

Vorwort

Der vorliegende 3. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz umfasst den Berichtszeitraum vom 1. Januar 1998 bis zum 31. Dezember 1999.

Er beinhaltet einen Überblick über aktuelle Themenbereiche und die Entwicklung des Datenschutzes und der Datensicherheit, wesentliche Erkenntnisse und Erfahrungen aus der Kontroll- und Beratungstätigkeit sowie Hinweise und Empfehlungen zu Verbesserungen des Datenschutzes.

Der Bericht wurde gem. § 40 Abs. 4 ThürDSG im Beirat vorberaten.

Erfurt, im Dezember 1999

Silvia Liebaug
Landesbeauftragte für den Datenschutz

3. Tätigkeitsbericht des TLfD

Berichtszeitraum vom 01.01.1998 bis 31.12.1999

Inhaltsverzeichnis

Abkürzungsverzeichnis

- 1. Einleitung**
 - 1.1 Die Dienststelle des TLfD**
 - 1.2 Der Beirat beim TLfD**
 - 1.3 Konferenzen und Arbeitskreise der DSB des Bundes und der Länder im Berichtszeitraum**
- 2. Europäischer Datenschutz**
 - 2.1 Die Umsetzung der EG Datenschutzrichtlinie in nationales Recht**
 - 2.2 Grundrecht auf Datenschutz in einer Charta der Grundrechte der EU**
 - 2.3 Europol**
 - 2.4 EG-Telekommunikationsdatenschutzrichtlinie**
 - 2.5 ENFOPOL**
 - 2.6 Entwurf eines Gesetzes zur Umsetzung von Richtlinien der Europäischen Gemeinschaft auf dem Gebiet des Berufsrechts der Rechtsanwälte**
 - 2.7 EG-Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen**
- 3. Datenschutz im Parlament**
 - 3.1 Verwaltungsvorschrift des TMJE zur Änderung der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) vom 25. Mai 1998 (4208-1/98) - JMBl 1998, Seite 22ff**

Mitteilung über Strafsachen gegen Abgeordnete
 - 3.2 Steht der „Datenschutz“ dem Informationsrecht der Abgeordneten im Wege?**
 - 3.3 Regelungen in der Geschäftsordnung des Thüringer Landtags zum Datenschutzbeauftragten**

- 4. Neue Medien - Multimedia**
- 4.1 **Vierter Rundfunkänderungsstaatsvertrag**
- 4.2 **Jugendschutz im Internet „jugendschutz.net“**
- 4.3 **Telekommunikationsdatenschutzverordnung (TDSV)**
- 4.4 **Telekommunikationsüberwachungsverordnung (TKÜV)**
- 4.5 **Oma's Geburtstag im Fernsehen**
- 4.6 **Elektronische Einwilligung vor der Veröffentlichung von personenbezogenen Daten im Internet**

- 5. Innenverwaltung - Kommunales - Sparkassen**
- 5.1 **Innenverwaltung**
- 5.1.1 **Entwurf für allgemeine Verwaltungsvorschriften zum Ausländergesetz (AuslG-VwV)**
- 5.1.2 **Neufassung der Verschlusssachenanweisung (VSA) für den Freistaat Thüringen und der ergänzenden Bestimmungen**
- 5.1.3 **Einführung einer Asylcard**
- 5.1.4 **Datenschutzrechtliche Kontrolle im Rahmen des Schengener Durchführungsübereinkommens (SDÜ) Ausschreibung zur Einreiseverweigerung im Schengener Informationssystem (SIS)**
- 5.1.5 **Kontrollen im Bereich Ausländerwesen**
- 5.1.6 **Verpflichtungserklärung zur Kostenübernahme nach § 84 Ausländergesetz (AuslG)**
- 5.1.7 **Auskunftserteilung bei „Scheinehe“-Verfahren**
- 5.1.8 **Kontrolle in einem Katasteramt**
- 5.1.9 **Kettenbriefe - ein Datenschutzproblem?**
- 5.1.10 **Aufbewahrung von Stasi-Überprüfungsakten**
- 5.2 **Kommunales**
- 5.2.1 **Übermittlung von Meldedaten an Adressbuchverlage**
- 5.2.2 **Übermittlung von Meldedaten an Parteien**
- 5.2.3 **Umgang mit Unterstützungsunterschriften bei Wahlen**
- 5.2.4 **Auslegung von Wählerverzeichnissen**
- 5.2.5 **Anhörungsbogen zur Bestimmung der Hauptwohnung**

- 5.2.6 Liste der Gewerbetreibenden von Gemeinde an Werbeagentur übergeben
- 5.2.7 Umgang mit Unterlagen nicht-öffentlicher Sitzungen
- 5.2.8 Tonaufnahmen von Kreistags- und Gemeinderatssitzungen
- 5.2.9 Unverhältnismäßige Fragen des Sozialamts zur eheähnlichen Gemeinschaft
- 5.2.10 Sozialhilfebeantragung durch Krankenhaus?
- 5.2.11 Beschriftung von Überweisungsträgern und Postsendungen
- 5.2.12 Rückgabe eines behördlichen Schreibens an den Adressaten
- 5.3 Sparkassen
- 5.3.1 Wechsel der Datenschutzkontrolle über die gemeinsame Sparkassenorganisation Hessen-Thüringen
- 5.3.2 Datenverarbeitung durch Sparkassen Versicherung
- 5.3.3 Datenverarbeitung von Sparkassen zur Kreditsicherung
- 6. Personalwesen
- 6.1 Personalaktenführungsrichtlinie
- 6.2 Personalakten im Justizbereich
- 6.3 Personalverwaltung der Lehrer
- 6.4 Beihilfearbeitung durch ein privatrechtliches Versicherungsunternehmen
- 6.5 Datenerhebung über Beschäftigungsverhältnisse von Ehepartnern durch die Oberfinanzdirektion Erfurt - Zentrale Gehaltsstelle - (ZG)
- 6.6 Verfahren bei Gehaltspfändungen
- 6.7 Verwaltungsvorschrift zur Thüringer Verordnung über Zuständigkeiten für die Feststellung, Berechnung und Anordnung der Zahlung der Bezüge von Bediensteten und Versorgungsempfängern (Thür-ZustVBezüge)
- 6.8 Rücksendung von Bewerbungsunterlagen
- 6.9 Abschottung der Arbeitsbereiche beim Polizeiärztlichen Dienst
- 6.10 Umgang mit Telefongesprächsdaten

- 7. Polizei**
- 7.1 Umgang mit Telefongesprächsdaten
- 7.2 Bundeseinheitliche Verwaltungsvorschriften für die Feststellung von Alkohol, Medikamenten und Drogen im Blut bzw. Urin bei Straftaten und Ordnungswidrigkeiten
- 7.3 Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (Prüffristenverordnung - PolPrüffristVO)
- 7.4 Verwaltungsvorschriften des TIM über die Aufgaben der Polizei bei der Verfolgung von Verkehrsverstößen
- 7.5 INPOL-neu
- 7.6 ViCLAS - Violent Crime Linkage Analysis System
- 7.7 Fahndung im Internet
- 7.8 Modellprojekt zur Prävention von Jugendkriminalität
- 7.9 Datenerhebung und Datenspeicherung anlässlich von Ringalarmfahndungen
- 7.10 Telefonaufzeichnungen bei der Thüringer Polizei
- 7.11 Personenverwechslung mit tragischen Folgen
- 7.12 Beschwerde zum Umgang mit personenbezogenen Daten bei der Thüringer Polizei
- 7.13 Datenverarbeitung der Thüringer Polizei in einem anderen Bundesland
- 7.14 Polizeiliche Bildmappen verschwunden
- 7.15 Einbruch beim Polizeiverwaltungsamt
- 7.16 Datenerhebungen in der Nachbarschaft und beim Arbeitgeber
- 7.17 Kontrolle im Thüringer Polizeiverwaltungsamt - Zentrale Bußgeldstelle
- 8. Verfassungsschutz**
- 8.1 Monatsbericht des TLfV
- 8.2 Sicherheitsüberprüfung

- 9. Finanzen, Steuern, Rechnungsprüfung**
- 9.1 Änderung der Abgabenordnung (AO)
- 9.2 Das Verfahren FISCUS
- 9.3 Elektronische Steuererklärung (ELSTER) über Internet
- 9.4 Steuerdatenabrufverordnung (StDAV)
- 9.5 Speicherkontenübergreifende Umbuchung im integrierten automatischen Besteuerungsverfahren (IABV) bei gleichnamigen Steuerpflichtigen
- 9.6 Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge
- 9.7 Kontrolle bei der Staatskasse
- 9.8 Zustellung eines Briefes durch ein Finanzamt
- 9.9 Weiterleitung eines Beschwerdeschreibens eines Bürgers durch die Sparkassenaufsicht an seine Sparkasse
- 9.10 Datenübermittlung von Standesämtern an Finanzämter bei Sterbefallanzeigen
- 9.11 Datenschutz beim Druck und Versand von Lohnsteuerkarten durch private Serviceunternehmen
- 9.12 Übersendung von Steuerunterlagen mittels Infobrief
- 9.13 Steuerliche Anerkennung von Auslandsgruppenreisen
- 9.14 Führung eines Fahrtenbuches durch Ärzte
- 9.15 Internes aus einer Rechnungsprüfungsstelle im Internet
- 10. Justiz**
- 10.1 Fehlende bereichsspezifische Regelungen bei der Justiz - Beratungen zum Strafverfahrensänderungsgesetz (StVÄG)
- 10.2 Mitteilungen in Straf- und Zivilsachen (MiStra, MiZi)
- 10.3 Thüringer Gesetz zur Ausführung der Insolvenzordnung (ThürAGInsO)
- 10.4 Akustische Wohnraumüberwachung und parlamentarische Kontrolle

- 10.5 Überwachung der Telekommunikation - Entwicklungen im Sicherheitsbereich - Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten
- 10.6 Einsatz von Lügendetektoren im Strafverfahren
- 10.7 Kontrollkompetenz des TLfD bei Gerichten
- 10.8 DNA-Analyse - Genetischer Fingerabdruck
- 10.9 Täter-Opfer-Ausgleich und Datenschutz
- 10.10 Fußfessel - Elektronisch überwachter Hausarrest
- 10.11 Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften
- 10.12 Weitergabe personenbezogener Daten an gemeinnützige Einrichtungen
- 10.13 Personendatenverwechslung - gleicher Name, gleicher Geburtstag
- 10.14 Strafverfahren gegen Ortsbürgermeister
- 10.15 Aktenbearbeitung durch Staatsanwälte zu Hause
- 10.16 Einsatz von EDV-Technik im Gerichtsvollzieherbüro
- 10.17 Automatisiertes Verfahren SIJUS-Straf-StA
- 10.18 Angemessener Datenschutz auch für Untersuchungsgefangene
- 10.19 Erhebung von Besucherdaten in einer Justizvollzugsanstalt
- 10.20 Neufassung der Dienstordnung für Notare
- 10.21 Auskunftersuchen öffentlicher Stellen bei der SCHUFA
- 10.22 Datenträgeraustausch aus den bei den Amtsgerichten geführten Schuldnerverzeichnissen

- 11. Gesundheits- und Sozialdatenschutz
- 11.1 Gesundheitsreform 2000
- 11.2 Erstes Gesetz zur Änderung des Medizinproduktegesetzes - versteckte Sozialdatenschutzänderung
- 11.3 Verordnung über die Gesundheitsuntersuchung von Asylbewerbern nach § 62 Abs. 1 AsylVfG
- 11.4 Thüringer Schiedsstellenverordnung nach § 78g SGB VIII
- 11.5 Regelung der Berufsausübung Thüringer Hebammen und Entbindungspfleger

- 11.6 Neufassung der Berufsordnungen der Landesärzte- und Landeszahnärztekammer Thüringen
- 11.7 Telemedizin: Das vernetzte Arzt-Patienten-Verhältnis
- 11.8 Umgang der Landesärztekammer mit Einkommensnachweisen zur Berechnung des Kammerbeitrags
- 11.9 Wiederaufgefundene Kurierpost eines Klinikums
- 11.10 Einsichtsrecht in Patientenunterlagen
- 11.11 Patientenakten nach Umzug gefunden
- 11.12 Umgang mit Patientenakten aus ehemaligen Polikliniken
- 11.13 Umfang der Einsicht in Krankenunterlagen durch Kassen und MDK
- 11.14 Modellvorhaben nach § 63 SGB V zur Optimierung der Diabetesversorgung
- 11.15 Kontrolle bei der Kassenärztlichen Vereinigung Thüringen (KVT)
- 11.16 Durchführung des Psychotherapeutengesetzes
- 11.17 Beitritt der AOK Thüringen zur ARGE-Mitte
- 11.18 Von der Chipkarte verfolgt
- 11.19 Veränderter ICD-10-Code im Abrechnungsverfahren
- 11.20 Telefonische Beauskunftung von Sozialdaten
- 11.21 Führung der Pflegedokumentation bei häuslicher Pflege
- 11.22 Kontrolle bei der LVA Thüringen
- 11.23 Sozialhilfedatenabgleich
- 11.24 Zusätzlicher Datenaustausch bei Sozialleistungen
- 12. Statistik
- 12.1 Volkszählung 2001
- 12.2 Umsetzung des Hochbaustatistikgesetzes
- 12.3 Was haben statistische Einzeldaten mit einer „Windhose“ zu tun?
- 12.4 Erhebung von Daten zur Durchführung vorbereitender Untersuchungen im Zusammenhang mit städtebaulichen Sanierungsmaßnahmen

- 13. Bildung, Wissenschaft und Forschung**
 - 13.1 Datenerhebungen für schulärztliche Untersuchungen
 - 13.2 Datenschutz bei Chroniken und Jahrbüchern von Schulen
 - 13.3 Listen über Teilnahme am Religionsunterricht
 - 13.4 Klassentreff Agentur
 - 13.5 Hochschulchipkarte „THOSKA“
 - 13.6 Automatisiertes Buchentleihverfahren in Universitätsbibliotheken
 - 13.7 Internationaler Schülervergleich (OECD-Studie „PISA“)
 - 13.8 Studenten als Forscher
- 14. Wirtschaft, Verkehr, Wohnungswesen, Umwelt**
 - 14.1 „Schwarze Listen“ bei der Handwerkskammer
 - 14.2 Datenübermittlungen durch das Finanzamt an Kammern
 - 14.3 Formular zur Energiebelieferung zu umfangreich
 - 14.4 Neuerungen im Straßenverkehrsrecht
 - 14.5 Kontrollen in Führerscheinstellen
 - 14.6 Sonderparkausweis mit zu vielen Daten
 - 14.7 Kfz-Zulassung via Internet?
 - 14.8 Adressveröffentlichung von Einspruchsführern
 - 14.9 Aushang von Mieterlisten durch Wohnungsbaugesellschaft
 - 14.10 Datenübermittlungen an Zweckverbände
 - 14.11 Datenverarbeitung bei der Abfallgebührenberechnung
 - 14.12 Auskunftserteilungen zu Prüfungen nach dem Landwirtschaftsanpassungsgesetz
 - 14.13 Kontrolle eines Amtes für Arbeitsschutz
- 15. Technischer und organisatorischer Datenschutz**
 - 15.1 Der Schritt in die Informationsgesellschaft
 - 15.2 Einsatz von Informationstechnik in der Landesverwaltung
 - 15.3 Das Corporate Network (CN) der Landesverwaltung

- 15.4 Konzentration der Rechenzentren der Landesverwaltung**
- 15.5 Projekt TESTA - Länderübergreifende Kommunikation**
- 15.6 Technische und organisatorische Kontrolltätigkeit**
- 15.6.1 Zum Ablauf einer Kontrolle**
- 15.6.2 Feststellungen und Hinweise im Rahmen der Kontrolltätigkeit**
- 15.6.3 Kontrolle im TIM**
- 15.6.4 Kontrolle der Oberfinanzdirektion (OFD)**
- 15.6.5 Kontrolle im Thüringer Landesverwaltungsamt**
- 15.7 Elektronische Kommunikation in der Landesverwaltung**
- 15.8 Internetnutzung durch öffentliche Stellen**
- 15.9 Eckpunkte der Deutschen Kryptopolitik als wirksames Mittel zur Gewährleistung von Datenschutz und Datensicherheit**
- 15.10 Datenschutz durch Technik-Einsatz transparenter Hard- und Software**
- 15.11 Die elektronische Geldbörse**
- 15.12 Das Jahr 2000 Problem**
- 15.13 Datenschutzrechtliche Aspekte bei der Einrichtung von Telearbeitsplätzen**
- 15.14 Identifikation und Authentifikation mittels biometrischer Verfahren**
- 15.15 Neue Anforderungen an den technischen Datenschutz**

Anlagen

Entschlüsseungen der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 19./20. März 1998 in Wiesbaden

- Anlage 1 Datenschutz beim digitalen Fernsehen
- Anlage 2 Datenschutzprobleme der Geldkarte

EntschlieÙungen der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Lnder am 05./06. Oktober 1998 in Wiesbaden

- Anlage 3 Prfungskompetenz der Datenschutzbeauftragten bei den Gerichten
- Anlage 4 Fehlende bereichsspezifische Regelungen bei der Justiz
- Anlage 5 Verweigerung der Auskunft durch das Bundesamt fr Finanzen auf Anfragen Betroffener ber ihre Freistellungsauftrge
- Anlage 6 Weitergabe von Meldedaten an Adressbuchverlage und Parteien
- Anlage 7 Entwicklungen im Sicherheitsbereich
- Anlage 8 Dringlichkeit der Datenschutzmodernisierung

EntschlieÙungen der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Lnder am 25./26. Mrz 1999 in Schwerin

- Anlage 9 Geplante erweiterte Speicherung von Verbindungsdaten in der Telekommunikation
- Anlage 10 Entwurf einer RatsentschlieÙung zur berwachung der Telekommunikation (ENFOPOL '98)
- Anlage 11 Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben
- Anlage 12 Transparente Hard- und Software

EntschlieÙung der Datenschutzbeauftragten des Bundes und der Lnder vom 17. Juni 1999

- Anlage 13 Parlamentarische Kontrolle von Lauschangriffen in den Bundeslndern

EntschlieÙung der Datenschutzbeauftragten des Bundes und der Lnder vom 16. August 1999

- Anlage 14 Angemessener Datenschutz auch fr Untersuchungsgefangene

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

Anlage 15 „Gesundheitsreform 2000“

Entschlüsse der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 07./08. Oktober 1999 in Rostock

- Anlage 16 Patientenschutz durch Pseudonymisierung
- Anlage 17 Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation
- Anlage 18 Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union
- Anlage 19 Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung
- Anlage 20 „Täter-Opfer-Ausgleich und Datenschutz“
- Anlage 21 Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Weitere Anlagen

- Anlage 22 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- Anlage 23 Umzugsrichtlinie
- Anlage 24 Organigramm

Sachregister

Abkürzungsverzeichnis

Abkürz.	Bedeutung
ABl.	Amtsblatt
Abs.	Absatz
ACCESS	Datenbanksystem von Microsoft
AK	Arbeitskreis
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
APC	Arbeitsplatz-Computer
ARGE-Mitte	Arbeitsgemeinschaft AOK Rechenzentrum Mitte
Art.	Artikel
ASMK	Arbeits- und Sozialministerkonferenz von Bund und Ländern
AsylVfG	Asylverfahrensgesetz
AuslG	Ausländergesetz
AuslG-VwV	Allgemeine Verwaltungsvorschrift zum Ausländergesetz
AVOS	Ahndung von Verkehrsordnungswidrigkeiten im Straßenverkehr
AZR	Ausländerzentralregister
bDSB	behördeninterner Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BGBI	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BLK	Bund-Länder-Kommission
BMF	Bundesfinanzministerium
BMI	Bundesministerium des Innern
BMWT	Bundesministerium für Wirtschaft und Technik
BR	Bundesrat
BR-Drs.	Bundesratsdrucksache
BSeuchG	Bundesseuchengesetz
BSHG	Bundessozialhilfegesetz

BSI	Bundesamt für Sicherheit in der Informations- technik
bspw.	beispielsweise
BStatG	Bundesstatistikgesetz
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
CEMT	Conférence européenne des ministères des trans- port, Europäische Konferenz der Verkehrsmini- ster
CN	Corporate Network
DEÜV	Datenerfassungs- und Datenübermittlungsver- ordnung
DIMI	Deutsches Institut für medizinische Dokumenta- tion und Information
DJT	Deutscher Juristentag
DLCI	Data Link Control Identifier
DNA-Analyse	Genetischer Fingerabdruck
DONot	Dienstordnung für Notare
DSB	Datenschutzbeauftragter/Datenschutzbeauftragte
DuD	Zeitschrift Datenschutz und Datensicherheit
DV	Datenverarbeitung
E-Commerce	Elektronic Commerce (elektronischer Handel)
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGStPO	Einführungsgesetz zur Strafprozessordnung
ELSTER	Elektronische Steuererklärung
E-Mail	Elektronic-Mail (elektronische Post)
EMRK	Europäische Menschenrechtskonvention
ENFOPOL	Enforcement Police, polizeiliche Zusammenar- beit
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUROPOL	Europäisches Polizeiamt
FAG	Fernmeldeanlagen-gesetz

FeV	Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaubnisverordnung)
FISCUS	Föderales Integriertes Standardisiertes Computerunterstütztes Steuersystem
GAUCK-Behörde	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehem. DDR
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz
GKV	Gesetzliche Krankenversicherung
GSM	Global Standard of Mobile Kommunikation
GVBl	Gesetz- und Verordnungsblatt
HessDSG	Hessisches Datenschutzgesetz
i. V. m.	in Verbindung mit
IABV	Integriertes Automatisches Besteuerungsverfahren
ID	Identifizierung
IHK	Industrie- und Handelskammer
IMA-IT	Interministerieller Ausschuss für Informationstechnik
IMK	Gemeinsame Konferenz der Innenminister und Senatoren der Länder
INPOL	Informationssystem der Polizei
Internet	weltweit größtes Computernetz
Intranet	internes Netzwerk
IP	Internet Protokoll
ISDN	Integrated Services Digital Network (dienstintegrierendes Digitalnetz)
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
IuKDG	Informations- und Kommunikationsdienstengesetz
IZ Steufa	Informationszentrale für den Steuerfahndungsdienst
JMBL	Justiz-Ministerialblatt
JURIS	Datenbank Juristisches Auskunftssystem
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt

Kfz	Kraftfahrzeug
KoopA-ADV	Kooperationsausschuss Automatisierte Datenverarbeitung Bund, Länder, Kommunalen Bereich
KVT	Kassenärztliche Vereinigung Thüringen
LaDiVA	Landeseinheitliches Dialogverfahren Ausländerwesen
LASF	Landesamt für Soziales und Familie
LfD	Landesbeauftragter für den Datenschutz
LKA	Landeskriminalamt
LPG	Landwirtschaftliche Produktionsgenossenschaft
LVA	Landesversicherungsanstalt
LwAnpG	Landwirtschaftsanpassungsgesetz
MDK	Medizinischer Dienst der Krankenkasse
MDR	Mitteldeutscher Rundfunk
MDSStV	Mediendienste-Staatsvertrag
MfS/AfNS	Ministerium für Staatssicherheit/Amt für nationale Sicherheit
MiStra	Mitteilungen in Strafsachen
MiZi	Mitteilungen in Zivilsachen
MPU	Medizinisch-Psychologische Untersuchung
MVS	Multiple Virtual Storage
NT	New technology
o. g.	oben genannt
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
Overlay-Netz	Überregionales Netz
PÄD	Polizeiärztlicher Dienst
PAG	Polizeiaufgabengesetz
PC	Personal Computer
PERSOS-S	Stellen- u. Personalverwaltungssystem - Schulen
PERSOS-TH	Stellen- u. Personalverwaltungssystem Thüringen
PIN	Personen-Identifikations-Nummer
PISA	internationale Schülerleistungsstudie (Programme for International Students Assessment)
PKW	Personenkraftwagen
PSN	Prozessor Serial Number

PsychThG	Gesetz über die Berufe des psychologischen Psychotherapeuten und des Kinder- und Jugendlichenpsychotherapeuten
PVA	Polizeiverwaltungsamt
RiStBV	Richtlinie für das Straf- und Bußgeldverfahren
RZ	Rechenzentrum
s. o.	siehe oben
SCHUFA	Schutzgemeinschaft für allg. Kreditsicherung
SchuVVO	Schuldnerverzeichnisverordnung
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SIJUS-Straf	Staatsanwaltschaftliches Informationssystem Geschäftsstellenautomation in Strafsachen bei Staatsanwaltschaften
SIS	Schengener Informationssystem
SLF	Sicherheitsleitfaden
sog.	sogenannte(n)
SPP	Schwerpunktpraxis
SPUDOK	Datei Spurendokumentation
StDAV	Steuerdatenabrufverordnung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehem. DDR
StVÄG	Strafverfahrensänderungsgesetz
StVG	Straßenverkehrsgesetz
TB	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdienstunternehmen-Datenschutzverordnung/Telekommunikations-Datenschutzverordnung
TESTA	Trans European Services für Telematics between Administrations
TFM	Thüringer Finanzministerium
THOSKA	Thüringer Hochschul- u. Studentenwerkskarte
ThürAbgÜpG	Thüringer Gesetz zur Überprüfung der Abgeordneten

ThürAGInsO	Thüringer Gesetz zur Ausführung der Insolvenzordnung
ThürBG	Thüringer Beamtengesetz
ThürDSG	Thüringer Datenschutzgesetz
ThürDSRegVO	Thüringer Datenschutzregisterverordnung
ThürGGO	Gemeinsame Geschäftsordnung für die Ministerien und die Staatskanzlei des Landes Thüringen
ThürKHG	Thüringer Krankenhausgesetz
ThürKWG	Thüringer Kommunalwahlgesetz
ThürMeldeG	Thüringer Meldegesetz
ThürPersVG	Thüringer Personalvertretungsgesetz
ThürSchiedsVO	Thüringer Verordnung über die Schiedsstelle
ThürSchulG	Thüringer Schulgesetz
ThürStAnz	Thüringer Staatsanzeiger
ThürVSG	Thüringer Verfassungsschutzgesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
ThürZustVBezüge	Thüringer Verordnung über Zuständigkeiten für die Feststellung, Berechnung und Anordnung der Zahlung der Bezüge von Bediensteten
TIM	Thüringer Innenministerium
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKM	Thüringer Kultusministerium
TKÜV	Telekommunikationsüberwachungsverordnung
TLfD	Thüringer Landesbeauftragter für den Datenschutz
TLfV	Thüringer Landesamt für Verfassungsschutz
TLRZ	Thüringer Landesrechenzentrum
TLS	Thüringer Landesamt für Statistik
TLVerma	Thüringer Landesvermessungsamt
TLVwA	Thüringer Landesverwaltungsamt
TMJE/TJM*	Thüringer Ministerium für Justiz und Europaangelegenheiten/Thüringer Justizministerium*
TMLNU	Thüringer Ministerium für Landwirtschaft, Naturschutz und Umwelt
TMSG/TMSFG*	Thüringer Ministerium für Soziales und Gesundheit/Thüringer Ministerium für Soziales, Familie und Gesundheit*

TMWFK*	Thüringer Ministerium für Wissenschaft, Forschung und Kultur/Thüringer Ministerium für Wissenschaft, Forschung und Kunst*
TMWI/TMWAI*	Thüringer Ministerium für Wirtschaft und Infrastruktur/Thüringer Ministerium für Wirtschaft, Arbeit und Infrastruktur*
TÜV	Technischer Überwachungsverein
u. a.	unter anderem (und andere)
u. ä.	und ähnliches
UMTS	Universal Mobiles Telekommunikationssystem
UNIFA	Unix im Finanzamt
VDR	Verband deutscher Rentenversicherungsträger
vgl.	vergleiche
ViCLAS	Violent Crime Linkage Analysis System
VmZ	Verwarnung mit Zahlungsanweisung
VPN	Virtual Private Networks
VSA	Verschlusssachenanweisung
VSITR	Richtlinien zum Geheimschutz von Verschlusssachen beim Einsatz von Informationstechnik
VSSR	Verschlusssachenrichtlinie
VVThürDSG	Verwaltungsvorschriften zum Vollzug des Thüringer Datenschutzgesetzes
VZR	Verkehrszentralregister
WWW	World Wide Web
z. B.	zum Beispiel
ZAS	Zentrale Abschiebestelle
ZBS	Zentrale Bußgeldstelle
ZFER	Zentrales Fahrerlaubnisregister
ZG	Zentrale Gehaltsstelle Thüringen
ZIV	Zentrum für Informationsverarbeitung der Thüringer Landesverwaltung
ZPO	Zivilprozessordnung

* Änderung der Bezeichnung nach Neuwahl und Regierungsbildung im Jahr 1999

1. Einleitung

Die Verfassung des Freistaat Thüringen bestimmt in ihrem Artikel 6, dass jeder das Recht auf Achtung und Schutz seiner Persönlichkeit und seines privaten Lebensbereiches sowie Anspruch auf Schutz seiner personenbezogenen Daten hat.

Zur Wahrung des Rechts auf Schutz der personenbezogenen Daten hat der Thüringer Landesbeauftragte für den Datenschutz als unabhängige Kontrollbehörde gegenüber den öffentlichen Stellen des Freistaats wichtige Aufgaben, basierend auf dem Thüringer Datenschutzgesetz, zu erfüllen. Ein besonderes Augenmerk gilt dabei den vorgebrachten Anliegen der Bürger, wenn sie sich an den TLfD gewandt haben, weil sie sich bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch öffentliche Stellen in ihren schutzwürdigen Belangen beeinträchtigt sahen. Effektiver Datenschutz wird nicht zuletzt dann gegeben sein, wenn die Bürgerinnen und Bürger aktiv ihre Rechte, die ihnen die Verfassung, die Gesetze und andere Rechtsvorschriften einräumen, wahrnehmen. Voraussetzung dafür ist, dass sie ihre diesbezüglichen Rechte auch kennen. Dass der Datenschutz mehr Bedeutung bekommen sollte, wird auch von den Bürgern gewünscht. Einer Anfang 1998 durchgeführten bundesweiten Repräsentativbefragung war zu entnehmen, dass mehr als die Hälfte der Bevölkerung diese Meinung äußerte.

Der vorliegende Tätigkeitsbericht für den Berichtszeitraum 1998/1999 wird nicht nur in Papierform veröffentlicht sondern steht auch allen Interessierten im Internet zur Verfügung.

1.1 Die Dienststelle des TLfD

Im Berichtszeitraum wurden zahlreiche Informations- und Kontrollbesuche in den öffentlichen Stellen Thüringens von den Mitarbeitern und Mitarbeiterinnen des TLfD durchgeführt. Gegenstand der Kontrolltätigkeit waren die Einhaltung datenschutzrechtlicher Vorschriften und die Prüfung von technischen und organisatorischen Maßnahmen, die erforderlich sind, um Datenschutz und Datensicherheit zu gewährleisten.

Aufgrund festgestellter Mängel beim Umgang mit personenbezogenen Daten wurden insgesamt 21 Beanstandungen gegenüber öffentlichen Stellen in Thüringen ausgesprochen.

Aufgrund der ausgesprochenen Beanstandungen, die auch nachrichtlich den jeweiligen Aufsichtsbehörden zugesandt wurden, haben in allen Fällen die Stellen die geforderten Maßnahmen getroffen und die gegebenen Hinweise des TLfD beachtet. Der Zeitraum der Umsetzung der angekündigten Maßnahmen in den betreffenden Stellen ist jedoch unterschiedlich gewesen. Mitunter haben sicherlich auch stattgefundene Nachkontrollen des TLfD dazu beigetragen, angekündigte Maßnahmen in der Praxis wirksam umzusetzen.

Datenschutz und Datensicherheit haben sich bereits nicht nur als Grundprinzip der Informationsgesellschaft entwickelt, sondern ist bei der weltweiten Datenübertragung ein gewichtiger Wettbewerbsfaktor in allen gesellschaftlichen Bereichen.

Zur Dienststelle beim TLfD zählen derzeit insgesamt 13 Mitarbeiterinnen und Mitarbeiter (Organigramm, Anlage 24). Anfang November ist die Dienststelle des TLfD innerhalb der Stadt Erfurt umgezogen. Durch die Unterbringung im Hochhaus am Landtag hat sich die räumliche Situation wesentlich verbessert. Ebenfalls wurde Anfang November 1999 das Internetangebot des TLfD erweitert, sodass sich interessierte Bürger auch auf diesem Wege über datenschutzrechtliche Vorschriften und -themen informieren können.

Es ist gegenwärtig zu verzeichnen, dass die Entwicklung der Informations- und Kommunikationstechnik überdimensional und rasant voranschreitet. Neue Herausforderungen, die die Informationsgesellschaft mit sich bringt, stehen auch vor dem Datenschutz.

Die automatisierte Datenverarbeitung in den öffentlichen Stellen in Thüringen kommt flächendeckend und vielseitig zur Anwendung. Dabei bringen neue Techniken und Technologien auch neue Aufgabenfelder und Aufgabenschwerpunkte mit sich. Die IT-Sicherheit spielt eine große Rolle. Von Seiten des Datenschutzes wird auf den Einsatz datenschutzfreundlicher Technologien verwiesen. Um eine effektive Kontrolltätigkeit der erforderlichen technischen und organisatorischen Maßnahmen des Datenschutzes und der Datensicherheit auch zukünftig gewährleisten zu können, habe ich für das Haus-

haltsjahr 2000 eine zusätzliche weitere Stelle für das Referat Technik beantragt. Leider wurde dem bislang nicht entsprochen.

1.2 Der Beirat beim TLfD

Gemäß § 41 ThürDSG besteht beim TLfD ein Beirat, bestehend aus neun Mitgliedern. Es bestellen sechs Mitglieder der Landtag, ein Mitglied die Landesregierung, ein Mitglied die kommunalen Spitzenverbände und ein Mitglied das Ministerium für Soziales, Familie und Gesundheit aus dem Bereich der gesetzlichen Sozialversicherungsträger. Für jedes Beiratsmitglied wird zugleich ein Stellvertreter bestellt. Nach § 41 Abs. 3 ThürDSG unterstützt der Beirat den Landesbeauftragten in seiner Arbeit.

Die Mitglieder des Beirats werden für vier Jahre bestellt, die Mitglieder des Landtags für die Wahldauer des Landtags. Nach der Landtagswahl im September 1999 wurden die Mitglieder und stellvertretenden Mitglieder vom Landtag neu gewählt. In der nachfolgenden Beiratssitzung wurde der Abgeordnete Bernd Wolf (CDU) erneut zum Vorsitzenden des Beirats beim TLfD gewählt.

1.3 Konferenzen und Arbeitskreise der DSB des Bundes und der Länder im Berichtszeitraum

Auch im vorliegenden Berichtszeitraum fanden turnusmäßig zweimal im Jahr Konferenzen der DSB des Bundes und der Länder sowie auch Sitzungen der jeweilig fachlich zuständigen Facharbeitskreise statt. Im Jahr 1998 führte der Hessische Datenschutzbeauftragte den Vorsitz der Konferenz und leitete so die 55. und 56. Konferenz. 1999 hatte der DSB von Mecklenburg-Vorpommern den Vorsitz der Datenschutzkonferenz inne und dem gemäß auch den Vorsitz in der 57. und 58. Konferenz.

