigt, wobei in einigen Fällen die Unterlagen zur TKÜ gemäß § 100 b Abs. 6 StPO bereits vernichtet waren. Die Form der Benachrichtigungen unterschied sich in den einzelnen Vorgängen, teilweise waren lediglich staatsanwaltschaftliche Verfügungen vorhanden, teilweise waren Abdrucke der gefertigten Benachrichtigungen abgeheftet.
In manchen Vorgängen konnte der Verbleib der durch die durchgeführten Maßnahmen entstandenen Unterlagen bzw. der Zeitpunkt der Vernichtung der Unterlagen nicht nachvollzogen werden. Vernichtungsniederschriften waren nicht durchgängig in den Vorgängen abgeheftet. In einem Fall waren die Unterlagen zur TKÜ noch vorhanden, weil sie möglicherweise im Rahmen der Vollstreckung einer Bewährungsstrafe relevant sein könnten.
Daraus ergaben sich die datenschutzrechtlichen Forderungen, in jedem Vorgang zu prüfen, ob der Beschuldigte und der Anschlussinhaber identisch sind, inwieweit im Rahmen der Einzelfallprüfung von einem erheblichen Eingriff in die Grundrechte des Anschlussinhabers auszugehen ist oder ob sonstige Gründe einer Benachrichtigung entgegenstehen. Dies sollte zur Nachvollziehbarkeit insbesondere beim Absehen von einer Benachrichtigung dokumentiert werden.
Bei der Form der Benachrichtigung sollte beachtet werden, dass Anschlussinhaber, gegen die kein Tatverdacht besteht, durch die Benachrichtigung nicht mehr Informationen erhalten, als für die Wahrnehmung ihrer Rechte erforderlich sind. Dies kann sich unter Umständen auch auf den Tatvorwurf gegen den Beschuldigten beziehen, der dem Beteiligten nicht zur Kenntnis gelangen müsste.
Über die nach § 100 b Abs. 6 StPO erforderliche Vernichtung der durch die Maßnahme erlangten Unterlagen, die unverzüglich unter Aufsicht der Staatsanwaltschaft erfolgen muss, wenn sie zur Strafverfolgung nicht mehr erforderlich sind, ist eine Niederschrift anzufertigen und zwecks Nachvollziehbarkeit in die Ermittlungsakte abzuheften. Die Vollstreckung einer Bewährungsstrafe rechtfertigt im Übrigen nicht die weitere Aufbewahrung der Unterlagen.

Die im Einzelnen vorgetragenen Hinweise wurden von den jeweils zuständigen Staatsanwaltschaften umgesetzt. So wurde z. B. auch eine Checkliste als Merkblatt für TKÜ-Maßnahmen entwickelt, durch das sichergestellt werden kann, dass die Benachrichtigungen der Beteiligten zeitnah erfolgen und hinreichend dokumentiert werden.

10.4 Insolvenzveröffentlichungen im Internet

Wie bereits im 4. TB (10.15) berichtet, wurden die Voraussetzungen der öffentlichen Bekanntmachungen im Insolvenzverfahren im Internet geschaffen. Durch die Verwaltungsvorschrift des TIM vom 29. Juni 2004 (JMBl. 2004, S. 48), die mit Wirkung vom 1. August 2004 in Kraft getreten ist, wurde bestimmt, dass die nach der Insolvenzordnung vorgeschriebenen öffentlichen Bekanntmachungen im Internet unter der Adresse www.insolvenzbekanntmachungen.de veröffentlicht werden. Die Löschungsfrist nach § 3 Abs. 1 der Verordnung zur öffentlichen Bekanntmachung in Insolvenzverfahren beträgt 1 Monat.
Wie bereits im 4. TB angesprochen, besteht immer noch das Problem, dass kein wirksamer Kopierschutz für die in dieser Datei gespeicherten Daten besteht, und nach dem Stand der Technik auch nicht möglich erscheint. Insoweit besteht daher die Gefahr, dass Dritte Daten aus Bekanntmachungen im Internet nach § 9 InsO übernehmen und über die geltenden Löschfristen hinaus weiterhin im Internet verbreiten.
Die DSB des Bundes und der Länder beschäftigen sich daher auch weiterhin mit den Möglichkeiten, um gegebenenfalls entsprechende Empfehlungen und Hinweise insbesondere für einen verbesserten Kopierschutz zu geben. Sobald sich verbesserte Möglichkeiten zum Kopierschutz ergeben, sind diese selbstverständlich im Rahmen der Veröffentlichung von Insolvenzmitteilungen im Internet umzusetzen.

10.5 Elektronischer Rechtsverkehr in der Justiz

Bundesweit werden unter dem Begriff Elektronischer Rechtsverkehr im Bereich der Justiz verschiedene Projekte im Rahmen der modernen Informations- und Kommunikationstechnik erprobt bzw. eingeführt. Dabei soll in den gerichtlichen Verfahren die Aktenbearbeitung in Papierform und die Kommunikation per Briefpost durch elektronische Verfahren ersetzt oder begleitet werden. Bereits durch das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001 und das Zustellungsreformgesetz (ZustRG) vom 25. Juni 2001 sowie das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) vom 22. März 2005 (BGBl I S. 873), das am 1. April 2005 in Kraft getreten ist, sind notwendige Rechtsgrundlagen für eine Vielzahl von Verfahrensarten in verschiedenen Gerichtsbarkeiten für eine breite Einführung des Elektronischen Rechtsverkehrs geschaffen.
Vorgesehen ist in Thüringen u. a. die Einführung des elektronischen Handelsregisters auf der Grundlage des Gesetzes über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG).
Im Anschluss an die Ausführungen im 4. TB (10.3) und 5. TB (10.4) ist zum elektronischen Grundbuch, das als Teil des elektronischen Rechtsverkehrs zu bezeichnen ist, zu berichten, dass die Umstellung der Grundbücher auf die elektronische Form in Thüringen abgeschlossen ist. Für Anfang 2006 ist die Einführung eines Web-Abrufverfahrens für das elektronische Grundbuch in Thüringen im Pilotbetrieb vorgesehen. Mit dieser Web-Lösung des Online-Abrufverfahrens werden differenziertere Benutzerkennungen ermöglicht, was bspw. eine Zuordnung von getätigten Abrufen innerhalb einer öffentlichen Stelle ermöglicht.
Da auch die Einführung des Web-Abrufverfahrens ein Sicherheitskonzept erfordert, auf dessen Grundlage die technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes festzulegen sind, hat das TJM, ein Zugangs- und Sicherheitskonzept, das die konkrete IT-Technik unter Berücksichtigung der landesspezifischen Gegebenheiten beschreibt, sowie Festlegungen zur Authentifizierung durch Verwendung von elektronischen Zertifikaten vorgelegt. Die Dokumente sollen allerdings erforderlichenfalls im Rahmen des Pilotverfahren fort-

geschrieben werden. Die Erstellung eines umfassenden verbindlichen neuen Sicherheitskonzepts soll sich anschließen.
Der TLfD wird das Verfahren weiterhin auch im Rahmen der bundesweiten Diskussion beobachten und begleiten.
Das Recht betroffener Grundstückseigentümer auf Auskunft, wer wann im automatisierten Verfahren auf seine Grundstücksdaten Zugriff genommen hat, konnte aufgrund der Prüfung im Rahmen einer vorliegenden Beschwerde praktisch nachvollzogen werden. Ein Beschwerdeführer hatte sich an ein Grundbuchamt gewandt und Auskunft zu erteilten Auskünften bzw. Grundbucheinsichten und Auszügen begehrt. Das Grundbuchamt selbst sah sich zunächst nicht in der Lage, diese Auskunft zu erteilen. Soweit das Grundbuch vor Umstellung auf das elektronische Verfahren in Papierform geführt wurde, bestand die Möglichkeit, dass im Grundbuchamt selbst nachvollzogen werden konnte, wem auf Antrag ein Auszug aus dem Grundbuch zu einem bestimmten Grundstück erteilt wurde. Die im Grundbuchamt zu den im elektronischen Auskunftsverfahren gewährten Einsichten geführten Protokolle ließen jedoch nicht erkennen, auf welches Grundbuchblatt zugegriffen wurde. Hierzu musste die zentrale Protokollierung beim Oberlandesgericht ausgewertet werden. Durch die Zusammenführung der Protokolldaten des OLG nach § 83 Abs. 2 Satz 2 Grundbuchverfügung (GBV) mit der Protokollierung im Grundbuchamt ergaben sich zwei Online-Abrufe im automatisierten Verfahren, wobei einmal im Grundbuchamt am Einsichts-PC Einsicht genommen wurde, wogegen nichts einzuwenden war. Auch gegen den weiteren Abruf war nichts einzuwenden, da es sich um eine Stelle handelte, der grundsätzlich ein berechtigtes Interesse für Auskünfte aus dem Grundbuch zusteht.

10.6 Beschwerden über Staatsanwaltschaften

Im Rahmen eines Ermittlungsverfahrens war eine Personalstelle vom zuständigen Ermittlungsbeamten gebeten worden, die Geburtsdaten, Geburtsorte sowie die Wohnanschriften dreier namentlich aufgeführter Personen mitzuteilen. In welcher Strafsache hier ermittelt wird, war aus dem Schreiben nicht zu entnehmen. Aus der Angabe der Zuständigkeit des Ermittlungsbeamten konnte jedoch der Eindruck entstehen, dass es sich um den Vorwurf der Korruption handeln müsste. Dieses Schreiben wurde auch ohne Schwärzungen in die Ermittlungsakte zu einer der aufgeführten Personen abgeheftet.
Das TLKA hat auf die datenschutzrechtlichen Bedenken zu dem grundsätzlich zulässigen Auskunftsersuchen erklärt, dass zukünftig die Festlegung zur Abwicklung des Schriftverkehrs geändert werde und die sachbearbeitende Organisationseinheit nur noch intern erkennbar sei.
Zur Abheftung des Schreibens ohne Schwärzung in die staatsanwaltschaftliche Ermittlungsakte hat die zuständige Staatsanwaltschaft mitgeteilt, dass es nicht erforderlich war, die Namen der in den anderen Ermittlungsverfahren Beschuldigten in den Ermittlungsakten zu dokumentieren. Es wäre somit sachgerecht gewesen, entsprechend einer Anweisung der Thüringer Generalstaatsanwaltschaft aus dem Jahre 2002 Schwärzungen der jeweils beiden anderen Beschuldigten vorzunehmen. Der Leitende Oberstaatsanwalt hat dies zum Anlass genommen, intern nochmals auf die striktere künftige Beachtung datenschutzrechtlicher Belange hinzuweisen.

In einem anderen Ermittlungsverfahren gegen Unbekannt wegen fahrlässiger Tötung zum Nachteil einer Person wandten sich dessen Hinterbliebene an den TLfD, weil sie davon Kenntnis erhalten hatten, dass offenbar in einem Ermittlungsverfahren gegen den Verstorbenen wegen fahrlässiger Körperverletzung durch eine Polizeidienststelle in einem anderen Bundesland Zeugenvernehmungen durchgeführt werden sollten. Darüber hinaus war dem Rechtsvertreter der Hinterbliebenen eine Kostenberechnung für die Kopie eines Gutachtens, das in einem gegen einen Dritten geführten völlig unabhängigen anderen Ermittlungsverfahren gefertigt worden war, zugesandt worden. Die zuständige Staatsanwaltschaft hat auf die versehentlich übersandte Rechnung über Kopierkosten vorgetragen, es habe sich um ein reines Versehen auf-

grund der Überlastung der Geschäftsstelle gehandelt. Es war daher davon auszugehen, dass es sich um einen Einzelfall handelt. Zu dem Vorgang, dass aus dem verstorbenen Opfer ein Täter geworden sein könnte, wurde vorgetragen, dass bei der Fertigung des Anschreibens die korrekterweise erforderlichen Ergänzungen „gegen Unbekannt“ und „zum Nachteil von“ versehentlich nicht aufgenommen worden waren. Auch dies wurde mit der Überlastung der Geschäftsstelle begründet. Aufgrund der Auswertung, die in der Staatsanwaltschaft anhand des vorliegenden Falls stattgefunden hat, sind jedoch aus datenschutzrechtlicher Sicht Maßnahmen getroffen worden, um derartige Fälle zukünftig auszuschließen.

10.7 Mitteilung einer Forderungsklage gegen Rechtsanwalt

Nach XII/2 Abs. 1 Buchstabe a der Anordnung über Mitteilungen in Zivilsachen (MiZi) können gegen Rechtsanwälte gerichtete Forderungsklagen vom Gericht an die zuständige Rechtsanwaltskammer mitgeteilt werden. Dies erfolgte auch im Fall eines Rechtsanwalts in Thüringen, der sich mit der Bitte um Prüfung der Vorgehensweise der Rechtsanwaltskammer gegen ihn an den TLfD wandte. Aufgrund einer gegen ihn eingereichten Klage sollte er der Rechtsanwaltskammer noch vor Ablauf der Erwiderungsfrist verschiedene Fragen beantworten. Er wurde aufgefordert, mitzuteilen, welche Vollstreckungstitel und Maßnahmen gegen ihn ergangen sind, inwieweit titulierte Forderungen getilgt bzw. Ratenzahlungs- und Tilgungsvereinbarungen getroffen sind, welche Einnahmen und Ausgaben er im laufenden sowie im Vorjahr – unter Vorlage der Gewinn- und Verlustrechnung eines Steuerberaters, Steuerbescheide und letzter Steuererklärung - erzielt hat, ob Gehälter des Büropersonals, Versicherungsbeiträge, Miete für die Praxis sowie Bürogeräte voll bezahlt sind und welche Rückstände bestehen. Auch sollte er angeben, welche privaten Einnahmen und Ausgaben er hat, ob Mietrückstände für die Privatwohnung bestehen, ob er sonstige Verbindlichkeiten hat, über Grundbesitz oder sonstiges Vermögen verfügt und ob es Tilgungs- und Ratenzahlungsabkommen mit Gläubigern gibt. Ich habe mich an die Rechtsanwaltskammer gewandt und in Frage gestellt, inwieweit bereits zu diesem frühen Zeitpunkt die Beantwortung der Fragen, die insbesondere auf die Vermögensverhältnisse und das Einkommen abzählen, für die Aufgabenerfüllung der Rechtsanwaltskammer - nämlich die Prüfung, ob möglicherweise ein Vermögensverfall vorliegt und damit berufliche Konsequenzen zu ziehen sind - erforderlich ist.
Bereits zur Änderung der MiZi mit Wirkung vom 1. September 1999 hat der TLfD die Auffassung vertreten, dass nicht jede Forderung, der sich Angehörige rechtsberatender Berufe ausgesetzt sehen, schon den Verdacht begründet, dass Vermögensverfall oder zumindest angespannte finanzielle Lage vorliegen muss.
Die Rechtsanwaltskammer Thüringen hat eingeräumt, dass im vorliegenden Fall zu drastisch reagiert wurde. Es wurde zugesagt, in vergleichbaren möglichen zukünftigen Fällen die Rechtsanwälte um eine einfache Erklärung ohne diese differenzierten Fragen zu bitten. Weitere Angaben werden von den Betroffenen erst und nur dann erhoben, wenn ein berufsrechtliches Verfahren einzuleiten ist. Dies ist auch wichtig im Hinblick darauf, dass die entsprechenden Antworten zur Personalakte der Betroffenen genommen werden, die unter Umständen auf Antrag des Betroffenen erst nach einer Frist von 5 Jahren aus der Personalakte entfernt werden.

10.8 Datenschutz im Strafvollzug

10.8.1 Untersuchungshaftvollzugsgesetz

Schon vor einiger Zeit (3. TB, 10.18) wurde die Auffassung und die Forderung der DSB des Bundes und der Länder für einen angemessenen Datenschutz auch für Untersuchungsgefangene dargelegt. Im Jahr 2004 wurde den Justizverwaltungen ein Referentenentwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft (GVU) zur Stellungnahme zugeleitet.

Der TLfD hat unter Bezugnahme auf die o. g. Entschließung der DSB dazu Stellung bezogen und zu folgenden Punkten Bedenken angemeldet:
Soweit vorgesehen ist, der Anstalt bei Erhebung der öffentlichen Klage eine Mehrfertigung der Anklageschrift zu übermitteln, sollte dies ausdrücklich von der Erforderlichkeit für die Aufgabenerfüllung abhängig gemacht werden.
Bei der Besuchsüberwachung und der Überwachung des Schriftwechsels sollte nach Haftgründen differenziert werden. Normenklar muss geregelt sein, unter welchen Voraussetzungen Post angehalten werden kann. Die Entscheidung über das Anhalten von Schreiben sollte in jedem Fall aufgrund des erheblichen Eingriffs in die Rechte der Betroffenen dem Gericht vorbehalten werden. Das Recht auf ungehinderten unüberwachten telefonischen Kontakt zwischen Verteidiger und Beschuldigtem muss auch in der Untersuchungshaft gewährleistet sein. Bei der Erhebung von personenbezogenen Daten ohne Mitwirkung der Betroffenen bei anderen Stellen sollte abgestuft werden. Im Einzelfall sollte zur Wahrung berechtigter Interessen der betroffenen Gefangenen von einer Mitteilung abgesehen werden. Auch Auskunfts- und Akteneinsichtsrechte der Betroffenen als wesentliche Datenschutzrechte dürfen nicht entwertet werden.
Für Untersuchungsgefangene hält der TLfD eine eigene Regelung zur Löschung von erkennungsdienstlichen Unterlagen für erforderlich. Eine Löschung sollte zumindest in den Fällen, in denen ein Freispruch erfolgt oder die Eröffnung des Hauptverfahrens abgelehnt oder eingestellt wird, weil ein Tatverdacht nicht besteht, auch ohne Antrag der Betroffenen erfolgen.
Das TJM hat die Stellungnahme des TLfD seiner Stellungnahme gegenüber dem BJM in vollem Umfang beigefügt. Zu einer parlamentarischen Beratung des Entwurfs ist es indes nicht gekommen. Es bleibt zu hoffen, dass in der nächsten Legislaturperiode eine gesetzliche Regelung für diesen Bereich beschlossen wird.

10.8.2 Jugendstrafvollzugsgesetz

Allseits anerkannt ist, dass Jugendliche im Strafvollzug nicht in allen Bereichen wie erwachsene Gefangene behandelt werden können. Aus dem datenschutzrechtlichen Blickwinkel sind sie jedoch wie Erwachsene Grundrechtsträger, sodass ihr informationelles Selbstbestimmungsrecht genauso zu beachten ist.
Seitens des BMJ wurde im April 2004 ein Referentenentwurf für eine bereichsspezifische Regelung vorgelegt. Zu diesem hat der TLfD gegenüber dem TJM Stellung genommen. Dabei wurden zu den beabsichtigten Regelungen zum Schriftverkehr mit der Außenwelt – bspw. auch mit dem TLfD, der bei erwachsenen Gefangenen nach § 29 StVollzG nicht der Überwachung unterliegt - im Jugendstrafvollzug aber vom Einverständnis der Personensorgeberechtigten abhängen soll, sowie zur Erhebung und Verwendung personenbezogener Daten unter Einbeziehung Dritter ohne Kenntnis des Betroffenen Bedenken geäußert.
Die Behandlung von jugendlichen Gefangenen, die ihre Strafe bereits verbüßt haben, aber eine in der Jugendstrafanstalt begonnene Ausbildungs- und Behandlungsmaßnahme abschließen wollen, muss sich insbesondere im Hinblick auf die Besuchs-Schriftverkehrskontrolle von derjenigen der weiterhin ihre Strafe Verbüßenden unterscheiden. Aus der Tatsache, dass sich der Betroffene freiwillig in der Anstalt befindet, kann nicht auf eine wirksame Einwilligung in diese Kontrollen geschlossen werden.
Ein überarbeiteter Referentenentwurf mit Stand März 2005 hat die Anmerkungen, die insgesamt von den DSB des Bundes und der Länder geäußert wurden, bislang nicht berücksichtigt.
Es bleibt zu hoffen, dass in der kommenden Legislaturperiode eine entsprechende und datenschutzgerechte gesetzliche Grundlage geschaffen wird.