Die Entschließungen der Konferenzen, denen ich auch zugestimmt habe, sind im vorliegenden Tätigkeitsbericht unter den Anlagen 1 bis 21 abgedruckt.

2. Europäischer Datenschutz

Wir leben in einer Zeit der Globalisierung, des Umbruchs und des Zusammenwachsens. Investiert wird in großem Umfang in Informationstechnologien, ein Ausbau weltweiter Kommunikationsnetze ist wahrnehmbar. Aus diesem Grunde wird immer mehr auch nach rechtlichen Rahmenbedingungen gefragt, um Rechtssicherheit und effektiven Rechtsschutz für die Bürger zu gewährleisten.

In diesem Zusammenhang kommt einer gemeinschaftlichen Grundrechtscharta eine besondere Bedeutung zu. Die Schaffung einer europäischen Charta der Grundrechte könnte explizit deutlich machen, dass die Gemeinschaft sowohl zur Sicherung der Marktfreiheiten in Europa als auch für die Freiheitsrechte der Bürger steht.

2.1 Die Umsetzung der EG Datenschutzrichtlinie in nationales Recht

In meinem 1. TB (4.1) und auch im 2. TB (2.1) habe ich bereits über die Verabschiedung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Anlage 22) berichtet. Vor dem Hintergrund, dass die Umsetzungsfrist der Richtlinie in nationales Recht im Oktober 1998 abgelaufen ist und damit die Gefahr eines Vertragsverletzungsverfahrens vor dem Europäischen Gerichtshof besteht, haben die DSB des Bundes und der Länder in einer erneuten EntschlieÙung (Anlage 11) auf den Zeitdruck der Novellierung des BDSG hingewiesen. Dabei ist es aus der Sicht der Konferenz erforderlich, dass das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist.

Auch in der vorangegangenen 56. Konferenz in Wiesbaden war die Dringlichkeit der Datenschutzmodernisierung ein zentrales Thema. In einer EntschlieÙung (Anlage 8) begrüÙte die Konferenz ausdrücklich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefassten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten.

Derzeit liegt ein überarbeiteter Entwurf des BMI zur Novellierung des BDSG in Form einer Kabinettsvorlage vor. Eine zeitnahe Verabschiedung der BDSG Novelle wird für dringend erforderlich gehalten, da das BDSG sicherlich auch bei der anstehenden Novellierung des ThürDSG eine entscheidende Rolle spielt.

2.2 Grundrecht auf Datenschutz in einer Charta der Grundrechte der EU

Schon auf ihrer Konferenz in Kopenhagen am 08.09.1995 haben die Datenschutzbeauftragten der Mitgliedsstaaten der EU eine von der deutschen Delegation vorgelegte Erklärung verabschiedet, die Forderungen auf

- ein Grundrecht auf Datenschutz in den vorgesehenen Europäischen Grundrechtskatalog aufzunehmen,
- für die personenbezogenen Datenverarbeitung durch die Organe der Europäischen Union selbst ein verbindliches Datenschutzrecht zu schaffen und
- eine unabhängige Datenschutzkontrollinstanz für die Institutionen der Europäischen Union einzurichten

enthält.

Eine ausdrückliche Aufnahme des Grundrechts auf informationelle Selbstbestimmung, ähnlich der in der Verfassung des Freistaats Thüringen getroffenen Regelungen, würde die freiheitssichernde Funktion dieses Grundrechtsaspektes besonders betonen und sein Gewicht gegenüber Verwaltung und Gesetzgebung hervorheben.

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 04. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern.

Die Datenschutzbeauftragten des Bundes und der Länder haben diesen Beschluss zum Anlass einer Entschließung auf der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Rostock am 07./08. Oktober 1999 (Anlage 18) genommen, die Initiative des Europäischen Rates zur Ausarbeitung einer Europäischen Grundrechtscharta nachhaltig zu unterstützen. Die Bundesregierung, der Bundestag und der Bundesrat wurden aufgefordert, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden

Katalog Europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen, um der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung zu tragen.

Insbesondere im Hinblick darauf, dass der Datenschutz in Thüringen Verfassungsrang hat, habe ich den Minister für Bundes- und Europaangelegenheiten und Chef der Staatskanzlei, der zwischenzeitlich vom Bundesrat für das Gremium zur Ausarbeitung einer EU-Charta der Grundrechte als Mitglied benannt wurde, sowie den Thüringer Justizminister um Unterstützung der Initiative gebeten. Es ist zu begrüßen, dass jeweils Unterstützung von beiden Ressorts in Thüringen versichert wurde.

2.3 Europol

Sowohl in meinem 1. TB (7.9) als auch im 2. TB (7.3) habe ich Ausführungen zu diesem Thema gemacht. Das Europol-Übereinkommen ist am 1. Oktober 1998 in Kraft getreten. Nachdem vor mehr als 4 Jahren das Europol-Übereinkommen beschlossen wurde, konnte nach Ratifizierung durch die Mitgliedsstaaten Europol zum 01. Juli 1999 seine Tätigkeit aufnehmen. Eine unabhängige Überprüfungsinstanz (GKI) gem. Art. 24 Abs. 1 erledigt ihre Aufgaben auf der Grundlage einer Geschäftsordnung, die im April 1999 in Kraft getreten und im Amtsblatt der Europäischen Gemeinschaften veröffentlicht ist (Nr. C 149 vom 28. Mai 1999). Rechtsfragen treten zum Beispiel bei der Entgegennahme und Verarbeitung der von Drittstaaten und -stellen an Europol gelieferten Daten auf. Während bei den im Innenverhältnis von den nationalen Stellen zur Verfügung gestellten personenbezogenen Daten und bei den durch die Analysetätigkeit bei Europol entstehenden eigenen Daten grundsätzlich gewährleistet ist, dass diese in rechtlich zulässiger Weise erhoben und verarbeitet wurden, gilt dies nicht uneingeschränkt für alle von Drittstaaten übermittelten Daten. In diesem Zusammenhang dürfen beispielsweise Informationen, bei denen offenkundig ist, dass sie von einem Drittstaat unter offensichtlicher Verletzung der Menschenrechte erhoben werden, nicht in das Informationssystem oder die Arbeitsdateien zu Analysezwecken gespeichert werden. Als kritisch ist anzusehen, dass eine umfassende und ausreichende

Rechtskontrolle für alle Amtshandlungen Europol's nach überwiegender Auffassung nicht besteht. Die Rechtskontrolle durch die gemeinsame Kontrollinstanz stellt hierfür keinen Ersatz dar, da sie nur die Zulässigkeit der Übermittlung der von Europol stammenden Daten kontrolliert und prüft, ob durch die Speicherung, Verarbeitung und Nutzung der bei Europol vorhandenen Daten die Rechte betroffen und verletzt werden. In einem formellen Verfahren entscheidet der Beschwerdeausschuss rechtskräftig nur über Beschwerden betroffener Personen wegen verweigerter Auskünfte oder über Beschwerden wegen verweigerter Berichtigung oder Löschung personenbezogener Daten. Andere bei Europol angesiedelten Kontrollen oder Überprüfungsmöglichkeiten durch ein Gericht sind nicht vorgesehen. Für die von Europol selbst zu verantwortenden Handlungen beim Umgang mit personenbezogenen Daten gibt es eine gerichtliche Kontrolle durch den Europäischen Gerichtshof nur für Streitigkeiten zwischen Europol und seinen Bediensteten. Die Geschäftsordnung der GKI sieht grundsätzlich öffentliche Anhörungsverfahren für Parteien und gegebenenfalls für Bürger und Sachverständige vor. Darüber hinaus hat ein Betroffener bei unzulässiger oder unrichtiger Datenverarbeitung die Möglichkeit einer nachträglichen Indizkontrolle durch ein nationales Gericht in den Mitgliedsstaaten, wenn er dort einen Prozess wegen eines ihm entstandenen Schadens führen kann. So kann sich in Deutschland ein Betroffener für andere Fälle von Rechtsbeeinträchtigungen überlegen, ob er dann Verfassungsbeschwerde wegen der unzulänglichen gerichtlichen Überprüfungsmöglichkeiten einlegt. Auch käme wegen nicht möglicher Klage beim EuGH eine Beschwerde beim Europäischen Gerichtshof für Menschenrechte wegen Verletzung der Art. 6 und 13 der Europäischen Menschenrechtskonvention in Betracht.

2.4 EG-Telekommunikationsdatenschutzrichtlinie

Diese Richtlinie, die am 15. Dezember 1997 erlassen wurde, wurde erst im Januar 1998 veröffentlicht, sodass sie noch nicht in meinem 2. TB Berücksichtigung fand (ABl. Nr. L 024/1 vom 30. Januar 1998 1 ff). Wie es in der Richtlinie ausdrücklich heißt, dient sie der Harmonisierung der Vorschriften der Mitgliedsstaaten, die erforderlich ist, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten insbesondere des Rechts auf Privatsphäre in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der Telekommunikation sowie den freien Verkehr dieser Daten und von Telekommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

Sie ergänzt ausdrücklich die EU-Datenschutzrichtlinie und stellt eine wichtige bereichsspezifische Regelung für den Bereich der Telekommunikation dar. So enthält sie allgemeine Ausführungen zur Netzsicherheit und zur Vertraulichkeit der Kommunikation und Vorgaben für die Datenverarbeitung bei der Gebührenabrechnung. Unter anderem gibt sie vor, dass die Möglichkeit der Rufnummerunterdrückung geschaffen werden muss. In nationales Recht umgesetzt werden sollte diese Richtlinie bis zum 24. Juli 1998. Mit der Neufassung der TDSV (siehe 4.2), zu der derzeit ein Regierungsentwurf vorliegt, soll die Umsetzung erfolgen.

2.5 ENFOPOL

Der Begriff „ENFOPOL“ steht als Abkürzung für Enforcement Police und bedeutet polizeiliche Zusammenarbeit.

Bei dem Dokument ENFOPOL 98 rev 2=ENFOPOL 19 geht es um die bestätigte Fortschreibung der Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs, abgedruckt im Amtsblatt der Europäischen Gemeinschaften, 39. Jahrgang (329, S. 1 ff). Sie hat eine Auflistung von technischen Anforderungen für die Realisierung der in nationaler Verantwortung liegenden rechtmäßigen Überwachungsmaßnahmen in modernen Telekommunikationssystemen zum Inhalt.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung die Bundesregierung aufgefordert, der Schaf-

fung gemeinsamer Standards nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien nicht konterkariert werde (Anlage 10). Zu einer Entschließung des EU-Rates ist es bisher nicht gekommen. Bei einer Entschließung des EU-Rates wird davon auszugehen sein, dass diese bei der Neufassung der TKÜV (Telekommunikationsüberwachungsverordnung, siehe 4.1), zu der es bisher lediglich ein Eckpunktepapier gibt, berücksichtigt wird.

2.6 Entwurf eines Gesetzes zur Umsetzung von Richtlinien der Europäischen Gemeinschaft auf dem Gebiet des Berufsrechts der Rechtsanwälte

Die Richtlinie 98/5/EG (ABl. EG Nr. L77 Seite 36) sieht eine Liberalisierung der Niederlassungsmöglichkeiten für Rechtsanwälte innerhalb der Europäischen Gemeinschaft vor und muss bis 14. März 2000 in nationales Recht umgesetzt werden.

Mit dem vorliegenden Gesetzentwurf der Bundesregierung (Bundestagsdrucksache 14/2269 vom 01. Dezember 1999) sollen in Übereinstimmung mit den Vorgaben der Richtlinie 98/5/EG die Voraussetzungen und das Verfahren, unter denen sich Rechtsanwälte aus anderen Mitgliedsstaaten in Deutschland niederlassen und die Eingliederung in die deutsche Anwaltschaft erlangen können, geregelt werden.

Zum Referentenentwurf dieses Gesetzes habe ich gegenüber dem Thüringer Ministerium für Justiz und Europaangelegenheiten Stellung genommen und gebeten, die datenschutzrechtlichen Aspekte gegenüber dem Bundesministerium für Justiz zu berücksichtigen: Gegen die vorgesehenen Datenübermittlungen der Staatsanwaltschaft nach Abschluss von Ermittlungen und vor Einreichung der Anschuldigungsschrift gegen die betroffenen Rechtsanwälte zum Zweck der Prüfung durch die zuständige Stelle im Herkunftsstaat, ob berufsrechtliche Maßnahmen zu ergreifen sind, habe ich datenschutzrechtliche Bedenken geäußert. Es sollte geprüft werden, ob nicht eine Mitteilung durch das Anwaltsgericht nach Entscheidung über die Eröffnung des Hauptverfahrens ausreichen könnte. Im Hinblick auf den intensiven Eingriff in das informationelle Selbstbe-

stimmungsrecht der Betroffenen durch die Übermittlungen sollten die Betroffenen von der Datenübermittlung Kenntnis erlangen. Darüber hinaus sollten auch die Vorschriften der StPO über das Zeugnisverweigerungsrecht, die Beschränkung der Beschlagnahme und des maschinellen Datenabgleichs sowie des Abhörens und Aufzeichnens des in der Wohnung nichtöffentlich gesprochenen Wortes auch für diese europäischen Anwälte für entsprechend anwendbar erklärt werden, um klarzustellen, dass ein europäischer Rechtsanwalt den gleichen Schutz wie ein inländischer Rechtsanwalt genießt. Das TMJE hat mir mitgeteilt, dass meine Stellungnahme an das federführende zuständige Bundesministerium der Justiz weitergeleitet wurde. Die geäußerten datenschutzrechtlichen Anregungen haben jedoch im vorliegenden Gesetzentwurf keinen Niederschlag gefunden.

2.7 EG-Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen

Nachdem in Deutschland durch das IuKDG vom 22. Juli 1997 Rahmenbedingungen für eine sichere digitale Signatur verabschiedet worden waren, worüber ich in meinem 2. TB (15.8) ausführlich berichtet habe, griff die Europäische Kommission im Jahre 1998 das Problem auf und erarbeitete einen eigenständigen Vorschlag. Ende November 98 hat der EU-Ministerrat sich einstimmig auf Grundregeln für digitale Signaturen geeinigt und eine Richtlinie beschlossen, deren Umsetzung innerhalb der nächsten 18 Monate zu erfolgen hat. Im Mittelpunkt der Richtlinie steht die Anerkennung der auf elektronischer Grundlage geleisteten Unterschrift. Diese steht damit der handschriftlichen Unterschrift gleich und kann in allen EU-Mitgliedstaaten bei Gerichtsverfahren als Beweismittel verwendet werden. Zum Nachweis der Identität der Geschäftspartner im Internet soll künftig eine Art digitaler Personalausweis durch Zertifizierungsstellen ausgestellt werden. Die Regeln sollen das Benutzen digitaler Signaturen und deren gesetzlicher Anerkennung vereinfachen, insbesondere beim grenzüberschreitenden E-Commerce wie auch im elektronischen Schriftverkehr mit Behörden. Die EU-Richtlinie sieht neben einer Signatur mit hohen Sicherheitsanforderungen auch eine einfachere Variante vor, die weniger stark regle-

mentiert ist. Diese Variante unterliegt künftig der freien Beweiswürdigung durch die Richter.

3. Datenschutz im Parlament

3.1 Verwaltungsvorschrift des TMJE zur Änderung der Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) vom 25. Mai 1998 (4208-1/98) - JMBI 1998, Seite 22f Mitteilung über Strafsachen gegen Abgeordnete

Durch Art. 8 des Justizmitteilungsgesetzes vom 18. Juni 1997 wurde § 8 Einführungsgesetz zur Strafprozessordnung (EGStPO) als gesetzliche Grundlage für die Übermittlung strafgerichtlicher Entscheidungen eingefügt. Danach sind Mitteilungen über das Verfahren abschließende Entscheidungen an den Präsidenten der gesetzgebenden Körperschaft geregelt. Nach Nr. 4 der VV des TMJE zur Änderung der RiStBV erhielt Nr. 192 Abs. 5 die Fassung, dass die Mitteilung nach § 8 EGStPO auf dem Dienstweg erfolgt.

3.2 Steht der „Datenschutz“ dem Informationsrecht der Abgeordneten im Wege?

Bereits in meinem 2. Tätigkeitsbericht (3.1, 3.2) habe ich die Thematik aufgegriffen. Da sich in der parlamentarischen Arbeit die Frage der Grenzen des parlamentarischen Fragerechts immer wieder stellen kann, möchte ich auch im vorliegenden Tätigkeitsbericht nochmals grundsätzliche Ausführungen dazu machen.

Gemäß Artikel 67 Abs. 1 der Verfassung des Freistaats Thüringen hat die Landesregierung parlamentarische Anfragen unverzüglich zu beantworten. Nur in ganz engen Grenzen kann die Beantwortung von Anfragen und Erteilung von Auskünften abgelehnt werden, beispielsweise dann, wenn schutzwürdige Interessen Einzelner, insbesondere des Datenschutzes, entgegenstehen, wobei die Ablehnung den Frage- oder Antragstellenden auf deren Verlangen zu begründen ist.

Indem sowohl das Informations- und Kontrollrecht des Parlaments als auch das Recht auf informationelle Selbstbestimmung Verfassungsrang haben, muss letztlich anhand des konkreten Einzelfalls eine Güterabwägung vorgenommen werden. Beide dienen der Kontrolle der Verwaltung im Rahmen der Gewaltenteilung und dem Öffentlichkeitsgrundsatz entsprechend der Schaffung einer größtmöglichen Transparenz für die Bürgerinnen und Bürger. Nicht automatisch hat der Datenschutz Vorrang vor dem Auskunftsrecht der Abgeordneten. Bei der Güterabwägung können vielfältige Aspekte eine Rolle spielen:

- liegt eine Einwilligung des Betroffenen vor, personenbezogene Daten zu übermitteln,
- Beachtung schutzwürdiger Belange Drittbetroffener,
- Form der Erörterung im Parlament (öffentliche, nichtöffentliche oder vertrauliche Sitzung),
- Sensibilität der personenbezogenen Daten,
- geht es beim Betroffenen um eine Person des öffentlichen Interesses,
- geht es um eine Auskunftserteilung im Zusammenhang mit dem Dienstverhältnis oder ist der unantastbare Bereich privater Lebensgestaltung betroffen,
- geht es um eine politische Bewertung und die öffentliche Haushaltskontrolle.

Diese nur beispielhaft angeführten Kriterien sind bei der Abwägung beider verfassungsmäßigen Prinzipien zu beachten und verhältnismäßig zum Ausgleich zu bringen.

3.3 Regelungen in der Geschäftsordnung des Thüringer Landtags zum Datenschutzbeauftragten

Im § 112 der Geschäftsordnung des Thüringer Landtags ist u. a. geregelt, dass der Landtag und seine Ausschüsse die Anwesenheit des Datenschutzbeauftragten verlangen können und der Datenschutzbeauftragte auf Verlangen des Landtags oder eines Ausschusses die Pflicht hat, sich in den Ausschüssen zu äußern. Ein Teilnahmerecht des TLfD an Sitzungen der Landtagsausschüsse ist in der Geschäftsordnung nicht vorgesehen. In der Vergangenheit bin ich

überwiegend im Rahmen der Beratung von Gesetzesvorlagen mit datenschutzrechtlichen Bestimmungen in den jeweiligen beratenden Ausschüssen anwesend gewesen, wo ich sowohl auf Anfragen der Ausschussmitglieder zur Verfügung stand sowie auch weiter gehende Begründungen zu datenschutzrechtlichen Empfehlungen und Vorschlägen meinerseits dargelegt habe. Die praktische Handhabung bzw. Beschlusslage der Ausschüsse war unterschiedlich:

Der Haushalts- und Finanzausschuss und der Umweltausschuss beschlossen, den Datenschutzbeauftragten zu denjenigen Tagesordnungspunkten einzuladen, die seine Aufgabenstellung betreffen.

Der Ausschuss für Arbeitsmarkt und Gesundheit und der Innenausschuss beschlossen, dass der Datenschutzbeauftragte generell zu denjenigen Tagesordnungspunkten eingeladen werden soll, zu denen er im Rahmen einer Zuschrift Stellung genommen hat. Der Justiz- und Europaausschuss beschloss, dass es bei Vorliegen einer Stellungnahme des Datenschutzbeauftragten zunächst dem Ausschussvorsitzenden vorbehalten bleiben soll, den Datenschutzbeauftragten unter Vorbehalt des Beschlusses des Ausschusses zur Sitzungsteilnahme einzuladen; über die Teilnahme am entsprechenden Tagesordnungspunkt werde gemäß der Geschäftsordnung der Ausschuss zu Beginn der Sitzung entschieden. Die Stellungnahme des Datenschutzbeauftragten sollte grundsätzlich drei Tage vor der Sitzung vorliegen.

Weitere Beschlusslagen in den übrigen Ausschüssen sind mir nicht bekannt.

Im Hinblick auf eine effektive, möglichst einheitliche Verfahrensweise habe ich angeregt, im § 112 der Geschäftsordnung eine Regelung aufzunehmen, die dem Datenschutzbeauftragten das Recht einräumt, an Sitzungen der Ausschüsse teilnehmen zu können, wenn datenschutzrechtliche Themen auf der Tagesordnung stehen. In diesem Zusammenhang sollte mir auch das Recht eingeräumt werden, mich zu datenschutzrechtlichen Aspekten äußern zu können. Ich habe die Landtagspräsidentin gebeten, meine Überlegungen zu gegebener Zeit an die zuständigen Landtagsgremien weiterzuleiten.

4. Medien

4.1 Vierter Rundfunkänderungsstaatsvertrag

Der im 2. TB (4.6) schon in Aussicht gestellte Vierte Rundfunkänderungsstaatsvertrag ist von den Regierungschefs zwischenzeitlich unterzeichnet worden und steht derzeit zur Transformation in Thüringer Landesrecht an. Er enthält in einem eigenen Unterabschnitt datenschutzfreundliche Regelungen, die neben dem Grundsatz der Datensparsamkeit auch Vorgaben zur elektronischen Einwilligung beinhalten, die Sicherungsmaßnahmen vorsehen, um Nutzer von unbedachten Einwilligungen abzuhalten. Vorgesehen wird auch die Möglichkeit der anonymen Nutzung sowie ein Datenschutzaudit für die Veranstalter, um ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten zu lassen. All dies entspricht den Forderungen der Datenschutzbeauftragten, die Gegenstand einer Entschließung der 55. Konferenz waren (Anlage 1).

Mit einer neuen Vorschrift im Gesetz zum Staatsvertrag über den MDR soll nunmehr auch in Thüringen eine Regelung verabschiedet werden, die es erlaubt, regelmäßig dem MDR Meldedaten zu übermitteln. Als Gründe für die Notwendigkeit dieser Regelung wurde angegeben, dass die bisherigen Instrumente, d. h. die Anmeldung durch den Teilnehmer selbst, Einzelanfragen bei den Einwohnermeldeämtern, Feststellungen bei der Tätigkeit des beauftragten Dienstes vor Ort sowie Auswertungen öffentlich zugänglicher Quellen (insbesondere Adressbücher) nicht zu einer größeren Verwirklichung der Gebührengerechtigkeit geführt haben. So stand 1997 im Bereich des MDR eine Anmeldequote von rund 88 % einer Ausstattungsquote mit Rundfunkgeräten von ca. 99 % der Haushalte gegenüber. Um dieses Missverhältnis zu beseitigen, sollen auch in Thüringen künftig alle erwachsenen Personen, die ihre Anschrift wechseln und bisher keine Rundfunkteilnehmer waren, vom MDR ermittelt und durch ein individuelles Anschreiben an eine mögliche Gebührenpflicht erinnert werden. Aufgrund von Erfahrungen in anderen Bundesländern wird dadurch im Bereich des MDR jährlich mit einer Bruttomehreinnahme in Höhe eines zweistelligen Millionenbetrags gerechnet. Voraussetzung dafür ist eine regelmäßige

Übermittlung von Meldedaten im Falle der An-, Abmeldung oder des Todes von volljährigen Einwohnern durch die Meldebehörden an die Landesrundfunkanstalt.

Diesen Argumentationen konnten sich selbstverständlich auch nicht die Datenschutzbeauftragten verschließen, wenngleich bei diesem Verfahren zur „Ermittlung möglicher Schwarz Hörer“ ein Überschuss von Daten über Personen übermittelt wird, deren Kenntnis nicht oder nur mittelbar von der Rundfunkanstalt zur Aufgabenerfüllung erforderlich ist. Dies betrifft insbesondere Personen, die tatsächlich persönlich kein Rundfunkgerät zum Empfang bereithalten oder solche Personen, bei denen der Ehepartner/Lebensgefährte bereits als Rundfunkeilnehmer angemeldet ist. Demgegenüber ist die Übermittlung von Angaben, die Rundfunkeilnehmer betreffen und zur Aktualisierung der beim MDR gespeicherten Daten genutzt werden sollen, datenschutzrechtlich unproblematisch.

Bei der datenschutzrechtlichen Gesamtbewertung des Verfahrens ist zur Beantwortung der Frage nach der Verhältnismäßigkeit zu beachten, dass die Datenübermittlung nicht den gesamten Einwohnermeldedatenbestand umfassen wird, sondern lediglich Daten über Personen, die ihre Wohnung wechseln, wobei der Anlass und der Umfang der Datenübermittlung unter Berücksichtigung von Auskunftssperren eindeutig bestimmt ist. Berücksichtigt man desweiteren die ausdrückliche Zweckbindung für die Daten und die Vorgabe einer auf maximal ein halbes Jahr begrenzten Speicherdauer, stellt letztlich die Lösung einen Kompromiss dar.

4.2 Jugendschutz im Internet „jugendschutz.net“

Auf der Grundlage des Jugendministerbeschlusses vom 20. Juni 1997 haben die obersten Landesjugendbehörden eine Vereinbarung getroffen, die die Schaffung einer länderübergreifenden Stelle mit Beauftragten für den Jugendschutz in den Mediendiensten zum Gegenstand hat. Die obersten Landesjugendbehörden haben das Land Rheinland-Pfalz beauftragt, eine entsprechende Institution einzurichten, was auch erfolgt ist. Sie nennt sich „jugendschutz.net“ und hat ihren Sitz in Mainz. Die Stelle selbst wird nicht hoheitlich tätig. Sie hat die Aufgabe, das Internet auf jugendschutzrelevante Inhalte zu durchsuchen und die Anbieter zu bewegen, diese Inhalte aus dem Angebot zu entfernen. Dabei erhebt und speichert sie per-

sonenbezogene Daten der Anbieter. Sie verfolgt selbst keine Ordnungswidrigkeiten, sondern informiert gegebenenfalls die jeweils zuständige oberste Landesbehörde. Bei Straftatverdacht (z. B. Verstoß gegen § 184 StGB) wird die Strafverfolgungsbehörde eingeschaltet. Ich habe keine Bedenken dazu geäußert, dass die datenschutzrechtliche Kontrolle von „jugendschutz.net“ vom Landesbeauftragten für den Datenschutz von Rheinland-Pfalz wahrgenommen wird. Nach dessen Information reicht es nach den Angaben der Stelle aus, dass der jeweilige Anbieter eine Abmahnung erhält, um entsprechende Inhalte aus dem Internet zu entfernen. Die jugendgefährdenden Angebote werden dabei mit den Daten des Anbieters und Informationen über seine Abmahnung automatisiert verarbeitet. Für die Aufsichtsbehörden werden lediglich Statistiken in anonymisierter Form erstellt. Das TMSG hat mitgeteilt, dass es Ziel ist, die länderübergreifende Stelle „jugendschutz.net“ als Dauereinrichtung zu führen. Dafür sei es wünschenswert, wenn die obersten Landesjugendbehörden durch entsprechende Änderung des § 18 des Mediendienste-Staatsvertrages dazu ermächtigt würden, eine solche länderübergreifende Stelle einzurichten. In diesem Zusammenhang wurde ebenfalls vom TMSG mitgeteilt, dass bislang sämtliche Hinweise von „jugendschutz.net“ von den Anbietern umgesetzt wurden.

4.3 Telekommunikationsdatenschutzverordnung (TDSV)

Wie ich schon im 2. TB (4.2) ausführte, bedarf es einer neuen Verordnung zum Datenschutz in der Telekommunikation, nachdem das TKG schon seit 1996 in Kraft getreten ist.

Im Frühjahr 1999 wurde ein neuer Entwurf einer Telekommunikationsdatenschutzverordnung (TDSV-E) bekannt, der vorsieht, die Speicherdauer von Verbindungsdaten, selbst bei unbestrittenen oder bezahlten Rechnungen, auf zwei Jahre festzuschreiben, während die Regelungen der Telekommunikationsdienste-Unternehmen-Datenschutzverordnung (TDSV) lediglich eine 80tägige Speicherfrist enthält. In der diesbezüglichen „Entschließung zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation“ (Anlage 9) haben sich die DSB des Bundes und der Länder anlässlich ihrer 57. Konferenz am 25. und 26. Mai 1999 gegen diese Absicht des Verordnungsgebers ausgesprochen, da sie mit der datenschutzrechtlich gebotenen Datensparsamkeit und Erforderlichkeit

unvereinbar ist. Ich habe dem TMWI die Entschließung zur Kenntnis gegeben und um Unterstützung der darin geäußerten Auffassung gegenüber dem BMWT gebeten. Der vorgelegte Entwurf der TDSV hat seine Ermächtigungsgrundlage in § 89 Abs. 1 TKG. Auch Nebenstellenanlagen wie z. B. in Krankenhäusern, Hotels sowie im Corporate Network (15.3) als geschlossene Benutzergruppen unterfallen der Anwendung des TDSV, da sie geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken (15.8).

Im überarbeiteten TDSV-E von Oktober 1999 ist geregelt, dass die Verbindungsdaten höchstens sechs Monate nach Beendigung der Verbindung zu speichern sind, womit der Forderung der DSB des Bundes und der Länder teilweise entsprochen wurde. Bezüglich dieses Verordnungsentwurfes habe ich gegenüber dem TMWAI u. a. angeregt, die Einführung des so genannten holländischen Modells zu prüfen, bei dem niemand entgegen seiner ausdrücklichen Einwilligung in Einzelverbindungsanzeige aufgenommen wird. Zugleich habe ich mich für eine Erweiterung der Rechte der Kunden im Zusammenhang mit der Aufnahme ihrer Daten in gedruckte und elektronische Verzeichnissen ausgesprochen und vorgeschlagen die Außerachtlassung von Kundenwidersprüchen künftig als Ordnungswidrigkeit zu qualifizieren. Weiterhin habe ich angeregt, die Möglichkeit einer „rückwirkenden Fangschaltung“ nur auf schwer wiegende Fälle zu beschränken, in denen der Kunde staatliche Ermittlungsbehörden einschalten kann.

4.4 Telekommunikationsüberwachungsverordnung (TKÜV)

§ 88 TKG ist Rechtsgrundlage für eine Verordnung, mit der Vorschriften über die Genehmigung der Abnahme von Überwachungseinrichtungen sowie über Jahresstatistiken zur Überwachungsmaßnahme geschaffen werden sollen. Ein im Frühjahr 1998 bekannt gewordener Entwurf für die Telekommunikationsüberwachungsverordnung ist zurückgezogen worden. Kritikpunkte daran waren, dass die Verpflichtung zur Bereitstellung von Überwachungsmaßnahmen auch auf Corporate Network zu Nebenstellenanlagen sowie den E-Mail-Verkehr und die Internet-Telekommunikation erstreckt wurde. Auch gab es unzureichende Ausnahmeregelungen für Nebenstellen in Krankenhäusern, Hotels und Firmennetzen. Zwar gibt es

noch keinen neuen Entwurf für eine TKÜV. Das BMWT hat jedoch zwischenzeitlich ein Eckpunktepapier vorgelegt, dass als Grundlage für einen neuen Entwurf dienen soll. Das TKG gibt den zu beachtenden Rahmen vor, indem grundlegende technische Erwägungen oder Gründe der Verhältnismäßigkeit zu beachten sind. In diesem Eckpunktepapier wird zwischen drei Fallgruppen differenziert. Gruppe 1 erfasst die Betreiber von TK-Anlagen, mit denen Telekommunikationsdienstleistungen für die Öffentlichkeit erbracht werden, während Gruppe 2 die Betreiber erfasst, mit denen Telekommunikationsdienstleistungen erbracht werden, die sich nicht an die Öffentlichkeit richten. Gruppe 3 erfasst die Betreiber von TK-Anlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden. Bei den Gruppen 2 und 3 geht das Eckpunktepapier davon aus, dass aus Gründen der Verhältnismäßigkeit keine permanenten technischen Vorkehrungen vorgehalten werden müssten, sondern hier im Einzelfall die zu überwachende Telekommunikation durch geeignete technische Maßnahmen gleichsam „herausgefiltert“ werden soll. Ausdrücklich betont das Eckpunktepapier, dass die Überwachungsvorschriften unabhängig vom jeweils benutzten Telekommunikationsnetz Geltung finden sollen, sodass auch eine Abwicklung eines Telefonats über das Internet dieses Telefonat nicht von Überwachungsvorschriften ausgenommen wird. Das Eckpunktepapier lässt noch manche Fragen offen, der Verordnungsentwurf wird gegenwärtig überarbeitet.

4.5 Oma's Geburtstag im Fernsehen

Seitens eines lokalen Fernsehsenders wurde ich gebeten, zur Beschaffung und Veröffentlichung von Geburts- und Sterbedaten durch einen Fernsehsender aus datenschutzrechtlicher Sicht Stellung zu nehmen.

Hierzu habe ich auf die Verpflichtung der Behörden hingewiesen, Rundfunkveranstaltern die zur Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen, soweit dem nicht Vorschriften über die Geheimhaltung und den Datenschutz entgegen stehen. Hierzu zählen auch die Vorschriften des Thüringer Meldegesetzes (ThürMeldeG). Gem. § 33 i. V. m. § 32 Abs. 1 ThürMeldeG dürfen bei Alters- und Ehejubiläen die Auskünfte an den Rundfunk nur Vor- und Familienname, Doktorgrade, Anschriften sowie Tag und Art des Jubiläums

umfassen, wobei der Betroffene das Recht hat, der Weitergabe seiner Daten zu widersprechen. Ergänzend habe ich darauf hingewiesen, dass eine Berichterstattung über Geburtstage aber dann keinen datenschutzrechtlichen Bedenken unterliegt, wenn die „Geburtsstagskinder“ darin eingewilligt haben, dass über ihren Geburtstag berichtet wird.

4.6 Elektronische Einwilligung vor der Veröffentlichung von personenbezogenen Daten im Internet

Bei Fragen von öffentlichen Stellen, unter welchen Voraussetzungen es zulässig ist, personenbezogene Daten auf Homepages im Internet zu veröffentlichen, gehe ich davon aus, dass es sich hierbei um eine Datenübermittlung an eine nicht näher bekannte Öffentlichkeit in ihrer weitreichendsten Form handelt. Wenn keine spezialgesetzliche Regelung eine solche Veröffentlichung erlaubt, ist diese nur zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und der Betroffene hierin eingewilligt hat. Gem. § 4 Abs. 2 Satz 2 ThürDSG muss die Einwilligung durch den Betroffenen schriftlich erklärt werden, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Da es sich bei der Veröffentlichung z. B. von Adressen auf der Homepage in der Regel nicht um Verbindungsdaten handelt (15.8), kommt hierfür eine direkte Anwendung der Vorschriften über die elektronische Einwilligung in § 3 Abs. 7 TDDSG nicht in Frage. Eine entsprechende Anwendung zur Konkretisierung der „anderen Form“ der Einwilligung nach § 4 Abs. 2 S. 2 ThürDSG halte ich aber für vertretbar. Danach kann die Einwilligung auch elektronisch erklärt werden, wenn die öffentliche Stelle die unter § 3 Abs. 7 Nr. 1-5 TDDSG aufgeführten Voraussetzungen für die Einwilligung (eindeutige und bewusste Handlung des Nutzers, nicht unerkennbar veränderbar, Erkennung des Urhebers, Protokollierung, Inhalt der Einwilligung jederzeit vom Nutzer abrufbar) erfüllt.

In einem konkreten Fall bat mich eine öffentliche Stelle um eine Stellungnahme zu der Frage, unter welchen Voraussetzungen es erlaubt sei, die E-Mail-Adressen, die Namen, den Wohnort und den Abiturjahrgang von ehemaligen Schülern auf der Schulhomepage zu veröffentlichen. Als bereichsspezifische Rechtsgrundlage für die Übermittlung personenbezogener Lehrer-, Eltern- und Schülerdaten

ist hier grundsätzlich das Thüringer Schulgesetz (ThürSchulG) heranzuziehen. Ob es sich hierbei um eine Veröffentlichung personenbezogener Daten der Schüler in Form von Jubiläums- und Jahresberichten oder Klassenübersichten handelt und es daher ausreicht, die Betroffenen gem. § 57 Abs. 6 ThürSchulG in geeigneter Weise auf deren Recht hinzuweisen, der Aufnahme ihrer Daten zu widersprechen, ist fraglich. Ich gehe im vorliegenden Fall vielmehr davon aus, dass es sich um eine Übermittlung personenbezogener Daten an Dritte handelt, die nach § 57 Abs. 4 Nr. 3 ThürSchulG nur zulässig ist, soweit eine rechtswirksame Einwilligung des Betroffenen vorliegt. Im Ergebnis halte ich es für vertretbar, wenn die Betroffenen, wie oben beschrieben, ihre Einwilligung zur Einstellung ihrer Daten in das Internet elektronisch erklären können.

5. Innenverwaltung-Kommunales-Sparkassen

5.1 Innenverwaltung

5.1.1 Entwurf für allgemeine Verwaltungsvorschriften zum Ausländergesetz (AuslG-VwV)

In Form der Bundesratsdrucksache 672/98 vom 9. Juli 1998 liegt nunmehr der Entwurf einer allgemeinen Verwaltungsvorschrift zum Ausländergesetz der Bundesregierung nach § 104 AuslG unter Berücksichtigung der bisherigen Verwaltungspraxis in den Ländern und gerichtlicher Entscheidungen vor. Mit Beschluss des Bundesrats (Bundesratsdrucksache 350/99 vom 16. September 1999) hat der Bundesrat mit verschiedenen Maßgaben die Zustimmung beschlossen. Die Bundesregierung muss entweder die Verwaltungsvorschriften mit diesen Abänderungsanträgen des Bundesrats erlassen oder ein neues Verfahren in Gang setzen.

Im Vorgriff auf das Inkrafttreten dieser allgemeinen Verwaltungsvorschriften werden einzelne Teile in den Ländern bereits angewendet, so z. B. die Verwendung von Kontrollstempeln und -einträgen bei Überprüfung des Personenverkehrs nach Nr. 4.1.5; 3.5.6; 63.4.0 und 63.6.1.2.0. Auf meine Anfrage an das TIM, ob das Verfahren in Thüringen ebenfalls durchgeführt wird, wurde mir dies bestätigt. Es werden Kontrollstempel und -einträge bei der Überprüfung des Per-

sonenverkehrs entsprechend Form und Inhalt des seitens des BMI vorgegebenen Musters verwandt. Danach wird mit Datum vermerkt, wer an welchem Ort von welcher Dienststelle angetroffen wurde. Weitere Eintragungen erfolgen nicht. Sowohl von den Ausländerbehörden als auch von den Polizeidienststellen wird das Anbringen der Kontrollstempel als wirksame Methode zur Kontrolle der Personenbewegung von ausländischen Staatsangehörigen gesehen. Aufgrund dieser Einträge konnten nach Mitteilung des TIM bei den Ausländerbehörden entsprechende Entscheidungen erfolgen.

Da sich die Eintragungen auf die vorbezeichneten Angaben beschränken, habe ich hierzu keine datenschutzrechtlichen Bedenken geäußert.

5.1.2 Neufassung der Verschlussachenanweisung (VSA) für den Freistaat Thüringen und der ergänzenden Bestimmungen

Beteiligt hat mich das TIM bei der Neufassung der VSA und der Richtlinien zum Geheimschutz von Verschlussachen (VS-IT-Richtlinie-VSITR) beim Einsatz von Informationstechnik. Die Neufassung der VSA wurde im Thüringer Staatsanzeiger (1999, S. 2716 f) veröffentlicht. In die Regelungen zu den VS-Richtlinien wurde ein Hinweis auf die datenschutzrechtlichen Bestimmungen aufgenommen, was von mir begrüßt wurde.

5.1.3 Einführung einer Asylcard

Die im 2. TB (5.1.1) erwähnte Machbarkeitsstudie liegt seit Herbst 1998 vor. Inhaltlich hatte sie den Auftrag, in verschiedenen Untersuchungssektoren, so die Bereiche Rechtswissenschaft einschließlich Datenschutz, Informatik, Betriebswirtschaft und Sozialwissenschaft einschließlich umfassender Kosten-/Nutzenprognose zukunftsweisende und bedarfsorientierte Lösungsvorschläge aufzuzeigen. Seitens des Bundesministeriums des Innern wurden nunmehr Überlegungen dahingehend angestellt, den Einsatz der Smart-Card im Asylverfahren im Modellversuch zu erproben. Nach Informationen des BfD haben sich die Innenressorts der Länder durchweg positiv für einen solchen Versuch ausgesprochen. Das TIM hat mich gebeten, zu der vorliegenden Studie aus meiner Sicht Stellung zu neh-

men, da sich auch Thüringen die Frage stellen wird, ob die in der Studie beschriebenen zweckgebundenen Anwendungen genutzt werden sollen.

Zu der Grundsatzfrage, aufgrund welcher Rechtsgrundlage ein Modellversuch zum Einsatz einer Smart-Card im Asylverfahren durchgeführt werden kann, wurde seitens des BMI eine „Einwilligungslösung“ präferiert, weil eine konkrete gesetzliche Regelung hierzu nicht vorliegt. Dabei müsste den Betroffenen hinreichend klar sein, worin sie einwilligen. Dies setzt voraus, dass sie die Tragweite der freiwilligen Entscheidung beurteilen können. Eine Erklärung, mit jeder Form der Verarbeitung ihrer personenbezogenen Daten einverstanden zu sein, reicht nicht aus. Umfang, Zweck und Empfänger von Daten müssen klar festgelegt sein. Weiterhin müssen die Konsequenzen einer Verweigerung der Einwilligung oder der späteren Rücknahme erkennbar sein. Dies scheint mit in diesem Bereich allerdings kaum abschätzbar.

Aufgrund der nach der Machbarkeitsstudie vorgesehenen Multifunktionalität der Smart-Card in einer Reihe von verschiedenen Anwendungsbereichen müsste darüber hinaus konkret geprüft werden, inwieweit die vorgesehenen Kommunikationsbeziehungen durch bestehende Gesetze bereits gedeckt sind oder neue gesetzliche Regelungen geschaffen werden müssen.

Zu der sog. Basisanwendung der Smart-Card im Asylverfahren bestehen aus datenschutzrechtlicher Sicht keine Bedenken, soweit nur die in einem Personalausweis üblichen Angaben zur Identifizierung, ergänzt durch elektronischen Fingerabdruck, Einwanderungsdaten und zugehörige Tatsachenfeststellungen erfasst werden.

Soweit die zweckgebundene Anwendung z. B. im Bereich Meldewesen, beim Zugang zum Arbeitsmarkt oder als Patientenkarte vorgesehen ist, bleibt unklar, weshalb dies mittels Chipkarten erfolgen soll. Im Übrigen müssten vor Beginn des Einsatzes weitere konkrete Regelungen zur praktischen Durchführung getroffen werden, etwa wie oft sich ein Betroffener im Rahmen des Verfahrens zur Aufenthaltssteuerung an der genannten Meldesäule melden müsste, um zu verhindern, dass eine Überwachung durchgeführt wird, die mit der

grundgesetzlich garantierten Achtung der Menschenwürde nicht vereinbar wäre.

Insgesamt besteht aufgrund der Fülle der zur Diskussion stehenden Informationen, die auf der Karte und im Hintergrundsystem gespeichert werden sollen, die Gefahr, dass verfassungsrechtlich unzulässige Persönlichkeitsprofile erstellt werden können. Daher müsste zumindest die Funktionalität der in der Machbarkeitsstudie dargestellten Schutzmechanismen insbesondere im Hinblick auf Zugriffe gewährleistet sein, was ohne Sicherheitsinfrastruktur, die offenbar noch ausgebaut werden muss, nicht möglich sein dürfte.

Nach Informationen des BfD hat die ständige Konferenz der Innenminister und -senatoren der Länder in ihrer Sitzung am 18./19. November 1999 den Beschluss gefasst, den Bundesminister zu bitten, dass er mit allem Nachdruck die Einführung einer Chipkarte im Asylverfahren betreibt und die Weichen für eine möglichst rasche Einführung der Chipkarte stellt. Dabei soll darauf geachtet werden, dass der vorgeschlagene Pilotversuch möglichst rasch - gegebenenfalls auch auf freiwilliger Basis - durchgeführt werden kann.

Das TIM hat mitgeteilt, dass aus Sicht des Freistaats Thüringen die Frage des Einsatzes einer Chip-Karte im Asylverfahren grundsätzlich weiter verfolgt werden sollte. Eine Beteiligung an dem Pilotversuch ist nicht vorgesehen.

5.1.4 Datenschutzrechtliche Kontrolle im Rahmen des Schengener Durchführungsübereinkommens (SDÜ) Ausschreibung zur Einreiseverweigerung im Schengener Informationssystem (SIS)

Seit in Kraft treten des SDÜ ist der freie Personenverkehr im Rahmen der Schengen-Kooperation für die Bürger Realität. Dies bedeutet die Möglichkeit für Staatsangehörige der Schengen-Länder und für Ausländer, bei Vorliegen der entsprechenden Voraussetzungen die Binnengrenzen an jeder beliebigen Stelle kontrollfrei zu überschreiten. Der Abbau der Grenzkontrollen hat auch in den Ländern, in denen die Inkraftsetzung des SDÜ zwischenzeitlich erfolgt ist, weiter stattgefunden. Um illegale Einreisen dennoch zu verhindern,

wurden in verschiedenen Bundesländern wie auch in Thüringen im Polizeiaufgabengesetz Befugnisse für die Durchführung verdachts- und ereignisunabhängiger Personenkontrollen zur Bekämpfung der grenzüberschreitenden Kriminalität oder zur Verhütung oder Unterbindung des unerlaubten Überschreitens der Landesgrenzen oder des unerlaubten Aufenthalts geschaffen.

Eine besondere Bedeutung kommt dem Schengener Informationssystem (SIS) zu, in dem Personenfahndungen zur Festnahme gem. Art. 95 SDÜ, Daten bezüglich Drittausländern, die zur Einreiseverweigerung ausgeschrieben sind (Art. 96 SDÜ) oder Personenfahndungen zur Aufenthaltsermittlung (Art. 98 SDÜ) gespeichert werden und für die berechtigten Stellen in allen Schengen-Staaten abrufbar sind.

Zur Überwachung der zentralen Datenverarbeitung des Schengener Informationssystems ist, wie im 2. TB (7.4) dargelegt, eine gemeinsame Kontrollinstanz eingerichtet worden, die auch die Tätigkeit der nationalen Datenschutz-Kontrollinstanzen in Bezug auf die Anwendung des Schengener Durchführungsübereinkommens koordiniert. Nach Art. 101 SDÜ kann ein Betroffener sein Recht auf Auskunft in jedem der Schengen-Staaten geltend machen. Die angesprochene Kontrollinstanz muss sich dann mit der Kontrollinstanz desjenigen Staates in Verbindung setzen, der eine Ausschreibung getätigt hat. Weil die Ausschreibungen im SIS in der Regel durch Behörden der Bundesländer erfolgt, werden die Ersuchen seitens des BfD an die zuständigen Landesbeauftragten weitergeleitet. Der BfD unterrichtet nach Stellungnahme der beteiligten Landesbeauftragten die ausländische Kontrollinstanz über das Ergebnis der datenschutzrechtlichen Kontrolle.

Der Bundesbeauftragte für den Datenschutz hat mir zuständigkeitshalber im Berichtszeitraum das Ersuchen eines ausländischen Staatsbürgers um Auskunft und Löschung seiner Daten im SIS übermittelt. Auf meine Nachfrage hatte mir die zuständige Ausländerbehörde erklärt, zu dem Betroffenen lägen die Voraussetzungen für die Abschiebung vor. Der Aufenthaltsort des Betroffenen sei allerdings unbekannt. Daraufhin sei die Ausschreibung zur Perso-

nenfahndung im INPOL sowie die Eingabe einer Einreisesperre im SIS gem. Art. 96 SDÜ erfolgt.

Nach dem Wortlaut des Art. 96 Abs. 2 und 3 SDÜ können Entscheidungen zur Eintragung einer Einreisesperre auf die Gefahr für die öffentliche Sicherheit und Ordnung oder die nationale Sicherheit, die die Anwesenheit eines Drittausländers auf dem Hoheitsgebiet der Vertragspartei bedeutet, gestützt werden, was insbesondere bei begangenen oder geplanten Straftaten der Fall ist, oder der Drittausländer ausgewiesen, zurückgewiesen oder abgeschoben worden ist.

Nachdem die Eintragung von Einreisesperren nach Art. 96 SDÜ wegen unterschiedlicher Handhabung in den Bundesländern Gegenstand einer bundesweiten Diskussion unter den Datenschutzbeauftragten wurde, habe ich mich an das TIM mit der Bitte um Mitteilung gewandt, ob nach dessen Auffassung die Möglichkeit besteht, einen Ausländer, für den zwar die Voraussetzung für eine Abschiebung vorliegen, eine Abschiebung wegen unbekanntem Aufenthalt jedoch nicht durchgeführt werden konnte, dennoch gem. Art. 96 SDÜ zur Einreiseverweigerung ausgeschrieben werden kann.

Das TIM hat mir hierzu mitgeteilt, dass Ausländer, deren Aufenthalt unbekannt ist, gem. § 66 Asylverfahrensgesetz in Verbindung mit Art. 95 SDÜ mit polizeilichen Mitteln zur Festnahme ausgeschrieben werden können. Die Eingabe einer Einreisesperre darf gem. § 8 Abs. 2 in Verbindung mit § 42 Abs. 7 Ausländergesetz und Art. 96 Abs. 3 SDÜ nur erfolgen, wenn der Ausländer auch tatsächlich aus- oder abgewiesen oder abgeschoben wurde. Die Ausländerbehörden wurden mit Erlass angewiesen, eine Einreisesperre nach Vollzug der Abschiebung bzw. Ausweisung vorzunehmen. Eine gleichzeitige Ausschreibung zur Festnahme und Einreiseverweigerung war somit grundsätzlich nicht vorgesehen.

Zwischenzeitlich hatte mir die Ausländerbehörde auf meine weitere Frage nach vorliegenden Gründen zur Eintragung der Einreisesperre im konkreten Fall bereits mitgeteilt, dass nach Prüfung des Sachverhaltes die Einreisesperre im SIS mangels vorliegenden Gründen nach Art. 96 SDÜ gelöscht wurde.

5.1.5 Kontrollen im Bereich Ausländerwesen

Im Berichtszeitraum habe ich im Bereich des Ausländerwesens insbesondere die automatisierte Datenverarbeitung der Ausländerdateien A und B nach der Ausländerdateienverordnung und den Datenaustausch mit dem Ausländerzentralregister (AZR) geprüft. Bei einem Teil der Ausländerbehörden kommt das Verfahren LaDiVA (Landeseinheitliches Dialogverfahren Ausländerwesen) in Auftragsdatenverarbeitung auf der Grundlage von Nutzungsverträgen zwischen dem jeweiligen Landratsamt und dem Thüringer Landesrechnungszentrum (TLRZ) zum Einsatz. Dieses Verfahren ermöglicht die vollständige Aufnahme und Fortschreibung von Ausländerdaten im Zuständigkeitsgebiet einer Ausländerbehörde. In der Sachbearbeitung der Ausländerbehörde wird dadurch die Führung der Ausländerdateien A und B nach der Ausländerdateienverordnung ermöglicht. Es bietet Suchfunktionen nach verschiedenen Kriterien, die Möglichkeit der Terminüberwachung durch maschinelle Fristenkontrolle, der Bearbeitung von personen- und terminbezogenen Wiederanträgen, des Drucks von Fristablaufschreiben und der Erstellung von Analysestatistiken. Das Programmsystem wird auf einem Großrechner im ZIV (Zentrum für Informationsverarbeitung der Thüringer Landesverwaltung), das zum Bereich der Oberfinanzdirektion Erfurt gehört, abgearbeitet. Die Datenübertragung zwischen den Ausländerbehörden und dem Großrechner erfolgt in unverschlüsselter Form über das Corporate Network (CN). Die systemtechnische Verfahrensbetreuung wird durch das TLRZ wahrgenommen. Das Verfahren LaDiVA habe ich bei einer kommunalen Ausländerbehörde und bei der für Entscheidungen über Abschiebungen zuständigen Zentralen Abschiebestelle im TIM (ZAS) als Auftraggeber und im TLRZ als Auftragnehmer kontrolliert. Bis Ende des Jahres 1998 erfolgte die Verarbeitung der Ausländerdaten im Rahmen von LaDiVA auf einem Großrechner beim TLRZ. Zum 1. Januar 1999 war jedoch dieser Rechner samt der zuständigen Mitarbeiter in das ZIV überführt worden. Der Nutzungsvertrag enthielt jedoch keinen Hinweis auf die Einbeziehung des ZIV bei der Erbringung der vereinbarten Leistungen. Die Auftraggeber waren hierüber nicht ausreichend informiert.

Der Vertrag enthielt insbesondere keine Regelungen zum Abschluss von Unterauftragsverhältnissen. Insbesondere fehlten auch die nach

§ 8 ThürDSG zutreffenden organisatorischen und technischen Festlegungen. Da gem. § 8 Abs. 1 ThürDSG das Landratsamt bei der Auftragsdatenverarbeitung für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich bleibt, habe ich die Überarbeitung des Nutzungsvertrags gefordert. Hierzu ist jedoch auch eine ausreichende Information seitens des Auftragnehmers über die verfahrens- und systemspezifischen Gegebenheiten erforderlich, um die entsprechenden vertraglichen Festlegungen treffen zu können. Gegenüber dem TLRZ habe ich gefordert, die Auftragnehmer konkret über die tatsächlichen Gegebenheiten und insbesondere auch auf die datenschutzrechtlichen Auswirkungen durch die neue Situation der technischen Realisierung der Verarbeitung im Rahmen von LaDiVA beim ZIV hinzuweisen.

Die bestehenden Dienstanweisungen des TLRZ entbehrten noch der Anpassung an die tatsächlichen Gegebenheiten bezüglich der Funktionsverlagerung. Zur Übertragung der Daten über das CN habe ich angeregt, die Daten zukünftig verschlüsselt zu übertragen und zwecks mittelfristiger Umsetzung diesbezügliche Überlegungen einzuleiten. Wegen der kurzen Zeitspanne zwischen der durchgeführten Kontrolle und der Abfassung des Tätigkeitsberichtes liegt noch keine Stellungnahme vor.

Aus der vorliegenden Datenschutzregistermeldung der ZAS war zu entnehmen, dass auch dort in Nutzung des Verfahrens LaDiVA Ausländerdateien A und B für alle Ausländer in Thüringen geführt werden. Dies hat sich bei der Kontrolle in der Praxis nicht bestätigt. Praktisch hatte sich aber das TIM für die ZAS vom TLRZ einen Zugriff auf die Ausländerdateien A und B der kommunalen Ausländerbehörden einrichten lassen. Als zuständige Stelle zur Entscheidung über Abschiebungen war die ZAS zweifellos befugt, personenbezogenen Daten von abzuschiebenden Ausländern zu verarbeiten. Zu diesem Zweck werden der ZAS ohnehin von den kommunalen Ausländerbehörden die entsprechenden Ausländerakten übersandt. Selbst wenn funktional in Bezug auf die anderen Ausländerbehörden die ZAS nicht Dritter, sondern Teil der Ausländerbehörden ist, wie seitens des TIM argumentiert wurde, rechtfertigt dies dennoch nicht den Zugriff auf sämtliche personenbezogenen Daten aller in LaDiVA gespeicherten Ausländer. Auch hier wäre an der konkreten Aufgabenerfüllung zu orientieren gewesen, sodass nur mit Einbeziehung

der kommunalen Ausländerbehörden ein Zugriff auf einzelne Datensätze gerechtfertigt gewesen wäre. Der Nutzungsvertrag ist zwischenzeitlich gekündigt worden, die Zugriffe wurden bis zum Ablauf der Kündigungsfrist gesperrt. Die datenschutzrechtlichen Bedenken sind damit ausgeräumt.

Bei der Prüfung der Anwendung des Verfahrens LaDiVA in einer kommunalen Ausländerbehörde habe ich in dem Datensatz der Ausländerdatei A ein mehrzeiliges Eingabefeld für „Notizen“ festgestellt. Dieses Feld wird nach Angaben der Ansprechpartner von den Ausländerbehörden für Angaben, die nach Ausländerdateienverordnung für die Ausländerdateien A und B nicht vorgesehen sind, genutzt. Die vorliegende Datenschutzregistermeldung des kontrollierten Landratsamtes enthielt jedoch keinen entsprechenden Hinweis. Nach § 80 Abs. 1 Satz 3 Ausländergesetz können die Ausländerbehörden allerdings weitere als in der Ausländerdateienverordnung genannte Daten verarbeitet werden, soweit das für die Aufgabenerfüllung erforderlich ist. Dies ist im Rahmen der datenschutzrechtlichen Freigabe nach § 34 Abs. 2 ThürDSG hinsichtlich der Erforderlichkeit der Datenarten zu prüfen. Aufgrund der kurzen Zeitspanne zwischen Kontrolle und Tätigkeitsbericht liegt ebenfalls noch keine Stellungnahme des betroffenen Landratsamtes vor.

Bei einer weiteren Ausländerbehörde habe ich die automatisierte Datenverarbeitung der Ausländerdateien A und B geprüft, bei der ein anderes Verfahren als LaDiVA im Einsatz war. Bei der Kontrolle wurde festgestellt, dass in dem automatisierten Verfahren weitere Datenarten als in dem TLfD vorliegenden Datenschutzregistermeldung verarbeitet wurden. Somit war eine neue datenschutzrechtliche Freigabe gem. § 34 Abs. 2 ThürDSG erforderlich.

Der Datenaustausch von kommunalen Ausländerbehörden mit dem AZR findet im Freistaat Thüringen zum Teil noch in Papierform statt, soweit noch kein Online-Zugang zum AZR beantragt oder genehmigt ist. Die Ausländerbehörden, die das Verfahren LaDiVA einsetzen, nutzen in der Regel den Abruf im automatisierten Verfahren zum AZR gem. § 22 AZR-G. Hierzu sind sie über eine Standleitung des Corporate Network (CN) mit einem Rechner im ZIV verbunden, der die Verbindung zum AZR herstellt.

Der Zugriff setzt jedoch eine Genehmigung des Bundesverwaltungsamtes (BVA) als Registerbehörde und die Zustimmung des TIM voraus. Im Rahmen der Genehmigung des Onlinezugriffs wird vom BVA für jeden Mitarbeiter einer Ausländerbehörde eine Nutzerkennung vorgegeben, die beim Zugriff gemeinsam mit einem frei wählbaren Passwort einzugeben ist. Damit besteht lesender und schreibender Zugriff.

Das Verfahren LaDiVA bietet darüber hinaus einen Datenaustausch mit dem AZR, indem bisher im AZR nicht erfasste Betroffene und Änderungen von AZR-Daten von der Ausländerbehörde direkt in das AZR geschrieben werden können. Parallel dazu ist eine Aktualisierung des eigenen Datenbestandes erforderlich. Alternativ ermöglicht der Mitteilungsdienst von LaDiVA, dass erfolgte Fortschreibungen im Datenbestand automatisch im AZR vollzogen werden, wodurch eine gesonderte nochmalige Eingabe vermieden wird. Hierzu erfolgt ein täglicher Filetransfer vom Großrechner im ZIV zum AZR. Die veranlassten Änderungen werden protokolliert. Insgesamt haben sich in diesem Zusammenhang keine datenschutzrechtlichen Bedenken ergeben.

5.1.6 Verpflichtungserklärung zur Kostenübernahme nach § 84 Ausländergesetz (AuslG)

Im 2. TB (5.1.7) hatte ich über die einvernehmliche Vorgehensweise des TIM im Rahmen der Verpflichtungserklärungen nach § 84 Abs. 1 AuslG berichtet, dass nur die erforderlichen Angaben und Unterlagen vom Betroffenen verlangt werden. Die Verpflichtungserklärungen zur Kostenübernahme nach § 84 AuslG haben den Zweck, sicherzustellen, dass der Gastgeber eines Ausländers in der Lage ist, für die Kosten aufzukommen, die im Rahmen des Besuches entstehen können.

Im Berichtszeitraum wurde bundeseinheitlich aus EU-Vereinlichungsgründen ein neues Formular zur Abgabe der Verpflichtungserklärung gem. § 84 AuslG eingeführt. Nach Abstimmung mit dem BfD und aufgrund eines Urteils des Bundesverwaltungsgerichts vom 24. November 1998 zur Frage der Wirksamkeit bzw. Be-

stimmtheit einer gegenüber der Ausländerbehörde abgegebenen Verpflichtungserklärung wurde auch das Hinweisblatt hierzu neu gefasst und in Thüringen umgesetzt. Der Betroffene (Gastgeber) ist nach dem Hinweisblatt auf die Freiwilligkeit seiner Angaben und Nachweise und das Ausmaß der eingegangenen Verpflichtung ebenso hinzuweisen wie auf die Strafbarkeit unrichtiger und unvollständiger Angaben.

Danach ist auf die Erhebung von Angaben, ob man Mieter oder Eigentümer einer Wohnung ist sowie auf Detailangaben zu Wohn-, Einkommens- und Vermögensverhältnissen künftig zu verzichten. Zur Problematik der Bonitätsprüfung des Betroffenen ist bestimmt, dass die hierzu vorgelegten Unterlagen zurückzugeben sind. Zur Beweissicherung kann die Ausländerbehörde jedoch Kopien der Belege zu den Akten nehmen. Soweit dies nicht erfolgt, sollte das Ergebnis der Bonitätsprüfung auf einem internen Formular festgehalten werden. Diese Dokumente sind jedoch nicht der Ausländerakte des Eingeladenen beizuheften, sondern getrennt aufzubewahren. Sobald feststeht, dass eine Inanspruchnahme aus der Verpflichtungserklärung nicht mehr erfolgen wird, sind diese Unterlagen zu vernichten.

Gegen dieses einheitliche Formular in Verbindung mit den Hinweisen zur Erhebung, Speicherung und Nutzung der personenbezogenen Daten ist aus datenschutzrechtlicher Sicht nichts einzuwenden.

5.1.7 Auskunftserteilung bei „Scheinehe“- Verfahren

Im 2. TB (5.1.5) hatte ich zur Problematik der Fragebögen zur Ermittlungen im Rahmen von Scheineheverfahren gem. § 92 Abs. 2 Nr. 2 Ausländergesetz berichtet. Im Berichtszeitraum ging mir eine Anfrage zur Regelung der „Scheinehen“- Problematik nach dem neuen Eherecht, das seit 01.07.1998 in Kraft ist, zu. Durch die Gesetzesänderung besteht gem. der §§ 1310 Abs. 1, 1314 Abs. 2 BGB und § 5 Abs. 4 Personenstandsgesetz für die Standesbeamten eine Untersuchungs- und Nachforschungsmöglichkeit im Wege der allgemeinen Amtshilfe zur Vermeidung von Scheinehen. Gem. § 1310 Abs. 1 Satz 2 BGB muss der Standesbeamte seine Mitwirkung an der Eheschließung verweigern, wenn die Ehe nach § 1314 Abs. 2 BGB aufhebbar wäre, was der Fall ist, wenn die Ehe nur zum Schein

geschlossen werden soll, um einem Ehegatten den Aufenthalt in der Bundesrepublik Deutschland zu ermöglichen, die Ehegatten sich aber darüber einig sind, keine Verpflichtung zur eheliche Lebensgemeinschaft begründen zu wollen.

Hierzu stellte sich die Frage, in welchem Umfang den Standesbeamten im Zusammenhang mit Eheschließungen bei ausländischen Ehepartnern ein Auskunftsrecht aus oder Akteneinsichtsrecht in Ausländerakten zukommt. Zunächst müssen konkrete Anhaltspunkte für eine beabsichtigte Scheinehe vorliegen. Den Betroffenen kann die Beibringung von Unterlagen aufgegeben werden, die eine Prüfung ermöglichen.

Zu einer einheitlichen Verfahrensweise wurden den Standesämtern seitens des TIM Hinweise und Informationen zum Vollzug des Eheschließungsrechtsgesetzes im Hinblick auf die Verhinderung von Scheinehen übergeben. In Zusammenarbeit mit der zuständigen Ausländerbehörde kann danach beim Vorliegen konkreter Verdachtsmomente eine Stellungnahme der Ausländerbehörde eingeholt werden kann, die formularmäßig erfolgt. Dies schließt generell eine Aktenübersendung und damit auch ein Akteneinsichtsrecht des Standesbeamten aus. Datenschutzrechtliche Bedenken bestehen zu dieser Vorgehensweise nicht.

5.1.8 Kontrolle in einem Katasteramt

Anlässlich einer Kontrolle in einem Katasteramt wurde festgestellt, dass das IT-System technische Sicherheitslücken auswies, die durch die Einführung neuer Servertechnik behoben werden sollen. Dass die Vergabe der Passwörter zur Authentifizierung der Nutzer in einem der eingesetzten Verfahren durch den Gruppenverantwortlichen erfolgt, habe ich als einen Mangel angesehen, der dem allgemeinen Grundsatz der Passwortvergabe widerspricht und deren Zweck unterläuft. Man hat sich bereiterklärt, im Zuge der Weiterentwicklung des Verfahrens zur Einführung ab Ende 1999 hierfür die technischen Voraussetzungen zu schaffen. Weiterhin stellte sich heraus, dass seitens des Katasteramtes Daten an das Landesvermessungsamt übermittelt wurden, ohne dass dies der Datenschutzregistrierung des Vermessungsamtes zu entnehmen war. Im Landes-

vermessungsamt werden die Daten gesammelt, gespeichert und dann an die Nutzer in der gewünschten Form weitergegeben und sodann gelöscht. Diese Verfahrensweise wird als eine Datenverarbeitung im Auftrag nach § 8 ThürDSG angesehen, die dem TLVermA seitens des TIM per Erlass übertragen worden ist. Dementsprechend ist eine Änderung in der Datenschutzregistermeldung vorgenommen worden.

5.1.9 Kettenbriefe - ein Datenschutzproblem?

Im letzten Jahr musste ich feststellen, dass nunmehr auch Thüringen von den bisher nur aus anderen Bundesländer bekannt gewordenen Kettenbriefaktionen eingeholt wurde. Im vorliegenden Fall waren Behörden gebeten worden, Kopfbögen und Visitenkarten an einen 7-jährigen krebserkrankten Jungen aus Großbritannien zu senden, der angeblich in das Guinnessbuch der Rekorde aufgenommen werden wollte. Gleichzeitig sollte das Schreiben an zehn weitere Personen, Behörden, Vereine oder Institutionen weitergeleitet und deren Anschriften als Anlage den Briefen beigelegt werden. Aus den mir zur Verfügung gestellten Unterlagen ging hervor, dass sich zwischenzeitlich auch einige oberste Landesbehörden beteiligt und dadurch bei nachgeordneten Einrichtungen berechtigte Zweifel an der Seriosität der Aktion ausgeräumt hatten.

Es ist nicht Aufgabe des Datenschutzbeauftragten zu beurteilen, inwieweit Behörden aus den verschiedensten Gründen auf solche Briefe reagieren können oder sollen. Dennoch bestehen auch aus datenschutzrechtlichen Gründen Bedenken hinsichtlich einer Teilnahme an derartigen Aktionen.

Die Gründe dafür liegen zunächst in der Unsicherheit, ob die unter der genannten Anschrift lebende Person tatsächlich Urheber und gewollter Adressat von entsprechenden Zuschriften ist. So sind zwischenzeitlich Fälle bekannt, in denen wegen der gigantischen Flut von Briefen Familien ihre Anschriften ändern mussten. Da systembedingt im Regelfall keinerlei Rückkopplung zum Urheber mehr möglich ist, sind derartige Folgen vorprogrammiert. Da bei einem Missbrauch des Namens und der Anschrift schutzwürdigen Belange (Privatsphäre) mitunter gravierend beeinträchtigt sein können, wäre in jedem Fall eine Versicherung hinsichtlich der Seriosität dieser

Daten vor einer Beteiligung notwendig. Wie zwischenzeitlich, im konkreten Beispiel in Thüringen festgestellt werden musste, ist unter der im Kettenbrief angegebenen Anschrift kein Junge entsprechenden Namens gemeldet. Insoweit bleibt in diesem Fall auch der tatsächliche Empfänger und die weitere Nutzung der zugesandten Visitenkarten und Briefbögen unklar. Dass dabei möglicherweise auch unseriöse Adresshändler als Initiatoren entsprechender Aktionen in Betracht kommen, ist nicht auszuschließen. Entsprechende Hinweise dafür gab es in der Vergangenheit bereits mehrmals.

Problematisch ist desweiteren, dass der Kettenbrief nicht nur an einen weiteren Verteiler versandt wird, sondern dieser Verteiler gleichzeitig als Information den neuen Empfängern mitgeteilt wird. Die Aufforderung in der mir bekannten Aktion in Thüringen zur Übermittlung der Anschriften von zehn weiteren Personen, Behörden, Vereine oder Institutionen, birgt die Gefahr, dass Privatanschriften (Anschriften von Privatbetrieben oder von einzelnen Personen) ohne deren Kenntnis und Willen an Dritte offenbart werden. Würde es sich dabei sogar um Privatanschriften von Beschäftigten (z. B. Beamten) handeln, wäre dies als Verstoß gegen beamtenrechtliche Bestimmungen zu werten.