10.8.3 Kontrolle einer JVA

In einer Justizvollzugsanstalt des Landes (JVA) wurde die Verarbeitung personenbezogener Daten insbesondere auch im Rahmen der Überwachung des Schriftwechsels kontrolliert.
Dabei war festzustellen, dass die den Gefangenen bei Haftantritt ausgehändigten Informationshilfen der Änderung bedürfen. Soweit dort für die Betroffenen als zukünftige Adresse die JVA angegeben war, war dieser Zusatz nicht zwingend, da sich Gefangene lediglich mit der Angabe der Straße und des Ortes anschreiben lassen können. Die Auflistung wichtiger Adressen – insbesondere Stellen, an die Petitionen gerichtet werden können - war bspw. auch durch die Anschrift des TLfD zu ergänzen, da sich auch Gefangene jederzeit ungehindert gemäß § 11 ThürDSG an ihn wenden können.
Der Umgang mit Besucherdaten, insbesondere in Bezug auf Einwilligungen der Besucher zur Einholung von im Einzelfall erforderlichen Auskünften von anderen Stellen war nicht zu kritisieren. Bei einer früheren Kontrolle in einer anderen JVA war seitens des TLfD die Aufbewahrung von Besucherdaten in der Gefangenenpersonalakte als Daten Dritter kritisiert worden. Besucherdaten sind gesondert aufzubewahren und nach der Entlassung des Betroffenen zu vernichten. Darauf sind die Besucher auch hinzuweisen. Dennoch befand sich in der eingesehenen Gefangenenpersonalakte eines aus einer anderen Anstalt verlegten Betroffenen ein Umschlag, in dem sich die Besucherunterlagen befanden. Eine weitere Aufgabenerfüllung der kontrollierten JVA war nicht festzustellen, sodass diese Unterlagen spätestens bei Entlassung des Gefangenen zu löschen sind.
Weiterhin stieß die dort verwendete formularmäßige Einwilligung Gefangener zur Weitergabe persönlicher Daten an die in der JVA tätigen Suchtberatungen auf Bedenken, da die in Frage kommenden Stellen nicht näher konkretisiert waren. Das Formular wurde entsprechend ergänzt.
Eine Erforderlichkeit der Abheftung von Anträgen Gefangener zur Führung von Ferngesprächen in der Gefangenenpersonalakte war nicht gegeben, da solche Anträge nur Abrechnungszwecken dienen. Sie werden zukünftig bei der zuständigen Abrechnungsstelle mit kurzer Löschfrist aufbewahrt.
Auch eine interne Verfügung zur Einsichtnahme in die Gefangenenpersonalakte durch Bedienstete wurde entsprechend der Erforderlichkeit überarbeitet.
Zur Überwachung des Schriftverkehrs von Gefangenen wurden keine Mängel festgestellt. Allerdings wurde in einer ebenfalls aus einer anderen JVA übernommenen Gefangenenpersonalakte ein Umschlag mit einer Briefkarteikarte aufgefunden, auf der sämtliche ein- und ausgehende Schreiben notiert waren. Abgesehen davon, dass für die Führung einer Briefkarteikarte aus den Grundsätzen der Überwachung des Schriftverkehrs keine Erforderlichkeit abgeleitet werden kann, kann eine solche Karte mit Daten Dritter nicht in der Gefangenenpersonalakte aufbewahrt werden.
Ein Schwerpunkt der datenschutzrechtlichen Kontrolle lag auch in den Regelungen zur Nutzung der automatisierten Datenverarbeitung. Die hierzu eingesehenen Richtlinien, die aufgrund der zentralen Zuständigkeit der IT-Leitstelle Thüringer Justizvollzug für alle Justizvollzugsanstalten gelten, bedurften Ergänzungen zu den Festlegungen zum Benutzerkennwort, zur Aufbewahrung von Datensicherungen, zur Nutzung der elektronischen Post, zur Virenkontrolle, zur Absicherung des Internetzugangs gegenüber dem Corporate Network sowie zur Differenzierung von regelmäßigen Datenübermittlungen und automatisierten Abrufen. Die Anregungen des TLfD in dieser Hinsicht wurden von der IT-Leitstelle aufgegriffen und umgesetzt.
Insgesamt wurde auch durch die erfreuliche Kooperationsbereitschaft sowohl der Bediensteten in der Justizvollzugsanstalt als auch der IT-Leitstelle allen datenschutzrechtlichen Forderungen und Empfehlungen nachgekommen.

10.8.4 Auskünfte an Betroffene im Strafvollzug

Die Arbeit eines Strafgefangenen wird nach § 43 StVollzG anerkannt durch Arbeitsentgelt und eine Freistellung von der Arbeit, die auch als Urlaub aus der Haft (Arbeitsurlaub) genutzt oder auf den Entlassungszeitpunkt angerechnet werden kann. Soweit eine Anrechnung als Freistellungstage nicht möglich ist, kann eine Ausgleichsentschädigung erhalten werden. In der Vergangenheit hatte ein Betroffener auf seinen Antrag auf Auskunft zu den bereits erarbeiteten Freistellungstagen auch den Wert der Ausgleichsentschädigung mitgeteilt bekommen. Nachdem er nunmehr erneut einen Antrag auf Auskunft über die bereits erarbeiteten Freistellungstage gestellt hatte, wurde ihm auf dem entsprechenden Computerausdruck der Arbeitsverwaltung der JVA der Wert der Ausgleichsentschädigung komplett geschwärzt. Er wandte sich an den TLfD, um Auskunft gemäß § 185 StVollzG i. V. m. § 19 BDSG zu allen über ihn gespeicherten Daten zu erhalten. Auf Nachfrage hat die JVA dem TLfD mitgeteilt, der Antrag des Betroffenen habe sich nur auf seine bisher erworbenen Freistellungstage bezogen. Insoweit wurden alle weiteren Angaben auf dem Ausdruck, auf den sich der Antrag nicht konkret bezog, geschwärzt. Gründe, weshalb ihm eine entsprechende Auskunft über den Wert der Ausgleichsentschädigung zu verweigern wäre, wurden nicht dargetan. Zudem hatte die Anstalt die Zuständigkeit des TLfD in dieser Angelegenheit in Frage gestellt. Da dem Betroffenen möglicherweise eine Auskunft nach § 185 StVollzG i. V. m. § 19 BDSG verweigert wurde, war hier selbstverständlich die Zuständigkeit des TLfD, der nach Anrufung die Rechtmäßigkeit einer Auskunftsverweigerung zu prüfen hat, gegeben.
Auf meinen Hinweis zur Konkretisierung des Antrags hat der Betroffene erneut einen Antrag auf Auskunft mit einer ausdrücklichen Bitte um Angabe des Wertes der Ausgleichsentschädigung gestellt. Nach Ablauf einiger Zeit und Nachfrage durch den TLfD wurde dem Betroffenen letztendlich die Auskunft erteilt, zumal keine Gründe zur Verweigerung der Auskunft ersichtlich waren.

Ein Gefangener wandte sich an den TLfD, weil ihm von der Anstaltsleitung die Kopie des Ergebnisses einer ärztlichen Laboruntersuchung verwehrt wurde, nachdem ihm zuvor auf seinen Wunsch besagte Unterlagen in Kopie ausgehändigt worden waren.
Daher wurde der Anstaltsarzt angeschrieben und um Mitteilung gebeten, aus welchen Gründen dem Betroffenen die Kopie der Unterlagen verwehrt werde.
Die Anstaltsleitung beantwortete die Anfrage damit, dass der Gefangene zwar bislang regelmäßig Kopien der Befunde erhalten habe, jedoch ein Rechtsanspruch darauf nicht abzuleiten sei. Auskünfte über die Ergebnisse der Befunde würden jedoch weiterhin erteilt und es könne auch Einsicht in die Unterlagen genommen werden. § 185 StVollzG sehe nämlich lediglich eine Auskunft, nicht aber Kopien vor. Die Erteilung von Kopien und gegebenenfalls Nachfragen hierzu auch von außerhalb der Anstalt, falls der Betroffene die Kopie anderen Personen zur Kenntnis gäbe, wäre darüber hinaus als erhebliche Belastung der Arbeitsfähigkeit anzusehen.
Hierzu wurde der JVA mitgeteilt, dass ein Patient in Freiheit nach § 10 Abs. 2 der Berufsordnung der Ärzte grundsätzlich in die ihn betreffenden Krankenunterlagen mit Ausnahme derjenigen Teile, welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten, Einsicht nehmen und Kopien der Unterlagen gegen Erstattung der Kosten verlangen könne. Nach der bisher ergangenen Rechtsprechung hierzu kann - auch aus dem informationellen Selbstbestimmungsrecht abgeleitet - auch Patienten im Strafvollzug das Recht auf Kopien der Unterlagen, welche keine subjektiven Eindrücke oder Wahrnehmungen eines Arztes enthalten, zustehen. Bei der Verweigerung der Herausgabe von Kopien bedarf es der Einzelfallprüfung. Sollte aus ärztlicher Sicht begründet dem Betroffenen keine Kopie übergeben werden können, müsste jedoch Auskunft oder Einsicht gewährt werden. Dabei müsste dem Betroffenen die Möglichkeit gegeben werden, alle Einzelheiten abzuschreiben.

Die Anstaltsleitung hielt an der Auffassung fest, dass dem Betroffenen nach § 185 StVollzG kein Recht zustehe, Kopien von objektivierbaren Befunden und Behandlungstatsachen aus seiner Gesundheitsakte zu erhalten. Der Betroffene habe lediglich Kopien verlangt, einen Antrag auf Auskunft und Einsicht jedoch nicht gestellt. Einer Beantwortung der von mir aufgeworfenen Frage, weshalb dem Betroffenen unter Berücksichtigung des Einzelfalls die gewünschte Kopie nicht wie in den Vorjahren gewährt werden kann, kam ein Gerichtsbeschluss zuvor, der der Anstalt auferlegte, dem Gefangenen in vierteljährlichen Abständen eine Kopie der medizinischen Befunde auf seine Kosten auszuhändigen. Hiergegen hatte die JVA zunächst Rechtsmittel eingelegt, später jedoch wieder zurückgenommen, so dass der Betroffene auch zukünftig weiterhin die gewünschten Kopien erhält.

11. Gesundheits- und Sozialdatenschutz

11.1 „Hartz IV“ und der Datenschutz

Seit nunmehr über einem Jahr erfolgt die Umsetzung der Reform des Arbeitsmarktes, kurz „Hartz IV“ genannt. Von Beginn an haben sich die DSB intensiv mit den damit verbundenen Datenschutzproblemen auseinandergesetzt und alle Möglichkeiten der Einflussnahme auf eine datenschutzgerechte Gestaltung genutzt (Anlage 9). Eine durchgreifende Verbesserung im Hinblick auf die Gewährleistung des Sozialgeheimnisses, dem Kernbereich des Sozialdatenschutzes, kann aber bisher noch nicht festgestellt werden.
Verändert haben sich aber die Inhalte von Anfragen und Beschwerden Betroffener. Während zunächst neben grundsätzlichen organisatorischen datenschutzrelevanten Problemen insbesondere Fragen nach dem „was“ (erhoben wird) im Vordergrund standen, werden nun häufiger Fragen zum „Umgang“ mit den erhobenen Daten gestellt.

Obwohl die Vorschriften des SGB II und damit die Zusammenführung der Arbeitslosenhilfe und der Sozialhilfe erst zum 1. Januar 2005 in Kraft traten, erhielten bereits im Sommer 2004 über 2,2 Millionen Empfänger von Arbeitslosenhilfe einen 16-seitigen Antragsvordruck. Sowohl der Inhalt als auch die Gestaltung der Formulare warfen auch in datenschutzrechtlicher Hinsicht eine Reihe von Fragen auf. Gleichzeitig führte der Druck zur möglichst frühzeitigen Abgabe der Anträge zu einem „Ansturm“ auf die eingerichteten „Außenstellen“ der BA bzw. die zusätzlichen „Beratungsstellen“ in den Kommunen, so dass sich in dieser Phase zunächst Hinweise und Beschwerden über fehlende Möglichkeiten einer „diskreten“ Beratung häuften. Bei Kontrollen des TLfD bestätigten sich die Informationen. Auch wenn in deren Ergebnis in der Regel nicht sofort optimale Bedingungen geschaffen werden konnten, so zeigte sich dennoch, dass häufig bereits durch geringfügige Veränderungen, z. B. durch die Nutzung transportabler „Trennwände“, kurzfristig Verbesserungen erreichbar waren. Zwischenzeitlich haben sich nach meinen Erkenntnissen die Bedingungen in allen ARGEn (Arbeitsgemeinschaften nach SGB II) und optierenden Kommunen soweit verändert, dass überall die Möglichkeit einer vertraulichen Beratung besteht, bei der Dritte die Gespräche nicht verfolgen können.

Aus datenschutzrechtlicher Sicht problematisch waren von Anfang an die von der Bundesagentur verwendeten Antragsvordrucke und Zusatzblätter, die aufgrund ihrer teilweise unklaren Formulierungen dazu führen können, dass die Antragsteller in Unkenntnis der Rechtslage Sachverhalte offenbaren, die zur Bearbeitung nicht benötigt werden. Da in dem vom Hilfesuchenden auszufüllenden Vordruck nicht eindeutig zwischen den Mitgliedern der Bedarfsgemeinschaft und den übrigen Haushaltsangehörigen unterschieden wird, zur ordnungsgemäßen Antragsbearbeitung aber nur von den Mitgliedern der Bedarfsgemeinschaften sehr detaillierte Informationen notwendig sind, betrifft dies insbesondere die nicht erforderliche Eintragung von Daten über Haushaltsmitglieder, die nicht zur Bedarfsgemeinschaft gehören. Während

z. B. Daten über die Einkommens- und Vermögensverhältnisse des in der eheähnlichen Gemeinschaft mit dem Antragsteller lebenden und zur Bedarfsgemeinschaft gehörenden Partners zur Berechnung der Leistung zwingend in den Antrag einzutragen sind, besteht keine Notwendigkeit diese Angaben etwa auch für die im Haushalt lebende Mutter eines erwachsenen Hilfe suchenden Arbeitslosen vorzunehmen.
Außer der fehlenden Bestimmtheit wiesen die Vordrucke weitere datenschutzrechtliche Mängel auf. So war zunächst eine Gestaltung des Vordrucks für die Verdienstbescheinigung für Erwerbstätige einer Bedarfsgemeinschaft vorgesehen, durch den dem Arbeitgeber nicht nur die Langzeitarbeitslosigkeit des Partners seines Mitarbeiters bekannt geworden wäre, sondern der ihn darüber hinaus auch über weitere für ihn nicht bestimmte Daten des Antragstellers informiert hätte. Dies konnte durch die Kritik der DSB kurzfristig verändert werden. Ebenso wurde, entgegen der ursprünglichen Planung, in den Anträgen auf eine generelle Erhebung und Speicherung von Daten über die Vermieter der Antragsteller verzichtet, da deren Kenntnis für die Antragsbearbeitung nur im Einzelfall erforderlich ist.
Da die BA auf den Einsatz der vorhandenen Antragsformulare bestand, wurden im Benehmen mit den DSB des Bundes und der Länder Ausfüllhinweise erarbeitet, die allerdings nur dann etwas bewirken können, wenn sie den Antragstellern auch tatsächlich zur Verfügung stehen. Hierzu musste der TLfD jedoch verschiedentlich feststellen, dass die Hinweise lediglich im Internet abrufbereit sind oder nur auf Nachfrage von den ARGEn ausgehändigt werden. Auch wenn sich die kontrollierten Stellen bereit erklärten, die Ausfüllhinweise in ihren Räumlichkeiten zumindest auszuhängen, muss davon ausgegangen werden, dass zahlreichen Antragstellern die Existenz dieser Informationen nicht bekannt sein dürfte.
Zwischenzeitlich hat die BA auf Forderung des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz alle Antragsvordrucke und die Zusatzblätter überarbeitet. Es bleibt nun zu hoffen, dass diese Formulare gemeinsam mit den neuen Ausfüllhinweisen baldmöglichst auch den Betroffenen zur Verfügung gestellt werden, um die Erhebung nicht erforderlicher Daten zu verhindern und das datenschutzgerechte Ausfüllen der Unterlagen zu ermöglichen.

Neben den Datenerhebungen zur Leistungsberechnung benötigen die ARGEn bzw. die optierenden Kommunen zur Erfüllung ihrer Aufgaben zur Arbeitsvermittlung noch weitere Informationen über die arbeitsfähigen Mitglieder der Bedarfsgemeinschaften. Für die Erhebung dieser Daten über die konkreten Voraussetzungen und möglichen Hemmnisse einer Berufstätigkeit durch die Fallmanager gibt es keine bundeseinheitlichen Vordrucke, was insbesondere auch der Tatsache geschuldet ist, dass die Daten in jedem Einzelfall sehr unterschiedlich sind und deshalb in der Regel im Rahmen eines Vermittlungsgespräches erhoben werden. Dies hat jedoch einzelne Stellen nicht gehindert, eigene Formulare zu entwickeln, die teilweise dem Betroffenen nur zur Vorbereitung des Gesprächs übergeben werden und bei ihnen verbleiben, teilweise aber auch zu den Vermittlungsakten genommen werden. Überprüfungen hierbei haben ergeben, dass in den Fragebögen in der Regel für den Betroffenen nicht deutlich wird, welche Angaben unverzichtbar und welche freiwillig sind. Außerdem werden häufig undifferenziert zunächst von allen Arbeitssuchenden Daten erhoben über Sachverhalte, die nur in Einzelfällen relevant sind. Dies betrifft insbesondere Angaben über die derzeitigen Lebensbedingungen, die familiäre Situation oder Krankheiten, deren Erhebung nur soweit erforderlich ist, als sie vom Arbeitssuchenden als Hemmnisse gegen bestimmte Tätigkeiten, Arbeitszeiten oder Arbeitsorte genannt werden. Es darf keinesfalls sein, dass die „Hilflosigkeit“ der Antragsteller dazu führt, dass sich die Betroffenen zunächst zu allen Lebensbereichen offenbaren müssen, obwohl nur ein Teil der Informationen für die praktische Vermittlungstätigkeit von Bedeutung ist. Während unzweifelhaft für eine effektive Arbeitsvermittlung der höchste Bildungsabschluss, vorliegende Berufsabschlüsse, besondere Fähigkeiten, Fertigkeiten, Kenntnisse und Erfahrungen sowie die bisherigen beruflichen Tätigkeiten des Arbeitslosen bekannt sein müssen, kann daraus bspw. nicht die Pflicht des Hilfesuchenden zur Abgabe seines „Lebenslaufs“ bei der ARGE

oder optierenden Kommune abgeleitet werden. Auch eine generelle Frage und Dokumentation, wie bzw. durch wen bei einer Arbeitsaufnahme die Betreuung der Kinder gesichert ist, ist zur Aufgabenerfüllung nicht erforderlich und daher unzulässig, solange die fehlenden Betreuungsmöglichkeiten nicht als Vermittlungshemmnis vom Arbeitssuchenden selbst angesprochen werden. Nicht erforderlich sind z. B. auch generelle Datenerhebungen über gesundheitliche Probleme, regelmäßige ärztliche und therapeutische Behandlungen oder vorgesehene Maßnahmen zur Verbesserung des Gesundheitszustandes, soweit diese zu keiner Einschränkung der Arbeitsfähigkeit führen (wie z. B. Behinderungen, Allergien). Um Datenerhebungen über das erforderliche Maß hinaus auszuschließen, müssen deshalb die Fragebögen entsprechend präzisiert oder mit Hinweisen versehen werden. Dies ist nur dann unproblematisch, wenn die Fragebögen (auch sog. Profilingbögen) nur zur Vorbereitung für das Vermittlungsgespräch durch den Arbeitslosen genutzt werden sollen und nicht zu den Akten genommen werden. In diesem Fall kann der Fallmanager die Erhebung der Daten im automatisierten Verfahren („coArb“ in der ARGE und „LÄMMkom“ in den optierenden Kommunen) auf die sich im Gespräch ergebenden vermittlungsrelevanten Daten beschränken.

Eine häufig gestellte Anfrage im Zusammenhang mit der Abgabe der Anträge ist die Notwendigkeit der Vorlage von Nachweisen und hierbei insbesondere von Kontoauszügen. Hierzu vertritt der TLfD die Auffassung, dass entsprechend den gesetzlichen Vorgaben ein Anspruch auf Leistungen nach dem SGB II nur besteht, wenn der Antragsteller im Bewilligungszeitraum erwerbsfähig und hilfsbedürftig ist. Nach § 9 Abs. 1 SGB II ist er aber nur hilfebedürftig, wenn unter anderem sein Lebensunterhalt nicht oder nicht ausreichend aus eigenen Kräften oder Mitteln gesichert werden kann, vor allem nicht aus einem zu berücksichtigenden Einkommen und Vermögen. Dabei ist zu beachten, dass nach § 31 SGB II kein voller Anspruch auf ALG II besteht, wenn der Betroffene sein Einkommen oder Vermögen in der Absicht vermindert hat, die Voraussetzungen für die Gewährung oder Erhöhung des Arbeitslosengeldes II herbeizuführen. Die Prüfung der Hilfebedürftigkeit eines Antragstellers setzt somit eine vollständige Auskunft und Nachweisführung seiner Einkommens - und Vermögensverhältnisse voraus. Die Bestimmung der Art und Weise, wie der Leistungsberechtigte seiner Pflicht, Beweismittel vorzulegen, nachkommt, steht im pflichtgemäßen Ermessen des Sozialleistungsträgers. Kontoauszüge sind hierbei erhebliche Beweismittel, weil sie geeignet sind, die Entscheidung über das Bestehen eines Leistungsanspruchs zu ermöglichen. Die Festlegung, über welchen Zeitraum die Kontoauszüge vorzulegen sind, trifft der Sozialleistungsträger unter Beachtung des Grundsatzes der Verhältnismäßigkeit. In der Regel betrifft dies die letzten 3 Monate. Dabei ist eine Schwärzung von Angaben nur insoweit möglich, als sie keine Kontobewegungen betreffen (z. B. Angabe des Kreditrahmens) oder den Verwendungszweck und den Betrag noch erkennen lassen (z. B. den Namen einer Partei, wenn der Überweisungsgrund: Mitgliedsbeitrag lesbar bleibt). Dies ergibt sich daraus, dass nicht nur alle Einnahmen von Interesse sondern u. U. selbst kleinere Ausgaben, wie Zahlungen an Lebensversicherungen, Ausbildungsversicherungen oder Bausparverträge u. ä. bei Feststellung der Hilfebedürftigkeit entscheidend sind. Selbstverständlich dürfen nach der Prüfung der Originalauszüge nur von den Auszügen Kopien zu den Akten genommen werden, die entscheidungsrelevante Daten enthalten, wobei auch darin die nicht erforderlichen Angaben zu schwärzen sind. Entsprechendes gilt auch für alle anderen Unterlagen, die im Rahmen der Antragstellung zur Leistungsberechnung oder ggf. auch im Rahmen der Arbeitsvermittlung von den Betroffenen vorgelegt werden.

Die bisher erzielten Ergebnisse und „Veränderungen“ zur Gewährleistung des Datenschutzes bei der Umsetzung des SGB II können aber nicht darüber hinwegtäuschen, dass auch weiterhin eine Vielzahl grundsätzlicher Datenschutzdefizite und -verstöße zu konstatieren ist. Obwohl viele dieser Probleme seit längerem bekannt sind und die DSB des Bundes und der Länder die BA auf den notwendigen Handlungsbedarf hingewiesen und ihre Unterstützung angeboten ha-

ben, sind insbesondere die Ergebnisse hinsichtlich einer datenschutzgerechten automatisierten Verarbeitung der Daten der Leistungsempfänger in den ARGEn völlig unbefriedigend. Die zur Leistungsberechnung genutzte Software A2LL ermöglicht es derzeit noch über 40.000 Mitarbeitern in der BA und den ARGEn, bundesweit auf die Daten aller von der BA und den ARGEN betreuten Leistungsempfänger zuzugreifen. Ein Berechtigungskonzept fehlt ebenso wie eine Löschkonzeption für falsche oder nicht mehr benötigte Daten. Darüber hinaus werden die Zugriffe nicht protokolliert, sodass eine Kontrolle, ob unbefugt auf die Daten zugegriffen wird, praktisch unmöglich ist. Dadurch konnte bisher bspw. bei einer Antragstellung für einen finanziellen Zuschuss wegen eines ernährungsbedingten Mehrbedarfs von der dafür ursächlichen Krebs- oder Aidserkrankung des Betroffenen oder eines Mitgliedes seiner Bedarfsgemeinschaft unbefugt Kenntnis genommen werden. In gleicher Weise bundesweit einsehbar ist das Verfahren coArb in dem im Rahmen der Arbeitsvermittlung zum Teil auch äußerst sensible Daten über Schulden, Ehe- oder Drogenprobleme des Arbeitssuchenden gespeichert werden. Dies betrifft unter Umständen selbst intimste Details aus dem Privatleben des Hilfesuchenden, die dieser dem Mitarbeiter anvertraut hat (z. B. Probleme im Zusammenhang mit einer ungeklärten Vaterschaft, wie anlässlich einer Prüfung bekannt wurde), da auch Beratungsvermerke in dem Verfahren coArb gespeichert werden. Zwischenzeitlich wird nach Auskunft der BA ein neues Verfahren entwickelt, welches detaillierte Berechtigungs- und Löschkonzeptionen enthalten und bis Mitte 2006 zum Einsatz gelangen soll. Es bleibt zu hoffen, dass den Forderungen der DSB nach engen regionalen Zugriffsbeschränkungen Rechnung getragen wird und die DSB des Bundes und der Länder rechtzeitig bei der Entwicklung beteiligt werden.

Neben den vorgenannten datenschutzrechtlichen Defiziten, die bereits zu Beginn der Umsetzung von „Hartz IV“ bekannt wurden, hat sich ein weiteres, in den Regelungen des SGB II angelegtes, Problem ergeben, dessen Tragweite zunehmend deutlicher wird. Wie der Presse Mitte des Jahres 2005 zu entnehmen war, wurden durch ein Call-Center im Namen der BA telefonische Befragungen zur Arbeitslosigkeit bei ausgewählten Bedarfsgemeinschaften durchgeführt. Begründet wurde dies damit, dass die vorliegenden Daten über die Hilfeempfänger bei den ARGEn nicht mehr dem aktuellen Stand entsprächen und zur Erhöhung der Effizienz ein Datenabgleich notwendig sei. Dies war für den TLfD Anlass, das Verfahren zu überprüfen. Dabei stellte sich heraus, dass auch ein Teil der ARGEn in Thüringen einem von der BA beauftragten Call-Center Daten ihrer Kunden für die telefonische Befragungsaktion übersandt hatten. Den ARGEn als Auftraggeberinnen lagen weder die zugrunde liegende Vereinbarung zwischen der BA und dem Call-Center vor, noch erfolgte von den ARGEn eine schriftliche Auftragserteilung entsprechend den gesetzlichen Vorgaben. Das Vorhandensein schriftlicher Unterlagen oder sonstiger Kenntnisse zum konkreten Verfahren und aktuellem Verfahrensstand war ebenfalls nicht festzustellen. Darüber hinaus waren die Betroffenen im Vorfeld weder schriftlich über die Befragung informiert noch auf ihre Datenschutzrechte hingewiesen worden. Aufgrund der festgestellten datenschutzrechtlichen Verstöße gegen Bestimmungen zur Auftragsdatenverarbeitung nach dem Thüringer Datenschutzgesetz sah sich der TLfD zu einer Beanstandung veranlasst. Die geforderte Stellungnahme hierzu erfolgte allerdings nicht durch die ARGEn, sondern durch die Zentrale der BA in Nürnberg, die u. a. erklärte, dass die ARGEn keine verantwortliche Stellen im Sinne der Datenschutzgesetze für die Daten der Leistungsempfänger seien und allein die BA über die Datenverarbeitungsverfahren entscheide. Nach Auffassung der BA handelt es sich bei den ARGEn um ihre „Außenstellen“ mit der Folge, dass zwar eine Kontrolltätigkeit des TLfD für die im Freistaat Thüringen liegenden ARGEn dem Grunde nach nicht in Frage gestellt wird, aber die ARGEn nicht Adressaten von Beanstandungen sein können. Demnach dürfte der TLfD datenschutzrechtliche Verstöße zwar feststellen, aber nicht ahnden, da für die Kontrolle der Arbeitsweise der BA wiederum der Bundesbeauftragte für den Datenschutz und nicht der TLfD zuständig ist. Diese von dem Bundes- und den Landesbeauftragten für den Datenschutz einhellig abgelehnte Sichtweise macht eine

praktische Datenschutzkontrolle unmöglich, denn zur Verfolgung und Sanktion festgestellter datenschutzrechtlicher Mängel wäre danach immer die Mitwirkung des Bundesbeauftragten erforderlich, eine „Arbeitsteilung“, die gesetzlich nicht vorgesehen ist. Gegen die von der Bundesagentur vertretene Auffassung spricht auch nach Meinung der DSB der klare Wortlaut des Gesetzes (§ 44 b Abs. 3 SGB II), wonach die ARGEn die Aufgaben der BA als Leistungsträger nach dem SGB II wahrnehmen und somit eigenständige Leistungsträger sind, die eigenverantwortlich Daten verarbeiten (§ 67 Abs. 9 SGB X).
Die baldige Lösung der Zuständigkeitsfragen ist sicher nicht nur für eine praktikable und datenschutzgerechte Kontrolle der ARGEn und damit für die Gewährleistung des Datenschutzes im Bereich des SGB II von erheblicher Bedeutung. Die derzeitige Haltung der BA behindert eine sachgerechte Arbeit der DSB, sodass schnellstmöglich bei allen Beteiligten Rechtsklarheit zu schaffen ist. Die Thematik stand auch auf der Tagesordnung der 70. Konferenz der DSB des Bundes und der Länder Ende Oktober in Lübeck, in der auch entsprechende Beschlüsse gefasst wurden (Anlagen 16 und 17). In diesem Zusammenhang wurde insbesondere auch kritisiert, dass im Ergebnis der durch die BA mit Hilfe eines privaten Call-Center durchgeführten freiwilligen Telefonbefragungen alle Leistungsbezieher und Leistungsbezieherinnen von Arbeitslosengeld II des Verdachts auf Leistungsmissbrauch bezichtigt wurden, die unter Berufung auf ihr Grundrecht auf informationelle Selbstbestimmung von ihrem Recht, die Beantwortung von Fragen am Telefon zu verweigern, Gebrauch gemacht hatten. Dieser Auffassung muss nachdrücklich begegnet werden.
Während zur Durchsetzung einer datenschutzkonformen Arbeitsweise bei der Umsetzung des SGB II in den Bereichen der ARGEn noch eine Vielzahl von Veränderungen notwendig sind, bestehen die mit der elektronischen Datenverarbeitung der Daten der Arbeitslosengeld II – Empfänger sowie die mit der Datenschutzkontrolle verbundenen vorgenannten Probleme in den zwei optierenden Kommunen Thüringens nicht. Wie sich auch anlässlich einer Kontrolle zeigte, verwenden die betreffenden Kommunen zur Leistungsberechnung und Arbeitsvermittlung ein eigenständiges Verfahren (LÄMMkom). Zugriff zu den darin gespeicherten Daten der Arbeitssuchenden und Hilfeempfänger haben ausschließlich die Mitarbeiter des jeweiligen Grundsicherungsamtes. Eine Übermittlung der Daten an andere Stellen erfolgt nicht. Da diese Beschränkung der Zugriffsrechte nach Auskunft einer optierenden Kommune zu keiner Beeinträchtigung ihrer Arbeit führen soll, bestärkt dies nur die DSB in ihrer Forderung nach baldigen engen und regional beschränkten Zugriffsrechten auf die von den ARGEn bundesweit genutzten Verfahren A2LL und coArb mit den Daten der Hilfeempfänger und Arbeitssuchenden.
Zusammenfassend kann nach den bisherigen Ergebnissen der Arbeitsmarktreform im Hinblick auf den Datenschutz festgestellt werden, dass von den Verantwortlichen auf Bundes- und Länderebene noch eine Fülle von Problemen zu lösen sind und dementsprechend dieses Thema weiterhin im Blickpunkt der DSB stehen wird.

11.2 Datenerhebungen eines Sozialamts zur Prüfung einer eheähnlichen Gemeinschaft

Ein Bürger beschwerte sich beim TLfD darüber, dass er anlässlich eines Besuches bei einer Bekannten von einer dort unangemeldet auftauchenden Mitarbeiterin des Sozialamtes mit seinem Namen angesprochen worden sei. Bei dem sich anschließenden Gespräch brachte dann die Mitarbeiterin zum Ausdruck, dass sie von einer eheähnlichen Gemeinschaft zwischen dem Besucher und der Wohnungsinhaberin ausginge. Sie machte dabei deutlich, dass dem Sozialamt weitere Informationen über den Besucher, dessen Wohnung in einer anderen Gemeinde gemeldet ist, vorliegen würden. Diese betrafen insbesondere sein Kraftfahrzeug, seine Berufstätigkeit und seine Arbeitsstätte. Bei der näheren Prüfung des Sachverhalts stellte sich heraus, dass es sich bei der betroffenen Wohnungsinhaberin um eine Sozialhilfeempfängerin handelte und die Kenntnisse des Sozialamtes ausschließlich auf einer mündlichen Anzeige beruhten. Darin war unter Hinweis auf eine bestehende jahrelange Beziehung zwischen der Wohnungsinhaberin

und dem „Besucher“ sowie die häufige „Anwesenheit“ seines Fahrzeugs der Verdacht auf Sozialleistungsmissbrauch geäußert worden. Da bei der Gewährung von Hilfeleistungen durch das Sozialamt nicht nur die Einkommensverhältnisse der Hilfesuchenden selbst sondern auch einer weiteren Person, insbesondere wenn sie mit ihr in einer eheähnlichen Gemeinschaft nach § 122 BSHG lebt, zu berücksichtigen sind, war das Sozialamt gemäß § 20 SGB X nicht nur berechtigt, sondern auch verpflichtet, von Amts wegen diesem Hinweis nachzugehen und den Sachverhalt aufzuklären. Dabei kann die Prüfung aber nur im Rahmen der datenschutzrechtlichen Bestimmungen nach den §§ 67 ff. SGB X erfolgen. Antragstellerin und Bezieherin der Sozialhilfe war im konkreten Fall ausschließlich die Wohnungsinhaberin. Insoweit war das Sozialamt zunächst auch nur befugt, ihre Angaben zu überprüfen, was aufgrund der Anzeige im konkreten Fall die Frage betraf, ob sie möglicherweise in einer eheähnlichen Gemeinschaft nach § 122 BSHG lebt. Dabei kann aufgrund des Hinweises in diesem Zusammenhang sicher die häufige Anwesenheit des Fahrzeugs eines mutmaßlichen Partners als Indiz für die gleichzeitige Anwesenheit des Fahrers und somit für die Möglichkeit einer eheähnlichen Gemeinschaft bewertet werden und die entsprechenden Datenerhebungen rechtfertigen. Das Sozialamt war somit befugt nicht nur den Namen des vermeintlichen Lebenspartners, sondern auch die Hinweise für eine mögliche eheähnliche Gemeinschaft wie die Anwesenheit im Haushalt, Angaben zum Fahrzeug zu erheben, da diese Daten zur Prüfung erforderlich waren. Demgegenüber gab es zur Prüfung der Frage, ob die Wohnungsinhaberin in einer eheähnlichen Gemeinschaft lebt oder nicht kein Erfordernis zur Erhebung und Speicherung der Arbeitsstelle des vermuteten Lebenspartners. Hierbei handelte es sich um eine Datenerhebung über das erforderliche Maß hinaus und um eine ungerechtfertigte und unzulässige Datenvorratshaltung, zumal diese Informationen nur mündlich vorgetragen worden waren. Im Ergebnis der Prüfung wurde deshalb diese Angabe zur Berufstätigkeit in den Unterlagen gelöscht. Darüber hinaus wurde die Verhaltensweise der Mitarbeiterin einer kritischen Wertung unterzogen. Nach § 67 a Abs. 2 SGB X sind Sozialdaten grundsätzlich beim Betroffenen selbst zu erheben. Dieser Vorgabe war zunächst auch entsprochen worden, da die Hilfeempfängerin von der Mitarbeiterin des Sozialamts zur Überprüfung der Angaben persönlich aufgesucht wurde. Aufgrund der Tatsache, dass das besagte Fahrzeug vor dem Haus stand, war die Mitarbeiterin aber davon ausgegangen, dass es sich bei der anwesenden männlichen Person um den vermeintlichen Lebenspartner handele und hatte ihn unmittelbar nach der Begrüßung durch die Wohnungsinhaberin mit der Frage hinsichtlich einer bestehenden eheähnlichen Gemeinschaft konfrontiert. Auch wenn das Verhalten der Hilfesuchenden keinen Widerspruch gegen eine Befragung der anwesenden männlichen Person erkennen ließ, gab es zu diesem Zeitpunkt noch keinen Grund, die Fragen nicht zunächst mit der Antragstellerin allein oder mit ihrer Einwilligung in Anwesenheit des „Besuchers“ zu klären. Ob und inwieweit in der Folge ggf. noch eine Einbeziehung bzw. Befragung der männlichen Person erforderlich gewesen wäre, kann insoweit dahingestellt bleiben. Im Ergebnis der Prüfung wurde der Vorgang mit allen Mitarbeitern des Sozialamtes ausgewertet, um künftig den Umfang und die Art und Weise der Datenerhebung auf das zur jeweiligen Aufgabenerfüllung erforderliche und zulässige Maß zu beschränken.