Soweit die Übersendung der Visitenkarten nicht von dem Betroffenen selbst in freier Entscheidung erfolgt, sondern diese möglicherweise in den Einrichtungen gesammelt und übersandt werden, besteht die Gefahr, dass der Einzelne sich einem sozialen Druck unterlegen fühlt, für eine gute Sache etwas tun zu müssen. Darüber hinaus wird ihm durch den Aufruf der Behörde eine vermeintliche Prüfung der Seriosität und des öffentlichen Interesses vermittelt, die tatsächlich nicht gegeben ist.

Aus datenschutzrechtlicher Sicht gleichfalls bedenklich wäre die Übersendung von Visitenkarten der Mitarbeiter ohne deren Zustimmung, auch wenn darauf keine Privatanschriften vermerkt sind, da es sich um eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs gem. § 22 ThürDSG handelt und dementsprechend eine Prüfung schutzwürdiger Interessen der Betroffenen vorangehen müsste.

Zusammenfassend ist deshalb festzustellen, dass Kettenbriefaktionen, die mit einer Übermittlung oder Aufforderung zur Übermittlung von personenbezogenen Daten verbunden sind durchaus, wenn auch nicht vordergründig, das informationelle Selbstbestimmungsrecht der jeweils Betroffenen berühren und dies, soweit eine Teilnahme aus anderen Gründen nicht ohnehin unterbleibt, entsprechend zu beachten ist.

5.1.10 Aufbewahrung von Stasi-Überprüfungsakten

Im Berichtszeitraum hat sich eine von den Datenschutzbeauftragten des Bundes und der Länder gebildete Ad-hoc Arbeitsgruppe mit dem Umgang mit Stasi-Überprüfungsakten beschäftigt und auf der Grundlage der gegebenen Situation und den bestehenden Rechtsgrundlagen für den öffentlichen Bereich in den verschiedenen Bundesländern Erfahrungen ausgetauscht. Bereits im 1. TB (6.5) habe ich Ausführungen zu diesem Thema gemacht. Darüber hinaus erhielt ich im Berichtszeitraum sowohl von Betroffenen als auch aus dem kommunalen Bereich verschiedene Anfragen hinsichtlich des Umgangs mit Stasi-Überprüfungsakten.

Für den Bereich der Landtagsabgeordneten wurde am 15.10.1998 das Thüringer Gesetz zur Überprüfung von Abgeordneten (ThürAbgÜpG) verkündet. Gem. § 1 Abs. 1 ThürAbgÜpG sind alle vor dem 1. Januar 1970 geborenen Landtagsabgeordneten ungeachtet früherer Überprüfungen ohne ihre Zustimmung auf eine wissenschaftliche Zusammenarbeit mit dem MfS/AfNS zu überprüfen und es ist festzustellen, ob sie deshalb unwürdig sind, dem Landtag anzugehören. Diese Regelung ist nach § 9 ThürAbgÜpG bis zum Ablauf der dritten Wahlperiode (planmäßig bis Herbst 2004) begrenzt. § 1 Abs. 3 ThürAbgÜpG sieht vor, dass nach Ausscheiden eines Abgeordneten bzw. nach Ende der Wahlperiode die angefallenen Unterlagen unverzüglich zu vernichten sind, sodass die Frage einer Archivierung nicht besteht. Darüber hinaus sieht § 3 Abs. 5 ThürAbgÜpG vor, dass Unterlagen des Überprüfungsgremiums (bestehend aus dem Landtagspräsidenten, seinen Stellvertretern und der gleichen Anzahl von Ersatzmitgliedern), das geheim tagt, gegen unbefugten Zugriff zu sichern sind und im Übrigen die Geheimschutzordnung des Landtags entsprechend anzuwenden ist. Nach § 8 Abs. 1 ThürAb-

gÜpG verliert der Abgeordnete sein Mandat, wenn nach der Bekanntgabe der Feststellung des erweiterten Gremiums der Landtag mit Zweidrittelmehrheit beschließt, dass der Abgeordnete unwürdig ist, dem Landtag anzugehören. Zur Vorbereitung der Entscheidung sieht § 8 Abs. 2 Satz 2 ThürAbgÜpG vor, dass die Abgeordneten in den Räumen des Landtags Einsicht in die das Überprüfungsverfahren betreffenden Unterlagen des Gremiums erhalten.

Den Bewerbern um einen Gemeinderats- bzw. Kreistagssitz wird seit der zweiten Wahlperiode Mitte 1994 nach § 12 Abs. 2 Thüringer Kommunalwahlgesetz (ThürKWG) eine Erklärung über die frühere Zusammenarbeit mit dem MfS/AfNS abverlangt, die mit der Wahlbekanntmachung veröffentlicht wird. Hat ein Bewerber diese Frage wahrheitswidrig verneint, verliert er nach § 30 Abs. 1 Satz 2 ThürKWG sein Amt, wobei diesen Amtsverlust die Rechtsaufsichtsbehörde feststellt (1. TB 5.1.1, 6.5.3). Da das ThürKWG keine ausdrücklichen gesetzlichen Regelungen zum Umgang mit den Stasi-Überprüfungsakten bei Gemeinderats- und Kreistagsmitgliedern enthält, habe ich mich beim TLVwA darüber informiert, an welchem Ort, wie lange die „GAUCK-Unterlagen“ aufzubewahren sind sowie welche Zugriffsberechtigung besteht und wie mit den Unterlagen nach Ablauf der Aufbewahrungsfrist umzugehen ist. Die bisherige Praxis bei den Landkreisen und kreisfreien Städten stellt sich dabei so dar, dass GAUCK-Unterlagen zu bestimmten Kreistagsmitgliedern, gegen die ein Verdacht auf eine Stasi-Mitarbeit bestand, grundsätzlich auf der Grundlage einer Beschlusslage der Gebietskörperschaft bei der GAUCK-Behörde angefordert wurden. Die Beauskunftung erfolgte von Seiten der GAUCK-Behörde an die Gebietskörperschaft. Erst wenn sich der Verdacht auf eine Stasi-Mitarbeit möglicherweise bestätigte, sind die Unterlagen an das LVwA zur Prüfung eines Amtsverlustes des Kreistagsmitgliedes gem. § 30 Abs. 6 ThürKWG übergeben worden. Für den Bereich der Gemeinderatsmitglieder sei entsprechend verfahren worden. Die Rechtsaufsichtsbehörde wurde dabei überwiegend auf Antrag der jeweiligen Gebietskörperschaft tätig. Vielfach seien die Fälle „intern“ im Gemeinderat bzw. im Kreistag in der Weise gelöst worden, dass Gemeinderats- bzw. Kreistagsmitglieder bereits zum Zeitpunkt der Kenntniserlangung von belastenden Stasi-Unterlagen durch den Gemeinderat bzw. den Kreistag Konsequenzen zogen und die Kan-

didatur ohne es auf eine Prüfung durch die Rechtsaufsichtsbehörde ankommen zu lassen, zurückgezogen bzw. auf ihr Mandat verzichtet haben. Die Frage, ob und in welchem Umfang es den Gebietskörperschaften auf der Grundlage ihres Selbstorganisationsrechts erlaubt ist, die ihnen angehörenden Mitglieder auf eine frühere Stasi-Zusammenarbeit zu überprüfen, wird derzeit noch vom TLVwA in Abstimmung mit dem TIM geprüft. Regelungen, wie lange die Unterlagen aufbewahrt werden bzw. wann diese Unterlagen vernichtet oder dem Archiv angeboten werden sollen, gibt es nicht. Ich habe dem LVwA auf der Grundlage meines Informationsbesuches empfohlen, sich bis zur eventuellen Schaffung von gesetzlichen Regelungen zum Umgang mit Stasi-Überprüfungsakten von Gemeinderats- und Kreistagsmitgliedern an der o. g. Überprüfung der Thüringer Landtagsabgeordneten zu orientieren. Danach wären nach Ausscheiden eines Mitgliedes bzw. nach Ende der Wahlperiode die angefallenen Unterlagen zu vernichten. Da keine spezialgesetzliche Regelung besteht, sind nach § 16 Abs. 2 ThürDSG personenbezogene Daten in Akten zu löschen, wenn die speichernde Stelle im Einzelfall feststellt, dass die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist. Allerdings sind die Daten gem. § 16 Abs. 3 ThürDSG vor der Vernichtung dem zuständigen Archiv zur Übernahme anzubieten.

Bei den Beschäftigten und Bewerbern im öffentlichen Dienst sind die Stasi-Überprüfungsakten Bestandteil der Personalakte. Diese Unterlagen bestehen aus der persönlichen Erklärung, den Bescheiden der GAUCK-Behörde sowie weiteren Unterlagen im Zusammenhang mit der Einstellung oder Weiterbeschäftigung. Nach § 97 Abs. 5 ThürBG sowie unter Ziff. 3.8 der hierzu erlassenen Personalaktenführungsrichtlinie (6.1) sind die Stasi-Überprüfungsakten in einer gegen unbefugten Zugriff besonders gesicherten Teilakte zu führen. Eine Anwendung der Richtlinie wird auch den Gemeinden, den Landkreisen, den anderen Gemeindeverbänden und den sonstigen unter der Aufsicht des Freistaats Thüringen stehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts empfohlen.

Hinsichtlich der Aufbewahrungsdauer der Stasi-Überprüfungsakten gehe ich davon aus, dass das StUG in § 29 Abs. 3 eine strenge

Zweckbindungsregelung für die öffentlichen Dienststellen als Empfänger der Unterlagen getroffen hat. Danach besteht der Verwendungszweck der Unterlagen darin, im Rahmen der Entscheidung über Einstellung oder Weiterbeschäftigung von öffentlichen Bediensteten zu überprüfen, ob diese hauptamtlich oder inoffiziell für den Staatssicherheitsdienst tätig waren (§ 21 Abs. 1 Nr. 6 StUG). Dies hat nach Maßgabe der dafür geltenden Vorschriften zu geschehen. Keinesfalls dürfen diese Unterlagen für andere Zwecke, etwa im Rahmen einer anstehenden Beförderung, herangezogen werden. Eine weitere bundesrechtliche Grenze der Verarbeitung und Nutzung der GAUCK-Unterlagen ist § 21 Abs. 3 StUG zu entnehmen, der für die Zeit nach dem 29.12.2006 ein absolutes Verwendungsverbot der Unterlagen für die Zwecke der Personalüberprüfung vorsieht. Diese sind wie die übrige Personalakte nach § 103 Abs. 1 ThürBG bis zum Ablauf von 5 Jahren nach Abschluss aufzubewahren und vor einer Vernichtung dem zuständigen Archiv anzubieten.

5.2 Kommunales

5.2.1 Übermittlung von Meldedaten an Adressbuchverlage

Die in den Meldegesetzen als Melderegisterauskünfte in besonderen Fällen bezeichneten Datenübermittlungen an Adressbuchverlage sowie an Parteien und Wählergruppen zu Zwecken der Wahlwerbung stellen aufgrund vielfacher Anfragen und Beschwerden ein Dauerthema bei den Landesbeauftragten für den Datenschutz dar. Aus diesem Grund haben sich die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung zur 56. Konferenz (vgl. Anlage 6) an die gesetzgebenden Körperschaften mit der Bitte gewandt, statt den bisher überwiegend geltenden Widerspruchslösungen künftig die Einwilligung der Betroffenen als Übermittlungsvoraussetzung in den Meldegesetzen vorzusehen. Begründet wird dies insbesondere damit, dass die Information über die Widerspruchsmöglichkeit häufig viele Menschen nicht erreicht und sie deshalb aus Unkenntnis von ihrem Recht nicht Gebrauch machen können. Um dies auszuschließen, sollte jeder Bürger grundsätzlich selbst darüber entscheiden können, ob seine Daten an die vorgenannten Empfänger bzw. zur Veröffentlichung übermittelt werden dürfen oder nicht. Die Einwilligungslösung als eindeutige Willenserklärung des Betroffe-

nen würde die Rechte der Bürgerinnen und Bürger verbessern und die bisherige Privilegierung der Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen aufheben. Weitere Gründe für eine Änderung der gegenwärtigen Widerspruchsregelung in Thüringen durch eine Einwilligungslösung, die im Übrigen zwischenzeitlich bereits in zwei Bundesländern erfolgte, sind in den vorangegangenen Tätigkeitsberichten (1. TB 5.2.4.7; 2. TB 5.2.4) bereits ausführlich dargelegt worden. Im Rahmen der Novellierung des Thüringer Meldegesetzes habe ich mich nachdrücklich für eine entsprechende Gesetzesänderung ausgesprochen. Leider wurde für diese grundsätzliche Änderung keine ausreichende Mehrheit gefunden, sodass auch künftig dem Bürger nur die Möglichkeit bleibt, wenn er entsprechende Datenübermittlungen zu seiner Person nicht wünscht, dies ausdrücklich gegenüber dem zuständigen Meldeamt zum Ausdruck zu bringen. Meine Aufgabe wird es deshalb künftig sein, auf die Probleme bei der Veröffentlichung von Meldedaten hinzuweisen und bei Kontrollen verstärkt darauf zu achten, dass die den Gemeinden vom Gesetzgeber auferlegte Informationspflicht über das Widerspruchsrecht der Betroffenen eingehalten wird.

Um den Eingriff in das informationelle Selbstbestimmungsrecht dennoch zu begrenzen wurde bei der Novellierung des Meldegesetzes eine Konkretisierung der Zweckbestimmung für die Datenübermittlung an Adressbuchverlage dahingehend beschlossen, dass künftig die Daten nur für die Herausgabe von Adressbüchern in Form von gedruckten Nachschlagewerken verwendet werden dürfen. Inwieweit dies letztlich den Endnutzer davon abhält, die Daten nicht in automatisierte Verfahren zu übernehmen und entsprechend zu verwerten, ist allerdings dahingestellt. Desweiteren wurde im Meldegesetz ein differenziertes Widerspruchsrecht aufgenommen. Danach kann der Betroffene der Übermittlung seiner Daten allgemein oder nur einer Veröffentlichung in bestimmten Teilen (Straßenverzeichnis) des Adressbuches widersprechen. Dadurch kann ein Nutzer des Adressbuches die Daten einer Person nur aus dem alphabetischen Namensverzeichnis entnehmen, während diese bei eingelekten Widerspruch im Straßen- bzw. Anschriftenverzeichnis nicht enthalten sind, wodurch die grundstücksbezogene Nutzung der Datensammlung eingeschränkt wird.

5.2.2 Übermittlung von Meldedaten an Parteien

Im Vorfeld der 1998 und 1999 in Thüringen auf allen Ebenen (Europa-, Bundes-, Landtags- und Kommunen) stattgefundenen Wahlen beantragten eine Reihe von Parteien bei den Meldeämtern die Übergabe von Adressdaten Wahlberechtigter. Da das Thüringer Meldegesetz den Meldebehörden erlaubt, Parteien und Wählergruppen im Zusammenhang mit allgemeinen Wahlen zum Zwecke der Wahlwerbung in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über Gruppen von Wahlberechtigten, soweit die Betroffene nicht widersprochen haben, zu erteilen (eine Verpflichtung aber nicht besteht), wandten sich viele Meldeämter an mich, mit der Bitte um eine datenschutzrechtliche Bewertung.

In meinen Antworten und Stellungnahmen (1. TB 5.2.4.5) habe ich stets darauf verwiesen, dass bei Einhaltung der im Thüringer Meldegesetz geforderten vorherigen Information der Betroffenen über ihr Widerspruchsrecht eine Auskunftserteilung im Rahmen der gesetzlich Vorgaben und Fristen zulässig ist. Ungeachtet dessen liegt es aber im Ermessen der Gemeinden bei Beachtung des Gleichbehandlungsgrundsatzes generell von einer Auskunftserteilung abzusehen.

Aus der Sicht des Datenschutzes wäre selbstverständlich immer statt einer Widerspruchslösung einer Einwilligungslösung der Vorzug zu geben. Aus diesem Grund habe ich auch der von den Datenschutzbeauftragten des Bundes und Der Länder verabschiedeten Entschließung zur „Weitergabe von Meldedaten an Adressbuchverlage und Parteien“ (Anlage 6) zugestimmt.

Dass bei der in Thüringen geltenden Widerspruchsregelung eine Beeinträchtigung des informationellen Selbstbestimmungsrechts nicht auszuschließen ist, ergibt sich nicht allein dadurch, dass vielfach öffentliche Bekanntmachungen nicht alle Einwohner aus den unterschiedlichsten Gründen erreichen, sondern auch dann, wie ich in einem Fall beanstanden musste, wenn der Begriff der öffentlichen Bekanntmachung fehlerhaft ausgelegt wird. So hat eine Stadtverwaltung ihre Bürger lediglich durch einen öffentlichen Aushang im

Meldeamt über ihr Widerspruchsrecht informiert. Dies entspricht aber nicht den gesetzlichen Anforderungen an eine öffentliche Bekanntmachung (§ 1 Abs. 2 der Thüringer Bekanntmachungsverordnung), weil weder eine Veröffentlichung im Amtsblatt noch in einer mindestens einmal wöchentlich erscheinenden Zeitung erfolgt war. Nur wenn die Gemeinde weniger als 3000 Einwohner gehabt hätte, wäre ein Anschlag an den hierfür allgemein bestimmten Stellen (Verkündungstafeln) ausreichend gewesen. Die beanstandete Stelle hat eine Information der Öffentlichkeit über die Lokalpresse umgehend nachgeholt.

5.2.3 Umgang mit Unterstützungsunterschriften bei Wahlen

Aufgrund einer Anfrage hatte ich mich im Berichtszeitraum mit dem Umgang von Unterstützungsunterschriften bei Wahlen zu beschäftigen. Ausgangspunkt waren dabei die unterschiedlichen Bestimmungen in Bundes-, Landes- und Kommunalwahlgesetzen.

Übereinstimmend gilt, dass bei Bundes-, Landes- und Kommunalwahlen bei der Einreichung von Wahlkreisvorschlägen von Parteien/Wählergruppen, die seit der jeweils letzten Wahl nicht aufgrund eigener Wahlvorschläge ununterbrochen im Bundestag/Landtag bzw. Kreistag oder Gemeinderat vertreten waren, die Unterstützung einer bestimmten Anzahl von Wahlberechtigten nachzuweisen ist. Durch dieses Verfahren sind die „Unterstützer“ gehalten, ihre politische Meinung und Überzeugung gegenüber dem Wahlleiter, den Mitgliedern des Wahlausschusses sowie gegenüber der Meldebehörde zu offenbaren. Da die Erhebung und Verarbeitung von Daten über politische Meinungen, religiöse oder philosophische Überzeugungen als besonders sensibel eingestuft wird und deshalb gem. Art. 8 der Europäischen Datenschutzrichtlinie vom 24. Juli 1995 („Bearbeitung besonderer Kategorien personenbezogener Daten“) unter besonderem Schutz steht, sind bei der Prüfung der Erforderlichkeit und der Verhältnismäßigkeit für die Erhebung, Verarbeitung und Nutzung derartiger personenbezogener Daten zum Schutz des informationellen Selbstbestimmungsrechts der Betroffenen besonders strenge Maßstäbe anzulegen.

In einer Vielzahl von Urteilen des Bundesverfassungsgerichtes so-

wie in den einschlägigen Kommentierungen zu den Wahlgesetzen wird grundsätzlich die Erforderlichkeit der Erhebung von Daten der „Unterstützer“ von Wahlvorschlägen begründet und deren Verfassungsmäßigkeit nicht in Frage gestellt. Darüber hinaus hat sich das Bundesverfassungsgericht auch mit der Frage beschäftigt, wie viele Unterstützungsunterschriften zum Nachweis der Ernsthaftigkeit einer Bewerbung nötig und verhältnismäßig sind, um zu verhindern, dass nicht ernst gemeinte oder von vornherein aussichtslose Wahlvorschläge aufgenommen werden. So wurden bei Bundestagswahlen 200 Unterstützungsunterschriften bei rund 160.000 Wahlberechtigten je Wahlkreis als verhältnismäßig betrachtet. Bei Landtagswahlen sind gegenwärtig 250 Unterstützungsunterschriften der Wahlberechtigten bei rund 45.000 Wahlberechtigten im Wahlkreis nötig und bei Kommunalwahlen werden 10 Unterstützungsunterschriften zuzüglich der 4fachen Zahl der zu wählenden Gemeinderatsmitglieder für einen Wahlvorschlag gefordert. Gründe für die unterschiedlichen Vorgaben sind auf Landes- und Kommunalebene im Hinblick auf die Erforderlichkeit und Verhältnismäßigkeit der Datenerhebung und damit der Offenbarung sensibler Daten nicht bekannt.

Während bei Bundes- und Landtagswahlen entsprechend der Anlagen zu den Wahlordnungen zur Nachweisführung der Willenserklärung zwingend jeweils für jeden einzelnen „Unterstützer“ ein separater Erhebungsbogen vorgeschrieben ist, der verhindert, dass tatsächliche oder vermeintliche „Unterstützer“ bei der Eintragung Kenntnis von Daten weiterer „Unterstützer“ erhalten, wird bei der Einreichung von Wahlvorschlägen für die Kommunalwahlen die Eintragung der „Unterstützer“ in einer Liste, auf dem zuvor bis zu 14 „Unterstützer“ eingetragen werden, verbindlich vorgeschrieben. Durch diese Verfahrensweise wird der „Unterstützer“, wenn er von seinem Recht der „Unterstützung eines Wahlvorschlages“ Gebrauch machen will, verpflichtet seine politische Orientierung und seine Daten auch nachfolgenden tatsächlichen oder vermeintlichen „Unterstützern“ gegenüber zu offenbaren.

In der Bundes- und Landeswahlordnung wurden spezielle strenge Regelungen zur ausschließlichen Zweckbindung der Vordrucke mit den Unterstützungsunterschriften aufgenommen. Danach dürfen Auskünfte aus diesen Unterlagen nur Behörden, Gerichten und son-

stigen amtlichen Stellen des Wahlgebietes und nur dann erteilt werden, wenn sie für den Empfänger im Zusammenhang mit der Wahl erforderlich sind. Ein solcher Anlass liegt insbesondere beim Verdacht von Wahlstraftaten, bei Wahlprüfungsangelegenheiten und bei wahlstatistischen Arbeiten vor. Entsprechende Regelungen fehlen in der Thüringer Kommunalordnung, sodass diesbezüglich die allgemeinen Bestimmungen des Thüringer Datenschutzgesetzes gelten. Danach wäre z. B. auch eine Nutzung zur allgemeinen Strafverfolgung, zur Verfolgung von Ordnungswidrigkeiten oder zur Durchführung wissenschaftlicher Forschung nicht ausgeschlossen.

Ich habe das TIM gebeten, die aufgezeigten Probleme bei einer Novellierung des Kommunalwahlgesetzes zu berücksichtigen. Das TIM hat zwischenzeitlich zugesagt, meine Wahlrechtsänderungsvorschläge im Falle einer Novellierung des Thüringer Kommunalwahlrechts in die Überprüfung einzubeziehen.

5.2.4 Auslegung von Wählerverzeichnissen

Bereits in meinem 1. TB (5.2.6.1) hatte ich darauf hingewiesen, dass aufgrund der gegenwärtigen Praxis der öffentlichen Auslegung der Wählerverzeichnisse über alle Wahlberechtigten die Gefahr besteht, dass sich im Einzelfall eine missbräuchliche Benutzung nicht ausschließen lässt, weil sich Personen im Rahmen der Einsichtnahme Kenntnis über Wohnanschriften von Wahlberechtigten beschaffen können, für die aus Gründen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnlichen schutzwürdigen Belangen der Betroffenen (Zeugen in Strafverfahren, Bewohner von Frauenhäusern, psychiatrischen Einrichtungen, Justizvollzugsanstalten oder deren Beschäftigte u. ä.) im jeweiligen Melderegister eine Auskunftssperre eingetragen ist. Insoweit kann der vom Gesetzgeber in den Meldegesetzen garantierte Schutz gefährdeter Personen hinsichtlich der Unterbindung einer Auskunftserteilung aus dem nicht-öffentlichen Melderegister unterlaufen werden.

Bereits in ihrer 49. Konferenz 1995 hatten die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung (1. TB, Anlage 20) auf diesen Widerspruch hingewiesen und vom Gesetzgeber eine Neuregelung gefordert, die diese Missbrauchsmöglichkeit ausschließt. Trotz mehrfacher Nachfrage konnte in der Vergangen-

heit bisher in Thüringen keine grundlegende Änderung herbeigeführt werden. Lediglich bei konkreten Anfragen der Gemeindeverwaltungen wurden diese darauf hingewiesen, durch geeignete organisatorische Maßnahmen die Kenntnisnahme der Daten von Wahlberechtigten, für die obige Auskunftssperre im Melderegister eingetragen ist, bei der Einsichtnahme von Dritten in Wählerverzeichnisse zu verhindern.

Dass die allgemeinen datenschutzrechtlichen Bedenken durchaus nicht praxisfern sind, zeigte das gegenüber dem TLfD zum Ausdruck gebrachte Unverständnis eines Justizvollzugsbeamten, der feststellen musste, dass sich eine Privatperson aus dem Wählerverzeichnis seine aus Sicherheitsgründen im Melderegister „gesperrte“ Anschrift beschafft und für einen im Zusammenhang mit seiner dienstlichen Tätigkeit stehenden „unliebsamen Privatbesuch“ genutzt hatte. Auch wenn dieses konkrete Vorkommnis keine unmittelbaren weiteren negativen Folgen für den Betroffenen nach sich zog, zeigte es den Verantwortlichen doch die Dringlichkeit einer Lösung. Unverzüglich wurden deshalb alle Wahlorgane im Freistaat Thüringen vom TIM angewiesen, bei der Auslegung der Wählerverzeichnisse künftig die Anschriften von Personen, für die im Melderegister ein entsprechender Sperrvermerk eingetragen ist, während der Zeit der Auslegung des Wählerverzeichnisses unkenntlich zu machen.

Dies erscheint zunächst aufgrund der gegenwärtig geltenden wahlrechtlichen Bestimmungen ein tragfähiger Kompromiss zu sein, um einerseits der Forderung zur Auslegung eines vollständigen Wählerverzeichnisses nachzukommen und andererseits den Schutz gefährdeter Personen, für die in den Melderegistern eine Auskunftssperre eingetragen ist, zu gewährleisten. Dabei darf jedoch nicht außer Acht gelassen werden, dass bereits durch die besondere Form der Darstellung der Daten einiger weniger Wahlberechtigter in den Wählerverzeichnissen (ohne Anschrift) die Tatsache über die „Gefährdung“ dieser Person gegenüber jedem Einsichtnehmenden offenbart wird. Darüber hinaus erfolgt natürlich bereits durch die Aufnahme von Angaben zur Person im Wählerverzeichnis die Bekanntgabe eines melderechtlichen Datums - ihrem Wohnort, was durchaus in kleineren Gemeinden bereits sehr informativ sein dürfte.

Desweiteren darf nicht verkannt werden, dass im Thüringer Meldegesetz nicht nur Schutzregelungen in Form von Auskunftssperren bei einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange für sog. einfacher Melderegisterauskünfte (Namen und Anschrift über eine einzelne bestimmte Personen) gelten. So sind die Meldebehörden nach dem Gesetz vor einer Auskunftserteilung über bestimmte Personengruppen, wie Bewohnern von Pflegeheimen, Betreuungseinrichtungen oder Haftanstalten zur Durchführung einer Einzelfallprüfung und Anhörung des Betroffenen im Hinblick auf mögliche entgegenstehende schutzwürdige Interessen verpflichtet. Dies kann gegenwärtig noch durch die Einsichtnahme in Wählerverzeichnisse unterlaufen werden.

Da es innerhalb der einzelnen Bundesländer zwischenzeitlich unterschiedliche Regelungen zum Verfahren der Auslegung von Wählerverzeichnissen gibt (insbesondere hinsichtlich der Auskunftserteilung bei melderichtlich gesperrten Daten) sollte die diesbezügliche Diskussion in der Bund-/Länder-Arbeitsgruppe „Wahlrecht“ fortgesetzt werden, mit dem Ziel, eine einheitliche Lösung, die sowohl die Forderung der Öffentlichkeit nach Transparenz der Wahlen wie auch das Recht auf informationelle Selbstbestimmung des Wahlberechtigten berücksichtigt, zu finden. Eine Möglichkeit wäre nach meiner Auffassung wie bereits in vielen Gemeinden praktiziert, die Nutzung automatisierter Wählerverzeichnissen, indem über Terminals in den Wahlbüros/Meldeämtern in Anwesenheit eines Mitarbeiters die Ordnungsmäßigkeit des Wählerverzeichnisses dahingehend geprüft werden kann, ob nach Eingabe des Namens, Vornamens und ggf. des Geburtstages oder der Anschrift die konkrete genannte Person darin eingetragen ist oder nicht, ohne dass weitere, d. h. nicht eingebene, Daten offenbart werden.

5.2.5 Anhörungsbogen zur Bestimmung der Hauptwohnung

Die Bestimmung des Haupt- oder Nebenwohnsitzes hat nicht nur für den Betroffenen selbst Konsequenzen hinsichtlich der Wahrnehmung von staatsbürgerlichen Rechten z. B. bei Wahlen oder Pflichten bei der Zahlung von Steuern und Abgaben, sondern ist für die Gemeinde eine entscheidende Bezugsgröße für die Zuweisung fi-

nanzieller Mittel aus dem Landeshaushalt, da insbesondere die Aufteilung der Gemeindeanteile an der Einkommenssteuer nach der Anzahl der Bewohner mit Hauptwohnung (Einwohner) in der Gemeinde erfolgt. Insoweit liegt es im vitalen Interesse jeder Gemeinde, dass alle Bewohner, die sich überwiegend im Einzugsgebiet aufhalten auch ihrer Meldepflicht nachkommen, indem sie ihre Hauptwohnung in der Gemeinde anmelden. Dass dabei im Einzelfall aus der Sicht des Datenschutzes der Grundsatz der Verhältnismäßigkeit nicht ausreichend beachtet wird, erfuhr ich durch die Eingabe eines Bürgers. Danach wurde in einer Gemeinde im Nachgang zur Anmeldung einer Nebenwohnung einem Einwohner ein Anhörungsbogen mit konkreten Fragestellungen zur Bestimmung der Haupt- oder Nebenwohnung zugesandt. Gefordert wurden Erklärungen, zu welchem Zweck und an welchen einzelnen Wochentagen er sich in der Gemeinde aufhält, wie viele Wochen, Monate oder Jahre die voraussichtliche Aufenthaltsdauer in der Gemeinde sein wird, in welcher Entfernung die beiden Wohnungen (Haupt- und Nebenwohnung) liegen, ob an den Wochenenden nach Hause gefahren wird, ob und wie lange man sich in den Ferien/Urlaub am „Heimatort“ aufhalten wird und wann und aus welchem Gründen man sich außerdem auch nicht in der Gemeinde aufhalten wird.

Selbstverständlich gehört es zu den Aufgaben der Meldebehörden zu prüfen, ob die von den Betroffenen vorgenommenen Angabe zur Haupt- oder Nebenwohnung den melderechtlichen Bestimmungen entsprechen. Nach dem Thüringer Meldegesetz hat jeder Einwohner bei jeder An- oder Ummeldung mitzuteilen hat, welche weitere Wohnung er hat und welche der Wohnungen seine Hauptwohnung ist. Wie aus den Erläuterungen zur Ausfüllung des Meldescheins Anlage 1 zur Thüringer Meldescheinverordnung zu entnehmen ist, soll dementsprechend der Betreffende selbst im Meldeschein seine Haupt- und Nebenwohnung eintragen. Um Missverständnisse auszuschließen, erhält er dazu mit den Anmeldeformularen auch „Hinweise zur Mitteilung über die Änderung der Hauptwohnung“, in denen er darüber informiert wird, dass die Hauptwohnung regelmäßig dort anzugeben ist, wo er sich zeitlich überwiegend aufhält. Ergänzend werden einige Ausnahmefälle erläutert und vermerkt, dass bei Unklarheiten, die Meldebehörde ihn dabei unterstützen wird, festzustellen, welche der Wohnungen die Hauptwohnung ist. Eine zusätz-

liche Datenerhebung ist weder nach dem Meldegesetz noch nach der Meldescheinverordnung bei der Anmeldung von Nebenwohnungen vorgesehen.

Insoweit kann es sich bei der Prüfung der Richtigkeit der Eintragung der Hauptwohnung im Meldeschein regelmäßig nur um Plausibilitätskontrollen (insbesondere hinsichtlich der Entfernung zwischen den Wohnorten) handeln. Ergeben diese Anhaltspunkte hinsichtlich einer fehlerhaften Bestimmung der Hauptwohnung, sind sicher auch mündliche Fragen nach den Gründen und den voraussichtlichen Zeiten des Aufenthaltes am Ort der Nebenwohnung erlaubt, ohne dass dies im Meldeamt gespeichert wird. Soweit dabei keine einvernehmliche Klärung erfolgt, kann die Meldebehörde nach § 28 Abs. 1 ThürVwVfG den Betroffenen im Rahmen der Anhörung auffordern, seine Gründe für die Bestimmung der Hauptwohnung darzulegen. Eine regelmäßige zusätzliche Datenerhebung insbesondere aber eine Pflicht zur Beantwortung vorgegebener Fragen, die nicht in jedem Fall entscheidungsrelevant sein müssen, widerspricht dem Grundsatz der Verhältnismäßigkeit, da hierbei eine Datenerhebung über das erforderliche Maß nicht auszuschließen ist. Die auf dem Anhörungsbogen enthaltenen Fragen sollten stattdessen dem Betroffenen lediglich als Orientierungshilfe mitgeteilt werden. Meinem diesbezüglichen Vorschlag künftig auf die Vorgabe eines Fragebogens zu verzichten, wurde seitens der Meldebehörde gefolgt.

5.2.6 Liste der Gewerbetreibenden von Gemeinde an Werbeagentur übergeben

Durch eine Eingabe wurde ich auf eine Verfahrensweise einer Gemeinde aufmerksam, die ein durchaus sinnvolles Ziel verfolgte, es dabei jedoch mit der Einhaltung datenschutzrechtlicher Vorschriften nicht so genau nahm. Um die Gemeinde mit ihren Einrichtungen in der Öffentlichkeit vorzustellen sowie den ortsansässigen Gewerbetreibenden die Möglichkeit zu geben, sich mit ihrem Leistungsangebot zu präsentieren, beabsichtigte die Kommune, einen Ortsprospekt von einer Werbeagentur erstellen zu lassen. Die Finanzierung der Broschüre sollte durch Werbeanzeigen der ortsansässigen Gewerbetreibenden erfolgen. Um der beauftragten Werbeagentur die Arbeit zu erleichtern und dieser die Möglichkeit zu geben, die Gewerbe-

treibenden gezielt anzusprechen, wurde einer Mitarbeiterin der Werbeagentur die Kopie einer Liste aller Gewerbetreibenden mit Angaben der Branche, der Adresse sowie des Namens des Inhabers übergeben. Diese Liste ging auf die beim Landratsamt als unterer Gewerbebehörde gespeicherten Gewerbeanzeigen zurück und wurde der Gemeinde als Steuerstelle vom Landratsamt entsprechend § 14 Abs. 5 Satz 2 Gewerbeordnung (GewO) i. V. m. § 138 Abgabenordnung (AO) übermittelt. Obwohl der Bürgermeister im Gemeindeblatt die Gewerbetreibenden auf die Beauftragung der Werbeagentur hingewiesen hat und der Mitarbeiterin dieser Agentur ein Legitimationsschreiben mit auf den Weg gegeben wurde, hat sich der Petent beim Hausbesuch darüber gewundert, wie die betreffende Mitarbeiterin der Werbeagentur in den Besitz der Liste der Gewerbetreibenden kommen konnte.

Auf meine Nachfrage hat die Gemeinde hinsichtlich der Erforderlichkeit dieser Datenübermittlung lediglich darauf hingewiesen, dass es „günstig gewesen sei“ für die Agentur den Ansprechpartner in den Gewerbebetrieben zu kennen. Eine Übermittlung auf der Grundlage der Vorschriften des § 14 GewO kam dabei deswegen nicht in Betracht, weil Adressat dieser Vorschriften die Gewerbebetriebe sind. Die Gemeinde hat diese Daten aus den Gewerbeanzeigen aber nur als Steuerstelle nach § 138 AO erhalten. Maßstab für eine Übermittlung an Dritte ist § 22 ThürDSG, dessen Voraussetzungen nicht vorlagen. Insbesondere konnte die Gemeinde nach § 22 Abs. 1 Nr. 2 ThürDSG nicht davon ausgehen, dass die betroffenen Gewerbetreibenden kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung gehabt haben. Dies wurde insbesondere durch die mir vorliegende Beschwerde belegt. Ich habe daher diesen Verstoß gegen Datenübermittlungsvorschriften gegenüber der Gemeinde beanstandet und diese aufgefordert, die Liste von der Werbeagentur unverzüglich zurückzufordern und sicherzustellen, dass dort keine unzulässig gefertigten Kopien verblieben sind. Dies ist im Nachgang geschehen. Zudem wird das zuständige Landratsamt aufgrund meiner Forderung zukünftig bei der Übermittlung derartiger Listen die Gemeinden auf die besondere Zweckbindung dieser zu Steuerzwecken übermittelten Daten hinweisen.

5.2.7 Umgang mit Unterlagen nicht-öffentlicher Sitzungen

Erneut musste ich mich auch im vergangenen Berichtszeitraum mit dem Umgang mit Unterlagen nicht-öffentlicher Sitzungen in kommunalen Vertretungskörperschaften befassen (2. TB 5.2.16). Im vorliegenden Fall waren im Rahmen einer öffentlichen Sitzung eines Kreisausschusses zur Erörterung eines Antrages auf Zuschuss zu den Sachkosten aus dem Kreishaushalt zur Finanzierung einer Beratungsstelle aus einer Vorlage für eine nicht-öffentliche Sitzung Daten zur tariflichen Eingruppierung einzelner Beschäftigter der Beratungsstelle genannt und somit der Inhalt einer vertraulichen Information unbefugt veröffentlicht worden. Veröffentlichungen von personenbezogenen Daten sind die weitreichendste Form einer Offenbarung, deren Zulässigkeit nach den Bestimmungen für Datenübermittlungen an nicht-öffentliche Stellen zu beurteilen ist. Dementsprechend dürfen personenbezogene Daten veröffentlicht werden, soweit dies durch spezialgesetzliche Regelungen ausdrücklich erlaubt oder bestimmt ist, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgabe erforderlich sind und die Zweckbindung der Daten dies zulässt oder der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene keine schutzwürdigen Interessen an dem Ausschluss der Übermittlung hat. Diese Voraussetzungen waren aber im vorliegenden Fall nicht gegeben, zumal durch die Zweckbestimmung der Vorlage - für eine nicht-öffentliche Sitzung - der weitere Umgang mit den Daten ausdrücklich als „nicht für die Öffentlichkeit bestimmt“ vorgegeben war. Als problematisch bei der Klärung des Sachverhaltes stellte sich insbesondere heraus, dass der Begriff des Personenbezugs häufig nicht weit reichend genug gesehen wird und dadurch die Bestimmbarkeit von Personen bzw. die Möglichkeit, dass Dritte mit einem entsprechenden Zusatzwissen durchaus eine personenbezogene Zuordnung der Daten vornehmen können, nicht erkannt wird. Darüber hinaus fällt es schwer, Informationen, die nur für nicht-öffentliche Sitzungen bestimmt sind, nicht in öffentlichen Sitzungen zu verwerten, insbesondere, wenn in den Sitzungen ähnliche Themen behandelt werden. Besonders schwierig wird diese Trennung, wenn die Unterlagen für eine nicht-öffentliche Sitzung langfristig übergeben werden und wie im

konkreten Fall vor der Beratung eine öffentliche Sitzung mit einer entsprechenden Thematik liegt.

Im Ergebnis meiner Beanstandung wurde deshalb die Problematik der Bereitstellung und Nutzung von Unterlagen für nicht-öffentliche Sitzungen im Kreistag eingehend erörtert und auf die datenschutzrechtlichen Bestimmungen insbesondere hinsichtlich der Verschwiegenheitspflicht der Kreistags- und Ausschussmitglieder sowie der Beachtung der Zweckbindung der Unterlagen hingewiesen. Darüber hinaus wurden innerhalb der Verwaltung Festlegungen getroffen, mit dem Ziel bei der Erarbeitung und Bereitstellung von Unterlagen für die Kreistagsmitglieder den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit noch stärker Beachtung zu schenken. Entsprechende ergänzenden Regelungen wurden auch für die Hauptsatzung vorgesehen.

5.2.8 Tonaufnahmen von Kreistags- und Gemeinderatssitzungen

Den TLfD erreichten im Berichtszeitraum mehrere Anfragen zur Zulässigkeit von Tonaufzeichnungen in Kreistags- bzw. Gemeinderatssitzungen. Bei entsprechenden Nachfragen stellte ich fest, dass diese in einigen Kreisen und Gemeinden, obwohl sie nur zur Erstellung der Niederschriften der Sitzungen angefertigt werden sollten, über einen längeren Zeitraum aufbewahrt und teilweise auch archiviert werden. Wie auch den Kommentaren zur Kommunalordnung zu entnehmen ist, kann durch Beschluss des Kreistages oder des Gemeinderates bestimmt werden, dass zur Erstellung der Niederschriften Tonaufnahmen während der Sitzungen zu fertigen sind. Dieses muss von den Anwesenden im Hinblick darauf, dass die Herstellung einer richtigen und vollständigen Niederschrift höher zu bewerten ist als das Persönlichkeitsrecht der Mitglieder an ihrem gesprochenen Wort, hingenommen werden. Den Grundsätzen des Datenschutzes folgend, sind die Aufnahmen aber, sobald sie für diesen Zweck, d. h. heißt zur Erstellung der Niederschrift nicht mehr benötigt werden, zu löschen. Da in den Sitzungen nicht nur die gewählten Vertreter sondern z. B. in Einwohnerfragestunden auch Bürger oder ansonsten auch ausgewählte Bedienstete der Verwaltung als mögliche Redner in Betracht kommen, kann auch nicht

durch einstimmigen Beschluss des informationellen Selbstbestimmungsrecht der vorgenannten Personen unbeachtet bleiben, in dem die Tonaufnahmen über diesen Zeitraum hinaus aufbewahrt und für andere Zwecke verwendet werden. Letztlich soll die Willensbildung des Rates freimütig und in aller Offenheit verlaufen. Allein durch das Bewusstsein eines Tonbandmitschnittes können insbesondere in kleineren Gemeinden weniger redegewandte Ratsmitglieder, Beschäftigte oder Bürger ihre Spontaneität verlieren und sich in ihrer Meinungsäußerung beschränken oder gegebenenfalls völlig schweigen. Anders als Wortprotokolle geben Tonaufzeichnungen eben nicht nur den Inhalt der Beratung wieder, sondern sie zeigen jede Nuance der Rede einschließlich der rhetorischen Fertigkeiten und Fehlleistungen, wie auch der sprachlichen Unzulänglichkeiten oder Gemütsbewegungen der Redner. Dies aufzuzeichnen ist aber nicht Zweck der Tonaufnahme, sondern sie soll lediglich als Hilfsmittel zur Erstellung einer richtigen und vollständigen Niederschrift der Sitzung dienen. Da ohnehin nach ihrer Genehmigung nur die Niederschrift zur öffentlichen Urkunde über den Inhalt und Verlauf der Sitzung wird, die Beweiszwecken dient und nach den Prozessordnungen erhöhte Beweiskraft haben kann, ist die Notwendigkeit der weiteren Aufbewahrung der Tonbandmitschnitte nicht mehr gegeben. Insoweit ist es deshalb Aufgabe der Protokollführers ggf. in Abstimmung mit dem Vorsitzenden zu entscheiden, welche Wortmeldungen wesentlich und im Einzelfall auch wörtlich (ggf. in Form eines vollständigen Wortprotokolls) in die Niederschrift aufzunehmen sind. Entsprechend der Zweckbestimmung der Tonaufnahmen sind diese bis zum Zeitpunkt der Genehmigung der Niederschrift aufzubewahren, um Zweifelsfälle darüber, ob der Sitzungsverlauf vollständig und richtig in der Niederschrift wiedergegeben ist, mit den Ratsmitgliedern klären zu können. Anschließend sind sie zu löschen.

Das Landesverwaltungsamt als Rechtsaufsichtsbehörde, welches meine Rechtsauffassung teilt, hat mitgeteilt, dass ein entsprechendes Rundschreiben an die Gebietskörperschaften vorgesehen ist.

5.2.9 Unverhältnismäßige Fragen des Sozialamts zur eheähnlichen Gemeinschaft

Nach § 122 BSHG dürfen Personen, die in eheähnlicher Gemeinschaft leben, hinsichtlich der Voraussetzungen sowie des Umfangs der Sozialhilfe nicht besser gestellt werden als Ehegatten. Das bedeutet für den Fall, dass der Partner einer solchen Gemeinschaft in wirtschaftliche Not gerät, das Sozialamt nur dann Leistungen der Sozialhilfe erbringen darf, wenn der eine Partner nicht in der Lage ist, für den anderen zu sorgen. Bereits in den Sozialhilfeantragsformularen wird der Hilfebedürftige danach gefragt, ob er in einer eheähnlichen Gemeinschaft lebt. Manchen Antragstellern ist oft selbst nicht ganz klar, ob sie ihre Beziehung mit einem Mitbewohner als reine Zweckgemeinschaft oder aber als eine eheähnliche Gemeinschaft im Sinne einer auf Dauer angelegte Verantwortungs- und Einstehensgemeinschaft ansehen würden, weshalb diese Frage z. T. unzutreffend verneint wird. Oder aber es wird ganz bewusst versucht, durch unzutreffende Angaben zu Unrecht Leistungen der Sozialhilfe zu erhalten. Besondere Schwierigkeiten bereitet die Ermittlung einer solchen eheähnlichen Gemeinschaft den Sozialämtern deshalb, weil anders als bei der Eheschließung kein formaler, staatlich vollzogener Rechtsakt die Einstehensgemeinschaft begründet, sondern vom Willen der Betroffenen abhängt, der nur über äußere Anhaltspunkte ermittelt werden kann, die sich regelmäßig im Kernbereich der privaten Lebensführung abspielen. Aus diesem Grund sind in diesen Fällen Konflikte mit dem Persönlichkeitsrecht geradezu vorprogrammiert.

Aufgrund einer Eingabe hatte ich Veranlassung einen Fall zu überprüfen, bei dem Mitarbeiter des Sozialamtes einen Hausbesuch bei einem Sozialhilfeantragsteller durchgeführt hatten, um die Angaben des Betreffenden in einem „Überprüfungsbogen zum § 122 BSHG“ vor Ort zu kontrollieren. Das Sozialamt hatte Anhaltspunkte dafür, dass der Antragsteller entgegen seinen Angaben in einer eheähnlichen Gemeinschaft mit seiner Untervermieterin zusammenleben könnte. Im Rahmen des Hausbesuches wurden dem Antragsteller anhand eines Fragebogens Angaben abverlangt, die teilweise sehr tief in die private Lebensführung eingreifen. So wurde z. B. danach gefragt, wer einkauft, die Wohnung reinigt und wie die Freizeit

gemeinsam verbracht wird. Gleichzeitig wurde festgestellt, dass der dem Antragsteller vermietete Raum weniger als die Hälfte der im Sozialhilfeantrag angegebene Größe umfasste. Obwohl dies gleich zu Beginn der Begehung festgestellt worden war, haben die Sozialamtsmitarbeiter den umfangreichen Fragebogen vollständig abgearbeitet.

Die Entscheidung zur Rückforderung der Sozialhilfe hat das Sozialamt jedoch nicht mit der Annahme einer eheähnlichen Gemeinschaft begründet, sondern ausschließlich auf den tatsächlich wesentlich kleineren angemieteten Raum und damit die geringere Mietzahlung gestützt, was bei der Nachberechnung zum Wegfall des Sozialhilfeanspruchs führte. Die Tatsache, dass die sehr weit in den privaten Lebensbereich zielenden Fragen gestellt und die Antworten erhoben wurden, obwohl sich schon bei der Begehung zeigte, dass eine Rückforderung der gezahlten Sozialhilfe aufgrund des wesentlich kleineren Zimmers erfolgen konnte, habe ich als unverhältnismäßige Datenerhebung gegenüber dem Sozialamt beanstandet.

In Gesprächen mit dem Sozialamt habe ich klargestellt, dass es den Trägern der Sozialhilfe möglich sein muss, auch in denjenigen Fällen, in denen begründete Zweifel daran bestehen, dass entgegen den Angaben des Betroffenen eine eheähnliche Gemeinschaft nach § 122 BSHG vorliegt, die erforderlichen und angemessenen Ermittlungen unter Mitwirkung der Betroffenen erfolgen können. Da jedoch in diesen Fällen regelmäßig der Kernbereich der privaten Lebensführung betroffen ist, muss sich diese Ermittlungstätigkeit streng am Verhältnismäßigkeitsgrundsatz im Einzelfall orientieren. Der Einsatz eines Fragebogens, dessen Fragen in jedem Fall vom Betroffenen erhoben werden, birgt daher die Gefahr, dass im Einzelfall eine Vielzahl sensibler Daten ohne Erforderlichkeit erhoben und gespeichert werden. Deshalb ist nunmehr das Sozialamt dazu übergegangen, den Mitarbeitern einen Fragenkatalog an die Hand gegeben, der auf die von der Rechtsprechung entwickelten Kriterien zur Annahme einer eheähnlichen Gemeinschaft abzielt. Von den Mitarbeitern sind dann unter Beachtung des Verhältnismäßigkeitsgrundsatzes anhand dieser Kriterien und auf den Einzelfall abgestellt nur die konkret erforderlichen Angaben zu ermitteln.

5.2.10 Sozialhilfebeantragung durch Krankenhaus?

Aufgrund einer Anfrage habe ich mich mit der Problematik befasst, unter welchen Voraussetzungen Sozialämter von Krankenhäusern personenbezogene Daten zur Prüfung eines Erstattungsantrags nach § 121 BSHG erheben dürfen. Hintergrund sind solche Konstellationen, bei denen die Patienten, die in Eilfällen in Krankenhäuser aufgenommen wurden, weder gesetzlich noch privat krankenversichert sind und auch sonst nicht in der Lage sind, die Krankenhausrechnung zu begleichen. Für diese Fälle sieht § 121 BSHG vor, dass das Krankenhaus solche Aufwendungen auf Antrag in gebotenem Umfang vom Sozialamt erstattet bekommt, wenn das Krankenhaus die Gründe für den Eilfall in angemessener Frist dem Sozialamt mitteilt. Dabei wurde von einem Sozialamt ein Antragsbogen für derartige Erstattungsansprüche verwendet, der zum einen eine ärztliche Bescheinigung über den Patienten enthielt, worin bestätigt wird, dass es sich bei der Behandlung nicht um eine körperliche oder geistige Behinderung handelt. Neben den Angaben zu den erbrachten Leistungen und zur Begründung der Eilbedürftigkeit der Behandlung wurden aber auch Angaben über das Einkommen des Patienten und dessen Ehegatten abgefragt. Dabei sollte der Patient durch seine Unterschrift auf dem Antragsvordruck eine Sozialhilfeantragstellung dokumentieren. Eine derartige Vermischung der Antragstellung nach § 121 BSHG und der Sozialhilfeantragstellung führt jedoch zwangsläufig dazu, dass Mitarbeiter der Krankenhausverwaltung personenbezogene Daten zu den wirtschaftlichen Verhältnissen des Patienten zur Kenntnis bekommen, die für ihre Aufgabenstellung in keiner Weise erforderlich sind. Demgegenüber halte ich die Angaben in der ärztlichen Bescheinigung für erforderlich, um dem Sozialhilfeträger die Entscheidung zu ermöglichen, ob sachlich eine Zuständigkeit des überörtlichen Trägers der Sozialhilfe nach § 39 BSHG (Eingliederungshilfe für Behinderte) oder aber des örtlichen Trägers der Sozialhilfe zur Bearbeitung des Erstattungsantrages nach § 121 BSHG vorliegt. Was die Vermischung der Angaben zur Erstattung nach § 121 BSHG und der Sozialhilfeantragstellung angeht, so habe ich nach längeren Gesprächen mit dem Sozialamt folgenden Vorschlag unterbreitet, um den Erfordernissen des Datenschutzes und der Praxis gleichermaßen Rechnung zu tragen:

Das Krankenhaus hält Antragsvordrucke auf Sozialhilfeleistungen vor. Kommt es zu einem Antrag nach § 121 BSHG des Krankenhauses, hat der Patient - auf seinen Wunsch hin, gegebenenfalls mit Hilfe einer Vertrauensperson (z. B. einem Angehörigen oder einem Mitarbeiter des Krankenhaussozialdienstes) - einen Sozialhilfeantrag auszufüllen. Das Krankenhaus nimmt von den einzelnen Angaben im Antrag keine Kenntnis, sondern stellt nur sicher, dass der Antrag ausgefüllt und an das Sozialamt weitergeleitet wird. Dies kann z. B. Einlegenlassen des Antrages in ein verschlossenes Kuvert (wie bei Arztbriefen) geschehen. Das Krankenhaus sendet daraufhin das geschlossene Kuvert zusammen mit seinem Antrag nach § 121 BSHG und den hierzu ergänzten medizinischen Angaben an das Sozialamt.

Ich gehe davon aus, dass mit dieser Verfahrensweise entstandene Irritationen aus datenschutzrechtlicher Sicht ausgeräumt werden können.

5.2.11 Beschriftung von Überweisungsträgern und Postsendungen

Im Jahre 1994 hatte das Bundesverwaltungsgericht entschieden, dass es nicht zulässig sei, die Zahlung von Sozialhilfe auf Überweisungsträgern generell mit dem Vermerk „Sozialleistung“ zu kennzeichnen. In einer Eingabe wurde ich darauf hingewiesen, dass landesweit bisher bei der Zahlung von Wohngeld auf den Überweisungsträgern stets die Abkürzung „WG“, „Monat/Jahr“ sowie die Anschrift des Wohngeldempfängers vermerkt wurden. Da es sich beim Wohngeld ebenso um eine Sozialleistung handelt und Sozialdaten generell o. g. besonderen Schutz unterliegen, bedurfte es für die Übermittlung des Hinweises auf die Zahlung einer Sozialleistung mangels einer entsprechenden Rechtsgrundlage der Zustimmung der Betroffenen, die aber in keinem Fall eingeholt worden war. Aufgrund meines Hinweises wurde deshalb das Verfahren dahingehend geändert, dass künftig auf den Überweisungsträgern ebenso wie auf den Kontoauszügen nur noch ein codierter Zahlungsgrund, der den Betroffenen bekannt ist, aufgenommen wird, um eine unbefugte Kenntnisnahme durch Dritte auszuschließen.

In entsprechender Weise gilt obiges auch - soweit möglich - bei der Beschriftung von Postsendungen. So wurde ich darüber unterrichtet, dass von einem Sozialamt bzw. einer Wohngeldbewilligungsstelle neben dem Stempelaufdruck (Freistempler) der Stadtverwaltung zusätzlich der Stempelaufdruck „Sozialamt“ bzw. „Wohngeldbewilligungsstelle“ aufgebracht worden war. Es stellte sich deshalb die Frage nach der Erforderlichkeit der zusätzlichen Absenderangabe auf dem Umschlag, da durch den Freistempler bereits der Absender hinreichend präzisiert wurde, um gegebenenfalls Rücksendungen zu ermöglichen. Aufgrund des zusätzlichen Stempelaufdrucks wurden unnötigerweise Dritten Informationen gegeben, die Hinweise auf die Beziehung des Betroffenen zu einem Sozialleistungsträger geben, was mangels einer Erforderlichkeit als Verstoß gegen die Bestimmung des Sozialgesetzbuches zu werten ist. Von der Stadtverwaltung wurden deshalb die Ämter aufgefordert, künftig im Schriftverkehr nach außen auf den Briefumschlägen bzw. im Fensterbereich der Umschläge nur Bezeichnungen (insbesondere Strukturnummern) zu verwenden, die keinen unmittelbaren Rückschluss auf den Inhalt der Sendung und den konkreten Absender innerhalb der Verwaltung geben.

In diesem Sinn habe ich im Übrigen auch bereits vor längerer Zeit entschieden, dass bei der Beantwortung von Eingaben an Privatpersonen auf den Umschlägen des TLfD statt der Behördenbezeichnung als Absender nur meine Postfachnummer gestempelt wird.

5.2.12 Rückgabe eines behördlichen Schreibens an den Adressaten

Ein Bürger bat mich um meine Mithilfe, von einer Gewerbebehörde ein an ihn adressiertes Schreiben zurück zu erhalten. Der Betroffene berichtete, dass er zu dem betreffenden Gewerbeamt gegangen sei, um sich dort über das im Schreiben angedrohte Bußgeld zu beschweren. Im Verlaufe des Gesprächs habe ihm eine Mitarbeiterin das Schriftstück an sich genommen und nicht wieder ausgehändigt. Entgegen der schriftlichen Mitteilung des Leiters des Gewerbeamts, wonach dieses Schreiben Bestandteil der Akte wäre und der Bürger das Original erhalten hätte, stellte sich auf meine Nachfrage heraus, dass dieses Schreiben in der Gewerbeamtsakte des Bürgers einge-

heftet war. Allerdings habe der Betroffene das Schreiben freiwillig zurückgelassen und es sei auch nicht bekannt, dass das Schreiben von ihm zurückgefordert worden sei.

Eine von mir in diesem Zusammenhang durchgeführte Kontrolle im Gewerbeamt ergab, dass das ursprünglich an den Betroffenen gerichtete Schreiben in der Akte abgelegt war. Da sich im Nachhinein nicht mehr aufklären ließ, ob der Bürger das Schreiben im konkreten Fall beim Gewerbeamt zurückgefordert hatte, dies aber nicht endgültig auszuschließen war, wies ich die Behörde zunächst auf § 13 ThürDSG hin, wonach dem Betroffenen auf Antrag Auskunft zu erteilen ist über die zu seiner Person gespeicherten Daten, den Zweck und die Rechtsgrundlage der Speicherung sowie die Herkunft der Daten und deren Empfänger, soweit diese Angaben gespeichert sind. Ebenfalls war nicht davon auszugehen, dass das Liegenlassen oder Zurückschicken eines Behördenschreibens einer Eigentumsaufgabe gleichkommt. Ich empfahl der Stelle, in solchen Situationen zukünftig einen gesonderten Aktenvermerk über die Rückgabe bzw. Nichtannahme eines behördlichen Schreibens zu erstellen. Außerdem bat ich im konkreten Fall die Stelle, das Schreiben an den Bürger nochmals zu übersenden.

Über ein Jahr später wandte sich der gleiche Bürger erneut an mich und beschwerte sich darüber, dass das o. g. Schreiben ihn bis dahin nicht erreicht hätte. Wie sich bei meiner nochmaligen Rückfrage bei dem Gewerbeamt herausstellte, wurde das Schreiben zwar, wie von mir erbeten, dem Betroffenen zugesandt, allerdings an eine Adresse, unter der dieser 2 Jahre zuvor von Amts wegen abgemeldet wurde. Der Briefumschlag kam mit dem Hinweis „unbekannt verzogen“ an das Gewerbeamt zurück. Obwohl der Stadtverwaltung bekannt war, dass dieser Bürger unter einer Postfachadresse zu erreichen ist und der Betroffene dort nicht angetroffen werden kann, erfolgte die Zusendung an die frühere Adresse. Dagegen habe ich gegenüber der Stadtverwaltung datenschutzrechtliche Bedenken erhoben und diese, unabhängig von den möglichen melderechtlichen Verstößen des Bürgers, aufgefordert, persönliche Schreiben, die keiner besonderen Zustellungsform bedürfen, an dessen Postfachadresse zu übersenden. Dies ist im Anschluss daran erfolgt.

5.3 Sparkassen

5.3.1 Wechsel der Datenschutzkontrolle über die gemeinsame Sparkassenorganisation Hessen-Thüringen

Nach Art. 34 Abs. 2 Satz 3 i. V. m. Art. 2 Abs. 1 Satz 2 des Staatsvertrages über die Bildung einer gemeinsamen Sparkassenorganisation Hessen-Thüringen ist meine Kontrollzuständigkeit über die gemeinsame Sparkassenorganisation Hessen-Thüringen Ende 1999 abgelaufen und turnusgemäß der Hessische Datenschutzbeauftragte seit dem 01.01.2000 für die folgenden vier Jahre die zuständige Kontrollbehörde für den Sparkassen- und Giroverband Hessen-Thüringen, die Landesbank Hessen-Thüringen, die Landesbausparkasse Hessen-Thüringen sowie die Sparkassen Versicherung. Unabhängig von dieser Regelung übe ich allerdings weiterhin die datenschutzrechtliche Kontrolle über die Thüringer Sparkassen aus.

5.3.2 Datenverarbeitung durch Sparkassen Versicherung

In Eingaben mehrerer Bürger beschwerten sich diese bei mir darüber, dass sie von der Sparkassen Versicherung ein an sie adressiertes Werbeschreiben erhalten hatten, in dem ihnen verschiedene Angebote auf Abschluss einer Versicherung unterbreitet wurden. Die Bürger hatte große Zweifel an der Rechtmäßigkeit einer Übermittlung ihrer Daten durch die Brandversicherungsanstalt, mit der seit einiger Zeit keine Vertragsverhältnisse mehr bestanden. Wie meine Recherche in der Sache ergab, haben nach dem Wegfall des Gebäude-Feuer-Versicherungsmonopols alle Hessischen Monopolanstalten zum 1. Juli 1997 unter dem Dach der Sparkassen Versicherung fusioniert. Die Adressdaten aller ehemaliger Kunden sind weiterhin für die wirtschaftliche Betreuung der Kunden genutzt worden, indem diese nach einer gewissen Frist nochmals angesprochen wurden und Produkte der Sparkassen Versicherung angeboten bekamen. In ihrer Stellungnahme hatte die Sparkassen Versicherung die Meinung vertreten, dass durch die Fusion der Monopolanstalten unter dem Dach der Sparkassen Versicherung die Versichertendaten gewissermaßen als „Erbe“ miteingegangen sind und aufsichtsbehördlicherseits akzeptiert wurde, die Daten für einen Zeitraum von ca. 3 Jahren für Werbemaßnahmen der Sparkassen Versicherung zu nutzen. Im

Ergebnis hatte ich den Bürgern mitgeteilt, dass die Verarbeitung und Nutzung der Versichertendaten von ehemaligen Kunden der hessischen Monopolanstalten aufgrund der gegebenen Konstellation keinen Verstoß gegen datenschutzrechtliche Bestimmungen darstellt und es nach § 28 Abs. 1 Nr. 2 BDSG vertretbar ist, diese Verarbeitung und Nutzung zu Werbezwecken für die Sparkassen Versicherung für zulässig zu erachten.

In einer weiteren Eingabe trug mir ein Bürger vor, dass er von der Sparkassen Versicherung die Einstellung der Übermittlung sämtlicher im Rahmen von Vertragsverhältnissen gespeicherten personenbezogenen Daten an Rückversicherer, andere Versicherer, Verband der Schadensversicherer, Vermittler usw. fordert. Ihm wäre bei Vertragsabschluss von dem Versicherungsaußendienstmitarbeiter weder ein Merkblatt zur Datenverarbeitung ausgehändigt noch sei er auf die Möglichkeit hingewiesen worden, von dessen Inhalt Kenntnis zu nehmen. Aus datenschutzrechtlicher Sicht ist es grundsätzlich so, dass eine Einwilligungserklärung nur gültig ist, wenn diese vom Betroffenen unterschrieben ist und er darüber hinaus bei Vertragsabschluss die Möglichkeit hatte, in zumutbarer Weise vom Inhalt des vom Versicherer bereitzuhaltenden „Merkblatts zu Datenverarbeitung“ Kenntnis zu nehmen. Seit einiger Zeit muss dieses Merkblatt aufgrund einer Vereinbarung zwischen den Obersten Aufsichtsbehörden der Länder und der Versicherungswirtschaft spätestens bei Vertragsabschluss übergeben werden. Fehlt es jedoch an einer rechtswirksamen Einwilligung, so sind die in den Einwilligungsklauseln enthaltenen Datenübermittlungen an Dritte unzulässig. Eine Datenverarbeitung darf dann nur im Rahmen des bestehenden Vertragsverhältnisses nach § 28 Abs. 1 Nr. 1 BDSG erfolgen. Die personenbezogenen Daten des Versicherungsnehmers aus bereits unzulässigerweise erfolgten Übermittlungen sind von den betroffenen Stellen gem. § 35 Abs. 2 Nr. 1 BDSG zu löschen. Im vorliegenden Fall konnte jedoch die Sparkassen Versicherung nachweisen, dass in allen Anträgen eine Einwilligungsklausel enthalten ist, die vom Antragsteller zu unterzeichnen ist und in der dieser auf das Merkblatt ausdrücklich hingewiesen wird. Darüber hinaus wurde mir die Kopie des Vertrags zur Verfügung gestellt, aus der klar hervorgeht, dass der Versicherungsnehmer die Einwilligungsklausel unterzeichnet hat. Zur weiteren Frage des Bürgers, ob ein Widerruf einer zuvor

erteilten Einwilligung möglich ist, wird lediglich in § 28 Abs. 3 BDSG insoweit eine Regelung getroffen, als der Betroffene danach bei der speichernden Stelle der Nutzung der Übermittlung seiner personenbezogenen Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung widersprechen kann. Ich musste aber dem Bürger mitteilen, dass eine Einwilligung dann nicht widerrufbar ist, wenn sie mit rechtsgeschäftlichen Abreden verbunden ist oder die weitere Abwicklung des Vertrages in Frage gestellt oder unbillig erschwert wird.

5.3.3 Datenverarbeitung von Sparkassen zur Kreditsicherung

Immer wieder fragen Bürger bei mir an, ob es datenschutzrechtlich zulässig ist, wenn die Sparkassen ohne erkennbaren Anlass ihre langjährigen Kunden dazu auffordern, schriftlich in die sog. SCHUFA-Klauseln einzuwilligen, obwohl ein ungestörtes Vertragsverhältnis besteht. Ich musste den Bürgern mitteilen, dass grundsätzliche datenschutzrechtliche Bedenken gegen die Übermittlung bestimmter personenbezogener Daten an die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) mit Einwilligung des Betroffenen nicht bestehen. Eine Einwilligung ist dann erforderlich, wenn „Positivmerkmale“ des Kontoinhabers (Personenstammsatz sowie Merkmale über die Beantragung, Aufnahme und vertragsgemäße Abwicklung) an die SCHUFA übermittelt werden. „Negativmerkmale“ sind Daten über nicht vertragsgemäßes Verhalten des Kunden und die Einleitung gerichtlicher Maßnahmen und dürfen von den Mitgliedern der SCHUFA ohne Einwilligung des Kunden dorthin übermittelt werden. In der Bundesrepublik sind praktisch alle Kreditinstitute Vertragspartner der SCHUFA, die nach dem Prinzip der Gegenseitigkeit arbeitet. Zur lückenlosen Aufrechterhaltung dieses Prinzips ist es erforderlich, dass alle Kreditinstitute bestimmte Sachverhalte über ihre Kunden mitteilen. Die Kreditinstitute sind zur Übermittlung dieser Daten sogar vertraglich verpflichtet. Allerdings werden im Normalfall den Kunden die SCHUFA-Klauseln bereits zum Zeitpunkt der Beantragung einer Geschäftsbeziehung zur Einwilligung vorgelegt.

Von einer Sparkasse habe ich erfahren, dass es noch Kunden gibt, deren Konten bei den ehemaligen Sparkassen der DDR geführt und

von den Sparkassen nach dem 03.10.1990 weitergeführt wurden. Da von diesen Kunden keine Einwilligungen in die sog. SCHUFA-Klauseln vorliegen, werden diese im Laufe der Zeit bei der Gelegenheit eines konkreten Anlasses, wie Ablauf der ec-Karte, Beantragung einer Kreditkarte, Veränderungen beim Dispositionskredit usw. zur Unterzeichnung vorgelegt. Bei einem auf Guthabenbasis geführten Konto ist eine Übermittlung an die SCHUFA zwar nicht erforderlich, wenn ein Kunde jedoch seine Einwilligung in die SCHUFA-Klauseln verweigert, ist die Sparkasse nicht verpflichtet, z. B. ein Girokonto mit einem Dispositionskredit auszustatten oder eine Kreditkarte auszustellen.

In einem anderen Fall berichtete mir ein Bürger darüber, dass ihm bereits vor Jahren ein Darlehen eingeräumt wurde, welches er wie vereinbart zurückzahlt und hierbei keine Unregelmäßigkeiten aufgetreten seien. Trotzdem habe ihn seine Sparkassenfiliale dazu aufgefordert, nunmehr einen 4-seitigen Erhebungsbogen zur Erstellung einer Vermögensübersicht auszufüllen. Ich hatte mich daraufhin an die Sparkasse gewandt und um Mitteilung gebeten, wieso während eines bereits laufenden Kreditvertrags sämtliche Vermögenswerte des Kunden festgestellt werden. Die Sparkasse legte mir ausführlich dar, dass diese nicht nur im Vorfeld einer Kreditvergabe das legitime Interesse habe, die Bonität des Kreditnehmers zu prüfen. Vielmehr seien die Kreditinstitute verpflichtet, die Kreditwürdigkeit auch für die Zukunft zu prognostizieren. Rein formal hat die Sparkasse auf eine Klausel im Kreditvertrag verwiesen, wonach der Darlehensnehmer jederzeit Einblick in seine wirtschaftlichen Verhältnisse zu gewähren hat und die Sparkasse berechtigt ist, Auskünfte bei Versicherungen, Behörden und sonstigen Stellen einzuholen, die sie zur Beurteilung des Darlehensverhältnisses für erforderlich halten darf. Nach den Allgemeinen Geschäftsbedingungen ist die Sparkasse im äußersten Fall berechtigt, von ihrem Kündigungsrecht Gebrauch zu machen, wenn z. B. eine wesentliche Verschlechterung oder eine erhebliche Gefährdung der Vermögensverhältnisse des Kunden eintritt. Die Maßnahmen würden aber nicht nur der Sparkasse dienen, sondern auch dem Kunden zugute kommen, weil damit die Möglichkeit bestünde, rechtzeitig unterstützende bzw. flankierende Maßnahmen zu ergreifen. Auf der Grundlage der mir von der Sparkasse übersandten Formblätter mit den dort gegebenen Hinweisen

und Aufklärungen konnte ich keinen datenschutzrechtlichen Verstoß durch die Sparkasse feststellen.