11.3 Sozialgeheimnis gilt auch gegenüber Verwandten

Ein Petent beschwerte sich darüber, dass die Mitarbeiterin eines Sozialamts an dessen Vater und Schwester unzulässigerweise Sozialdaten zu seiner Person übermittelt habe. Eine durchgeführte Kontrolle beim Sozialamt hat ergeben, dass der Vater und die Schwester des Petenten beim Sozialamt vorgesprochen und mitgeteilt hatten, der Petent sei über Jahre hinweg von seinen Eltern finanziell unterstützt worden, ohne dies dem Sozialamt mitgeteilt zu haben. Daraufhin hat die Mitarbeiterin nicht nur erklärt, dass diese Angaben möglicherweise dazu führen könnten, dass der Petent die Hilfe zum Lebensunterhalt, einmalige Beihilfen und wahrscheinlich auch das Wohngeld unberechtigterweise erhalten habe, sondern dass die Hilfe zum Le-

bensunterhalt des Petenten als Vorschuss auf eine beantragte Erwerbsunfähigkeitsrente gezahlt werde. Damit hat die Mitarbeiterin des Sozialamtes nähere Umstände des vom Sozialamt dem Petenten gewährten Bezugs von Sozialleistungen offenbart. Für diese Übermittlung von Sozialdaten an Dritte ist nach den §§ 67 d ff SGB X kein Erlaubnistatbestand ersichtlich. Daher habe ich diese Verletzung des Sozialgeheimnisses gegenüber der Kommune beanstandet und anhand des aktuellen Falles eine nochmalige Belehrung der Mitarbeiter des Sozialamts über ihre Pflichten beim Umgang mit Sozialdaten gefordert. Dem ist das Sozialamt nachgekommen. Selbst wenn es sich wie im vorliegenden Fall bei den Dritten um Verwandte handelt, ist vom Sozialamt auch diesen gegenüber das Sozialgeheimnis zu wahren.

11.4 Elektronische Gesundheitskarte

Mit dem am 01.01.2004 in Kraft getretenen Gesetz zur Modernisierung der gesetzlichen Krankenversicherung - GKV-Modernisierungsgesetz (GMG) wurde u. a. in der Vorschrift des § 291 a SGB V festgelegt, dass die Krankenversichertenkarte (§ 291 SGB V) die als Krankenscheinersatz in Chipkartenform eingeführt wurde, bis spätestens 1. Januar 2006 zu einer elektronischen Gesundheitskarte erweitert wird. Die Karte soll neben ihren bisherigen Funktionen als Krankenversichertenkarte weitere Anwendungen auf verpflichtender und auf freiwilliger Basis enthalten. So muss sie bspw. Anwendungen für die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form (elektronisches Rezept) bieten. Ebenso soll sie die Möglichkeit verschiedener Anwendungen (Notfalldaten, Arzneimitteldokumentationen, elektronischer Arztbrief, elektronische Patientenakte, eigene Daten des Versicherten (Patientenfach) sowie Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für den Versicherten (Patientenquittung)) enthalten, die zur Verwendung gelangen, wenn der Versicherte damit einverstanden ist. Zur Gewährleistung der Patientenrechte in datenschutzrechtlicher Hinsicht sind konkrete Maßnahmen in § 291 a SGB V bestimmt. So müssen bspw. die Krankenkassen die Versicherten spätestens bei der Versendung der Karte umfassend über deren Funktionsweise informieren. Mit dem Erheben, Verarbeiten und Nutzen von Daten der Versicherten darf erst begonnen werden, wenn diese jeweils gegenüber Arzt, Zahnarzt oder Apotheker ihre auf der Karte zu dokumentierende und auf einzelne Anwendungen beschränkbare Einwilligung erklärt haben. Auch dürfen Zugriffe auf bestimmte Daten nur in Verbindung mit einem elektronischen Heilberufsausweis erfolgen.
Aus dem Blickwinkel des Datenschutzes ist es bei der Einführung der Gesundheitskarte von zentraler Bedeutung, dass der Patient wie bisher die Entscheidungsfreiheit darüber behält, welchem Arzt oder Apotheker er welche persönlichen (medizinischen) Daten offenbart. Es darf nicht das Ergebnis der Einführung eines Informationsverarbeitungsmediums wie der Gesundheitskarte sein, dass Patienten rechtlich oder faktisch gezwungen würden, Beschäftigten im Gesundheitsbereich pauschal Einblick in ihre medizinischen Daten gewähren zu müssen.

Um das komplexe Vorhaben „Elektronische Gesundheitskarte“ datenschutzrechtlich zu begleiten, wurde eine Unterarbeitsgruppe des Arbeitskreises Gesundheit und Soziales sowie des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten gebildet. Hier werden Probleme im Zusammenhang mit der Einführung des vorgesehenen Verfahrens erörtert wie bspw. eine Forderung von Patientenverbänden nach einer Änderung der gesetzlichen Regelungen dahingehend, dass eine Einsichtnahme in die medizinischen Daten durch den Versicherten „von zu Hause aus“ ermöglicht werden sollte. Offen ist derzeit auch die Frage, wer auf Verlangen des Versicherten Daten löschen darf bzw. ob diese Befugnis nur bestimmten Personen wie dem Haus- oder Vertrauensarzt zustehen soll.

Zwischenzeitlich ist das Projekt soweit gediehen, dass das BMGS eine „Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte“ vom 2. November

2005 erlassen hat. Darin werden die Rahmenbedingungen von Testmaßnahmen festgelegt, mit denen die elektronische Gesundheitskarte einschließlich der erforderlichen Telematikinfrastruktur erprobt werden soll. In diesem Zusammenhang wurde auf der 70. Konferenz der DSB des Bundes und der Länder am 27./28.10.2005 zur Einführung von Testregionen der elektronischen Gesundheitskarte, die ebenfalls Bestandteil der Rechtsverordnung ist, ein Beschluss gefasst, in dem u. a. die Berücksichtigung der Rechte der Versicherten im Rahmen des Testverfahrens gefordert wird. Aus datenschutzrechtlicher Sicht ist es zweckmäßig und notwendig, in den geplanten Teststufen bereits alle im Gesetz definierten Anwendungen sowie die datenschutzrechtlich geforderten Funktionalitäten (differenzierte Eingriffsrechte, gesicherte Anbindung der Teilnehmer, Einwilligung) zu testen. Anderenfalls ist nicht ausgeschlossen, dass durch Vorentscheidung in der Testphase die elektronische Gesundheitskarte einseitig auf datenschutzunfreundliche Konzepte festgelegt wird.

In Thüringen sind derzeit keine Testregionen vorgesehen. Der Erfahrungsaustausch mit den DSB des Bundes und der Länder wird jedoch auch in dieser Thematik intensiv betrieben, damit die gesetzlichen Festlegungen im Sinne des informationellen Selbstbestimmungsrechts der Patienten angemessen umgesetzt werden. Gleichzeitig werden auch mit den zuständigen Stellen in Thüringen datenschutzrechtliche Fragen im Zusammenhang mit der Einführung der elektronischen Gesundheitskarte diskutiert.

11.5 Gutachtentransfer zwischen AOK Thüringen und MDK Thüringen

Im 4. TB (11.11) wurde darüber berichtet, dass elektronisch übermittelte Gutachtenergebnisse nach der Übermittlung vom MDK an die AOK Thüringen und deren Ausdruck gelöscht werden sollten, um keine automatisiert auswertbaren Datensammlungen über medizinische Daten bei der AOK Thüringen entstehen zu lassen. Da in der Folgezeit ein vergleichbares Pilotprojekt des AOK Bundesverbandes bei der AOK Hessen initiiert worden ist, hat die AOK Thüringen ein Übergangsverfahren vorgeschlagen. Danach werden die MDK-Ergebnismitteilungen nach Bearbeitungsschluss bei der AOK auf einen Datenträger gespeichert, der gesondert zugriffssicher verwahrt wird. Die MDK-Ergebnismitteilungen werden dann nach deren Ausdruck im EDV-System gelöscht. Bis zu einer Entscheidung des Modellprojekts auf Bundesebene habe ich diesem Übergangsverfahren zugestimmt.

Das Pilotprojekt des AOK Bundesverbandes hatte die elektronische Übermittlung von Gutachtenergebnissen vom MDK an die Pflegekasse zum Gegenstand. Das Projekt wurde vom Hessischen DSB, vom BfD und vom TLfD unter Beteiligung des Arbeitskreises Gesundheit und Soziales der Konferenz der DSB des Bundes und der Länder begleitet, wobei eine Reihe von Empfehlungen zur Verbesserung der technischen und organisatorischen Maßnahmen der Datensicherheit gegeben werden konnten. Diese betrafen insbesondere die ausreichende Verschlüsselung der Gutachten beim elektronischen Versand sowie die Beschränkung der Zugriffsrechte sowohl beim MDK als auch bei der AOK auf das erforderliche Maß. Aufgrund dieser Veränderungen hat der Hessische Datenschutzbeauftragte in Abstimmung mit den DSB des Bundes und der Länder das Verfahren aus Datenschutzsicht als akzeptabel bewertet. Diese Bewertung des Pilotverfahrens veranlasste die AOK Thüringen/Pflegekasse das Verfahren zur elektronischen Übermittlung von Gutachtenergebnissen vom MDK Thüringen an die AOK/ Pflegekasse ebenfalls einzusetzen. Im Rahmen eines Informationsbesuchs hat sich der TLfD über die Umsetzung der im Rahmen der Pilotierung gegebenen Hinweise aus technischer und organisatorischer Hinsicht informiert. Dabei konnte festgestellt werden, dass diese Empfehlungen weitgehend übernommen worden sind. Darüber hinaus wurde die AOK Thüringen/Pflegekasse aufgefordert, Ergänzungen zu den tatsächlich praktizierten Verfahren in die bereits bestehende Dienstanweisung aufzunehmen. Dies betraf den Nachweis, dass die Nach-

richt tatsächlich beim Empfänger angekommen ist (Quittierungsverfahren), die Zugriffsprotokollierung, d. h. welche Mitarbeiter einen schreibenden Zugriff auf die sonstigen Daten (außer der Ergebnismitteilung, die als PDF-Datei nicht verändert werden kann) des Verfahrens haben sowie die Vermeidung eines doppelten Versands der Ergebnismitteilungen. Gleichzeitig wurde der AOK Thüringen empfohlen, bei einer möglichen Weiterentwicklung des Verfahrens zu prüfen, inwieweit künftig auch die lesenden Zugriffe auf die Ergebnismitteilungen zumindest stichprobenartig protokolliert und die Protokolle stichprobenartig ausgewertet werden.

Von der AOK wurde angekündigt, dass nach der Einführung des elektronischen Gutachtenversands bei der Pflegekasse ein Vorschlag zur Veränderung des Verfahrens des Gutachtentransfers vom MDK zur AOK unterbreitet werden soll, um die Übergangsregelung zu beenden. Gegenüber der AOK habe ich meine Bereitschaft signalisiert, einen entsprechenden Vorschlag datenschutzrechtlich zu prüfen. Bislang hat die AOK jedoch einen solchen Vorschlag nicht vorgelegt.

11.6 Mängel beim Umgang mit DMP-Daten durch Auftragnehmer der ARGE DMP

Mit dem am 1. Januar 2002 in Kraft getretenen Gesetz zur Reform des Risikostrukturausgleichs wurden in §§ 137 f und 137 g SGB V die Voraussetzungen zur Einführung sog. strukturierter Behandlungsprogramme für chronische Krankheiten (Disease-Management-Programme, abgekürzt: DMP) geschaffen. Mit diesen Programmen, in die sich die Versicherten freiwillig einschreiben können, soll die Behandlungsqualität von chronisch Kranken u. a. durch eine systematische Dokumentation der Behandlung und daraus regelmäßig zu ziehenden Schlussfolgerungen und Empfehlungen verbessert werden. Durch eine Koppelung mit dem sog. Risikostrukturausgleich unter den gesetzlichen Krankenkassen werden die Kassen belohnt, wenn sie derartige strukturierte Behandlungsprogramme anbieten und sich daran möglichst viele Versicherte beteiligen. Dahinter steht das Ziel, dass diejenigen Kassen mit vergleichsweise vielen chronisch kranken Versicherten einen Ausgleich für ihre Anstrengungen zur Verbesserung der Behandlungsqualität und damit zur Vermeidung von weiteren Folgekosten erhalten.

Zur Durchführung von zugelassenen DMP ist daher eine Erfassung detaillierter Behandlungsdaten durch den teilnehmenden Arzt mit Einwilligung des Patienten erforderlich. Der Umfang der im Rahmen der zugelassenen DMP zu erfassenden Daten sowie deren Weiterübermittlung an die Krankenkassen bzw. an die von diesen zur Auswertung errichteten Arbeitsgemeinschaften ist in der auf der Grundlage von § 266 Abs. 7 SGB V vom Bundesgesundheitsministerium erlassenen Risikostrukturausgleichsverordnung (RSAV) geregelt. § 28 f Abs. 2 Satz 1 Nr. 1 RSAV sieht vor, dass in den hierzu geschlossenen Verträgen einer Arbeitsgemeinschaft nach § 219 SGB V die Dokumentationsbögen der teilnehmenden Ärzte zur Pseudonymisierung des Versichertenbezugs zu übermitteln sind. Wie auch in anderen Bundesländern haben die Kassenärztliche Vereinigung und die Landesverbände der gesetzlichen Krankenkassen eine solche Arbeitsgemeinschaft (ARGE DMP) gegründet, deren geschäftsführender Gesellschafter die AOK Thüringen ist. Die ARGE DMP hat wie auch die ARGEn aus sechs weiteren Bundesländern aus Kostengründen ein Privatunternehmen mit Sitz in Bayern mit der gesamten Verarbeitung der Sozialdaten nach § 80 SGB X beauftragt. In Thüringen betrifft dies die Daten aus den drei zugelassenen strukturierten Behandlungsprogrammen zu Diabetes mellitus Typ 2, koronaren Herzerkrankungen und Brustkrebs. Nach § 80 Abs. 5 Satz 1 Nr. 2 SGB X hätte eigentlich der überwiegende Teil der Speicherung des gesamten Datenbestandes bei der ARGE verbleiben müssen, sodass diese Art der Verarbeitung nicht zulässig gewesen wäre. Auf die diesbezügliche Kritik der Datenschutzbeauftragen hin hat das Bundesgesundheitsministerium kurzerhand eine Gesetzesänderung auf den Weg gebracht, mit der als Ausnahme von § 80 Abs. 5

SGB X in § 137 f Abs. 6 SGB V die Übertragung des gesamten Datenbestandes an den Auftragnehmer zugelassen wird.

In der Folgezeit sollte sich zeigen, dass die Regelung in § 80 SGB V mit gutem Grund geschaffen wurde, da mit der Übertragung des gesamten Datenbestandes an den Auftragnehmer besondere Gefahren verbunden sind. Dies wiegt hier besonders schwer, da es sich bei den in den DMP verarbeiteten Daten um sensible Gesundheitsdaten handelt: Der Auftragnehmer hatte nunmehr seinerseits eine Tochterfirma mit der Auswertung der von den teilnehmenden Ärzten übersandten handschriftlich ausgefüllten Dokumentationsbögen beauftragt, was u. a. dadurch erfolgen sollte, dass die Daten eingescannt und mit Hilfe eines Texterkennungsprogramms in auswertbare Datenbanken übernommen werden. Aufgrund des Hinweises eines ehemaligen Mitarbeiters des Unterauftragnehmers wurde bekannt, dass dieser entgegen der Festlegungen im Vertrag Dateien an eine Tochtergesellschaft in Vietnam übermittelt hat. Der Auftraggeber hat daraufhin diese Datenschutzverletzung der ARGE mitgeteilt. Da die gebotenen Protokollierungen nicht vorgenommen worden sind, konnte nur sehr eingeschränkt aufgeklärt werden, zu welchem Zweck und in welchem Umfang diese Daten ins Ausland übermittelt wurden. Der Fall wurde von den auftraggebenden ARGEn unter Beteiligung des Hessischen Datenschutzbeauftragten intensiv geprüft. So wurden als Sofortmaßnahmen die Datenverarbeitung von dem Subunternehmen zum Auftragnehmer zurückverlagert und die Leitungsebene des beteiligten Personals ausgetauscht. Ob es zu strafrechtlich relevanten Handlungen gekommen ist, wird derzeit von der zuständigen Staatsanwaltschaft geprüft.

Da der TLfD keine Kontrollbefugnisse für den in Bayern ansässigen Auftragnehmer besitzt, konnte lediglich bei der ARGE geprüft werden, ob dieser ausreichende vertragliche Regelungen mit dem Auftragnehmer vereinbart hat. Die hierzu geschlossenen Verträge enthielten zur Einbeziehung von Unterauftragnehmern die Bestimmung, dass diese nur mit vorheriger schriftlicher Einwilligung des Auftraggebers eingeschaltet werden dürfen. Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Subunternehmer sollen nach dieser Klausel so gestaltet werden, dass sie den Bestimmungen zwischen Auftraggeber und Auftragnehmer entsprechen. Nähere Bestimmungen insbesondere zur Frage, ob die Daten im Ausland verarbeitet werden dürfen, enthalten die Verträge nicht. Zudem war den Verträgen selbst nicht zu entnehmen, dass ein Unterauftragnehmer mit der Bearbeitung der Dokumentationsbögen beauftragt worden ist. Dies konnte man lediglich mittelbar den Ausschreibungsunterlagen entnehmen, die dem TLfD jedoch erst im Rahmen der Überprüfung vorgelegt worden sind. Da der Auftragnehmer alle von den ARGEn geforderten Sofortmaßnahmen zur Datensicherheit erfüllt hat und kurzfristig auch kein anderes Unternehmern für diese Aufgabe zu finden war, wurde die Datenverarbeitung - allerdings mit künftig intensiveren Kontrollen des Auftragnehmers - fortgesetzt. Von der ARGE DMP Thüringen habe ich gefordert, eine Vertragsänderung mit dem Auftragnehmer durchzusetzen, wonach künftig die Einschaltung von Subunternehmern sowie die Verarbeitung der Daten im Ausland ausgeschlossen ist. Zu einem daraufhin von der ARGE übermittelten Vertragsentwurf, habe ich noch einige weitere Verbesserungsvorschläge aus Datenschutzsicht gemacht.

11.7 Umfang zulässiger Datenerhebungen beim Antrag auf Befreiung von Zuzahlungen nach §§ 61 ff SGB V

Mit dem Inkrafttreten des Gesetzes zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz) zum 01.01.2004 wurden auch die Voraussetzungen zur Befreiung von Zuzahlungen geändert. Nach der Neuregelung gelten bestimmte Belastungsgrenzen (2 % des jährlichen Bruttoeinkommens bzw. 1 % bei Vorliegen einer schwerwiegenden chronischen Erkrankung), bei deren Überschreiten die Versicherten keine weiteren Zuzahlungen

mehr zu leisten brauchen. Die Krankenkassen benötigen jedoch zur Feststellung der Überschreitung der Belastungsgrenze erforderliche Daten von den Versicherten, die die Befreiung beantragen. Für die Höhe der jeweiligen persönlichen Belastungsgrenze benötigen die Krankenkassen bestimmte Informationen und Nachweise, etwa zu Einnahmen und den geleisteten Zuzahlungen. In diesem Zusammenhang erhielt der TLfD eine Anfrage, bei der sich der Ehepartner einer Versicherten darüber wunderte, dass von der Krankenkasse im Rahmen der Bearbeitung eines Antrags seiner Frau auf Befreiung von den Zuzahlungen nach Sparbuch und Wohneigentum zu seiner Person gefragt wurde, obwohl er gar nicht bei dieser Krankenkasse versichert ist. Eine Überprüfung bei der Krankenkasse hat ergeben, dass in diesem Fall lediglich nach den Zinsgewinnen und eventuellen Einnahmen aus Wohnungseigentum, jedoch nicht nach den Guthaben bzw. dem Wert des Wohnungseigentums selbst gefragt wurde. Die Regelungen zu Zuzahlungen finden sich in den §§ 61 ff. SGB V. Die Belastungsgrenze, also der Anteil, den die Versicherten im Kalenderjahr höchstens selber zu zahlen haben, ist in § 62 SGB V geregelt. Nach § 62 Abs. 2 SGB V werden bei der Ermittlung der Belastungsgrenzen Zuzahlungen und Bruttoeinnahmen zum Lebensunterhalt der mit dem Versicherten in gemeinsamen Haushalt lebenden Angehörigen der Versicherten und des Lebenspartners jeweils zusammengerechnet. Daraus ergibt sich, dass die Krankenkasse neben der Klärung des Einkommens der Versicherten auch nach dem Einkommen des Ehepartners fragen durfte. Zu den Einnahmen zum Lebensunterhalt gehören bspw. auch Einnahmen aus Kapitalvermögen wie Zinsen aus Sparguthaben oder Einkünfte aus Vermietung und Verpachtung. Aus diesem Grund war die entsprechende Datenerhebung datenschutzrechtlich nicht zu beanstanden, was dem Petenten mitgeteilt wurde.

11.8 Einzug des Unfallversicherungsbeitrages für Beschäftige in Privathaushalten durch die Bundesknappschaft

Mit einer zum 1. Januar 2006 in Kraft tretenden Ergänzung des § 185 Abs. 4 SGB VII soll für geringfügig beschäftigte Personen in Privathaushalten ein einheitlicher Unfallversicherungsbeitrag festgelegt werden sowie der Beitragseinzug durch den Bundesverband der Unfallkassen e. V. (BUK) sichergestellt werden. Bisher sind für den Einzug der Beiträge zur Unfallversicherung für diese Haushaltshilfen die Unfallversicherungsträger im kommunalen Bereich zuständig. In Thüringen ist dies die Unfallkasse Thüringen. An dieser Zuständigkeit soll sich grundsätzlich auch nichts ändern. Die bei der Bundesknappschaft eingerichtete Minijob-Zentrale ist nach § 28 i Satz 5 SGB IV bereits jetzt Einzugsstelle für den Gesamtsozialversicherungsbeitrag. Werden der Minijob-Zentrale im sog. Haushaltscheckverfahren Haushaltshilfen gemeldet, so informiert sie den zuständigen Unfallversicherungsträger hierüber, der dann den Beitrag bei den Arbeitgebern einzieht. Dieses Verfahren soll nunmehr insoweit vereinfacht werden, dass die Unfallversicherungsträger im kommunalen Bereich mit der Bundesknappschaft eine Vereinbarung nach § 88 SGB X abschließen, mit der sie die Bundesknappschaft (Minijob-Zentrale) beauftragen, die Unfallversicherungsbeiträge für die jeweiligen Unfallversicherungsträger einzuziehen. Der Entwurf der Vereinbarung wurde dem TLfD durch die Unfallkasse Thüringen mit der Bitte um Stellungnahme aus datenschutzrechtlicher Sicht übermittelt. Es wurden einige Anregungen zur Klarstellung im Vertrag gegeben, die weitgehend berücksichtigt wurden.

11.9 Einschaltung von Gutachtern und Beratungsärzten durch die Unfallkasse Thüringen

Bei der Einschaltung von ärztlichen Beratern und Gutachtern durch die Unfallversicherungsträger (UVT) im Rahmen der Prüfung von Leistungen werden immer wieder die Datenschutzrechte der Betroffenen nicht ausreichend eingehalten. Als eines der Hauptprobleme stellt sich

dabei die Umsetzung des § 200 Abs. 2 SGB VII dar, der die UVT verpflichtet, vor Erteilung eines Gutachtenauftrags und der damit verbundenen Übermittlung von medizinischen Daten an den Gutachter dem Betroffenen mehrere Gutachter zur Auswahl vorzuschlagen. Darüber hinaus ist der Betroffene auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X gegen eine beabsichtigte Übermittlung seiner Daten an einen bestimmten Gutachter hinzuweisen. Aufgrund einer Eingabe habe ich bei einer Kontrolle eines UVT festgestellt, dass dem Betroffenen lediglich ein Gutachter zur Auswahl vorgeschlagen worden ist. Aufgrund des Wortlauts von § 200 Abs. 2 SGB X, wonach mehrere Gutachter vorgeschlagen werden sollen, ist anerkannt, dass im Ausnahmefall auch nur ein Gutachter vorgeschlagen werden kann, wenn z. B. zu bestimmten Fachgebieten keine ausreichende Zahl von Spezialisten zur Verfügung stehen. Allerdings waren diese Umstände im konkreten Fall nicht der Akte zu entnehmen. Deshalb habe ich gegenüber dem UVT gefordert, diese Fälle künftig nachvollziehbar zu dokumentieren. Gravierender war jedoch die Tatsache, dass der Hinweis auf die beabsichtigte Beauftragung nicht schriftlich, sondern anlässlich eines Telefonats erfolgt ist. Dabei konnte nicht mehr geklärt werden, ob der Mitarbeiter des UVT den Betroffenen auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X hingewiesen hatte. Dies ging aber nach allgemeinen Beweisregeln zu Lasten des UVT, der nach § 200 Abs. 2 SGB VII im Zweifel nachweisen muss, dass er seiner Pflicht zum Hinweis des Betroffenen auf sein Widerspruchsrecht nachgekommen ist. Auch dem vom UVT vorgetragenen Einwand, dass der Betroffene bereits zu Beginn des Verfahrens in allgemeiner Form auf sein Widerspruchsrecht hingewiesen worden sei, konnte nicht gefolgt werden. Der Hinweis hat vor Erteilung des Gutachtenauftrags und mit konkretem Bezug hierauf zu erfolgen, da der Betroffene erkennen können muss, an welchen Gutachter seine Daten zu welchem Zweck übermittelt werden sollen. Diesen Verstoß gegen § 202 Abs. 2 SGB VII habe ich gegenüber dem UVT beanstandet. Der UVT hat auf die Beanstandung damit reagiert, dass nunmehr den Versicherten gegenüber ausschließlich schriftliche Hinweise auf ihr Widerspruchs- und Gutachterwahlrecht gegeben werden. Zudem wurden die gegenüber den Versicherten verwendeten Vordrucke für Anschreiben dahingehend verändert, dass künftig ausdrücklich darauf hingewiesen wird, dass der Widerspruch schriftlich zu erklären ist.

Aufgrund von Eingaben habe ich mit dem UVT zudem die Rolle von sog. Beratungsfachärzten und deren Abgrenzung zu Gutachtern problematisiert. Da den Mitarbeitern der UVT häufig die notwendigen medizinischen Fachkenntnisse fehlen, um beurteilen zu können, ob zur Antragsentscheidung ein fachärztliches Gutachten eingeholt werden muss, beauftragen diese häufig Beratungsfachärzte, zu einzelnen Fragen anhand der ihnen vorliegenden Unterlagen. Diese außerhalb des UVT, z. B. in Krankenhäusern tätigen Ärzte haben mit dem UVT einen Beratervertrag abgeschlossen, in dem sie sich u. a. zur Verschwiegenheit verpflichten. Allerdings bleiben sie im Verhältnis zum UVT Dritter, so dass eine Einsichtnahme dieser Beratungsfachärzte in die beim UVT vorliegenden medizinischen Unterlagen als eine Übermittlung anzusehen ist, für die es einer Rechtsgrundlage bedarf. Hier kommt § 69 Abs. 1 Nr. 1 i. V. m. § 76 Abs. 2 Nr. 1 SGB X in Betracht mit der Folge, dass der Versicherte auf sein Widerspruchsrecht hinzuweisen ist. Davon kann in denjenigen Fällen eine Ausnahme gemacht werden, in denen dem Beratungsfacharzt Einzelfragen ohne Nennung des Namens des Versicherten oder aber anonymisierte Aktenauszüge zur Beurteilung vorgelegt werden. In einem von einem Petenten vorgetragenen Fall war jedoch die beratungsfachärztliche Stellungnahme nach Form, Inhalt und Umfang so gestaltet, dass sie schon fast als Gutachten anzusehen war. Es besteht also die Gefahr, dass bei entsprechender Ausführlichkeit der Stellungnahme das nach § 202 Abs. 2 SGB VII vorgegebene Gutachterwahlrecht einschließlich des Widerspruchsrechts gegen den konkret zu beauftragenden Gutachter umgangen werden könnte. Gegenüber dem UVT habe ich daher unter Bezugnahme auf ein Rundschreiben des Bundesverbandes der Unfallkassen aus dem Jahr 2003 zur Abgrenzung des Gutachters vom beratenden Arzt empfohlen, eine klare Abgrenzung bereits bei den Aufträgen an den Beratungsfacharzt vorzunehmen. Für eine solche Abgrenzung

sollte bereits aus der schriftlichen Auftragserteilung an die Beratungsfachärzte ausdrücklich hervorgehen, dass es sich um eine Beratung und nicht ein medizinisches Gutachten handelt. Die Anfragen sollten sich zudem auf konkrete medizinische Sachverhalte beschränken und nach Möglichkeit anhand anonymisierter Unterlagen erfolgen. Der UVT hat mir mitgeteilt, dass er in denjenigen Fällen, in denen vom Beratungsfacharzt eine Stellungnahme eingeholt werden soll, die einem Gutachten gleichkommt § 200 Abs. 2 SGB VII anwendet. Für die verbleibenden Fälle einer Stellungnahme des Beratungsfacharztes kommt daher entweder nur eine Anonymisierung der Unterlagen oder aber zumindest ein Widerspruchsrecht des Versicherten nach § 76 Abs. 2 SGB X in Frage. Zu letzterem habe ich den UVT aufgefordert, dem Versicherten eine Liste aller Beratungsfachärzte zugänglich zu machen, um eine Grundlage zur Ausübung seines Widerspruchsrechts zu erhalten. Dem ist der UVT gefolgt.

11.10 Diskretionsschutz im Wartebereich eines Krankenhauses

Von einem Patienten einer Klinik wurde der TLfD darüber informiert, dass vor der Durchführung einer diagnostischen Untersuchung der behandelnde Arzt seine persönlichen Daten über seine Krankheitsgeschichte sowie seinen aktuellen Gesundheitszustand im Flur des Krankenhauses aufgenommen habe. Von den Daten konnten andere Patienten, die ebenfalls auf dem Flur anwesend waren, Kenntnis erlangen, soweit sie sich in Hörweite befanden. Eine Anfrage im Krankenhaus hat diesen Sachverhalt bestätigt, der damit begründet wurde, dass keine ausreichenden räumlichen Voraussetzungen im derzeit noch genutzten Krankenhausgebäude existieren. Abhilfe solle dadurch geschaffen werden, dass in den neu zu beziehenden Räumlichkeiten eine räumliche Trennung des Gesprächsbereichs vom Wartebereich erfolgt. Auch wenn vielfach im Krankenhaus Situationen bestehen, in denen Mitpatienten Kenntnis über die Erkrankungen der anderen Patienten erhalten können, so sollte dies doch soweit wie möglich durch technische und organisatorische Maßnahmen ausgeschlossen werden. Hierzu sind die Krankenhäuser nach § 27 Abs. 10 Thüringer Krankenhausgesetz auch verpflichtet. Sofern im täglichen Miteinander des Krankenhausalltags die Patienten sich aus eigener Initiative gegenseitig über ihre Erkrankungen informieren, geschieht dies mit Wissen und Wollen der Patienten. Das Krankenhaus sollte jedoch solche Rahmenbedingungen schaffen, dass dem Patienten hierfür eine Wahlmöglichkeit bleibt und er nicht faktisch gezwungen wird, seine Daten Dritten gegenüber zu offenbaren, obwohl er das nicht möchte. Als Reaktion hierauf hat das Krankenhaus mitgeteilt, dass die betroffenen Bereiche nochmals darauf hingewiesen worden sind, Anamneseerhebungen, Untersuchungen, Befundbesprechungen oder Behandlungsgespräche etc. grundsätzlich nicht im Bereich von wartenden Patienten durchzuführen.

11.11 Einsicht in Patientenunterlagen Verstorbener durch deren Angehörige

Im Berichtszeitraum baten in mehreren Fällen Angehörige von Verstorbenen den TLfD um Unterstützung, denen die Einsichtnahme in die Patientenunterlagen des Verstorbenen mit der Begründung verweigert wurde, dass hierzu keine Einwilligung des Verstorbenen vorliege. Gemäß § 203 Abs. 1 Nr. 1 StGB hat der Arzt über alles, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekannt geworden ist, zu schweigen. Nach § 203 Abs. 4 StGB sowie § 9 der Berufsordnung der Landesärztekammer Thüringen gilt dies im Grundsatz auch über den Tod des Patienten hinaus. Allerdings kann der Umfang der ärztlichen Schweigepflicht mit dem Tod des Patienten abnehmen. In diesem Fall hängt die Offenbarungsbefugnis des Arztes jedoch grundsätzlich nicht davon ab, ob die Erben oder Hinterbliebenen dies gestatten. Vielmehr ist auf den – auch mutmaßlichen – Willen des Verstorbenen abzustellen. Demzufolge muss der mutmaßliche Wille des Patienten erforscht werden, sofern eine positive Willensäußerung des Verstorbenen nicht feststellbar ist. Die Ermittlung des mutmaßlichen Willens des Verstorbenen ist nach der Rechtsprechung des Bundesgerichtshofs Aufgabe des Geheimnisträgers selbst, also

des Arztes. Er hat in Ermangelung eines geäußerten Willens zu prüfen, ob Anhaltspunkte dafür bestehen, dass der Verstorbene die ganze oder teilweise Offenlegung der Krankengeschichte gegenüber seinen Hinterbliebenen oder Erben mutmaßlich missbilligen würde. Dabei soll auch das Anliegen der die Einsicht begehrenden Personen (Geltendmachung von Ansprüchen, Wahrung nachwirkender Persönlichkeitsbelange des Verstorbenen) eine entscheidende Rolle spielen. Beharrt der Arzt auf seiner Schweigepflicht, kann er sich nicht darauf beschränken, die Offenbarung „aus grundsätzlichen Erwägungen“ zu verweigern. Vielmehr wird von ihm die gewissenhafte Erfüllung strenger, ins Einzelne gehender, Prüfungspflichten und auch die Darlegung erwartet, auf welche Belange des Verstorbenen sich seine Weigerung stützt. Diese Auffassung wird auch auf Nachfrage vom Thüringer Ministerium für Soziales, Familie und Gesundheit geteilt. Die jeweiligen Stellen haben sich nach erneuter Prüfung dazu bereit erklärt, die gewünschten Auskünfte an die Angehörigen zu erteilen.

11.12 Regelungen zum Neugeborenen-Screening

In den letzten Jahren wurden zwischen den DSB des Bundes und der Länder datenschutzrechtliche Fragen zum Neugeborenenscreening erörtert. Dabei ging es nicht darum, die Durchführung des Screenings in Frage zu stellen, sondern ausschließlich um einen datenschutzkonformen Umgang mit den Erhebungsdaten sowie den Blutproben. In diesem Zusammenhang wurde auch vom TLfD die Verfahrensweise im Thüringer Landesamt für Lebensmittelsicherung und Verbraucherschutz (TLLV) als einziges öffentliches Labor in Thüringen geprüft, in dem bis Ende März 2005 das Screening mit Ausnahme der Tandem-Massenspektrometrie, die im Universitätsklinikum Leipzig erfolgte, durchgeführt wurde.
Beim Neugeborenenscreening werden den Neugeborenen mit Einwilligung der Mutter im Laufe des 2. bis 3. Lebenstags im Rahmen der zweiten Vorsorgeuntersuchung wenige Bluttropfen aus der Ferse entnommen und auf eine sog. Testkarte getropft. Diese Blutproben werden dann speziellen Untersuchungsmethoden in einem Speziallabor zur Früherkennung bestimmter angeborener Erkrankungen unterzogen. Die Ergebnisse werden anschließend den jeweiligen Geburtseinrichtungen, Ärzten oder Hebammen mitgeteilt. Diese sind nach der ärztlichen Berufsordnung verpflichtet, die jeweiligen Befunde für mindestens 10 Jahre aufzubewahren. Entsprechend der „Richtlinie zur Organisation und Durchführung des Neugeborenenscreenings auf angeborene Stoffwechselstörungen und Endokrinopathien in Deutschland“ vom 20.03.1997 sollen zur Sicherung einer späteren Überprüfbarkeit des Screeningergebnisses die Testkarten unter geeigneten Bedingungen gleichfalls für 10 Jahre aufbewahrt werden.
Mit der Änderung der Richtlinie aufgrund des Beschlusses des gemeinsamen Bundesausschusses der Ärzte und Krankenkassen vom 21.12.2004 und der Bestätigung durch das Bundesministerium für Gesundheit und Soziales erfolgte eine Erweiterung des Neugeborenenscreenings unter Vorgabe der Untersuchungsmethoden, der Zeitpunkte, der Anforderungen an die durchzuführenden Labore, der Qualifikation der Ärzte und der Befundübermittlung. Da danach künftig die gesamten Laborleistungen an einem Laborstandort erfolgen sollen, werden seit dem Frühjahr 2005 die Laboruntersuchungen außerhalb von Thüringen durchgeführt.
Entsprechend der geänderten Richtlinie werden dort künftig die Blutproben auch nur noch für einen Zeitraum von 3 Monaten aufbewahrt, sodass sich die Frage nach der Erforderlichkeit und der Zweck für die weitere Aufbewahrung der „alten“ anonymisierten Blutproben im TLLV stellt. Diesbezüglich befindet sich der TLfD noch mit dem TMSFG im Gespräch.

11.13 JobCard

Angestoßen durch eine Initiative der Bundesregierung läuft zurzeit ein Projekt zur Einführung elektronischer Signaturverfahren in der Sozialverwaltung, kurz als „JobCard-Verfahren“ bezeichnet. Ziel ist die Schaffung einer zentralen Datenbank, in der Arbeits- und Einkommensda-

ten aller abhängig Beschäftigten zur Entlastung der Arbeitgeber gespeichert werden. Derzeit stellen etwa 2,8 Millionen Arbeitgeber Jahr für Jahr ca. 60 Millionen Bescheinigungen in Papierform aus, damit Arbeitnehmer ihnen nach den Sozialgesetzen zustehende Leistungsansprüche gegenüber unterschiedlichen Sozialbehörden geltend machen können. Künftig sollen regelmäßig die zu bescheinigenden Daten (z. B. zum Gehalt oder zu Arbeitszeiten) vom Arbeitgeber an eine Zentrale Speicherstelle (ZSS) übermittelt werden. Im Bedarfsfall, etwa bei der Beantragung von Arbeitslosen-, Wohn- oder Kindergeld kann der zuständige Sozialleistungsträger mit Vollmacht des Arbeitnehmers die jeweils erforderlichen Nachweise bei der ZSS abrufen und verarbeiten. Die Vollmacht zum Abruf erteilt der Leistungsberechtigte mit seiner persönlichen Signaturkarte, die nach Anmeldung und Legitimation bei einer Registrierungsstelle für die Teilnahme am JobCard-Verfahren freigeschaltet wird. Eine Zertifizierungsstelle (Trust-Center) erstellt Schlüssel und Zertifikate für die am System beteiligten Parteien und generiert u. a. die Signaturkarte für den Arbeitnehmer, nachdem er diese über die Registrierungsstelle beantragt hat. Die Signaturkarte stellt ein qualifiziertes elektronisches Zertifikat im Sinne des Signaturgesetzes (2. TB, 15.8; 4. TB, 15.8) dar und soll damit den Zugriffsschutz auf die Leistungsdaten gewährleisten.