6. Personalwesen

6.1 Personalaktenführungsrichtlinie

In meinem 1. TB (6.1.1) als auch im 2. TB (6.1) habe ich dargestellt, dass ich die Verabschiedung einer Personalaktenführungsrichtlinie sehr begrüßen würde. Selbige wurde im Berichtszeitraum vom TIM in Kraft gesetzt und ist im Thüringer Staatsanzeiger Nr. 42/1998, Seite 1812-1816 veröffentlicht worden. Es wird darin empfohlen, diese für die Führung von Personalakten von Beamten der Gemeinden, der Landkreise, der anderen Gemeindeverbände und sonstigen unter der Aufsicht des Freistaats stehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts entsprechend anzuwenden. Die Richtlinie enthält Regelungen zu den Bestandteilen, zur Gliederung und zur Führung der Personalakte sowie zu deren Zugang, einschließlich der Gewährung der Akteneinsicht zur Vorlage und zum Erteilen von Auskünften aus der Personalakte als auch Hinweise zum Umgang mit Bewerbungsunterlagen.

6.2 Personalakten im Justizbereich

Im 2. TB (6.5) hatte ich berichtet, dass ich die Personalaktenführung bei verschiedenen Stellen im Justizbereich und die der Personalaktenführung zugrundeliegende Verwaltungsvorschrift des TJM vom 01.10.1992 beanstandet hatte. Seitens des TMJE war daraufhin zugesagt worden, eine novellierte Fassung der Verwaltungsvorschrift im Einklang mit den gesetzlichen Bestimmungen zu erarbeiten. Vor Inkraftsetzung sollte jedoch die Personalaktenführungsrichtlinie (6.1) abgewartet werden. Nachdem diese zwischenzeitlich vorliegt, hat mir auf Nachfrage das TMJE im Mai 1999 den 3. Entwurf der Verwaltungsvorschrift „Ergänzende Bestimmungen zu der Personalaktenführungsrichtlinie des Thüringer Innenministeriums vom 21. September 1998 (ThürStAnz Seite 1812) für den Geschäftsbereich des TMJE“ mit Stand vom 3. März 1999 zur Kenntnis übersandt. Insgesamt war nach dem vorliegenden Entwurf davon auszugehen, dass die bislang vorhandenen Unterlagen bei den einzelnen

Stellen eine Reduktion erfahren werden, was eine meiner Forderungen war. Er sollte nach Auskunft des TMJE allerdings nochmals überarbeitet werden. Ein Bereich, der mit dem vorliegenden Entwurf nicht geregelt ist, ist die Frage der Aufbewahrungsfristen von Personalakten der Angestellten und Arbeiter sowie von Bewerbungsschreiben. Die Aufbewahrungsfrist für diese Unterlagen sind in den „Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden“, die bundeseinheitlich als Verwaltungsvorschrift umgesetzt sind, geregelt. Danach werden Personalakten von Arbeitern und Angestellten 20 Jahre nach Ausscheiden aus dem Dienst und Bewerbungsschreiben von Bewerbern, die nicht in Personalakten einmünden, fünf Jahre aufbewahrt. Bewerbungsschreiben sollten nach meiner Auffassung nur so lange aufbewahrt werden, wie dies zur Dokumentation des Eingangs und der Rücksendung der Unterlagen erforderlich ist. Bezüglich der Aufbewahrung von Personalakten von Arbeitern und Angestellten habe ich zu Bedenken gegeben, dass hier die Aufbewahrungsfristen nach § 103 des Thüringer Beamtengesetzes, wonach die Aufbewahrung von Personalakten von Beamten lediglich fünf Jahre nach deren Abschluss beträgt, entsprechend angewendet werden sollten, da keine Gründe für eine andere Behandlung ersichtlich sind. Die Diskussion ist noch nicht abgeschlossen. Eine aktuelle Fassung des Entwurfs liegt noch nicht vor.

6.3 Personalverwaltung der Lehrer

Bereits im 1. TB (6.4) als auch in meinem 2. TB (6.4) habe ich Ausführungen zur Personalverwaltung der Lehrer gemacht. Im zurückliegenden Berichtszeitraum stand die nach Auflösung der Abteilung 4 des Landesverwaltungsamtes erforderliche Neuverteilung der Aufgaben der Lehrpersonalverwaltung zwischen den staatlichen Schulämtern und dem TKM und den daraus resultierenden datenschutzrechtlichen Konsequenzen im Mittelpunkt. Die Übernahme der bei den Landratsämtern aufbewahrten Personalakten der vor dem 03.10.1990 aus dem Schuldienst ausgeschiedenen Lehrer und Erzieher durch die staatlichen Schulämter ist weitgehend abgeschlossen. Wie aus der Stellungnahme der Landesregierung zum 2. TB zu entnehmen war, sind die alten Personalakten zum Großteil in die staat-

lichen Schulämter verbracht worden. In den anderen Fällen wurden Vereinbarungen mit den zuständigen Kreisarchiven geschlossen, wonach diese die Personalakten im Auftrag der Schulämter weiter aufbewahren. Diese Art der Auftragsdatenverarbeitung halte ich im Hinblick auf die zum Teil bestehende Raumnot in den Schulämtern für eine Übergangszeit für akzeptabel.

Nachdem die Abteilung 4 des Landesverwaltungsamtes 1997 aufgelöst und die Aufgaben auf die staatlichen Schulämter bzw. das TKM verteilt wurden, mussten auch die aktuellen Personalakten an die staatlichen Schulämter übergeben werden. Dadurch bedingt konnte die bislang bei den staatlichen Schulämtern praktizierte und von mir bereits mehrfach beanstandete doppelte Personalaktenführung beendet werden. Um festzustellen, ob dies in der Praxis auch tatsächlich erfolgt, habe ich im Berichtszeitraum ein Schulamt einer datenschutzrechtlichen Kontrolle unterzogen. Diesem waren die Personalakten vom Landesverwaltungsamt übergeben worden. Die bis dahin geführten Personalnebenakten waren zum Zeitpunkt der Kontrolle noch nicht aufgelöst. Ich habe das Schulamt aufgefordert, diese Personalnebenakten aufzulösen, wobei die für die Personalakte erforderlichen Unterlagen diesen beigelegt, nicht benötigte Originale an die Betroffenen zurückgegeben und alle Kopien von in der Personalakte bereits vorhandenen Unterlagen vernichtet werden sollten. Dies ist zwischenzeitlich größtenteils erfolgt.

Die dort vorgefundene Personalaktenführung wies allerdings noch weitere Mängel auf. So waren den Akten jeweils nach Jahren geordnete Abwesenheitsblätter beigelegt, auf denen die Abwesenheitszeiten des Mitarbeiters (z. B. Krankheit, Urlaub etc.) eingetragen waren, die seit der Einstellung bzw. Übernahme des Lehrers - im konkreten Fall seit 1990 - aufgetreten sind. Für eine Aufbewahrung dieser Listen über mehrere Jahre bestand keinerlei Erforderlichkeit. Nach meiner Beanstandung hat das Schulamt die Listen aus den Personalakten entfernt. Verbesserungsbedürftig war auch die Tatsache, dass die Personalakten nicht durchnummeriert waren, was die Überprüfung der Vollständigkeit der Personalakte erschwert. Schließlich waren zur Akte gehörende ärztliche Gutachten zwar in einem Briefumschlag beigelegt, der jedoch nicht zugeklebt war. Um den Zugriff auf derart sensible personenbezogene Daten nur für

den erforderlichen Fall zu ermöglichen, habe ich das Schulamt aufgefordert, künftig entsprechend der Personalaktenführungsrichtlinie des TIM zu verfahren und die Umschläge mit dem Vermerk „ärztliche Unterlagen“ zu kennzeichnen, wobei das Öffnen und Schließen des Umschlags durch Unterschrift und Datumsangabe zu bestätigen ist. Eine entsprechende Verfahrensweise wie auch die Durchnummerierung der Akten ist weitgehend erfolgt.

Die automatisierte Verarbeitung von Lehrerpersondaten erfolgt mit dem Stellen- und Personalverwaltungssystem PERSOS-S auf der Basis des Datenbankprogramms ACCESS. Es handelt sich dabei um eine auf die Bedürfnisse des Schulbereichs angepasste Fassung des bereits in der Landesverwaltung zur Anwendung kommenden Systems PERSOS-TH (1. TB 15.5.3). Das System wurde den Schulämtern vom TKM zum Einsatz übergeben. Weder beim Schulamt noch beim TKM war zum Zeitpunkt der Kontrolle eine datenschutzrechtliche Freigabe des Verfahrens vorhanden. Diesen Verstoß gegen § 34 Abs. 2 ThürDSG habe ich gegenüber dem TKM beanstandet und um eine kurzfristige Nachholung der Freigabe sowie der Erstellung eines Anlagen- und Verfahrensverzeichnisses gebeten, was zwischenzeitlich erfolgt ist. Auch das im Einsatz befindliche automatisierte Verfahren zur Registrierung von Postaus- und -eingängen wurde vom TKM erst nach meiner Beanstandung gegenüber dem Schulamt freigegeben und ein Anlagen- und Verfahrensverzeichnis erstellt sowie eine Meldung zum Datenschutzregister abgegeben. Mit Einführung des Verfahrens PERSOS-S in den Schulämtern wurden diese vom TKM aufgefordert, regelmäßig einmal im Monat einen kompletten Abzug der in PERSOS-S gespeicherten Lehrerpersondaten dem TKM zu übermitteln. Die regelmäßige Übermittlung sämtlicher automatisiert gespeicherter Personaldaten hatte ich bereits im 1. Berichtszeitraum - damals vom Landesverwaltungsamt zum TKM - beanstandet, da für eine Datenübermittlung in diesem Umfang keine Erforderlichkeit bestand. Damals hat das TKM - wenn auch unter Anmeldung von Bedenken - der Beanstandung dadurch abgeholfen, dass die regelmäßige Datenübermittlung eingestellt und der Datenbestand beim TKM gelöscht wurde. Die erneute Aufnahme der regelmäßigen Übermittlung sämtlicher Personaldaten von den Schulämtern an das TKM wurde vom TKM damit gerechtfertigt, dass dies zur Erfüllung der Aufgaben der

Stellenbewirtschaftung, der Haushaltsüberwachung, der Personalplanung sowie der Prozessführung erforderlich sei. Diese Begründung hielt ich für zu pauschal, um derart umfangreiche Datenübermittlungen zu rechtfertigen. Es bedurfte eines längeren Schriftwechsels sowie Gespräche mit dem TKM, um den Umfang der regelmäßig von den Schulämtern dem TKM zu übermittelnden Daten auf das für die Aufgabenerfüllung des TKM tatsächlich erforderliche Maß zu reduzieren. Danach werden dem TKM von den Schulämtern nunmehr neben den Stammdaten Angaben zum Umfang des Beschäftigungsverhältnisses, der Art der dienstlichen Verwendung, der Vertragsart, der Stellenbesetzung sowie der vorhandenen Ausbildung übermittelt.

Die automatisierte Verarbeitung dieser Personaldaten habe ich bei einem Kontrollbesuch im TKM einer näheren Prüfung unterzogen. Zum Termin wurde die bis dato noch nicht vorliegende Dienstvereinbarung mit dem Hauptpersonalrat zum Einsatz des Verfahrens zur Personaldatenverarbeitung vorgelegt. Die Prüfung ergab, dass der Umfang der regelmäßig von den Schulämtern übermittelten Daten tatsächlich dem Stand entsprach, der in den Gesprächen mit mir festgelegt worden war. Es war zudem auch die von mir geforderte differenzierte Einrichtung von Zugriffsrechten realisiert worden. Damit wird sichergestellt, dass in den jeweiligen Referaten des TKM die Mitarbeiter nur auf diejenigen Lehrerpersonaldaten Zugriff haben, die der jeweils dort bearbeiteten Schulart angehören. Allerdings gab es hierzu so gut wie keine schriftlichen Festlegungen. Solche Regelungen sind jedoch nach meiner Auffassung notwendig, um sicherzustellen, dass auch im Vertretungsfall bzw. bei Personalwechsel diese Datenschutzvorkehrungen eingehalten werden. Darüber hinaus waren im TKM grundlegende organisatorische Regelungen zum Datenschutz und zur Datensicherheit nur sporadisch in der Geschäftsordnung oder der allgemeinen Dienstanweisung des TKM geregelt. Im Nachgang zur Kontrolle wurde vom TKM ein vorläufiges Sicherheitskonzept für die Arbeit mit Informationstechnik erstellt, das die Grundlage für organisatorische Regelungen zum Datenschutz und zur Datensicherheit bilden soll. Derzeit bin ich mit dem TKM noch im Gespräch, wie das Sicherheitskonzept und die organisatorischen Regelungen für den sensiblen Bereich der Personaldatenverarbeitung der Lehrer gefasst werden sollen. Ich hoffe,

dass künftig auf dieser Grundlage die Verarbeitung personenbezogener Daten der Lehrer durch das TKM und die nachgeordneten Dienststellen im Einklang mit den datenschutzrechtlichen Vorschriften erfolgen wird.

6.4 Beihilfebearbeitung durch ein privatrechtliches Versicherungsunternehmen

Bereits in meinen vorangegangenen Tätigkeitsberichten (1. TB 6.2.3; 2. TB 6.16) habe ich Ausführungen zur Thematik der Beihilfebearbeitung gemacht. Im Berichtszeitraum habe ich mit den kommunalen Aufsichtsbehörden die Frage hinsichtlich der Rechtsgrundlagen und der Zulässigkeit der Beihilfebearbeitung durch eine Versicherung diskutiert. Im Zuge der Kontrolltätigkeit im kommunalen Bereich wurde festgestellt, dass Beihilfen für Beschäftigte durch eine Versicherung abgewickelt werden. Ich habe erwähnt, dass m. E. das ThürBG keine Möglichkeit einer Auftragsdatenverarbeitung vorsieht.

Das TLVwA hatte sich in einem Schreiben dahingehend geäußert, dass aus kommunalrechtlicher Sicht die Übermittlung sensibler personenbezogener Daten an eine Versicherung für rechtlich bedenklich gehalten wird. Die Beihilfebearbeitung solle seiner Meinung nach für Landesdienststellen durch Behörden erfolgen. Von Seiten des TIM wurde erklärt, dass im Interesse der Kommunen und ihrer Mitarbeiter eine rechtlich einwandfreie Lösung gefunden werden soll, wobei gegebenenfalls auch eine erforderliche Rechtsänderung in die Prüfung einbezogen werde. Zuvor soll geklärt werden, wie viele Kommunen in der Beihilfebearbeitung auf externe Unterstützung angewiesen sind.

6.5 Datenerhebung über Beschäftigungsverhältnisse von Ehepartnern durch die Oberfinanzdirektion Erfurt - Zentrale Gehaltsstelle - (ZG)

Bei Neueinstellung und danach in regelmäßigen Abständen erhielten die Bediensteten des Freistaats Thüringen von der ZG ein im Berichtszeitraum verwandtes Formular „Erklärung zum Familienzuschlag/Ortszuschlag/Sozialzuschlag/Anwärterverheiratetenzuschlag“

(Erklärung F, O, S, A) zur Berechnung bzw. Überprüfung der Zahlung der Zuschläge. Zu dem genannten Formular lag die Beschwerde des Ehepartners eines Bediensteten vor, der sich gegen die Angabe seines Arbeitgebers wandte. Bei den Angaben über den Ehegatten war bei der Frage, ob die angegebene Tätigkeit des Ehegatten eine Beschäftigung im öffentlichen Dienst oder bei einem dem öffentlichen Dienst gleichgestellten Arbeitgeber sei, „nein“ angekreuzt gewesen. Auch die Fragen nach Versorgungsbezügen und der Empfang von Versorgungsbezügen nach einer Ruhegehaltordnung aufgrund einer Beschäftigung im öffentlichen Dienst war verneint worden. Dennoch war seitens der ZG die genaue Bezeichnung und Anschrift des Dienstherrn, Arbeitgebers, Personalnummer und Aktenzeichen angefordert worden. Auf meine Anfrage hat die ZG mitgeteilt, dass es immer wieder zu Auslegungsschwierigkeiten bei den Beschäftigten komme. Daher erscheine es sinnvoll, den Arbeitgeber des Ehegatten zu erfragen, um dann im Wege einer Vergleichsmittelteilung feststellen zu können, ob im konkreten Fall eine dem öffentlichen Dienst gleichgestellte Tätigkeit vorliegt, um Überzahlungen zu vermeiden. Gleichzeitig wurde darauf hingewiesen, dass das Formular der Erklärung neu gefasst wird, wobei mir die Gelegenheit gegeben wurde, aus datenschutzrechtlicher Sicht Stellung zu nehmen. Da in dem überarbeiteten Formular nunmehr der Hinweis aufgenommen wurde, dass die Angaben zum Arbeitgeber des Ehegatten nur auszufüllen ist, soweit der Ehegatte im öffentlichen Dienst beschäftigt ist, werden nicht erforderliche Datenerhebungen vermieden. Man versicherte, dass zwischenzeitlich die Nebenstellenleiter und Sachbearbeiter darauf hingewiesen worden seien, die Angabe des Arbeitgebers nicht mehr abzufordern, wenn aus der Beantwortung der übrigen Fragen eindeutig hervorgehe, dass der Ehepartner nicht im öffentlichen Dienst oder bei einem dem öffentlichen Dienst gleichgestellten Arbeitgeber beschäftigt ist.

6.6 Verfahren bei Gehaltspfändungen

Im Kreise der Datenschutzbeauftragten des Bundes und der Länder wurde die Problematik diskutiert, dass in einigen Ländern jeder Gehaltspfändungs- und Überweisungsbeschluss von der Bezugsstelle der personalverwaltenden Stelle und zwar unabhängig von der Höhe des Betrages und der Häufigkeit solcher Maßnahmen, mitge-

teilt wird. Unter dem Gesichtspunkt des Erforderlichkeitsgrundsatzes greifen undifferenzierte Mitteilungen nicht unerheblich in das Persönlichkeitsrecht der Betroffenen ein, wenn sie auch in die bei der personalverwaltenden Stelle geführte Personalakte Eingang finden. Auf meine Anfrage an die OFD Erfurt - Zentrale Gehaltsstelle (ZG), wann die personalführenden Stellen darüber informiert werden, dass Pfändungen, Aufrechnungen oder offen gelegte Abtretungen zu realisieren sind, wurde mir mitgeteilt, dass grundsätzlich informiert wird, eine diesbezügliche Regelung jedoch nicht existiert. Ich habe gegen das Verfahren, jede Pfändung und offen gelegte Abtretung der personalführenden Dienststelle mitzuteilen, datenschutzrechtliche Bedenken geäußert. Eine Unterrichtung kann nur dann vorgenommen werden, wenn dies zu deren Aufgabenerfüllung erforderlich ist. Dies ist aber nur dann der Fall, wenn in Betracht kommt, dass die Mitteilung Anlass für eine fürsorgerische oder dienstrechtliche Maßnahme sein kann. Die Einleitung von Zwangsvollstreckungsmaßnahmen gegen einen Beschäftigten des Freistaats Thüringen lässt nicht zwingend die Schlussfolgerung auf leichtfertiges Schuldenmachen und damit die Notwendigkeit für die Einleitung eines Disziplinarverfahrens oder gegebenenfalls arbeitsrechtlicher Maßnahmen zu. Im Kreise der Datenschutzbeauftragten ist man sich darüber einig, dass entscheidende Kriterien für die Zulässigkeit der Übermittlung die Höhe und/oder die Häufigkeit der gegenüber Bediensteten geltend gemachten Forderungen sind, wobei die Einkommenshöhe mit zu berücksichtigen ist. Das TFM hat mitgeteilt, in Bälde dem TLfD einen Standpunkt dazu abzugeben.

6.7 Verwaltungsvorschrift zur Thüringer Verordnung über Zuständigkeiten für die Feststellung, Berechnung und Anordnung der Zahlung der Bezüge von Bediensteten und Versorgungsempfängern (ThürZustVBezüge)

Schon in meinen vorangegangenen Tätigkeitsberichten (1. TB 6.3.1; 2. TB 6.7) hatte ich auf eine ausstehende Verwaltungsvorschrift verwiesen, in der Regelungen zum Umgang mit der Bezügeakte, die bei der OFD - Zentrale Gehaltsstelle - geführt werden, getroffen werden sollten. In ihrer Stellungnahme zu diesem TB verwies die Thüringer Landesregierung darauf, dass Voraussetzung dafür eine

Änderung von § 9 Abs. 3 des Thüringer Besoldungsgesetzes sei, wozu es noch ausstehender Klärungen bedürfe.

Bislang ist die vorgesehene Regelung noch nicht verabschiedet.

6.8 Rücksendung von Bewerbungsunterlagen

In einer Eingabe trug mir ein Bürger vor, dass er von einem landeseigenen Kreditinstitut gebeten wurde, von ihm bereits übergebene Bewerbungsunterlagen erneut zu übersenden, da man die zunächst erhaltenen im Hause nicht auffinden konnte. Nach dem nochmaligen Übersenden der Bewerbungsunterlagen meldete sich das Kreditinstitut eineinhalb Jahre nicht mehr, worauf der Bürger um die Rücksendung seiner sämtlichen Bewerbungsunterlagen bat. Er erhielt daraufhin aber trotz mehrmaliger Aufforderung seine Bewerbungsunterlagen nur in einfacher Ausfertigung zurück. In der Stellungnahme des Kreditinstituts zum Vorgang wurde darauf verwiesen, dass nicht mehr nachvollziehbar sei, wo sich die ursprünglich erhaltenen Bewerbungsunterlagen befinden oder ob sie bereits zurückgegeben worden waren.

Diesen Vorfall nahm ich zum Anlass, dem Institut einen Kontrollbesuch abzustatten. Im Ergebnis dieser datenschutzrechtlichen Prüfung konnte der Verbleib der Bewerbungsunterlagen allerdings auch nicht mehr aufgeklärt werden. Ich vertrat in diesem Zusammenhang den Standpunkt, dass die Personalverwaltung den lückenlosen Nachweis über ein- und ausgegangene Bewerbungsunterlagen zu führen hat. Außerdem hielt ich die Verfahrensweise, von einem Bewerber das Ausfüllen des sehr detaillierten Personalfragebogens zu verlangen, obwohl zu diesem Zeitpunkt keine Einstellung beabsichtigt war, für nicht erforderlich, ebenso auch einige im Personalfragebogen enthaltene Fragen. Insbesondere war es als nicht erforderlich zu bewerten, die Namen und die Berufe der Eltern sowie den Beruf des Ehepartners im Personalbogen festzuhalten oder zu erfragen, ob man mit Mitarbeitern des Kreditinstituts bzw. anderer Geldinstitute verwandt oder verschwägert ist und wie hoch das bisherige Jahresgehalt war.

Das Kreditinstitut hat daraufhin in der Personalabteilung eine bereits seit längerem erstellte, schriftliche Arbeitsanweisung zum Umgang mit Bewerbungsunterlagen praktisch umgesetzt. Zukünftig sollen

zudem Personalfragebögen erst beim Zustandekommen eines Arbeitsvertrags ausgefüllt und im Falle des Scheiterns der Einstellung diesen Bogen dem Bewerber zusammen mit seinen übrigen Bewerbungsunterlagen zurückgegeben werden. Außerdem wurde der Personalfragebogen überarbeitet, wobei teilweise Fragestellungen weggelassen bzw. zumindest als freiwillig zu beantworten gekennzeichnet wurden.

6.9 Abschottung der Arbeitsbereiche beim Polizeiarztlichen Dienst

Der Polizeiarztliche Dienst (PÄD) hat für die Thüringer Polizei unterschiedliche Aufgaben der medizinischen Behandlung und Begutachtung zu erfüllen. Zum einen wird für einen bestimmten Teil der Thüringer Polizei vom PÄD eine medizinische Betreuung durchgeführt. Dies betrifft insbesondere die in Ausbildung befindlichen Polizisten, die im Rahmen der freien Heilfürsorge u. a. die Leistungen des PÄD in Anspruch nehmen können. Daneben werden für den Dienstherrn des Polizisten sozialmedizinische Gutachten über die Polizeidiensttauglichkeit der Beamten erstellt sowie arbeitsmedizinische Vorsorgeuntersuchungen durchgeführt. Schließlich rechnet der PÄD auch die medizinischen Leistungen ab, die von den Beamten mit freier Heilfürsorge in Anspruch genommen worden sind. Es handelt sich also um Arbeitsgebiete, die strikt voneinander getrennt durchzuführen sind. So ist in § 98 Satz 5 ThürBG festgelegt, dass die Unterlagen über Heilfürsorge stets als Teilakte und von der übrigen Personalakte getrennt aufzubewahren ist (sog. Abschottung). Für den PÄD bedeutet dies, dass die Unterlagen über die freie Heilfürsorge, aber auch über die sonstigen medizinischen Behandlungen von den Unterlagen zur sozialmedizinischen Begutachtung zu trennen sind, weil diese Begutachtungen direkt dem Dienstherrn z. B. im Rahmen von Personalentscheidungen zur Verfügung gestellt werden. Darüber hinaus sind auch die organisatorischen Strukturen so zu wählen, dass bei der Begutachtung der Polizeidiensttauglichkeit keine Erkenntnisse aus der Heilbehandlung oder Heilfürsorge verwendet werden können. Dies entspricht den Regelungen im Angestelltenbereich, wonach der Dienstherr ohne Einwilligung des Bediensteten keine ihn betreffenden medizinischen Daten vom Hausarzt oder seiner Krankenversicherung anfordern darf.

Bei einer Kontrolle beim PÄD habe ich festgestellt, dass eine personelle und organisatorische Trennung dieser Bereiche durchgehend vorliegt. Allerdings war hier, wie auch in anderen Bundesländern, eine einheitliche Aktenführung insoweit festzustellen, als nach Beendigung der Heilfürsorge von Polizeianwärtern deren Unterlagen in das zentrale Zwischenarchiv überführt und dort zusammen mit den Unterlagen zur sozialmedizinischen und betriebsmedizinischen Begutachtung sowie zur medizinischen Betreuung in einer Akte abgelegt wurden. Dadurch hätte die ansonsten im täglichen Betrieb durchgesetzte Abschottung bei einer erneuten Vorlage der Akten umgangen werden können, indem alle Teilakten dem jeweiligen Bereich vorgelegt werden. Darüber hinaus waren noch keine Festlegungen zur Aufbewahrungsdauer der Unterlagen getroffen. Dies war nach meiner Auffassung jedoch von besonderer Bedeutung, weil vom PÄD ca. 35.000 - 40.000 Gesundheitsakten der ehemaligen Polizei-Polikliniken übernommen worden sind. Auf meine Aufforderung hin hat inzwischen der PÄD eine „Arbeitsrichtlinie zur Aufbewahrung von und zum Umgang mit Behandlungs- und Untersuchungsunterlagen im Polizeiärztlichen Dienst“ erlassen. Danach werden die jeweiligen Teilakten in unterschiedlichen Archivräumen gelagert und sind nur dem zuständigen Sachgebiet zugänglich. Zudem wurden differenzierte Aufbewahrungsfristen für die Aussonderung der Akten getroffen.

6.10 Umgang mit Telefongesprächsdaten

Bereits in meinem 1. TB (15.7) habe ich grundsätzliche Ausführungen zum Betrieb von Telekommunikationsanlagen und zum Umgang mit Telefongesprächsdaten gemacht. Auch im Berichtszeitraum wurden wiederum Anfragen in diesem Zusammenhang an mich herangetragen. Aus diesem Grunde möchte ich auch im vorliegenden Bericht nochmals einige Kerngedanken dazu aus datenschutzrechtlicher Sicht darlegen:

- Da mittels Telefonanlagen auch das Verhalten der Beschäftigten überwacht werden kann, ist die Einführung und Anwendung daher durch den Personalrat mitbestimmungspflichtig. Im Sinne der Transparenz und Nachvollziehbarkeit sind die Regelungen dazu den betroffenen Bediensteten bekannt zu geben.

- Bei Nebenstellen, die Mitgliedern der Personalvertretungen oder Stellen mit vergleichbarer Funktion (besondere Vertrauensstellung, Schweigepflichten) für ihre Tätigkeit zur Verfügung gestellt werden, dürfen dienstliche Gespräche nur summarisch ausgewertet werden. Es sollte diesem Personenkreis ein Anschluss zur Verfügung gestellt werden, bei dem auf eine Speicherung der Zielnummer generell verzichtet wird.
- Bei dienstlichen Gesprächen bestehen gegen die Speicherung der Nebenstellenummer, der Zielnummer, der Gebühreneinheiten sowie des Zeitpunkts des Gesprächs für Abrechnungs- bzw. Kontrollzwecke keine datenschutzrechtliche Bedenken. Ausdrücke von gespeicherten Telefongesprächsdaten sind nur dem Vorgesetzten zugänglich zu machen. Ein Listenumlauf oder eine Verknüpfung mit anderen Daten hat zu unterbleiben. Telefongesprächsdaten sind zu löschen, sobald ihre Speicherung nicht mehr erforderlich ist. Für gespeicherte Zielnummern dienstlicher Gespräche wird ein Zeitraum von 3 Monaten nach ihrer Entstehung für angemessen gehalten.
- Bei privat geführten Gesprächen dürfen die dazu gespeicherten Daten ausschließlich zur Abrechnung mit dem Betroffenen verwendet werden. Ein vollständiger Ausdruck der angewählten Zielnummer zur eindeutigen Identifizierung des Gesprächspartners ist nur bei strittigen Fällen zulässig. Ansonsten erfolgt bei privaten Gesprächen der Ausdruck ohne Zielnummer oder ohne vollständige Zielnummer (ohne die letzten drei Ziffern). Bei Verdacht einer übermäßigen Inanspruchnahme kann ein Ausdruck ohne Zielnummern bzw. verkürzt für einen bestimmten Zeitraum zur Durchführung der Dienstaufsicht gefertigt werden. Die Daten privater Gespräche sind sofort nach erfolgter Abrechnung zu löschen. Listenausdrucke sind unmittelbar nach erfolgter Kontrolle zu vernichten bzw. wenn dies aufgrund der Rechnungsprüfung für geboten erscheint. Ausgedruckte Zielnummern bei der Abrechnungsstelle sind sofort nach Klärung der Streitigkeiten zu vernichten.

7. Polizei

7.1 Erstes Gesetz zur Änderung des Bundesgrenzschutzgesetzes vom 25. August 1998

Seit Inkrafttreten des Ersten Gesetzes zur Änderung des Bundesgrenzschutzgesetzes am 1. September 1998 kann der Bundesgrenzschutz zur Verhinderung unerlaubter Einreisen Personen auf dem Gebiet der Bahnanlagen und in Zügen anlassunabhängig überprüfen, wenn aufgrund von Lageerkenntnissen oder grenzpolizeilichen Erfahrungen anzunehmen ist, dass diese Orte zur unerlaubten Einreise genutzt werden. So können also Personen auf Bahnhöfen, in Zügen oder auch Flughäfen mit grenzüberschreitendem Verkehr kurzzeitig angehalten und befragt werden, es kann verlangt werden, dass mitgeführte Ausweispapiere oder Grenzübertrittspapiere zur Überprüfung ausgehändigt werden. Es ist daher sowohl auf den Straßen als auch auf den Bahnhöfen und im Zug mit verdachtsunabhängigen Kontrollen zu rechnen. Insgesamt entspricht dies einer Identitätsfeststellung wie im allgemeinen Polizeirecht. Zwar stellt die Identitätsfeststellung allein einen relativ geringfügigen Eingriff in das Persönlichkeitsrecht dar, zieht in der Regel aber weitere Maßnahmen wie den Datenabgleich mit polizeilichen Dateien nach sich, was aber im Hinblick auf den erstrebten Zweck, nämlich der Verhinderung illegaler Einreise sowie von Straftaten z. B. Schlepperunwesen als verhältnismäßig anzusehen ist.

7.2 Bundeseinheitliche Verwaltungsvorschriften für die Feststellung von Alkohol, Medikamenten und Drogen im Blut bzw. Urin bei Straftaten und Ordnungswidrigkeiten

Zu der genannten Verwaltungsvorschrift (1. TB 7.3) lag im Berichtszeitraum der Entwurf einer überarbeiteten bundeseinheitlichen Verwaltungsvorschrift über die Feststellung von Alkohol-, Medikamenten- und Drogeneinfluss bei Straftaten und Ordnungswidrigkeiten, Sicherstellung und Beschlagnahme von Führerscheinen vor. Es ist beabsichtigt, ihn durch eine gemeinsame Verwaltungsvorschrift des TJM und des TIM umzusetzen. Die maßgeblichen datenschutzrechtlichen Vorgaben, wie z. B. der Verzicht auf die Übermittlung

von Anschrift, Geburtstag und Geburtsmonat des Betroffenen an die Untersuchungsstelle oder die Ankreuzmöglichkeiten zu den Angaben des Orts der Alkohol-/Medikamenten-/Drogenaufnahme haben Berücksichtigung gefunden.

7.3 Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (Prüffristenverordnung - PolPrüffristVO)

In § 40 Polizeiaufgabengesetz (PAG) sind Regelungen für die polizeiliche Datenerhebung und -verarbeitung getroffen, die Fristen für die Überprüfungen und Aufbewahrungen von Daten normieren. Der Gesetzgeber hat in § 45 Abs. 2 PAG das TIM ermächtigt, das Nähere für die Überprüfungsfristen durch eine Rechtsverordnung zu regeln. An der Erarbeitung dieses Entwurfes hat mich das TIM beteiligt. Von den ursprünglichen Überlegungen, sich an den gesetzlichen Höchstfristen zu orientieren, ist das TIM im Laufe der Diskussion abgegangen und hat in dem Verordnungsentwurf, der derzeit dem TJM zur Rechtsprüfung vorliegt, differenzierte Regelungen getroffen, die auf die jeweiligen Straftaten abstellen, sodass die zunächst bestehenden datenschutzrechtlichen Bedenken ausgeräumt wurden.

7.4 Verwaltungsvorschrift des TIM über die Aufgaben der Polizei bei der Verfolgung von Verkehrsverstößen

In einer Verwaltungsvorschrift vom 1. Dezember 1998 traf das TIM Regelungen zum Verfahren bei Ordnungswidrigkeiten und Verkehrsvergehen. In den eingeführten Formularen zur schriftlichen Äußerung als Beschuldigter und zur Beschuldigtenvernehmung bei Vergehen sind umfangreiche Datenerhebungen vorgesehen, bei denen zwar in der Überschrift auf die Freiwilligkeit verwiesen wird, sich aber die grundsätzliche Frage stellt, weshalb im Rahmen von Verkehrsverstößen Daten wie Beruf zur Tatzeit, Stellung im Beruf, Arbeitgeber, Personalien des Ehegatten, Eltern des Beschuldigten, gesetzlicher Vertreter, Pflegeeltern, Institution der Betreuung, Bewährungshelfer überhaupt gefragt wird, da hierfür eine Erforderlichkeit in jedem Fall nicht erkennbar ist. Das TIM hat zunächst die Auffassung vertreten, zu den Datenerhebungen bestünden weit gehende Übereinstimmungen mit anderen Ländern, räumte aber ein,

dass nicht alle Angaben benötigt werden. Danach erhielt das TIM Unterstützung vom TMJE, das diese Angaben weitgehend für unerlässlich ansah. Bezüglich der Formulare im Bereich der Verkehrsordnungswidrigkeiten arbeitet zwischenzeitlich der Bund-Länder-Fachaus-schuss für Straßenverkehrsordnungswidrigkeiten an einer Vereinheitlichung der Vordrucke. Eine weitere Beteiligung des TLfD von Seiten des TIM wurde zugesagt.

7.5 INPOL-neu

Seit geraumer Zeit wird beim Bundeskriminalamt (BKA) in einer Bund-Länder-Arbeitsgruppe an der Erarbeitung einer Neukonzeption des polizeilichen Informationsverbundes INPOL-neu gearbeitet, in die auch der BfD und Landesdatenschutzbeauftragte eingebunden sind. Parallel zu dieser Projektgruppe ist ebenfalls eine Arbeitsgruppe INPOL-Land (AGIL) eingerichtet worden, die sich mit den Fragen der Anbindung der Landesdatenerhaltungs- und Vorgangbearbeitungssysteme befasst. Auf Thüringer Seite wird das Projekt vom Lenkungsausschuss INPOL des TIM begleitet, zu dessen Sitzungen der TLfD verschiedentlich eingeladen wurde. INPOL-neu ist darauf angelegt, dass im Rahmen eines Rechner-Rechner-Verbundes mit einer zentralen Kommunikationsschnittstelle, auf die die Teilnehmer von den jeweiligen Arbeitsplatzsystemen zugreifen. Der Kreis der Teilnehmer an INPOL-neu entspricht dem der Teilnehmer am jetzigen INPOL-System, zu denen das BKA, die Länderpolizeien sowie der Bundesgrenzschutz zählt. Von der Konzeption her sollen alle Erkenntnisse zu einer Person sowie die Personengrunddaten lediglich einmal in die Datenbank eingegeben werden. Es ist vorgesehen, den Nutzern unterschiedliche Zugriffsmöglichkeiten einzuräumen, wobei auch Berechtigungen für bestimmte Funktionen (lesender, verändernder, löschender Zugriff) gegeben werden können, die auch individuell kombiniert werden. Dadurch soll verhindert werden, dass jeder Nutzer uneingeschränkten Zugriff auf sämtliche erfassten personenbezogenen Daten hat. Die Zugriffsberechtigungen werden auf Nutzerseite durch die Länder vergeben. Bei INPOL ist auf §§ 11 Abs. 1, 34 Abs. 2 Bundeskriminalamtsgesetz (BKAG) abzustellen, wonach die in das polizeiliche Informationssystem einzubeziehenden Daten bestimmt werden müssen und im Wege der Errichtungsanordnung ihre Bezeichnungen, Zweck, Inhalt und Voraussetzung für

Datenübermittlungen festzulegen sind. Insbesondere muss immer im Auge behalten werden, dass nur Straftaten von länderübergreifender, internationaler oder erheblicher Bedeutung INPOL-relevant sind, wie dies § 2 Abs. 1 BKAG ausdrücklich festlegt. Im Zusammenhang mit INPOL-neu wurde bei der Einrichtung von Verbunddateien das Problem an mich herangetragen, ob nach Inkrafttreten des BKAG für Verbunddateien vorrangig die Vorschriften des BKAG Anwendung finden. Ich habe mich hierzu dahingehend geäußert, dass sich aus der Gesetzessystematik des § 11 Abs. 3 BKAG ergibt, dass die landesgesetzlichen Regelungen vom BKAG nicht überlagert werden, da nur die Behörde, die Daten zu einer Person eingegeben hat, befugt ist, diese zu ändern, zu berichtigen oder zu löschen. Wenn dies Thüringer Polizeidienststellen sind, ist daher nach meiner Auffassung das Thüringer Polizeirecht anwendbar. Es ist mitunter feststellbar, dass Bundesländer ihre Landesdaten beim BKA speichern lassen, auch wenn sie noch nicht die Erheblichkeitsschwelle des § 2 Abs. 1 des BKAG erreicht haben, und die aus diesem Grunde nicht in INPOL-neu gespeichert werden dürfen. Mit dem BfD bin ich hier der Auffassung, dass schon nach dem Wortlaut von § 2 Abs. 5 BKAG, wonach das BKA die Länder auf Ersuchen bei deren Datenverarbeitung unterstützen kann, eine dauerhafte Datenverarbeitung des BKA für die Landespolizeibehörden rechtlich nicht zulässig ist. In Betracht kommen kann dies allenfalls in besonderen Ausnahmefällen, wobei nach § 2 Abs. 5 BKAG dies dann nach den Weisungen der Länder und gemäß deren Vorschriften über die Datenverarbeitung im Auftrag zu erfolgen hat. Die abschließende Klärung der hier bestehenden Fragen steht noch aus.

7.6 ViCLAS - Violent Crime Linkage Analysis System

Unter der Bezeichnung ViCLAS - Violent Crime Linkage Analysis System - Analyse-System zur Verknüpfung von Gewaltverbrechen verbirgt sich ein kanadisches Computerprogramm, das in der Lage ist, die Besonderheiten von Kriminalfällen miteinander zu vergleichen und Analysen anzustellen. Bei diesem Verfahren handelt es sich um einen neuen Dateitypus, der, insbesondere auch wegen Erhebungen und Nutzungen umfangreicher und sensibler Daten, im Hinblick auf die beabsichtigte bundesweite Einführung datenschutzrechtlicher Begrenzungen bedarf, da hier Datenerhebungen vorgese-

hen sind, die in ihrer Eingriffstiefe sehr weitgehend sind, ohne dass sie auch zu Analysezwecken zwingend geboten erscheinen. In meiner Stellungnahme an das TIM habe ich darauf verwiesen, dass der Fragenkatalog erheblich reduziert werden kann, da die Erhebungen, insbesondere bei Opfern und Personen, die mit dem Fall in Verbindung stehen können, zu weitgehend sind. So erscheinen Fragen, die den engeren Lebensbereich und die Intimsphäre berühren, aus datenschutzrechtlicher Sicht allenfalls akzeptabel, wenn ihre Beantwortung auch in einem Zusammenhang mit dem Anlass, Tatort oder der vermuteten Gefahr einer weiteren Straftat steht. Seitens des TIM hat man mir mitgeteilt, dass nach der Erarbeitung des Entwurfs der „Errichtungsanordnung“ für die Datei eine Diskussion unter Beachtung meiner geäußerten datenschutzrechtlichen Bedenken geführt werde.

7.7 Fahndung im Internet

Das Internet als neues Medium enthält zum Teil auch strafbare Inhalte, die Gegenstand der polizeilichen Ermittlungen sein müssen. Vor diesem Hintergrund, insbesondere im Zusammenhang mit der Verbreitung von kinderpornografischen Inhalten, hat sich die ständige Konferenz der Innenminister und Senatoren der Länder (IMK) 1998 mit der Frage der Koordination von anlassunabhängigen Recherchen im Internet befasst. Hierbei wurde die Auffassung vertreten, dass die Aufgabe der anlassunabhängigen Recherchen im Internet und in den Onlinediensten durch eine zentrale Stelle für das gesamte Bundesgebiet wahrgenommen werden sollte. Mit der Durchführung dieser Recherchen wurde das Bundeskriminalamt betraut. Nach Mitteilung des TIM sind Thüringer Dienststellen, einschließlich des LKA, mit anlassunabhängigen Recherchen nicht befasst; von diesen Dienststellen wird allerdings die Bearbeitung von Verdachtsmeldungen sichergestellt. Im Kreise der Datenschutzbeauftragten werden die datenschutzrechtlichen Fragen in neuem Zusammenhang derzeit eingehend erörtert.

7.8 Modellprojekt zur Prävention von Jugendkriminalität

Zur Bekämpfung der Jugendkriminalität hat das TMSG in Zusammenarbeit mit dem TIM Anfang 1998 ein auf drei Jahre angelegtes Modellprojekt begonnen, bei dem Kinder und Jugendliche zwischen

10 und 16 Jahren, die erstmals in krimineller Weise in Erscheinung getreten sind (z. B. Ladendiebstahl etc.) und bei denen kein staatsanwaltschaftliches Ermittlungsverfahren eingeleitet wird, an geeignete Einrichtungen wie Sportvereine und Jugendgruppen vermittelt werden. Hierzu werden in den teilnehmenden Modellstädten sog. Kontaktstellen bei freien Trägern der Jugendhilfe oder bei den Jugendämtern eingerichtet. Diese Kontaktstellen haben die Aufgabe, den in Erscheinung getretenen Jugendlichen zu beraten und auf Angebote im Freizeitbereich hinzuweisen bzw. an Sportvereine und andere Vereine zu vermitteln. Dabei wird der Jugendliche von der Polizei im Rahmen der Vernehmungen nach der Tat aufgefordert, sich bei der Kontaktstelle zu melden. Im Anschluss daran werden sowohl dem Jugendamt als auch der Kontaktstelle Name und Anschrift des auffällig gewordenen Jugendlichen mitgeteilt, damit diese Stellen auf den Jugendlichen zugehen können. In diesem Zusammenhang traten bei Vorbereitungen des Modellprojektes Unsicherheiten auf, inwieweit eine Rechtsgrundlage zur Übermittlung dieser Daten von der Polizei an das Jugendamt und den freien Träger (Kontaktstelle) vorliegt. In Gesprächen mit den am Modellprojekt Beteiligten habe ich als Rechtsgrundlage hierfür § 41 Abs. 3 PAG angesehen. Sozialdatenschutzrechtliche Vorschriften sind in diesem Fall nicht einschlägig, da eine personenbezogene Datenübermittlung lediglich von der Polizei zu den Trägern der Jugendhilfe erfolgen soll. Eine Rückübermittlung an die Polizei, ob und mit welchem Ergebnis der einzelne Jugendliche sich bei den Kontaktstellen gemeldet und von dort weitervermittelt wurden, soll nicht erfolgen. Die zuständigen Polizeidienststellen werden in regelmäßigen Abständen ohne Angaben personenbezogener Daten nur darüber informiert, in welchem Umfang das Angebot der Kontaktaufnahme durch die vermittelten Jugendlichen in Anspruch genommen wurde. Vom TIM wurde diese Verfahrensweise in einem entsprechenden Erlass den zuständigen Polizeidienststellen zur Kenntnis gegeben. Damit sehe ich in diesem Bereich die datenschutzrechtlichen Anforderungen als erfüllt an.

7.9 Datenerhebung und Datenspeicherung anlässlich von Ringalarmfahndungen

Aus dem Kollegenkreis ist das Problem an mich herangetragen worden, ob bei sog. Ringalarmfahndungen an den Kontrollstellen bei Durchfahrtskontrollen die Kfz-Kennzeichen aller durchfahrender Fahrzeuge erhoben werden können oder ob dagegen datenschutzrechtliche Bedenken bestehen. Nach § 163 d StPO dürfen Daten, die bei einer Personenkontrolle nach § 111 StPO angefallen sind, nur in einer Datei gespeichert werden, wenn Tatsachen die Annahme rechtfertigen, dass die Auswertung der Daten zur Ergreifung des Täters oder zur Aufklärung der Straftat führen kann und die Maßnahme nicht außer Verhältnis zur Bedeutung der Sache steht. Ich habe hierzu die Auffassung vertreten, dass es danach nicht zulässig ist, alle Pkw-Daten zu erfassen. Diese Ansicht ist auch seitens des TIM geteilt worden, das neben den rechtlichen Bedenken auch die Einrichtung einer derartigen Datei im Hinblick auf die eingeschätzte Trefferwahrscheinlichkeit nicht für zweckmäßig erachtet hat. Wie mir zwischenzeitlich mitgeteilt wurde, ist in dem anfragenden Bundesland von dem Vorhaben Abstand genommen worden.

7.10 Telefonaufzeichnungen bei der Thüringer Polizei

Die Presse fragte beim TLfD an, wie es datenschutzrechtlich zu bewerten ist, dass angeblich bei einer Polizeidienststelle alle eingehenden Telefonate aufgezeichnet werden. Der TLfD setzte sich diesbezüglich mit dem TIM in Verbindung, um sich über die praktische Verfahrensweise in den Polizeidienststellen zu informieren. Es erfolgte auch eine Kontrolle vor Ort in einer Polizeidienststelle.

Es bestätigte sich die Vermutung, dass in einigen Polizeidienststellen alle unmittelbar mit dem Dienstgruppenleiter geführten Gespräche aufgezeichnet wurden, ohne dass eine Differenzierung danach vorgenommen wurde, ob möglicherweise Rechtfertigungsgründe zur Abwehr von Gefahren und zum Schutz von Leben oder die Einwilligung zur Aufzeichnung durch den Betroffenen vorliegen. Das TIM sagte zu, die im Einsatz befindliche Technik dahingehend zu modifizieren, dass bei der Möglichkeit, Gespräche aufzuzeichnen, weiter differenziert werden solle, um tatsächlich sicherzustellen, dass das,

was nicht erforderlich für das Handeln der Polizei ist, nicht mehr aufgezeichnet werden soll. Im Zusammenhang mit der ausgesprochenen Beanstandung gem. § 39 ThürDSG wies ich darauf hin, dass es einer eindeutigen Klarstellung und Abgrenzung bedarf, welche Anlässe eine Aufzeichnung rechtfertigen und wie mit Aufzeichnungen zu verfahren ist, um eine einheitliche rechtmäßige Praxis zu gewährleisten. Danach wurde ich an der Erstellung einer Dienstanweisung „Aufzeichnung von Telefongesprächsinhalten in der Thüringer Polizei“ (DA AvTgi-ThPol) beteiligt, die in ihrer in Kraft getretenen Fassung meine datenschutzrechtlichen Forderungen und Anregungen weitgehend berücksichtigt, sodass ich die ausgesprochene Beanstandung für behoben ansehe.

7.11 Personenverwechslung mit tragischen Folgen

Nach der Veröffentlichung von Medienberichten, denen zu entnehmen war, dass ein harmloser Wanderer aus Köln mit dem „Mörder von Remagen“ verwechselt und von der Thüringer Polizei erschossen worden ist, lag die Vermutung nahe, dass Mängel beim Umgang mit personenbezogenen Daten vorgelegen haben könnten, weshalb auch eine diesbezügliche Fragestellung an das TIM gerichtet wurde. Die datenschutzrechtliche Relevanz beim vorliegenden Sachverhalt liegt in der Beurteilung der Notwendigkeit, Erforderlichkeit und Verhältnismäßigkeit der Datenerhebung und -verarbeitung gemäß den Grundsätzen des PAG. Als Landesbeauftragte für den Datenschutz ist es meine Aufgabe, den Umgang mit personenbezogenen Daten bei den öffentlichen Stellen des Freistaats Thüringen zu kontrollieren und zu bewerten. Bei festgestellten Verletzungen von Vorschriften über den Datenschutz oder sonstigen Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten wird eine Behebung in angemessener Frist gefordert.

Maßstab einer Bewertung ist die Prüfung, ob richtige und geeignete Datengrundlagen Ausgangspunkt des polizeilichen Handelns waren. Die Prüfungspflicht der Polizei für die Datengrundlagen hat in diesem Zusammenhang umso gründlicher zu sein, je tiefer der Eingriff in das Persönlichkeitsrecht des Betroffenen erfolgt. Auf mein Auskunftsverlangen an das TIM, mitzuteilen, welche Maßnahmen eingeleitet wurden, die geeignet erscheinen, derartige Vorkommnisse zukünftig weitestgehend auszuschließen, wurde mitgeteilt, dass

bspw. die Aus- und Fortbildung der Thüringer Polizei reformiert wird. Auch soll eine Arbeitsgruppe unter Leitung des LKA Vorschläge zur Verbesserung der Informationssteuerung in öffentlichkeitswirksamen Fahndungsfällen erarbeiten.

7.12 Beschwerde zum Umgang mit personenbezogenen Daten bei der Thüringer Polizei

Die Beschwerde eines Bürgers war mir Anlass, die Rechtmäßigkeit der Erhebung, Speicherung und Übermittlung personenbezogener Daten anhand des konkret geschilderten Sachverhalts bei den zuständigen Dienststellen der Thüringer Polizei zu kontrollieren. Gegenstand der vorliegenden Beschwerde war der Umstand, dass sich personenbezogene Daten des Petenten in einer Übersicht über Klientel des „linken/rechten Spektrums“ befanden. Im Zuge der Kontrollen des TLfD stellte sich heraus, dass allein der Umstand, dass das Fahrzeug des Beschwerdeführers im Umfeld eines polizeibekannten Treffpunktes der „rechten Szene“ festgestellt wurde, für ausreichend angesehen worden war, den Fahrzeughalter diesem Klientel zuzuordnen. Diese Schlussfolgerung ohne entsprechende gesicherte weitere Erkenntnisse ist nach meiner Ansicht nicht vertretbar. Ohne nähere Prüfung können fahrzeuggebundene Handlungsweisen jedenfalls nicht von vornherein jeweils dem Halter zugeordnet werden, zumal Fahrzeughalter ihr Fahrzeug auch anderen Personen zur Verfügung stellen.

Die Zuordnung des Petenten zu einem bestimmten Klientel aufgrund unzureichend gesicherter Erkenntnisse habe ich beanstandet, da dies einen schwer wiegenden Eingriff in sein Persönlichkeitsrecht darstellt. Im Ergebnis meiner ausgesprochenen Beanstandung wurden die personenbezogenen Daten des Beschwerdeführers gem. § 45 Abs. 2 PAG vollständig gelöscht. Zur zukünftigen Verfahrensweise sicherte die beanstandete Stelle zu, bei der Erhebung und Übermittlung personenbezogener Daten in ähnlich gelagerten Fällen äußerst zurückhaltend zu agieren. In diesem Sinne seien auch die nachgeordneten Dienststellen angewiesen worden.

Beanstandet hatte ich im Zuge meiner Kontrollbesuche auch eine Polizeidienststelle, da mir während des Kontrollbesuches keine Ein-

sichtnahme in den kompletten Aktenvorgang möglich war, obwohl dieser vorher angekündigt worden war. Dies wurde kurzfristig behoben.

7.13 Datenverarbeitung der Thüringer Polizei in einem anderen Bundesland

Auf Anfrage des TLfD im TIM, ob es Überlegungen gibt, im Polizeibereich Daten in benachbarten Bundesländern verarbeiten zu lassen, teilte das TIM u. a. mit, dass das LKA Thüringen als Auftraggeber (AG) mit dem Bayrischen Landeskriminalamt als Auftragnehmer (AN) eine Vereinbarung zur Datenverarbeitung der Datei des Landes Thüringen „Spurendokumentation“ (SPUDOK-TH) geschlossen hat. Gleichfalls wurde die bereits im Dezember 1998 geschlossene diesbezügliche Vereinbarung übersandt. Da es sich dabei um Auftragsdatenverarbeitung im Sinne des § 8 ThürDSG handelt, bleibt der AG, im vorliegenden Fall also das LKA Thüringen, für die Einhaltung der Vorschriften des ThürDSG und anderer Vorschriften über den Datenschutz verantwortlich. In der zugrunde liegenden Vereinbarung ist zwar festgelegt, dass der AG jederzeit und ohne Vorankündigung die Einhaltung der Vereinbarung überprüfen kann, eine vertragliche Regelung gem. § 8 Abs. 6 ThürDSG, die auch eine Kontrollmöglichkeit des TLfD beim AN vorsieht, wurde jedoch nicht aufgenommen. Ich habe diesbezüglich das TIM wissen lassen, dass ich es für erforderlich halte, eine dahingehende schriftliche Vertragsergänzung nachzuholen. Hierzu habe ich auch einen konkreten Formulierungsvorschlag unterbreitet. Das TIM hat diesen Vorschlag dem Bayrischen Staatsministerium des Innern mit der Bitte um Kenntnisnahme und Zustimmung unterbreitet. Diesem wurde jedoch von Seiten des Bayrischen Staatsministeriums des Innern nicht zugestimmt; es hat vielmehr eine Kontrolle im Bayrischen LKA nur durch den Bayrischen Landesbeauftragten für den Datenschutz und seine Mitarbeiter für vertretbar gehalten. Ich habe daraufhin dem TIM mitgeteilt, dass ich die vorliegende Vereinbarung zur Datenverarbeitung der „SPUDOK-TH“ nach wie vor aus datenschutzrechtlicher Sicht als mangelbehaftet ansehe. Das TIM hat mitgeteilt, dass entgegen der Auffassung des TLfD im hier diskutierten Fall der § 8 Abs. 6 ThürDSG nicht zum Tragen kommt und verweist auf die Verwaltungsvorschrift zum Vollzug des ThürDSG,

wonach die Vorschrift des § 8 Abs. 6 ThürDSG nur für private Auftragnehmer gelte.

Dies findet aber m. E. keinerlei Stütze im eindeutigen Wortlaut des § 8 Abs. 6 ThürDSG, der nur vom „Auftragnehmer“ (ohne Differenzierung in öffentliche oder nicht-öffentliche Auftragnehmer) spricht, auf den die Vorschriften des ThürDSG nicht anwendbar sind. Bei einer eindeutigen Formulierung im Wortlaut erübrigt sich eigentlich die Auslegung nach Sinn und Zweck der Regelung unter Zuhilfenahme der Begründung. Doch selbst wenn man die Begründung zum Entwurf des ThürDSG (Landtagsdrucksache 1/439, Seite 30) heranziehen würde, so ergäbe sich nichts anderes. Dort wird auf die Entsprechung mit § 4 Abs. 2 HessDSG hingewiesen. Der einschlägigen Kommentierung zum Hessischen Datenschutzgesetz ist aber keineswegs zu entnehmen, dass es eine Beschränkung der Kontrollunterwerfung ausschließlich auf nicht-öffentliche Auftragnehmer gibt.

Eine Lösung der vorliegenden Problematik im Sinne der Vorschriften des ThürDSG konnte bislang nicht gefunden werden.

7.14 Polizeiliche Bildmappen verschwunden

Aufgrund von Hinweisen aus der Presse erhielt ich Kenntnis davon, dass Fotomaterial über die rechtsextremistische Szene in einem unverschlossenen Panzerschrank auf einem Schrottplatz aufgefunden worden war, was mir Veranlassung gab, der Angelegenheit nachzugehen. Dabei stellte sich heraus, dass in der Polizeidienststelle nicht geklärt werden konnte, wo Lichtbildunterlagen verblieben waren, die nach Erhalt einer neuen Lichtbildmappe ausgesondert worden waren. Regelungen hierzu gab es nicht; auch hatte man versäumt, sich bei einer vorgesetzten Dienststelle darüber zu erkundigen, wie hier verfahren werden sollte. Ich habe gegenüber der Polizeidienststelle eine Beanstandung ausgesprochen, da hier keine Maßnahmen getroffen worden waren, die verhinderten, dass Unbefugte auf Daten zugreifen konnten, was als grober Verstoß nach § 9 Abs. 3 ThürDSG von mir bewertet wurde. Das TIM ist meiner Anregung gefolgt, Festlegungen zum Umgang mit dienstlichem Schriftgut in den Behörden Einrichtungen, Dienststelle der Thüringer Polizei zu treffen.

Aufgrund dessen habe ich die Beanstandung als ausgeräumt angesehen.

7.15 Einbruch beim Polizeiverwaltungsamt

Ein Zeitungsbericht über einen Einbruch im Thüringer Polizeiverwaltungsamt und das Abhandenkommen zweier Rechner gab mir Veranlassung, eine Kontrolle im Thüringer Polizeiverwaltungsamt durchzuführen. Dabei stellte sich heraus, dass auf einem der abhanden gekommenen Computer keine personenbezogenen Daten, sondern nur Angebote im Rahmen von Vergabeverfahren gespeichert waren. Auf dem anderen Computer, bei dem es sich um einen Laptop handelte, befand sich Administrationssoftware, sodass eine missbräuchliche Nutzungsmöglichkeit nach Mitteilung des PVA ausgeschlossen erscheint. Nach dem Einbruch wurden geeignet erscheinende Sicherheitsmaßnahmen ergriffen, sodass keine weiteren Maßnahmen aus datenschutzrechtlicher Sicht zu fordern waren.

Im Rahmen der Kontrolle habe ich festgestellt, dass über die zum Datenschutzregister gemeldeten Dateien hinaus seit längerem ein automatisiertes Verfahren zur Erfassung der Arbeitszeit der Bediensteten im Einsatz war, ohne dass eine datenschutzrechtliche Freigabe gem. § 34 ThürDSG vorlag. Dies wurde beanstandet. Mit der danach erfolgten Freigabe durch das TIM war die Beanstandung ausgeräumt.

7.16 Datenerhebungen in der Nachbarschaft und beim Arbeitgeber

Gegen einen Thüringer Bürger wurden gleich zweifach im Zusammenhang mit Verkehrsordnungswidrigkeiten durch eine Polizeiinspektion Amtshilfeersuchen zur Fahrerermittlung durchgeführt. Ich habe dies zum Anlass genommen, in der zuständigen Polizeidienststelle eine Kontrolle durchzuführen. Nachdem die Adresse ermittelt worden war, hatten die Polizeibediensteten in der Nachbarschaft das Fahrerfoto gezeigt und Erkundigungen darüber eingeholt, ob man den Fahrer und seine Arbeitsstelle kenne. Der Beschwerdeführer wurde daher auch noch an seiner Arbeitsstelle von der Polizei aufgesucht. Die Erhebung personenbezogener Daten bei unbeteiligten

Nachbarn oder der Arbeitsstelle stellt einen erheblichen Eingriff in die Privatsphäre des Betroffenen dar und kann nur dann in Betracht kommen, wenn zuvor versucht wurde, den Betroffenen zu unterschiedlichen Zeiten aufzusuchen. Wird der Betroffene zu Hause nicht angetroffen oder wirkt er bei der Fahrerermittlung nicht mit, zum Beispiel durch Aussageverweigerung, Nichtfolgeleistung auf Vorladungen, stellt ein Datenabgleich in der Meldebehörde mit dem Fahrerfoto im Verhältnis zur Befragung von Dritten einen geringeren Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen dar. Ein Datenabgleich nach § 22 Passgesetz oder § 29 Thüringer Meldegesetz sollte daher als milderer Mittel vorrangig angewandt werden.

Im Vorfeld sollten Aufzeichnungen durch die Polizeibediensteten getätigt werden, die belegen, dass sowohl ein Aufsuchen mehrmals zu unterschiedlichen Zeiten als auch ein Meldedatenabgleich zu keinem Erfolg geführt hat, bevor eine Befragung der Nachbarn durchgeführt wird. Im vorliegenden Fall lag eine entsprechende Dokumentation nicht vor, sodass nicht nachvollziehbar war, wann erfolglos versucht worden war, bei dem Betroffenen persönlich die Daten zu erheben. Für die zuständige Polizeidirektion ist die vorgeschriebene Verfahrensweise zwischenzeitlich angeordnet worden. Man hat mir versichert, dass dies auch dienstaufsichtlich überwacht wird. Mit der Verwaltungsvorschrift über die Aufgaben der Polizei bei der Verfolgung von Verkehrsverstößen vom 1. Dezember 1998 (Thüringer Staatsanzeiger S. 2359 ff) hat das TIM meinen Bedenken Rechnung getragen und eine entsprechende Regelung getroffen.

7.17 Kontrolle im Thüringer Polizeiverwaltungsamt - Zentrale Bußgeldstelle

Hinweise auf Probleme beim Versand von Unterlagen in Bußgeldverfahren habe ich zum Anlass genommen, in der Zentralen Bußgeldstelle (ZBS), die organisatorisch als Abteilung 3 im Polizeiverwaltungsamt angesiedelt ist, eine datenschutzrechtliche Kontrolle durchzuführen.

Die Ahndung von Verkehrsordnungswidrigkeiten im Straßenverkehr erfolgt als Massenverfahren über das automatisierte Verfahren AVOS. Dabei kann jeder Sachbearbeiter auf alle Datensätze zugreifen, was mit der Erforderlichkeit der gegenseitigen Vertretung be-

gründbar war. Alle Eingabeaktivitäten werden jedoch in einer Historiendatei festgehalten und im Menü aufgezeigt, sodass der zuständige Bearbeiter jeweils prüfen kann, wann wer welche Daten eingegeben und verändert hat.

Der Umgang mit Passwörtern war zum Zeitpunkt der Kontrolle noch nicht konkret geregelt. Dies ist im Nachgang zur Kontrolle erfolgt.

Zum Verfahren bei Anträgen auf Akteneinsicht liegt eine Dienstanweisung vor, nach der bei telefonischen Anfragen zu bestimmten Sachverhalten wird in der Regel Auskunft erteilt wird, wenn ein Aktenzeichen und der Name des Betroffenen angegeben werden kann.

Bußgeldbescheide werden zentral ausgedruckt und über eine Kuvertiermaschine verschlossen. Aufgrund veralteter Technik kam es in der Vergangenheit vor, dass z. B. zwei Anhörungsbögen in einen Umschlag verbracht wurden, sodass Empfänger auch einen für einen Dritten bestimmten Anhörungsbogen erhalten konnten. Hierzu lagen dem TLfD entsprechende Hinweise vor. Bei der Vorführung der Kuvertiermaschine im Rahmen der Kontrolle geschah es auch, dass Bescheide und Zahlungsformulare nicht richtig einander zugeordnet wurden, weil ein Zahlschein sich verkantet hatte. Solche Vorkommnisse führen dazu, dass der zuständige Bedienstete die Maschine anhalten, die vorherigen Umschläge öffnen, neu sortieren und wieder verschließen muss. Eine automatische Gewichtskontrolle, die auf mögliche Fehler aufmerksam machen könnte, gab es nicht. Es waren aber bereits zum Zeitpunkt der Kontrolle alle erforderlichen Maßnahmen zur Neuanschaffung einer zuverlässigen neuen Kuvertiermaschine in die Wege geleitet worden, um zukünftig datenschutzrechtliche Verstöße durch den Versand von Unterlagen an unbeteiligte Dritte auszuschließen. Die Auswertung von Filmen bei Geschwindigkeitsüberschreitungen erfolgt in der Zentralen Filmauswertestelle als gesondertes Sachgebiet der ZBS.

Die Halterermittlung erfolgt im automatisierten Verfahren durch Übermittlung des Kfz-Kennzeichens über Standleitung zum Verkehrszentralregister und Übernahme der Halterdaten nach Übersendung. Bestreitet der Halter die Fahrereigenschaft, ohne den tatsächlichen Fahrer anzugeben, werden aus den vorliegenden Filmen mit Hilfe von Computertechnik „Dreierfolgen“ gefertigt. Diese bestehen aus einer Gesamtaufnahme des Fahrzeugs und jeweils einer Detailaufnahme des Kennzeichens und des Fahrers. Diese werden einem

Formblatt beigelegt und den örtlich zuständigen Polizeidienststellen übersandt. Durch diese erfolgt vor Ort die Fahrerfeststellung. Aufgrund meiner Forderung war auf dem Anhörungsbogen bereits der Hinweis enthalten, dass unter Umständen ein Lichtbildabgleich mit dem Pass- und Melderegister durchgeführt werden kann (1. TB 7.5.1; 2. TB 7.10). Die Vorgänge werden in der zentralen Registratur in Papierform aufbewahrt. Bei so genannten Verwarnungen mit Zahlungsanweisungen (VmZ) wird in das Bußgeldverfahren übergeleitet, sofern keine Zahlung erfolgt. Bei Zahlungseingang werden die Datensätze im automatisierten Verfahren AVOS automatisch gelöscht. In unregelmäßigen Zeitabständen wird von den Sachbearbeitern eine Sichtung und Aussonderung der abgeschlossenen Verfahren bis 75,00 DM vorgenommen.

Auch für die Zentrale Bußgeldstelle ist vorgesehen, dass die automatisierte Verarbeitung personenbezogener Daten durch Umsetzung des Rechnerbetriebes zukünftig im ZIV stattfinden wird.

8. Verfassungsschutz

8.1 Monatsbericht des TLfV

Aufgrund einer Erwähnung im Monatsbericht des TLfV gab es Einlagen, bei denen kritisiert wurde, dass jemand, der eine Demonstration angemeldet hatte, im Monatsbericht Erwähnung gefunden hatte. Eine Überprüfung im TLfV ergab jedoch, dass die namentliche Erwähnung keinen Bedenken unterlag, da die beschwerdeführende Person eine Demonstration angemeldet hatte, an der auch Personen teilgenommen haben, die nach § 2 Abs. 1 Satz 2 ThürVSG Gegenstand der Beobachtung des TLfV waren. Hier ergab sich ein Sachzusammenhang, der auch die Anmeldung der Veranstaltung betraf, auch wenn die Organisation, für die die Veranstaltung angemeldet worden war, nicht Gegenstand der Beobachtung durch das Landesamt für Verfassungsschutz war.

8.2 Sicherheitsüberprüfung

Wie ich schon in meinen vorangegangenen Tätigkeitsberichten (1. TB 8.1; 2. TB 8.2) ausgeführt habe, bedarf es zur Durchführung von Sicherheitsüberprüfungen einer gesetzlichen Grundlage, die für

Thüringen bislang nicht geschaffen wurde. Welche Probleme entstehen können, wird deutlich aus einem Rechtsstreit, der bis an das Bundesverfassungsgericht gelangte. Ein Beschwerdeführer hatte in Bayern Auskunft über Daten, auf die das negative Ergebnis einer Sicherheitsüberprüfung gestützt wurde, verlangt, was abgelehnt worden war. Mir war nach §§ 94, 77 Bundesverfassungsgerichtsgesetz Gelegenheit zur Äußerung gegeben worden. In meiner Stellungnahme an das Bundesverfassungsgericht habe ich deutlich gemacht, dass im vorliegenden Fall nicht ersichtlich sei, warum eine Auskunft über den festgestellten Charakterzug des Beschwerdeführers die weitere Arbeit des Verfassungsschutzes gefährde. Das Bundesverfassungsgericht hat in seiner Entscheidung (1 BvR 385/90) vom 27. Oktober 1999 nicht auf den Auskunftsanspruch des Beschwerdeführers, den er aus dem Recht auf informationelle Selbstbestimmung ableitet abgestellt, sondern aufgrund der Rechtsschutzgarantie des Art. 19 Abs. 4 GG, § 99 Abs. 1 Satz 2 in Verbindung mit Abs. 2 Satz 1 VwGO mit Art. 19 Abs. 4 des Grundgesetzes für unvereinbar angesehen und den Bundesgesetzgeber verpflichtet, bis zum 31. Dezember 2001 ein verfassungsmäßigen Zustand herzustellen.