Die Komplexität des angestrebten JobCard-Verfahrens veranlasste die 67. Konferenz der DSB des Bundes und der Länder, eine Arbeitsgruppe einzusetzen, die sich mit dem Projekt in rechtlicher und technischer Hinsicht befassen soll. Der AG JobCard gehören Mitglieder des Arbeitskreises Gesundheit und Soziales und des Arbeitskreises Technik der DSB an. Im Vordergrund der Begleitung durch den Datenschutz steht mit Blick auf das Grundrecht auf informationelle Selbstbestimmung die verfassungsrechtliche Zulässigkeit des JobCard-Verfahrens ebenso wie die Prüfung von Verfahren, mit denen eine mögliche Gefährdung des Grundrechts auch auf technischem Wege minimiert werden kann.

Rechtlich problematisch ist der Umstand, dass ein großer zentraler Bestand von Daten geschaffen werden soll, obwohl im Zeitpunkt der Datenerhebung keineswegs feststeht, dass eine Behörde zu Leistungszwecken tatsächlich Bedarf an den Daten hat oder haben wird. Damit ist das Problem einer nach der Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung unzulässigen Datenvorratsspeicherung ebenso wie die Frage der Verhältnismäßigkeit tangiert. Die Erforderlichkeit der Speicherung von - sensiblen - personenbezogenen Datensätzen ist sehr fragwürdig, wenn nicht einmal klar ist, ob die Daten überhaupt jemals benötigt werden.

Ebenfalls kritisch zu prüfen ist die Frage, ob das Verfahren mit dem Grundsatz der Zweckbindung vereinbar ist. In jedem Falle sind Verantwortlichkeiten und beteiligte Stellen bereits im Vorhinein zu bestimmen, weiter sollte der konkrete Verwendungszweck gesetzgeberisch auf die Erteilung der vorgesehenen Bescheinigungen festgelegt werden, wobei es zum gegenwärtigen Zeitpunkt allerdings nicht absehbar ist, für welche Verwendungszwecke der Datenbestand künftig noch genutzt werden soll.

Neben den rechtlichen Problemen haben sich auch Fragestellungen auf der technischen Seite des Datenschutzes im JobCard-Verfahren ergeben. Das derzeitige Konzept sieht vor, die Daten verschlüsselt bis zur ZSS zu übertragen. Hier werden sie entschlüsselt auf Plausibilität geprüft und mit einem sog. Master-Key verschlüsselt vorgehalten. Beim Abruf der Daten werden diese zunächst wieder mit dem Master-Key entschlüsselt und erneut verschlüsselt an die abrufende Behörde übertragen. Der aufgezeigte Verfahrensablauf weist insofern für die Vertraulichkeit der Daten Schwachstellen auf, als diese zwischenzeitlich im Klartext vorliegen und alle gespeicherten Daten in der zentralen Datenbank mit dem gleichen Schlüssel kryptiert gespeichert werden. Ein mögliches korrumpieren dieses Schlüssels, würde die Vertraulichkeit der hier ge-

speicherten Daten gefährden. Um diese Schwachstellen auszuschließen und weiterhin die Vertraulichkeit der Daten vom Absenden des Arbeitgebers bis zum Empfang bei der abrufenden Behörde durchgängig unter Mitwirkung des betroffenen Arbeitnehmers abzusichern, wurde seitens der DSB eine sog. ENDE-zu-ENDE Verschlüsselung favorisiert. In diesem Fall würden die Bescheinigungsdaten von den Arbeitgebern mit dem öffentlichen Schlüssel des jeweiligen Leistungsempfängers verschlüsselt übertragen und in der zentralen Datenbank abgespeichert. Somit wären die Leistungsempfänger als einzige in der Lage, ihre Daten zu entschlüsseln und den abrufenden Stellen zur Bearbeitung bereitzustellen. Der Arbeitskreis Technik der DSB erarbeitete dazu im Auftrag der 68. Konferenz der DSB des Bundes und der Länder die Rahmenbedingungen für einen entsprechenden Gutachtenauftrag für die mögliche Integration der ENDE-zu-ENDE Verschlüsselung in das konzipierte Projekt JobCard. Im Auftrag des Bundesministeriums für Wirtschaft und Arbeit und des Bundesbeauftragten für den Datenschutz wurde dieses Gutachten vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt. Das BSI kam in dem Gutachten zu dem Ergebnis, dass eine ENDE-zu-ENDE Verschlüsselung technisch möglich ist. Insgesamt wird vom BSI jedoch eingeschätzt, dass diese Form der Verschlüsselung wenig flexibel und mit einem Mehraufwand verbunden ist. Deshalb wird im Rahmen des Projekts beabsichtigt, eine ENDE-zu-ENDE Verschlüsselung nicht weiter zu verfolgen.

Ob die derzeit favorisierte technische Lösung jedoch zum Einsatz gelangt, hängt vom Ergebnis der Prüfung der noch offenen, o. g. rechtlichen Fragen ab. Um hier endgültig Klarheit zu erlangen, ist die Bundesregierung von den DSB aufgefordert worden, die verfassungsrechtliche Zulässigkeit des JobCard-Verfahrens zu prüfen und das Ergebnis vorzulegen.

11.14 Umfang der Datenerhebung in einer REHA-Werkstätte

Durch eine Anfrage wurde der TLfD darauf aufmerksam gemacht, dass eine Rehabilitationswerkstätte, die von einer öffentlichen Stelle betrieben wird, zur Ergänzung des dortigen Datenbestandes einen Fragebogen an die Angehörigen bzw. Betreuer der in der Einrichtung betreuten psychisch und physisch behinderten Menschen zur Ausfüllung übergeben hat. In dem Fragebogen sollten neben allgemeinen Grunddaten auch Angaben zur Behinderung, zu chronischen Erkrankungen des Betreuten, erforderlichen Hilfsmitteln, Kontaktpersonen sowie zur medizinischen Betreuung (behandelnde Ärzte, erfolgte Impfungen sowie zu verabreichende Medikamente) gemacht werden. In der Anfrage wurde insbesondere bemängelt, dass keinerlei datenschutzrechtliche Hinweise auf dem Fragebogen angebracht seien sowie dass nicht für alle Angaben eine Erforderlichkeit erkennbar sei. Daraufhin wurde im Rahmen eines Kontrollbesuchs in der Rehabilitationswerkstätte die Erforderlichkeit der einzelnen Angaben hinterfragt. Im Ergebnis war festzustellen, dass die im Fragebogen begehrten Daten zum größten Teil für die Betreuung der behinderten Menschen in der Einrichtung erforderlich sind. So sind bspw. Angaben über den betreuenden Arzt erforderlich, um im Notfall mit diesem Kontakt aufnehmen zu können. Entsprechendes gilt für die Angaben von Behinderungen und chronischen Erkrankungen, um dies bei der Rehabilitationsarbeit in der Einrichtung zu berücksichtigen. Auch Angaben zu Impfungen gegen Tetanus sowie Hepatitis A und B sind sowohl im Interesse der Betreuten als auch der Einhaltung lebensmittelrechtlicher Vorschriften erforderlich, da die Werkstätte u. a. auch im Bereich der Lebensmittelverpackung tätig ist. Darüber hinaus enthielt jedoch der Bogen auch eine Zahl von Angaben, die zwar nützlich jedoch nicht als zwingend erforderlich anzusehen waren. Hierzu gehört bspw. die Angabe der Konfession oder der Nationalität. Diese Angaben sind auf Anregung des TLfD in dem Fragebogen nunmehr als freiwillig gekennzeichnet. Entscheidender war jedoch, dass die in dem Fragebogen erhobenen z. T. sensiblen personenbezogenen Daten des Betroffenen neben der Nutzung für die Durchführung der beruflichen Rehabilitation in der Werkstätte im Einzelfall auch mit Einwilligung des Betroffe-

nen an Dritte (z. B. Kostenträger oder behandelnde Ärzte) übermittelt werden sollen. Nach § 26 ThürDSG i. V. m. § 4 a Abs. 1 BDSG setzt eine wirksame Einwilligungserklärung insbesondere voraus, dass der Betroffene auf den Zweck der beabsichtigten Übermittlung so konkret wie möglich hingewiesen wird. Auf Hinweis des TLfD hat die Rehabilitationseinrichtung eine Einwilligungserklärung aufgenommen, aus der sich jedenfalls beispielhaft ergibt, an welchen potentiellen Adressatenkreis und für welche Einzelzwecke im Rahmen der Durchführung der beruflichen Rehabilitation eine Übermittlung erfolgen darf. Gleichzeitig wurde eine Erklärung aufgenommen, wonach die in dem Fragebogen angegebenen Ärzte von ihrer Schweigepflicht entbunden werden, soweit dies für die Durchführung der beruflichen Rehabilitation erforderlich ist. Damit wird sowohl dem berechtigten Anliegen der Werkstätte, die erforderlichen Informationen zur optimalen Betreuung des Betroffenen zu erhalten als auch der notwendigen Transparenz gegenüber diesem Rechnung getragen.

12. Wirtschaft, Arbeit, Bau und Verkehr

12.1 Unzulässige Datenvorratshaltung durch Gewerbeamt

Ein Bürger wandte sich an den TLfD und beschwerte sich darüber, dass das Gewerbeamt zur Prüfung seiner wirtschaftlichen Verhältnisse eine umfassende Offenlegung seiner gesamten Einkommens- und Vermögensverhältnisse verlangte. Hintergrund hierfür war die Antragstellung des Beschwerdeführers auf Erteilung einer Erlaubnis nach § 34 c GewO. Für diese Maßnahme muss das Gewerbeamt gemäß des Thüringer Verwaltungskostengesetzes (ThürVWKostG) eine Rahmengebühr festlegen. Im konkreten Fall machte der Antragsteller gegenüber dem Gewerbeamt geltend, dass nach seiner Auffassung das Gewerbeamt ohne konkrete Prüfung der Umstände seines Einzelfalls eine Pauschalgebühr festgelegt hatte, die dem arithmetischen Mittel der vorgesehenen Rahmengebühr entspricht. Daraufhin forderte das Gewerbeamt den Petenten auf, seine gesamten Einkommens- und Vermögensverhältnisse einschließlich aller zu tätigenden Ausgaben darzulegen. Dabei hatte sich das Amt auf § 9 Nr. 3 ThürVWKostG berufen, wonach die Rahmengebühr u. a. nach den wirtschaftlichen Verhältnissen des Gebührenschuldners zu bemessen ist.
In der Stellungnahme des TLfD gegenüber der Gewerbebehörde wurde darauf hingewiesen, dass nach § 9 ThürVWKostG die Rahmengebühr nach der Bedeutung des Gegenstandes und dem wirtschaftlichen Nutzen für die Beteiligten, nach der mit der Amtshandlung verbundenen Müheverwaltung zu bemessen ist. Die Prüfung der wirtschaftlichen Verhältnisse stellt lediglich ein weiteres Bemessungskriterium dar. Bei der Prüfung der wirtschaftlichen Verhältnisse des Gebührenschuldners ist die Verhältnismäßigkeit der Maßnahme zu beachten. Im vorliegenden Fall hielt der TLfD das Erheben von Kosten, die dem Antragsteller z. B. für Versicherungsprämien, Telefon- oder Betriebskosten entstehen, zur Festsetzung einer Rahmengebühr nicht für erforderlich.
Die Gemeinde teilte dem TLfD mit, dass sie sowohl bei dem Petenten als auch in zukünftigen Fällen auf das Erheben dieser Daten verzichtet. Damit ist dem Anliegen des Petenten Rechnung getragen worden.

12.2 Thüringer Verordnung zur Durchführung des Thüringer Gesetzes über die Öffentlich bestellten Vermessungsingenieure

Nach In-Kraft-Treten des Thüringer Gesetzes über die Öffentlich bestellten Vermessungsingenieure (ThürGÖbVI), das Teil des Thüringer Gesetzes zur Neuorganisation des Kataster- und Vermessungswesens vom 22. März 2005 war, war dem TLfD der Entwurf einer Thüringer Verordnung zur Durchführung des Gesetzes über die Öffentlich bestellten Vermessungsingenieure (ThürDVOzGÖbVI) zur weiteren Umsetzung des Reformvorhabens im Kataster- und

Vermessungswesen zur Stellungnahme zugeleitet worden. Die Ausführungen des TLfD zur Personalaktenführung durch die Öffentlich bestellten Vermessungsingenieure zu den bei ihnen Beschäftigten haben in der im GVBl. 2005, S. 312 ff bereits veröffentlichten Fassung der Verordnung vom 4. August 2005 Berücksichtigung gefunden.
Weitere Bedenken wurden zu den von den Bewerbern zur Prüfung der persönlichen Bestellungsvoraussetzungen geforderten Unterlagen geäußert. Da die Bewerber mit der Bewerbung eine Auskunft der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes einreichen sollen, dass sich aus den erschlossenen Unterlagen keine Hinweise auf eine hauptamtliche oder inoffizielle Tätigkeit für den Staatssicherheitsdienst ergeben haben, stellte sich die Frage, ob eine solche Auskunft überhaupt oder rechtzeitig mit der Bewerbung eingereicht werden kann. Das Recht auf Auskunft für Betroffene ist in § 13 Stasi-Unterlagen-Gesetz geregelt. Nach Abs. 2 umfasst die Auskunft eine Beschreibung der zu der Person des Betroffenen vorhandenen und erschlossenen Unterlagen und eine Wiedergabe ihres wesentlichen Inhalts. Sie kann aber zunächst auf Antrag des Betroffenen ausdrücklich auch auf die Prüfung und Mitteilung beschränkt werden, ob Unterlagen vorhanden sind, die auf eine hauptamtliche oder inoffizielle Tätigkeit des Betroffenen für den Staatssicherheitsdienst hinweisen. Da das zuständige TMBV nochmals die Erforderlichkeit der Auskunft begründet hat und eine angemessene Frist für die Vorlage von Bewerberunterlagen einräumen will, wird dem Anliegen Rechnung getragen.

12.3 Papierloses Verfahren zwischen Fahrerlaubnisbehörde und der DEKRA bei der Fahrerlaubnisprüfung

Das TMWAI hatte den TLfD über einen geplanten Pilotversuch zur elektronischen Datenübermittlung zwischen der Technischen Prüfstelle und den Fahrerlaubnisbehörden zur Durchführung der theoretischen und praktischen Fahrerlaubnis unterrichtet. Der TLfD hat den Pilotversuch, an dem acht Fahrerlaubnisbehörden teilgenommen haben, begleitet und hierzu auch eine Fahrerlaubnisbehörde kontrolliert.
Nach dem bisherigen herkömmlichen Verfahren finden die Datenübermittlungen entweder in Papierform oder per Diskette auf dem Postweg oder durch Botengang statt. Die Datenübermittlung ausschließlich auf elektronischem Wege stellt eine eGovernment-Anwendung dar, die von Anfang bis Ende „medienbruchfrei“ durchgeführt werden kann. Das nunmehr federführende TMBV verspricht sich hiervon eine Beschleunigung und Vereinfachung der verwaltungsinternen Vorgänge, aus denen sich Einsparpotentiale ergeben sollen. Allerdings muss nach wie vor eine Fahrerlaubnisakte angelegt werden, da der Bewerber für eine Fahrerlaubnis verschiedene Unterlagen in Papierform vorzulegen hat (z. B. Sehtestbescheinigung, Erste-Hilfe- Teilnahme-Bescheinigung, Lichtbild usw.). Derzeit wird dem Führerscheinerwerber nach bestandener Prüfung das Führerscheindokument noch nicht direkt übersandt, so dass dieses noch bei der Führerscheinstelle abgeholt werden muss. In der Zwischenzeit erhält der Fahrerlaubnisinhaber eine vorläufige, begrenzt gültige Fahrerlaubnisbestätigung.
Der TLfD hat bei dem Pilotprojekt insbesondere die Einhaltung der gemäß § 9 ThürDSG erforderlichen technischen und organisatorischen Maßnahmen kontrolliert. Da die Datenübermittlungen über das Internet erfolgen, war es unumgänglich, hierbei ein entsprechendes Verschlüsselungsverfahren anzuwenden. Die Verbindung wird mit einer SSL-128 Bit-Verschlüsselung durchgeführt, die nach dem derzeitigen Stand der Technik als angemessen gilt.
Bei der datenschutzrechtlichen Kontrolle in der Fahrerlaubnisbehörde wurde festgestellt, dass bislang Löschungsfristen für die Übertragungsdatensätze fehlen. Nach Mitteilung des TMBV gibt es hierzu keine Festlegungen. Die Löschfristen sollen daher in einer gemeinsamen Runde zwischen dem TMBV und den Fahrerlaubnisbehörden erarbeitet werden.

12.4 Unzulässige oder Überschussdaten bei der Verwarnung aufgrund einer Verkehrsordnungswidrigkeit

Aufgrund einer Verkehrsordnungswidrigkeit erhielt eine Fahrzeughalterin eine schriftliche Verwarnung vom Thüringer Polizeiverwaltungsamt - Zentrale Bußgeldstelle. Im Adressfeld war ungewöhnlicherweise auch der Geburtsname der Betroffenen mit dem Zusatz „u. a." angegeben. Das Schreiben enthielt auch noch den Namen des Ehegatten und eine Ortsangabe unter dem Geburtsdatum. Seine schriftliche Beschwerde, dass er pauschal als möglicher Verursacher bei der Zentralen Bußgeldstelle geführt werde, wurde vom TLfD zum Anlass einer Nachfrage an die Zentrale Bußgeldstelle genommen, weshalb diese Daten angegeben sind und woher sie stammen. Die Zentrale Bußgeldstelle erklärte, diese Daten per Datenfernleitung vom Kraftfahrtbundesamt erhalten zu haben. Die rückübermittelten Halterdaten würden automatisch in den Anhörungsbogen gedruckt und unmittelbar übersandt. Eine Einflussnahme eines Mitarbeiters der Zentralen Bußgeldstelle sei nicht möglich. Da die genannte Darstellung der personenbezogenen Daten völlig unüblich und nach Meinung der Zentralen Bußgeldstelle gleichfalls rechtlich zu beanstanden waren, verwies es an die Daten erhebende Stelle, nämlich die für die Betroffenen zuständige Kraftfahrzeugzulassungsstelle. Eine dort durchgeführte datenschutzrechtliche Kontrolle ergab, dass in dem Antrag auf Zulassung des betroffenen Fahrzeugs zwei Halter angegeben worden waren. Da die damals eingesetzte Software einen zweiten Halter nicht vorgesehen hatte, hat man dem Namen der Ersthalterin den Geburtsnamen beigefügt und mit dem Zusatz „u. a." versehen, was bedeutet, dass mehrere Halter des Fahrzeugs existieren. An der für den Geburtsnamen vorgesehenen Stelle wurde der vollständige Name des Ehegatten als Zweithalter eingefügt. Der gesamte Eintrag zu den Fahrzeughaltern wurde an das Kraftfahrtbundesamt übermittelt. Bei der Halterabfrage wurde von dort somit auch der Geburtsname als Bestandteil der Adresse mitgeteilt. Das zwischenzeitlich eingesetzte Verfahren enthält nunmehr die Möglichkeit, einen Zweithalter gesondert einzutragen. Unmittelbar im Anschluss an die Kontrolle wurde die Korrektur zu den Betroffenen vorgenommen.
Die stichprobenweise Einsicht in weitere Datensätze ergaben keine Hinweise auf entsprechende Handhabungen, sodass davon ausgegangen werden kann, dass es sich aufgrund der Konstellation nur um wenige Ausnahmefälle handelt, bei denen es zu Fehleintragungen kommen konnte.
Im Ergebnis der Kontrolle wurde auch gefordert, den Dateiinhalt des zum Einsatz kommenden Verfahrens zur Erfassung der Halterdaten zur Aufnahme in das Verfahrensverzeichnis nach § 10 ThürDSG nochmals zu überprüfen und den Vorgaben entsprechend zu überarbeiten. Dem ist die Stelle nachgekommen.
Wenn jedoch für ein Fahrzeug mehrere Halter eingetragen sind, werden diese im Falle eines Verkehrsverstoßes auch zukünftig im Rahmen einer Halterabfrage von der zuständigen Verfolgungsbehörde einbezogen werden. Dies entspricht den Vorschriften und unterliegt keinen datenschutzrechtlichen Bedenken.

12.5 Übermittlung von Personaldaten an die Fahrerlaubnisbehörde

Nach einer längeren Krankheit eines Mitarbeiters in einer Kommune wurde festgestellt, dass aufgrund der eingetretenen gesundheitlichen Einschränkungen ein weiterer Einsatz als Selbstfahrer nicht mehr möglich ist. In diesem Zusammenhang wurde die Frage aufgeworfen, ob und unter welchen Voraussetzungen die Übermittlung von Personaldaten durch das Personalamt an das Ordnungsamt bzw. die Führerscheinstelle für eine eventuelle Überprüfung der Fahrtauglichkeit möglich sei. Hierzu wurde folgende Auffassung vertreten: Gemäß § 97 Abs. 1 ThürBG dürfen Personalaktendaten nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in die anderweitige Verwendung ein. Nach Abs. 3 dürfen auch nur diejenigen Beschäftigten einer öffentlichen Stelle Zugang zu Personal-

akten und somit zu den entsprechenden Daten haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur soweit dies zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Aufgrund dieser abschließenden Regelung ist das Personalamt nicht berechtigt, von sich aus anderen Stellen auch innerhalb der Verwaltung über persönliche Sachverhalte der Beschäftigten zu informieren, soweit dies nicht im Rahmen der Personalverwaltung oder -bewirtschaftung erforderlich ist. Daher ist bei entsprechenden Hinweisen auf eine mögliche Fahruntüchtigkeit sicher angezeigt und notwendig, den jeweiligen Vorgesetzten eines Beschäftigten darüber zu informieren, dass Bedenken gegen den weiteren Einsatz des Mitarbeiters als Selbstfahrer bestehen. Falls die Führung des Kfz zu den vereinbarten Arbeitsaufgaben zählt, wäre dies ggf. auch mit einer amtsärztlichen Untersuchung zu verbinden. Eine Erforderlichkeit zur Einbeziehung der für den Wohnort des Mitarbeiters zuständigen Führerscheinstelle besteht zur Klärung der arbeitsrechtlichen Fragen nicht. Eine zulässige zweckfremde Verarbeitung der Personaldaten wäre lediglich zur Abwehr einer unmittelbar drohenden Gefahr für die öffentliche Sicherheit (vgl. § 20 Abs. 2 Nr. 6 ThürDSG sowie § 34 StGB) gegeben. Damit besteht durchaus eine „Ausnahmeregelung“, die aber an besonders strenge Voraussetzungen geknüpft ist. Der Besitz eines Führerscheins allein stellt sicherlich noch keine unmittelbar drohende gegenwärtige Gefahr dar, die eine Übermittlung von Personaldaten an das jeweilige Ordnungsamt rechtfertigen kann. Hierzu bedarf es nicht nur weiterer Erkenntnisse und Gründe für die tatsächlich bestehende unmittelbare Verkehrsgefährdung, sondern insbesondere auch einer sachgerechten Entscheidung des geeigneten Adressaten einer solchen Information. Dies dürfte zur Unterbindung einer unmittelbar bestehenden Verkehrsgefährdung (z. B. bei der Führung eines Fahrzeugs unter Drogen oder Alkohol) in der Regel nur die Polizei sein. Eine Unterrichtung der Führerscheinstelle wäre dann durch die Vollzugsbeamten, nicht jedoch durch das Personalamt gegeben.

12.6 Einbestellung eines Führerscheininhabers bei einer Fahrerlaubnisbehörde ohne Rechtsgrundlage

Ein Bürger beschwerte sich gemäß § 11 ThürDSG darüber, dass er von der Fahrerlaubnisbehörde eines Landratsamtes auf Grund einer Mitteilung einer Grenzpolizeistelle vorgeladen wurde, ohne ihn vom Inhalt dieser Übermittlung zu informieren. Der TLfD hatte sich daraufhin schriftlich an die Fahrerlaubnisbehörde gewandt und um Mitteilung zum konkreten Sachverhalt sowie zur Rechtsgrundlage gebeten. In dem Antwortschreiben der Behörde wurde die Meinung vertreten, dass der Petent nicht zur Vorsprache aufgefordert, sondern um die Kontaktaufnahme in seinem eigenen Interesse gebeten worden sei. Auskünfte aus der Fahrerlaubnisakte wollte die Fahrerlaubnisbehörde im Übrigen dem TLfD nicht erteilen.
Daraufhin wurde im Landratsamt eine datenschutzrechtliche Kontrolle durchgeführt, wobei Einsicht in die Fahrerlaubnisakte des Betroffenen genommen und der Inhalt geprüft wurde. Die Akte enthielt neben den üblichen Bestandteilen auch Unterlagen im Zusammenhang mit einer Dienstaufsichtsbeschwerde, der datenschutzrechtlichen Kontrolle sowie eine Mitteilung der Grenzpolizei. Danach wurde bei einer Grenzkontrolle des Betroffenen, dem zuvor die inländische Fahrerlaubnis entzogen worden war, Unterlagen zu einem Antrag auf eine ausländische EU-Fahrerlaubnis gefunden.
Nach Auffassung der Fahrerlaubnisbehörde sei sie verpflichtet gewesen, den Betroffenen auf die Folgen des Erwerbs einer ausländischen Fahrerlaubnis hinzuweisen und in Erfahrung zu bringen, ob er bereits die ausländische Fahrerlaubnis besitzt. Danach sei ggf. über einen Entzug der Fahrerlaubnis zu entscheiden gewesen.
Nach § 46 Absatz 5 Satz 2 Fahrerlaubnisverordnung (FeV) erlischt das Recht zum Führen von Kraftfahrzeugen im Inland mit einer ausländischen Fahrerlaubnis, wenn dem Betroffenen die Fahrerlaubnis in der Bundesrepublik entzogen wurde. Liegt eine Sperrfrist für die Wiedererlangung einer Fahrerlaubnis vor, ist das Führen eines Kraftfahrzeugs in der Bundesrepublik mit

einem ausländischen EU-Führerschein gemäß § 28 Abs. 4 Nr. 3 FeV als Fahren ohne gültigen Führerschein zu werten. In einer vom Thüringer Ministerium für Bau und Verkehr am 21.07.2004 auf der Grundlage des Urteils des EuGH vom 29.04.2004 über die Anerkennung von im Ausland unter Verstoß gegen das Wohnortprinzip erworbenen Führerscheinen erlassenen Verwaltungsvorschrift werden die Fahrerlaubnisbehörden angewiesen, in diesen Fällen das Kraftfahrtbundesamt über den Sachverhalt mit der Bitte zu informieren, die jeweilige ausländische Ausstellungsbehörde um Rücknahme des Führerscheins zu ersuchen.
Im Ergebnis der Kontrolle im Landratsamt wurde festgestellt, dass die Unterlagen zur Dienstaufsichtsbeschwerde und zur datenschutzrechtlichen Überprüfung sowie die Mitteilung der Grenzpolizei nicht die Fahrerlaubnis betreffen. Die geforderte Entfernung dieser Unterlagen aus der Führerscheinakte ist inzwischen erfolgt.

13. Bildung, Wissenschaft, Forschung

13.1 Thüringer Lehr- und Lernmittelverordnung

Das TKM hatte dem TLfD den Entwurf zur Änderung der Thüringer Lehr- und Lernmittelverordnung mit der Bitte um Prüfung zugesandt. Gemäß § 12 a der Verordnung werden die Eltern und volljährigen Schüler an den Kosten der Lernmittelfreiheit mit einem Eigenanteil, der sog. Lernmittelpauschale beteiligt. Wenn Familien bestimmte Sozialleistungen beziehen, werden die Betroffenen von der Zahlung dieser Pauschale auf Antrag befreit. Haben Familien mehrere Kinder, so wird die Pauschale auf Antrag ermäßigt. Das Vorliegen der jeweiligen Voraussetzungen ist von den Betroffenen nachzuweisen.
Aus datenschutzrechtlicher Sicht bestanden hiergegen zunächst keine Bedenken, da das Nähere zur Nachweisführung der Befreiungs- und Ermäßigungstatbestände im Zusammenhang mit der zu erhebenden Lehrmittelpauschale gesondert in noch zu erlassenden Durchführungsbestimmungen geregelt werden sollte. Der TLfD bat um weitere Beteiligung an dem Verfahren.
Eine Nachfrage beim TKM ergab später, dass die Durchführungsbestimmungen zwischenzeitlich ohne vorherige Beteiligung des TLfD erlassen wurden. Dem TLfD lagen zu dieser Zeit im Zusammenhang mit der Verordnung bereits sowohl mehrere Beschwerden von betroffenen Eltern und Lehrern als auch Anfragen von der Presse vor.
In einer Stellungnahme gegenüber dem TKM wurde der Erlass der Durchführungsbestimmungen ohne die vorherige Einbeziehung des TLfD kritisiert und im Übrigen auf die fehlenden Regelungen beim Umgang mit den Nachweisen für eine Befreiung von der Lernmittelpauschale bzw. für eine ermäßigte Pauschale hingewiesen. Der TLfD forderte das TKM auf, die Durchführungsbestimmungen dahingehend zu ergänzen, dass nicht, wie teilweise vorgesehen, jedem Klassenleiter, sondern ausschließlich dem Schulleiter selbst und höchstens zwei von ihm beauftragten Personen die Befreiungs- bzw. Ermäßigungsnachweise vorzulegen sind. Darüber hinaus wurde auf fehlende Hinweise aufmerksam gemacht, wonach von den Betroffenen auf den Nachweisen nicht erforderliche Angaben geschwärzt und die Anträge in verschlossenen Briefumschlägen in der Schule abgegeben werden sollten. Auch wurde auf die fehlenden Regelungen hingewiesen, dass die Nachweise nach Prüfung den Betroffenen (insbesondere bei Originalen) zurückzugeben ansonsten zu vernichten sind und wie die anschließende Verfahrensweise der Dokumentation über die erfolgte Nachweisvorlage und der Abgleich mit dem korrekten Zahlungseingang zu gestalten ist.
Die Forderungen des TLfD wurden durch entsprechende Ergänzungen zu den Durchführungsbestimmungen vom TKM umgesetzt.
Um sich eine Übersicht darüber zu verschaffen, wie die Schulen in der Praxis die geänderte Thüringer Lehr- und Lernmittelverordnung umsetzen, führte der TLfD kurzfristig in Schulen mehrerer Schulamtsbereiche Kontrollen durch. Im Ergebnis wurde festgestellt, dass in den Schulen Unsicherheit darüber bestand, wie sich der Umgang mit den Nachweisen nach der

Einordnung in eine der Fallgruppen zur Festlegung der Höhe der Lernmittelpauschale gestalten soll. Nicht selten wurden die Unterlagen weiterhin von der Schule gespeichert. Der TLfD wies in diesen Fällen auf die ergänzten Durchführungsbestimmungen hin und forderte die Schule auf, nach Prüfung und Bestätigung der jeweiligen Fallgruppe die Nachweise umgehend und vollständig zu vernichten. Die Schulen kamen der Forderung kurzfristig nach.

13.2 Erhebung von Notfalldaten der Schüler an den Schulen

Im Berichtszeitraum erhielt der TLfD die Anfrage, ob Eltern verpflichtet seien, in eine sog. Notfallkarte, die für ihr Kind an der Schule geführt werde, ihre Arbeitsstätten, ihre Krankenkasse und die Tatsache, dass der Schüler familienversichert sei, einzutragen. Begründet wurde auf meine Anfrage die Erforderlichkeit für die Datenerhebung von der Schule und dem Schulamt damit, dass die Kenntnis der Arbeitsstelle zur Herstellung eines Kontaktes im Notfall und Angaben zur Krankenversicherung bei Rettungsdiensteinsätzen von den Hilfskräften und bei einem Unfall von der Unfallkasse benötigt werden.
Hierzu wurde festgestellt, dass gemäß § 136 ThürSchulO von der Schule lediglich Daten zur Herstellung des Kontaktes in Notfällen zu erheben sind. Dabei entscheidet der Sorgeberechtigte, auf welche Art und Weise (über Kontaktpersonen, Betriebs- oder Privatanschriften oder Kommunikationseinrichtungen, wie Telefon, Fax o. ä.) er im Notfall am schnellsten erreicht werden kann und teilt dies der Schule mit. Eine Pflicht zur Mitteilung der Arbeitsstelle gegenüber der Schule besteht nicht und wäre insbesondere bei bestimmten Tätigkeiten (z. B. bei einem Nachtpförtner) auch nicht gerechtfertigt. Zur Frage der Erhebung und Vorhaltung der Kassenzugehörigkeit der Schüler an den Schulen teilte mir das zuständige kommunale Amt für den Rettungsdienst mit, dass eine entsprechende Forderung zur vorsorglichen Erhebung der Daten für einen möglichen Rettungsdiensteinsatz nicht bestehen würde und die Kenntnis lediglich bei der Rechnungslegung von Vorteil sein könne. Bezüglich der Unfallmeldung erklärte die Unfallkasse, dass seit dem 1. August 2002 mit der Einführung eines neuen bundeseinheitlichen Vordrucks zur Erhebung und Feststellung von Leistungen und Abrechnungen mit Leistungserbringern (Unfallanzeige für Kinder in Tageseinrichtungen, Schüler, Studierende) auf die Erhebung der Kassenzugehörigkeit verzichtet wird.
Aufgrund der vorgenannten Erkenntnisse wurde die betreffende Schule aufgefordert, die Notfallkarte entsprechend den gesetzlichen Vorgaben zu ändern, was auch erfolgte.

13.3 Regelungen bei Sportunfällen von Schülern

Eine Beschwerde hatte das Auskunftsrecht zu einem 1991 im Sportunterricht erlittenen Unfall zum Gegenstand. Der Petent benötigte in einem sozialgerichtlichen Verfahren Nachweise dafür, dass der Sportunfall Ursache für eine gesundheitliche Beeinträchtigung gewesen ist.
In der in der Schule durchgeführten datenschutzrechtlichen Kontrolle wurden die zum Unfall aufbewahrten Unterlagen geprüft. Zu der Frage des Petenten, weshalb im Unfallbuch der Schule ein anderer Zeitpunkt angegeben ist als in den ärztlichen Aufzeichnungen, konnte keine Erklärung gegeben werden. Jedoch konnte die Möglichkeit einer Manipulation des Unfallbuches ausgeschlossen werden.
Gemäß der für 1991 gültigen Schulordnung des Thüringer Kultusministeriums waren in den Schülerbögen die für den Bildungsweg wesentlichen Feststellungen, Beobachtungen und Empfehlungen aufzunehmen. Demgegenüber enthielt der vom Petenten in Kopie vorgelegte Schülerbogen keine Eintragungen, obwohl sich seine schulischen Leistungen nach dem Unfall maßgeblich verschlechtert hatten. Dies ist als ein Unterlassen einer erforderlichen Verarbeitung von Schülerdaten anzusehen, was als eine Verletzung datenschutzrechtlicher Vorschriften gewertet wurde. Es wurde gefordert, zu gewährleisten, dass künftig die Schülerbögen entsprechend der Vorschriften der Thüringer Schulordnung ausgefüllt werden. Darauf hin teilte die Schulleitung

mit, dass die Lehrer auf die Verpflichtung hingewiesen wurden und jeder Klassenleiter hierfür verantwortlich sei.

13.4 Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten mit Einwilligung der Betroffenen verarbeitet. Nach der derzeitigen Rechtslage verlieren diese Daten nach einer Übermittlung an den Forscher regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Dies halten die DSB des Bundes und der Länder für unbefriedigend und haben sich in einer Entschließung (Anlage 3) auf der Konferenz der DSB des Bundes und der Länder am 25./26. März 2004 für die Einführung eines Forschungsgeheimnisses für medizinische Daten ausgesprochen. In einer ersten Stellungnahme hat das Bundesministerium der Justiz zwar zugesagt, gesetzgeberischen Handlungsbedarf hinsichtlich der Normierung der Strafbarkeit der unbefugten Offenbarung personenbezogener medizinischer Forschungsdaten zu prüfen. Allerdings werde eine Änderung der StPO zur Einführung eines Zeugnisverweigerungsrechts für Forscher und deren Berufshelfer sowie das damit zusammenhängende Beschlagnahmeverbot medizinischer Forschungsdaten nicht erwogen, weil es hierfür kein besonders schützenswertes Vertrauensverhältnis zwischen Forschern und den Betroffenen gebe.

13.5 Leistungsvergleiche und wissenschaftliche Untersuchungen an Schulen

Immer öfter erhalten die Eltern schulpflichtiger Kinder von der Schule einen Brief, in dem ihnen mitgeteilt wird, dass ihr Kind an der Schule an einem Leistungsvergleich teilnehmen wird oder an einer wissenschaftlichen Untersuchung mitwirken soll. Dabei gibt es seit dem Jahr 2003 eine Änderung dahingehend, dass die Teilnahme der Kinder nicht mehr generell von der Entscheidung der Sorgeberechtigten abhängig ist. Durch eine Neufassung des § 57 Thüringer Schulgesetz (ThürSchulG) kann nunmehr das TKM bei internationalen, nationalen oder regionalen Vergleichsuntersuchungen, die auf seine Veranlassung in den Schulen durchgeführt werden, eine Auskunftspflicht für das Schulpersonal, die Schüler und deren Eltern festlegen. Von dieser Möglichkeit wird insbesondere bei den zwischenzeitlich allseits bekannten PISA-Tests in Thüringen Gebrauch gemacht, in dem durch eine Teilnahmepflicht des Schulpersonals und der Schüler an diesem Leistungsvergleich die Repräsentativität der Ergebnisse in jedem Fall gewährleistet wird. Dies bedeutet jedoch nicht, dass deshalb der Datenschutz weniger Beachtung findet. Wie bei den bisherigen Tests ist festzustellen, dass von der Projektbetreuung des Leibnitz-Instituts für Pädagogik der Naturwissenschaften an der Universität Kiel und dem TKM den datenschutzrechtlichen Fragen bei der Vorbereitung und Durchführung der Leistungsvergleiche durchaus die gebotene Aufmerksamkeit geschenkt wird. Dieses Interesse zeigt sich insbesondere dadurch, dass in Vorbereitung des Haupttests der dritten PISA-Erhebung für das Jahr 2006 sowie des Feldtests 2005 in 5 Bundesländern (darunter Thüringen) die Unterlagen dem TLfD rechtzeitig und umfassend zur datenschutzrechtlichen Beurteilung zur Verfügung gestellt und die in der Folge gegebenen Anregungen auch aufgegriffen und beachtet wurden. Diese Hinweise betrafen den Inhalt der Informationsschreiben zur Aufklärung der Teilnehmer am Leistungsvergleich und Fragen zur konsequenten Durchsetzung der gegenüber den Eltern und Schülern versicherten Vertraulichkeit ihrer Angaben, um eine Kenntnisnahme einzelner Ergebnisse oder des Inhalts von Fragebögen durch das Schulpersonal auszuschließen.
Neben den Leistungsvergleichen (wie z. B. PISA) werden im Kultusbereich auch andere wissenschaftlichen Untersuchungen durchgeführt, für die keine Teilnahmepflicht für das Schulpersonal bzw. die Schüler besteht. So beteiligen sich derzeit auch Thüringer Schulen an einer bundesweiten „Studie zur Entwicklung von Ganztagsschulen“ (StEG), die vom Deutschen Institut für Internationale Pädagogische Forschung (DIPF), dem Deutschen Jugendinstitut (DJI) und

dem Institut für Schulentwicklungsforschung (IfS) im Auftrag des Bundesministeriums für Bildung und Forschung durchgeführt wird. Ziel der Studie ist es, Ergebnisse über Veränderungen an Schulen, die Ganztagsangebote eingeführt haben, zu erforschen, um daraus Empfehlungen zur künftigen Ausgestaltung dieser Angebote und der Arbeit an diesen Schulen abzuleiten. Die Besonderheit dieser Studie, an der sich insgesamt rund 500 Schulen beteiligen, besteht darin, dass es sich um eine Längsschnittuntersuchung handelt, bei der die gleichen Schüler, Eltern und Lehrer der Klassenstufen 3, 5, 7 und 9 insgesamt dreimal (2005, 2006 und 2008) befragt werden. Um zu erreichen, dass die einzelnen Angaben tatsächlich dem gleichen Schüler über den gesamten Zeitraum zugeordnet werden können, ohne dass der mit der Durchführung der wissenschaftlichen Studie betrauten Einrichtung die tatsächliche Identität des Schülers bekannt wird, erhält jeder Schüler von der Schule eine individuelle Identifikationsnummer. Die damit zusammenhängenden datenschutzrechtlichen Fragen wurden im Vorfeld der Studie mit den Landesdatenschutzbeauftragten umfassend erörtert. Im Ergebnis wurden den Projektverantwortlichen eine Vielzahl von Anregungen für eine datenschutzkonforme Verfahrensweise gegeben. In diesem Zusammenhang wurde auch deutlich gemacht, dass eine zu starke Differenziertheit der Antwortmöglichkeiten in den Fragebögen bei der Auswertung zu einer personenbezogenen Zuordnung führen kann, was in jedem Fall, z. B. durch höhere Aggregationsstufen, auszuschließen ist. Weitere Hinweise betrafen die Notwendigkeit einer umfassenden Information der Beteiligten über das Verfahren und die Freiwilligkeit ihrer Mitwirkung sowie Fragen zur Gewährleistung der Vertraulichkeit, die alle von der Projektleitung aufgegriffen und berücksichtigt wurden.

13.6 Datenabgleiche zwischen den Ämtern für Ausbildungsförderung und dem Bundesamt für Finanzen

Wie bereits ausführlich im 5. TB unter 13.4 dargestellt, hatte der TLfD gegenüber dem TMWFK die Rechtsauffassung vertreten, dass die Durchführung des regelmäßigen Datenabgleichs aller BAföG-Empfänger zwischen den Ämtern für Ausbildungsförderung und dem Bundesamt für Finanzen zur Feststellung, ob Zinseinkünfte bei den BAföG-Empfängern angefallen sind, als bedenklich anzusehen ist. Erst mit dem 21. Gesetz zur Änderung des BAföG vom 02.12.2004 (BGBl. I S. 3127) wurde in § 41 Abs. 4 BAföG nachträglich eine Regelung geschaffen, die den Datenabgleich erlaubt. Ab dem Jahre 2005 sind die Datenabgleiche aus datenschutzrechtlicher Sicht damit zulässig. Wie die Abgleiche der Jahre 1999 bis 2004 ergeben haben, erfolgte der Leistungsmissbrauch in einem solchen Umfang, dass die Durchführung von Stichproben oder die Überprüfung von Verdachtsfällen kein geeignetes Mittel mehr darstellten. Der TLfD hat daher seine datenschutzrechtlichen Bedenken zurückgestellt.
In diesem Zusammenhang wurde ein Amt für Ausbildungsförderung kontrolliert. Dabei stellte sich heraus, dass der Stelle nicht bekannt war, aufgrund welcher Veranlassung das Thüringer Landesrechenzentrum die Daten der BAföG-Empfänger an das Bundesamt für Finanzen zum Zwecke des Datenabgleichs übermittelt. Der TLfD hatte im Anschluss an die Kontrolle das TKM um eine Übersendung der Auftragsdatenverarbeitung zwischen dem TKM als Auftraggeber und dem TLRZ als Auftragnehmer gebeten. Wie aus der Vereinbarung hervorging, stammt diese aus dem Jahre 1996. Da hierin die Auftragsdatenverarbeitung für den o. g. Datenabgleich nicht geregelt ist, bat ich das TKM um eine Änderung der vertraglichen Vereinbarung. Dies ist inzwischen auch erfolgt.

14. Landwirtschaft, Naturschutz und Umwelt

14.1 Getrennte Entgelte für Schmutz- und Niederschlagswasser

In Thüringen werden von immer mehr Gemeinden die Abwasserabgaben getrennt nach Entgelten für Schmutz- und Niederschlagswasser berechnet. Hierzu müssen von den Grundstückseigentümern Daten zu den bebauten und befestigten Flächen des jeweiligen Grundstücks erhoben werden. Damit folgen die Gemeinden mehreren Verwaltungsgerichtsentscheidungen, in denen festgestellt wird, dass die Splittung der Abwassergebühren in eine Schmutz- und eine Regenwassergebühr aus Gründen der Gebührengerechtigkeit und der Rechtssicherheit zwingend erforderlich ist.
Ein Wasser- und Abwasserzweckverband legte mir mit der Bitte um eine datenschutzrechtliche Prüfung den Entwurf eines Erhebungsbogens zur Einführung einer solchen gesplitteten Abwassergebühr vor. Obwohl der Bogen selbst, dem darüber hinaus ein ausführliches Erläuterungsblatt beigefügt war, hinsichtlich der darin erhobenen Grundstücksdaten grundsätzlich den datenschutzrechtlichen Anforderungen entsprach, fehlte ein entsprechender Hinweis nach § 19 Abs. 3 ThürDSG, aufgrund welcher Rechtsvorschrift die Grundstückseigentümer zur Auskunft verpflichtet sind. Wie sich herausstellte, enthielt die zu diesem Zeitpunkt gültige Beitrags- und Gebührensatzung des Zweckverbands keine Regelungen über die Splittung der Entgelte und die entsprechenden Berechnungsgrundlagen. Da die Verarbeitung und Nutzung personenbezogener Daten gemäß § 4 Abs. 1 ThürDSG nur zulässig ist, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat, war im vorliegenden Fall nicht von einer Mitwirkungspflicht der betroffenen Grundstückseigentümer auszugehen.
Der vom Zweckverband vertretenen Auffassung, dass sich aus § 15 Abs. 1 Nr. 3a ThürKAG i. V. m. §§ 90, 93 AO die Mitwirkungs- bzw. Auskunftspflicht für die Betroffenen ergibt, konnte ich nicht beitreten. Eine Mitwirkungspflicht nach diesen Vorschriften besteht nämlich nur dann, wenn ein Abgaben erheblicher Sachverhalt zu ermitteln ist. Wie bereits oben angeführt, war der Abgabentatbestand der Splittung von Schmutz- und Niederschlagswasser vom Zweckverband bis dahin aber nicht in der Satzung enthalten.
Im Vorfeld einer durch mich angekündigten Kontrolle des Zweckverbands, teilte dieser mir mit, dass in einer weiteren Satzungsänderung zwischenzeitlich die Festlegung getroffen wurde, getrennte Gebühren für die Einleitung von Schmutz- und Niederschlagswasser zu erheben. Somit besteht nunmehr eine Rechtsvorschrift, die die Grundstückseigentümer verpflichtet, die erforderlichen Angaben (z. B. Art und Größe der versiegelten Flächen) zur Berechnung insbesondere der Gebühren für die Einleitung des Niederschlagswassers gegenüber dem Zweckverband zu machen.
Darüber hinaus forderte ich als Ergebnis meines Kontrollbesuchs den Zweckverband auf, Lösch- bzw. Aufbewahrungsfristen sowohl für die in Papierform vorliegenden Erhebungsbögen als auch für die elektronisch gespeicherten Daten festzulegen, das automatisierte Verfahren gemäß § 34 Abs. 2 ThürDSG freizugeben, nach § 10 ThürDSG ein Verzeichnis über die vorhandenen automatisierten Verfahren zu führen und auf der Grundlage eines Sicherheitskonzeptes die nach § 9 Abs. 2 ThürDSG zu treffenden technischen und organisatorischen Maßnahmen schriftlich zu fixieren.
Im Ergebnis ist der Zweckverband allen datenschutzrechtlichen Forderungen nachgekommen.

14.2 Touristenzählung

Wie verschiedenen Presseartikeln zu entnehmen war, werden Touristen auf häufig frequentierten Wanderwegen von Walderholungsgebieten unter Verwendung einer Infrarot-Lichtschranke elektronisch gezählt. Der TLfD nahm die Information zum Anlass, beim TMLNU anzufragen,

ob bei diesem Verfahren das Erheben personenbezogener Daten ausgeschlossen ist. Wie sich herausstellte, werden die Zählungen lediglich durch die Unterbrechung des Infrarotstrahls ausgelöst, so dass personenbezogene Daten hierbei nicht erhoben werden.
Ergänzend teilte das Ministerium mit, dass für ein Projekt „Besuchermonitoring“ an jeweils einem bestimmten, touristisch genutzten Wanderweg zeitweise eine automatisierte Kamera installiert wird. Sobald eine Person in den Auslösebereich der Kamera gelangt, wird eine Aufnahme erstellt. Eine Identifizierung der mit der Kamera aufgenommenen Bilder ist aber nicht möglich, da bewusst nur unscharfe Bilder entstehen, wobei die Kamera in einem so großen Abstand zu dem betroffenen Wegrand installiert wird, dass die Personen nur sehr klein und im Profil abgebildet sind. Mit den Aufnahmen wird lediglich statistisch ausgewertet, auf welche Weise (Wanderer, Radfahrer, Reiter) durch wie viele Personen der jeweilige Weg genutzt wird. Die Kamerabilder werden nach der Auswertung gelöscht.
Datenschutzrechtliche Bedenken gegen das in der beschriebenen Weise praktizierte Verfahren hat der TLfD nicht, weil seine Forderungen, wonach sichergestellt sein muss, dass eine Identifizierung der Personen auf den Bildern ausgeschlossen ist, erfüllt sind.

Anlage 1

Entschließungen zwischen den Konferenzen 2004

Übermittlung von Flugpassagierdaten an die US-Behörden

(Umlaufentschließung/13. Februar 2004)

Die Datenschutzbeauftragten des Bundes und der Länder bestärken die Bundesregierung darin, sich für Verbesserungen des Datenschutzes bei der Übermittlung von Flugpassagierdaten an die Zoll- und Sicherheitsbehörden der USA einzusetzen.

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zoll- und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden z.B. Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrung wegen einer Erkrankung eines Fluggastes, Hotel- und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen.
Die US-Zollbehörden wollen alle Reservierungsdaten mindestens 3,5 Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere 8 Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. Septembers 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensichtlich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservierungsdatenbanken nicht für Sicherheitszwecke, sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerikanischen Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen. Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.

Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im sog. CAPPS II-System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten Abgleich mit Fahndungslisten als auch mit Informationen aus dem privaten Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die

Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Artikel 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29.01.2004 deutlich herausgearbeitet. Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zurzeit praktiziert wird, muss ausgeschlossen werden.

Anlage 2

Entschließung
der 67. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 25./26. März 2004 in Saarbrücken

Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

Anlage 3

Entschließung
der 67. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 25./26. März 2004 in Saarbrücken

Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnern und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden - anders als insbesondere den behandelnden Ärztinnen und Ärzten - nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

Anlage 4

Entschließung
der 67. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 25./26. März 2004 in Saarbrücken

Automatische Kfz-Kennzeichenerfassung durch die Polizei

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.

Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz- Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

Anlage 5

Entschließung
der 67. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 25./26. März 2004 in Saarbrücken

Personennummern

Das Bundesverfassungsgericht hat schon in seinem "Volkszählungsurteil" aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z.B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

Anlage 6

67. Konferenz der Datenschutzbeauftragten des
Bundes und der Länder
am 25./26. März 2004 in Saarbrücken

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder schließt sich voll inhaltlich der folgenden Entschließung an:

Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Entschließung zu Radio-Frequency Identification
vom 20. November 2003 (Übersetzung)

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

a. sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;
b. wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;
c. dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und
d. soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

Anlage 7

Entschließung
der 68. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. Oktober 2004 in Saarbrücken

Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum "großen Lauschangriff" in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des "unantastbaren Kernbereichs der privaten Lebensgestaltung" und die Bestimmung des Kreises der Menschen "des persönlichen Vertrauens" offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

Anlage 8

Entschließung
der 68. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. Oktober 2004 in Saarbrücken

Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

Anlage 9

Entschließung
der 68. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 28./29. Oktober 2004 in Saarbrücken

Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20.09.2004 sog. "Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II" zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

Anlage 10

Entschließungen zwischen den Konferenzen 2004/2005

Staatliche Kontenkontrolle muss auf den Prüfstand!

(Umlaufentschließung/26. November 2004)

Das "Gesetz zur Förderung der Steuerehrlichkeit" vom 23.12.2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z.B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.

Nunmehr sollen neben Finanzbehörden auch andere Behörden, z. B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das "an Begriffe des Einkommensteuergesetzes" anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von "Begriffen" verwendet (neben den Begriffen "Einkommen" und "Einkünfte" etwa auch "Wohnung", "Kindergeld", "Arbeitnehmer"), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z.B. anlässlich Steuererklärung, BaföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen.

Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Artikel 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

Anlage 11

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Bundesratsinitiative mehrerer Länder zur Ausweitung der DNA-Analyse 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 sog. 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.

Anlage 12

Entschließungen zwischen den Konferenzen 2004/2005

Einführung biometrischer Ausweisdokumente
(Umlaufentschließung/1. Juni 2005)

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützer 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.

Anlage 13

Entschließung
der 69. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 10./11. März 2005 in Kiel

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 Entschließungen 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 Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Anlage 14

Entschließung
der 69. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 10./11. März 2005 in Kiel

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 Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

Anlage 15

Entschließung
der 70. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. Oktober 2005 in der Hansestadt Lübeck

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.

Anlage 16

Entschließung
der 70. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. Oktober 2005 in der Hansestadt Lübeck

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 Löschungskonzept 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 Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

Anlage 17

Entschließung
der 70. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. Oktober 2005 in der Hansestadt Lübeck

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 privaten Callcentern 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.

Anlage 18

Entschließung
der 70. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. Oktober 2005 in der Hansestadt Lübeck

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.

Anlage 19

Entschließung
der 70. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. Oktober 2005 in der Hansestadt Lübeck

Telefonieren mit Internettechnologie (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 Internettelefonie 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 Datenschutzmängel, 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.

Anlage 20

Entschließung
der 70. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. Oktober 2005 in der Hansestadt Lübeck

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 Dammbruch zulasten des Datenschutzes unverdächtiger 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 Telekommuni-

kation 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 könnten. 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.

Anlage 21

Entschließung
der 70. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. Oktober 2005 in der Hansestadt Lübeck

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 intensivierte 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.

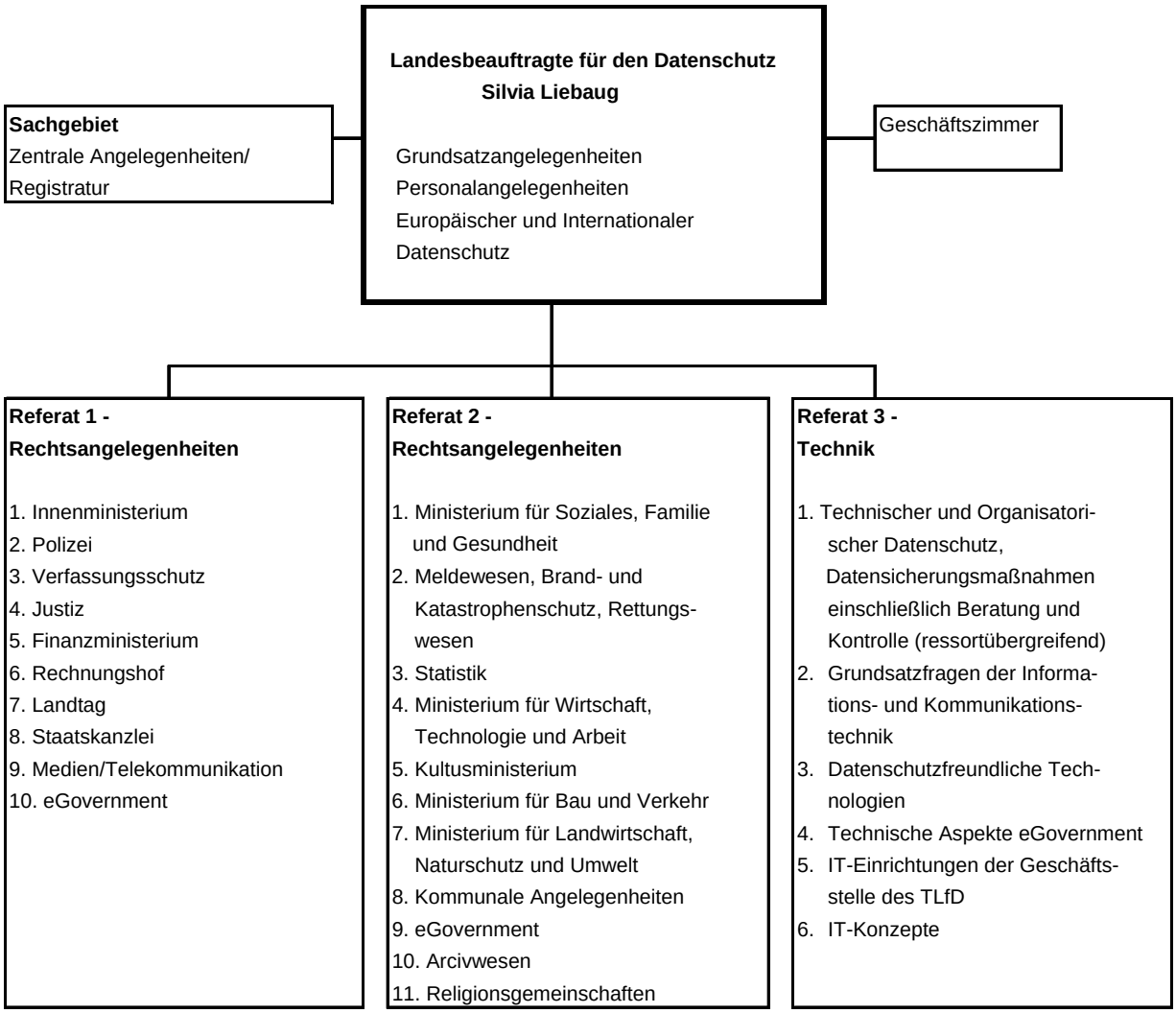
Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen 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.

Anlage 22

Thüringer Landesbeauftragter für den Datenschutz (TLfD)



Anschrift
Jürgen-Fuchs-Str. 1
99096 Erfurt

Postanschrift
PF 90 04 55
99107 Erfurt

Tel. 0361/37719-00
Fax 0361/37719-04
E-Mail:poststelle@datenschutz.thueringen.de
Internet: www.datenschutz.thueringen.de

Sachregister