9. Finanzen, Steuern, Rechnungsprüfung

9.1 Änderung der Abgabenordnung (AO)

Bereits im 1. TB (9.1.8) und 2. TB (9.1) hatte ich über die Vorschläge der DSB des Bundes und der Länder bezüglich der Verbesserung des bereichsspezifischen Datenschutzes in der AO berichtet. Zur Frage der Änderung der AO vertrete ich die Auffassung, dass eine Verweisungsvorschrift auf die Anwendbarkeit der Landesdatenschutzgesetze hilfreich wäre. Auch sollten grundlegende Regelungen zur automatisierten Datenverarbeitung hinsichtlich Speicherzweck, Übermittlung an andere Behörden, Speicherdauer und Löschfristen sowie eine Regelung zum Auskunfts- und Akteneinsichtsrecht Betroffener aufgenommen werden. Desweiteren sollte eine Regelung der AO im Hinblick auf den internationalen Datenaustausch zwischen Steuer- und Zollverwaltungen die Einhaltung der Rechtsvorschriften vorschreiben, die in den beteiligten Mitgliedsstaaten in Umsetzung der EU-Datenschutzrichtlinie erlassen wurden. Aufgrund

der Rechtsunsicherheit darüber, welche personenbezogenen Daten bei einer Kontoeröffnung durch Kreditinstitute gem. § 154 Abs. 2 Satz 1 AO zu erheben sind, habe ich vorgeschlagen, zur Klarstellung in der AO ausführlich festzuschreiben, welche personenbezogenen Daten zu erheben sind. Das TFM hat mir hierzu mitgeteilt, dass erwogen werde - in Anlehnung an § 9 Abs. 1 Satz 2 Geldwäschegesetz - in einem Anwendungserlass zu § 154 AO die Verpflichtung zum Kopieren der Vorder- und Rückseite des Ausweisdokumentes aufzunehmen.

9.2 Das Verfahren FISCUS

Im Rahmen der Neukonzeption der Automation in der Steuerverwaltung wird auf der Grundlage eines am 17. Mai 1995 in Kraft getretenen Verwaltungsabkommens der 16 Bundesländer und des Bundes ein gemeinsames bundesweites Automatisierungsprojekt mit der Bezeichnung FISCUS (Föderales Integriertes Standardisiertes Computerunterstütztes Steuersystem) entwickelt. Es ist vorgesehen, in den nächsten Jahren alle bestehenden automatisierten Verfahren der Steuerverwaltung schrittweise (9.5) durch das Verfahren FISCUS abzulösen. Die Entwicklung erfolgt arbeitsteilig in Arbeitsgruppen, deren Tätigkeit durch eine Leitstelle im Bundesministerium der Finanzen koordiniert wird. Die Thüringer Finanzverwaltung ist mit zwei Schwerpunkten an FISCUS beteiligt. Zum einen werden für die künftigen FISCUS-Verfahren in den Ländern einheitliche Schulungsunterlagen und interaktive Lernprogramme sowie Online-Hilfen und sämtliche aufgabenspezifischen DV-Arbeitsanleitungen für die Finanzamtsbediensteten bundesweit erstellt. Desweiteren wird der maschinelle Datenaustausch zwischen FISCUS und allen externen Partnern der Steuerverwaltung, wie z. B. Banken, Bundesbehörden und Kfz-Zulassungsstellen realisiert.

Bei einem Gespräch zwischen Vertretern der Thüringer Finanzverwaltung und dem TLfD wurde der Sachstand des Verfahrens FISCUS dargelegt. Zur Frage der Verschlüsselung der Datenübermittlung wurde ausgeführt, dass in Thüringen die Übermittlung im Corporate Network über Hardware mittels Kryptoboxen bei den Finanzämtern zum Zentrum für Informationsverarbeitung (ZIV) erfolgt. Auch nach Einführung des Verfahrens FISCUS werden

diese Kryptoboxen weiterhin zum Einsatz kommen. Der Projektteil Verschlüsselung innerhalb von FISCUS wird durch ein Entwicklerteam eines anderen Bundeslandes erarbeitet. Zur Problematik der Authentizität wird diskutiert, die Abgabenordnung dahingehend zu ändern, dass auf eine Unterschrift der Steuererklärung verzichtet werden kann, um durch Einsatz von Verfahren der Telekommunikation und der elektronischen Signatur (9.3; 2. TB 15.7.5) in Zukunft die Steuererklärung in Papierform entbehrlich zu machen. Von den FISCUS-Teilprojekten sind bislang das Projekt Fachinformationssystem und der Verfahrensteil Vollstreckung fertig gestellt worden. Der Verfahrensteil Vollstreckung soll etwa im Jahre 2001 in der Thüringer Finanzverwaltung eingeführt werden.

Durch die Einführung von FISCUS werden voraussichtlich verschiedene datenschutzrechtlich problematische Bereiche einer datenschutzgerechten Lösung zugeführt. So soll in FISCUS ein Koordinierungsmerkmal zur eindeutigen Identifizierbarkeit einer Person innerhalb der Steuerverwaltung eingeführt werden. Eine datenverarbeitungsinterne Verwendung dieses Koordinierungsmerkmals ist unbedenklich, wenn sichergestellt ist, dass keine allgemeine Verknüpfung unter den Besteuerungsarten bzw. einzelnen Steuerfällen hergestellt werden kann.

Weiterhin ist in FISCUS vorgesehen, eine Beraterdatei zu führen, in der Steuerberater und vergleichbare Personen mit Anschrift und Ordnungsnummer gespeichert werden sollen. Solange diese Datei zur Bearbeitung von Fristverlängerungsanträgen, Erklärungseingang und Adressierung von Steuerbescheiden dient, gibt es keine Bedenken. Aus datenschutzrechtlicher Sicht bedenklich erscheint es jedoch, durch einen Abgleich dieser Datei mit dem Berufsregister, ohne auf einen konkreten Einzelfall abzustellen, die Befugnis zur geschäftsmäßigen Hilfeleistung in Steuersachen zu prüfen.

Auf der Grundlage einer Verwaltungsvereinbarung der Bundesländer, ist beim Finanzamt Wiesbaden II eine Informationszentrale für den Steuerfahndungsdienst (IZSteufa) geschaffen worden. Aufgabe der IZSteufa ist es, Informationen zu Steuerstraftätern von den mit der Steuerfahndung betrauten Finanzämtern der Bundesländer entgegenzunehmen, diese auszuwerten und Auskünfte zu erteilen. Streitig ist die Rechtsgrundlage der Verarbeitung in der IZSteufa. Die Daten

werden derzeit in einer manuellen Steuerstraftäterkartei gespeichert, wobei eine einheitliche Löschfrist von zehn Jahren vorgeschrieben ist. Die Datenschutzbeauftragten des Bundes und der Länder haben sich insbesondere dagegen gewandt, dass die Daten der Zentrale ohne jede Differenzierung erst nach zehn Jahren gelöscht werden. Im Rahmen der Entwicklung von FISCUS war vorgesehen, auch die Informationsbeziehungen der Steuerfahndung neu zu konzipieren, sodass zukünftig die Einrichtung der IZSteufa entfallen könnte. Nach Auskunft des TFM ist es jedoch derzeit fraglich, ob eine zentrale oder dezentrale Speicherung der Steuerfahndungsdaten in Betracht gezogen wird. Im Arbeitskreis Steuerverwaltung der Datenschutzbeauftragten des Bundes und der Länder wurde vereinbart, die Entwicklung und Einführung von FISCUS-Teilprojekten im Bereich der eigenen Landessteuerverwaltung datenschutzrechtlich zu begleiten und sich darüber auszutauschen.

9.3 Elektronische Steuererklärung (ELSTER) über Internet

Seit Anfang des Jahres 1999 besteht die Möglichkeit, dass Bürger und Steuerberater, die über die entsprechende technische Ausstattung verfügen, im Rahmen eines Feldversuches, an dem auch die Thüringer Finanzverwaltung beteiligt ist, die Steuererklärung auf elektronischem Wege via Internet abgeben können. Das hierzu erforderliche Programm ELSTER wird durch die Bayerische Finanzverwaltung federführend für alle Bundesländer entwickelt. Es kann in die im Handel befindlichen Steuerberechnungsprogramme integriert werden und steht den Softwareherstellern kostenlos zur Verfügung. Zweck dieser Entwicklung ist es, den Erfassungsaufwand bei den Finanzämtern zu verringern. Derzeit schickt das ELSTER-Programm die Steuererklärung, nachdem es diese zur Gewährleistung von Vertraulichkeit und Integrität verschlüsselt und mit einem Hash-Code versehen hat, nicht nur elektronisch an das zuständige Finanzamt, sondern erzeugt noch zusätzlich einen verkürzten schriftlichen Ausdruck der Steuererklärung. Dieser muss - wie gewohnt - mit einer Unterschrift versehen und zusammen mit den zugehörigen Anlagen zum Finanzamt übersandt werden. Der Finanzbeamte überprüft die elektronisch übermittelten Daten auf Übereinstimmung mit der „Papiererklärung“. Nach Auskunft des Thüringer Finanzministeriums wird darüber diskutiert, die AO da-

hingehend zu ändern, dass auf eine Unterschrift der Steuererklärung verzichtet werden kann, um im Verfahren ELSTER in Zukunft die zusätzliche Übersendung der Steuererklärung in Papierform entbehrlich zu machen.

In den Arbeitskreisen Technik und Steuerverwaltung der Datenschutzbeauftragten des Bundes und der Länder wurde vereinbart, die weitere Entwicklung und Einführung des Verfahrens Elektronische Steuererklärung (ELSTER) datenschutzrechtlich zu begleiten und sich darüber auszutauschen. Ich habe gegenüber dem Thüringer Finanzministerium darauf hingewiesen, dass die Absicherung des Rechners des Absenders problematisch erscheint und deshalb sowohl eine Absicherung des Zugangs/Zugriffs auf den Nutzer-PC als auch dessen Schutz gegenüber dem öffentlichen Netz zu gewährleisten ist. Da die hierfür erforderlichen Sicherheitsmaßnahmen im Privatbereich sich der direkten Einflussnahme der Projektleitung von ELSTER entziehen, habe ich angeregt, bspw. innerhalb der Internetpräsentation des Verfahrens ELSTER gegenüber den Absendern der Steuererklärung auf diese Sicherheitsaspekte hinzuweisen.

Desweiteren habe ich das TFM gebeten, die im ZIV der Thüringer Landesverwaltung im Zusammenhang mit dem Verfahren ELSTER geführten Dateien auf das Erfordernis einer Meldung nach § 3 ThürDSRegVO zu prüfen und mich vom Ergebnis der Überprüfung zu unterrichten. Es wurde mitgeteilt, dass eine datenschutzrechtliche Freigabe sowie die entsprechende Meldung an das Datenschutzregister vorbereitet werden.

9.4 Steuerdatenabrufverordnung (StDAV)

Seit geraumer Zeit bin ich damit befasst, die Arbeiten des BMF an einer bundeseinheitlichen Regelung zum automatisierten Abruf von Steuerdaten - einem Verfahren gem. § 7 ThürDSG - im Arbeitskreis Steuerverwaltung der DSB des Bundes und der Länder datenschutzrechtlich zu begleiten, wobei ich dem TFM gegenüber das Fehlen von Regelungen zu Sicherheitsmaßnahmen bei der Übertragung von Daten im öffentlichen Netz bemängelt und den Einsatz von Verschlüsselung mit Hilfe z. B. kryptographischer Verfahren als erforderlich angesehen habe, um die Vertraulichkeit der abgerufenen hochsensiblen Steuerdaten zu wahren.

Das BMF hat im November 1998 eine Verwaltungsregelung über den automatisierten Abruf von Steuerdaten des Bundesamts für Finanzen und der Finanzämter erlassen. Ich habe gegenüber dem TFM deutlich gemacht, dass keine grundsätzlichen datenschutzrechtlichen Bedenken gegen diese Regelung bestehen würden, wobei nach einer Übergangsfrist die Möglichkeit der von den DSB des Bundes und der Länder geforderten Verschlüsselung der Daten und der Passworte bei einer Übertragung im öffentlichen Netz erneut zu prüfen sei.

Im September 1999 wurde dem BfD der Entwurf einer Verordnung über den automatisierten Abruf von Steuerdaten des Bundesamtes für Finanzen, der Finanzämter und Gemeinden von Seiten des BMF zugeleitet. In § 8 Abs. 2 dieses Verordnungsentwurfes ist geregelt, dass die im öffentlichen Netz übermittelten Daten zu verschlüsseln sind. Damit wird einer wichtigen datenschutzrechtlichen Forderung Rechnung getragen. In einer Stellungnahme hat der BfD gegenüber dem BMF u. a. angeregt, in die Verordnung auch Rechnungsprüfungsverfahren einzubeziehen und die vorgesehene Abrufbefugnis von Entwicklungs- und Betreuungspersonal nicht grundsätzlich zu erteilen, sondern auf die Ausnahmefälle zu beschränken, in denen der Abruf echter Steuerdaten zur Aufgabenerfüllung erforderlich ist. Weiterhin wurde empfohlen, sichere Authentisierungsverfahren für Abrufberechtigte, entsprechend den Empfehlungen im BSI-Grundschutzhandbuch, festzulegen, neben der Datenverschlüsselung auch eine Verschlüsselung von Passwörtern vorzusehen, eine Protokollierung der Anmelde-Fehlversuche festzuschreiben sowie die Anzahl der Fehlversuche, die zu einer Sperrung der Datenverbindung führt, von fünf auf drei zu vermindern, was einer Standardvorgabe von PC-Sicherheitssoftware entsprechen würde.

Ich habe mich dieser Auffassung angeschlossen. Darüber hinaus habe ich angeregt, die Gültigkeitsdauer der Passworte in § 8 Abs. 4 des Verordnungsentwurfes von sechs auf drei Monate zu vermindern, was die rechtzeitige Erkennung einer missbräuchlichen Passwortnutzung erleichtern und eine Angleichung mit Standardvorgaben von PC-Sicherheitssoftware herstellen würde. Weiterhin ist eindeutig zu regeln, wie Passworte zu gestalten sind (1. TB 15.14.2). Neben der Regelung zu einer verbindlichen Protokollierung von Zugriffs- und Sicherheitsverletzungen sollte auch die regelmäßige

Auswertung der Protokollierungsdaten vorgeschrieben sein, um eine Früherkennung von systematischen Ausspähversuchen zu erleichtern.

9.5 Speicherkontenübergreifende Umbuchung im integrierten automatischen Besteuerungsverfahren (IABV) bei gleichnamigen Steuerpflichtigen

Von einem Datenschutzbeauftragten eines anderen Bundeslandes erhielt ich Kenntnis einer Beschwerde darüber, dass eine Bürgerin von einem Finanzamt mehrfach mit einer Person verwechselt worden sei, die den gleichen Namen und Vornamen trägt und auch am gleichen Tage geboren wurde. Durch die Übereinstimmung dieser Daten wurde ihr Steuerguthaben von Programmen des IABV zur speicherkontenübergreifenden Umbuchung mit Steuerrückständen der anderen Steuerpflichtigen verrechnet. Diese Verfahrensweise führte dazu, dass durch die mit der speicherkontenübergreifenden Umbuchung verbundene Umbuchungsmitteilung Steuerdaten einer Steuerpflichtigen einer anderen Person gegenüber offenbart worden waren, was eine Verletzung des Steuergeheimnisses darstellt. Darüber hinaus wurde die Steuerpflichtige gegenüber der Finanzverwaltung unzutreffend als säumige Steuerzahlerin dargestellt. Ich habe die Thüringer Steuerverwaltung gebeten zu prüfen, ob die gleichen Umbuchungsprogramme wie im Beschwerdefall Verwendung finden und ggf. mitzuteilen durch welche Maßnahmen ein derartiger Datenschutzverstoß zukünftig verhindert werden kann.

Nach Auskunft der OFD Erfurt wird das Verfahren zur maschinellen speicherkontenübergreifenden Umbuchung aufgrund langjähriger Forderungen des Bundesrechnungshofes inzwischen bundesweit eingesetzt, um automationsunterstützt insbesondere Kraftfahrzeugsteuerrückstände mit Ansprüchen aus Veranlagungssteuern aufzurechnen. Aufgerechnet wird zwischen Speicherkonten einer natürlichen Person, wenn Name, Vorname, Geburtsdatum und Anrede in den Speicherkonten übereinstimmen. Auf die Prüfung der Anschrift wird verzichtet, damit auch die Speicherkonten von Steuerbürgern geprüft werden können, die z. B. wegen Umzug oder Zweitwohnsitz in unterschiedlichen Finanzämtern geführt werden. Seit Einführung und massenhaften Anwendung des Verfahren kam es in der Thürin-

ger Steuerverwaltung in wenigen Fällen zu fehlerhaften speicherkontenübergreifenden Umbuchungen. In diesen Fällen sind die Finanzämter angewiesen, alle beteiligten Speicherkonten mit einem Sperrvermerk zu versehen, um eine künftige unzutreffende maschinelle Umbuchung zu verhindern. Beschwerden liegen mir bislang nicht vor. Im Rahmen der Neukonzeption der Automation in der Steuerverwaltung ist vorgesehen, das derzeitige Verfahren IABV bundesweit schrittweise durch das Verfahren föderales integriertes standardisiertes computerunterstütztes Steuersystem (FISCUS) abzulösen. In FISCUS soll ein datenverarbeitungsinternes Koordinierungsmerkmal verwendet werden, welches die zeitweilige Verknüpfung von verschiedenen Steuerkonten einer Personen innerhalb einer Landessteuerverwaltung ermöglicht, wodurch eine Verletzung des Steuergeheimnisses infolge fehlerhafter Identitätsprüfung ausgeschlossen sein soll. Für die Thüringer Steuerverwaltung ist die Einführung dieses Verfahrens ab dem Jahre 2003 vorgesehen.

Im Kreise der Datenschutzbeauftragten der Länder wurde die Möglichkeit erwogen, eine Liste der in Frage kommenden Speicherkonten zu erstellen und bei der Identitätsprüfung im derzeitigen Verfahren einzubeziehen, wodurch solche Fehler bei der Identitätsprüfung vermieden werden können. Im Hinblick auf den dafür erforderlichen hohen Entwicklungsaufwand und unter Berücksichtigung der relativ geringen Fehlerzahlen des derzeitigen Verfahrens habe ich vor dem Hintergrund der anstehenden Einführung des Verfahrens FISCUS von datenschutzrechtlichen Forderungen bezüglich des derzeitigen Verfahrens der speicherkontenübergreifenden Umbuchung abgesehen.

9.6 Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

Vom BfD erhielt ich Kenntnis von Beschwerden darüber, dass vom Bundesamt für Finanzen den Auftraggebern von Freistellungsaufträgen die Auskunft über ihre dort gespeicherten Daten verweigert worden ist. Dem lag folgender Sachverhalt zugrunde: Beim Bundesamt für Finanzen werden für Kontrollzwecke alle Freistellungsaufträge gespeichert, die Kunden z. B. ihrer Bank oder ihrer

Bausparkasse erteilt haben, um den Abzug von Steuern von ihren Zinsen zu vermeiden. Hierfür melden die Banken und vergleichbare Institute dem Bundesamt einmal jährlich die Namen und Anschriften der Auftraggeber und die Höhe, über die der Freistellungsauftrag jeweils erteilt worden ist. Hat ein Auftraggeber das Bundesamt um Auskunft über seine dort gespeicherten Daten gebeten, etwa weil er wegen eines Wohnungswechsels, durch Änderung seiner Bankverbindungen oder aus anderen Gründen die Übersicht über die von ihm erteilten Freistellungsaufträge verloren hatte, ist sie ihm verweigert worden. Gestützt wurde diese Verweigerung auf einen Erlass des BMF vom 14. April 1997.

Diese Auskunftsverweigerung verstößt gegen den datenschutzrechtlichen Auskunftsanspruch von Bürgern gegenüber der Verwaltung, welcher in § 19 BDSG geregelt ist. Der BfD hat dies gegenüber dem BMF beanstandet, was allerdings zunächst nicht zu einer Änderung der Verwaltungspraxis führte. Daraufhin wurde auf Initiative des BfD anlässlich der 56. Konferenz der Datenschutzbeauftragten von Bund und Ländern am 5./6. Oktober 1998 in Wiesbaden eine diesbezügliche EntschlieÙung verabschiedet (Anlage 5). Hierin wird vom BMF die Aufhebung des zugrundeliegenden Erlasses gefordert.

Ich habe dem TFM die EntschlieÙung der Konferenz übersandt und um Mitteilung darüber gebeten, wie in der Praxis der Thüringer Finanzverwaltung Auskunftersuchen von Betroffenen gehandhabt werden. Nach Auskunft des TFM waren keine Beschwerdefälle im seinem Geschäftsbereich aufgetreten. Nachdem zwischenzeitlich die KonferenzentschlieÙung an das BMF herangetragen worden war, hat das BMF am 5. Januar 1999 den beanstandeten Erlass aufgehoben und zugleich das Bundesamt für Finanzen angewiesen, dem Auftraggeber von Freistellungsaufträgen nach pflichtgemäßem Ermessen Auskunft zu den über ihn gespeicherte Daten zu erteilen, soweit der Betroffene hierfür ein berechtigtes Interesse darlegt oder dies ohne weitere Ermittlungen ersichtlich ist und keine Versagungsgründe vorliegen.

9.7 Kontrolle bei der Staatskasse

Im Berichtszeitraum wurde in der Staatskasse Erfurt das Verfahren zur Aufrechnung von Forderungen Steuerpflichtiger mit Ansprüchen

aus deren Steuerschuldverhältnis kontrolliert. Im Rahmen der Bearbeitung von Auszahlungsanordnungen des Freistaats wird seitens der Staatskasse geprüft, ob mit Steuerforderungen aufgerechnet werden kann. Zu diesem Zweck wurde der Staatskasse Erfurt von Seiten des TFM ein direkter lesender Zugriff auf das Integrierte Automatische Besteuerungsverfahren der Thüringer Steuerverwaltung (IABV) ermöglicht. Dadurch erlangen Mitarbeiter der Staatskasse Kenntnis von personenbezogenen Daten Steuerpflichtiger, die dem Steuergeheimnis gem. § 30 AO unterliegen. Die Mitarbeiter der Staatskasse, die mit dem Zugriff auf Steuerdaten betraut wurden, sind hinsichtlich des Daten- und Steuergeheimnisses verpflichtet worden. Derzeit werden sämtliche Abfragen im IABV zu Nachweiszwecken manuell auf den Auszahlungsanordnungen protokolliert.

Nach Punkt 6 der geltenden Steuerdatenabrufverordnung (StDAV) sind für den Betrieb eines Abrufverfahrens angemessene technische und organisatorische Vorkehrungen zu treffen, um Abrufe durch Nichtbeteiligte sowie eine Überschreitung der Abrufberechtigung zu verhindern und die nachträgliche Feststellung zu ermöglichen, auf Grund wessen Abrufberechtigung Daten abgerufen werden konnten. Gemäß Punkt 8 StDAV ist auf Grund programmgesteuerter Aufzeichnungen zu prüfen, ob der Aufruf nach § 30 Abs. 6 Satz 1 AO zulässig war.

Eine programmgesteuerte Protokollierung der Nutzerzugriffe auf die Steuerdaten wird erst mit der Einführung des Nachfolgeprojektes „UNIX im Finanzamt“ (UNIFA) verwirklicht werden. Wegen der fehlenden programmgesteuerten Protokollierung im Sinne der StDAV habe ich die Zulässigkeit des Abrufs als nicht uneingeschränkt gegeben beurteilt. Da von den Ansprechpartnern dargelegt wurde, dass mit dem Aufrechnungsverfahren Steuerausfälle in erheblichem Umfang vermieden werden können und das Nachfolgeprojekt die umfassende programmgesteuerte Protokollierung vorsieht, habe ich die datenschutzrechtlichen Bedenken bis zur Einführung des Nachfolgeprojektes zurückgestellt. Eine konkrete Angabe, bis wann dies der Fall sein wird, steht noch aus.

9.8 Zustellung eines Briefes durch ein Finanzamt

Von einem Bürger erhielt ich einen verschlossenen Brief eines Finanzamtes, der im Eingangsbereich eines Mehrfamilienhauses gele-

gen habe, in dem auch er wohne. Der Adressat sei nicht im Hause wohnhaft. Ich habe den Brief an das absendende Finanzamt gesandt und um Auskunft gebeten, aufgrund welcher Rechtsgrundlage der Brief am angegebenen Ort abgelegt worden sei. Nach Auskunft der OFD hatte ein Vollzugsbeamter des zuständigen Finanzamtes den Adressaten mehrfach nicht angetroffen. Im Rahmen der Vollstreckung sei dessen Wohnung aufgrund einer gerichtlichen Anordnung unter Hinzuziehung eines Schlüsseldienstes geöffnet worden. Man habe festgestellt, dass die Wohnung leergeräumt gewesen sei. Daraufhin sei sie mit einem neuen Schloss versehen und ordnungsgemäß verschlossen worden. Ein Schreiben, in welchem der Betroffene über die Durchsuchung und die Möglichkeit, den neuen Wohnungsschlüssel bei der Stadtverwaltung abzuholen, informiert worden sei, habe man in den Briefkasten des Betroffenen eingeworfen. Auch noch zu diesem Zeitpunkt seien sowohl die Wohnung als auch der Briefkasten mit dem Namen des Betroffenen bezeichnet gewesen. Wie das Schreiben des Finanzamtes in den öffentlich zugänglichen Bereich des Hausflurs gelangt war, konnte nicht mehr nachvollzogen werden.

Ausweislich einer OFD-Verfügung als anzuwendende Verwaltungsvorschrift sind - sofern nach einer Wohnungsöffnung der Einbau eines neuen Schlosses erforderlich ist - die Vollstreckungsbeamten verpflichtet, außerhalb der Wohnung an gut sichtbarer Stelle einen kuvertierten Hinweis anzubringen, welcher darüber informiert, dass der Wohnungsschlüssel unter Vorlage des Personalausweises bei der nächsten Polizeidienststelle abgeholt werden kann. Abweichend von dieser Vorschrift ist im Bereich des betroffenen Finanzamtes der Schlüssel im Rahmen einer Amtshilfe bei der Stadtverwaltung, die die Abholung der Schlüssel rund um die Uhr gewährleistet, zu hinterlegen, da die Polizeidienststelle aus Arbeitsüberlastung die Schlüsselverwahrung abgelehnt habe.

Gegenüber der OFD habe ich angeregt, die Verwaltungsvorschrift bezüglich der Schlüsselverwahrung für das betroffene Finanzamt und die dortige Verwaltungspraxis einander anzugleichen. Soweit im Rahmen einer Vollstreckungsmaßnahme festgestellt wird, dass eine Mietwohnung unbewohnt ist und das Türschloss gewechselt wurde, wird seitens der Finanzverwaltung künftig so vorgegangen, dass

dem Vermieter mitgeteilt wird, dass der Schlüssel bei der Finanzamtverwaltung abgeholt werden kann.

9.9 Weiterleitung eines Beschwerdeschreibens eines Bürgers durch die Sparkassenaufsicht an seine Sparkasse

Im Wege der Beschwerde hatte sich ein Betroffener wegen der Verfahrensweise der Sparkassenaufsicht im Thüringer Finanzministerium gem. § 11 ThürDSG an mich gewandt. Der Beschwerde lag folgender Sachverhalt zugrunde: Der Beschwerdeführer hatte die Sparkassenaufsicht um Prüfung gebeten, ob das Verhalten der Sparkasse in seinem Fall rechtmäßig gewesen sei, woraufhin die Sparkassenaufsicht das Beschwerdeschreiben an die Sparkasse weitergeleitet hat. Folglich hatte die Sparkasse Kenntnis darüber, dass sich ein bestimmter Kunde an die Sparkassenaufsicht gewandt hatte. Der Betroffene befürchtete durch die Offenbarung seiner personenbezogenen Daten im Zusammenhang mit der Beschwerde die Schädigung seines Ansehens bei der Sparkasse.

Nach § 21 i. V. m. § 20 ThürDSG ist eine Datenübermittlung an andere Stellen im öffentlichen Bereich zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelten Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und die Voraussetzungen nach § 20 ThürDSG vorliegen, zu denen u. a. die Einwilligung zählt.

Bei der Übersendung der Beschwerde war die Aufsichtsbehörde zunächst davon ausgegangen, dass, wenn jemand dazu auffordert, „eine Sache zu klären“, eine mutmaßliche Einwilligung zur Übermittlung von personenbezogenen Daten vorliegt. Das dem nicht zwingend so ist, zeigt das Vorliegen der datenschutzrechtlichen Beschwerde. Die Datenübermittlung erfolgte nach Auffassung der Sparkassenaufsicht aber auch im Interesse des Betroffenen, der möglicherweise eine Kulanzentscheidung der Sparkasse hätte erwarten können. Die datenschutzrechtliche Prüfung ergab, dass von einer Einwilligung des Betroffenen zur Weitergabe seiner personenbezogener Daten nicht ausgegangen werden konnte. Auch war ein Erfordernis der Datenweitergabe zur Aufgabenerfüllung nicht erkennbar, da die Bearbeitung der Beschwerde auch unter Verwendung von anonymisierten Daten des Beschwerdeführers möglich gewesen wäre. Die Datenweitergabe war also nicht erforderlich und

somit als unzulässig zu bewerten. Mein Vorschlag, die Betroffenen künftig zur Vermeidung von Missverständnissen bezüglich des Vorliegens einer Einwilligung zur Datenübermittlung konkret zu befragen, wurde durch die Sparkassenaufsicht aufgegriffen.

9.10 Datenübermittlung von Standesämtern an Finanzämter bei Sterbefallanzeigen

Im Rahmen einer Prüfung hatte ein Standesamt die Frage aufgeworfen, in welchem Umfang die Standesämter ermächtigt oder verpflichtet sind, im Auftrag der Finanzämter Vermögensdaten Verstorbener bei der Entgegennahme einer Sterbefallanzeige zu erheben. Während in dem als Anlage zur Erbschaftssteuereinführungsverordnung beigefügten Muster einer Erbschaftsteuer-Totenliste, die die Standesämter nach der geltenden Dienstanweisung auszufüllen und den Finanzämtern zu übergeben haben, eine Formulierung enthalten ist, nach der alle Fragen, über die das Sterbebuch keine Auskunft gibt, zu beantworten sind, „soweit sie der Standesbeamte aus eigenem Wissen oder nach Befragen des Anmeldenden beantworten kann“, enthält der Verordnungstext lediglich die Vorgabe, dass die Angaben - soweit bekannt - zu ergänzen sind.

Da sich auch andere Landesdatenschutzbeauftragte aufgrund gleichartiger Fragestellungen mit der Problematik beschäftigten, gelangten nach gemeinsamer Beratung die DSB des Bundes und der Länder zu der Auffassung, dass die im Muster der Erbschaftssteuereinführungsverordnung enthaltene Bestimmung nicht über die im Verordnungstext enthaltene Regelung hinausgehen kann. Insoweit lässt sich aus der Regelung nur eine Übermittlungsbefugnis für Standesbeamte bei vorhandenen Erkenntnissen, nicht aber eine Erlaubnis zur eigenen Datenerhebung bzw. Befragung der Sterbefallanzeigenden ableiten. Dies wäre ansonsten aus datenschutzrechtlicher Sicht insbesondere deshalb bedenklich, weil überwiegend von Bestattungsbetrieben die Todesfälle angezeigt werden, die bei einer regelmäßigen Fragestellung durch die Standesämter ihrerseits möglicherweise eine Berechtigung oder Verpflichtung für Recherchen bzw. zur Erhebung von Daten über verwandtschaftliche Verhältnisse und Vermögenswerte des Verstorbenen bei den Angehörigen ableiten könnten. Da eine Auskunftspflicht der Anmeldenden aber in keiner Weise gege-

ben ist, bedarf es, auch wenn diese unaufgefordert Auskünfte zum Vermögen erteilen, seitens des Standesamtes den allgemeinen datenschutzrechtlichen Grundsätzen folgend, eines Hinweises, dass diese Informationen an die Finanzämter übermittelt werden.

Das TIM hat zwischenzeitlich meiner Bitte entsprochen und eine diesbezügliche Unterrichtung der Standesämter veranlasst. Darüber hinaus ist nach dem Entwurf der 14. Dienstanweisungsänderungsverwaltungsvorschrift für Standesbeamte und ihre Aufsichtsbehörden mit einer weiteren Klarstellung zu rechnen.

9.11 Datenschutz beim Druck und Versand von Lohnsteuerkarten durch private Serviceunternehmen

Wie im 2. TB (9.7) berichtet, hatte ich gegenüber dem TFM angeregt, in Vorbereitung des Druckes der Lohnsteuerkarten für das Steuerjahr 1999 alle erforderlichen Maßnahmen zu treffen, um bei der Beauftragung von privaten Serviceunternehmen sowohl den Datenschutz als auch das Steuergeheimnis zu gewährleisten. Die Dringlichkeit der Angelegenheit ergab sich daraus, dass in den letzten Jahren zahlreiche Kommunen private Unternehmen mit dem Druck von Lohnsteuerkarten beauftragt haben, wodurch Mitarbeiter dieser Unternehmen Kenntnis von sensiblen personenbezogenen Daten, die dem Steuergeheimnis gem. § 30 AO unterliegen, erlangen konnten. Ich hatte gegenüber dem TFM deutlich gemacht, dass es sich bei der Ausstellung und der Versendung von Lohnsteuerkarten durch Privatunternehmen um eine Auftragsdatenverarbeitung im Sinne von § 8 Abs. 6 ThürDSG handelt. Die auftragerteilende öffentliche Stelle ist für die Einhaltung der Vorschriften dieses Gesetzes verantwortlich und hat bei der Gestaltung des Vertrages zur Auftragsdatenverarbeitung dafür Sorge zu tragen, dass sich der private Auftragnehmer der Kontrolle des TLfD unterwirft (§ 8 Abs. 6 Satz 1 ThürDSG). Da die Vorschrift des § 30 AO nur auf Amtsträger oder gleichgestellte Personen anwendbar ist, sind die Mitarbeiter der betreffenden Dienstleistungsunternehmen nach dem Verpflichtungsgesetz auf die Einhaltung des Steuergeheimnisses zu verpflichten.

Bisher nicht geregelt war, welche öffentliche Stelle für die Verpflichtung dieser „Nichtamtspersonen“ zuständig ist. Hierzu hat das TFM am 10. August 1998 eine „Anordnung über die Zuständigkeit

für die Verpflichtung von nichtbeamteten Personen nach dem Verpflichtungsgesetz im Geschäftsbereich des Finanzministeriums“ erlassen, die mit Veröffentlichung im Thüringer Staatsanzeiger in Kraft getreten ist. Danach liegt die Zuständigkeit bei den Gemeinden, die private Dienstleistungsunternehmen mit der Ausstellung und dem Versand von Lohnsteuerkarten beauftragt haben. In einer Verfügung der OFD von Oktober 1998 wurden die Gemeinden darauf hingewiesen, dass sie bei der Auswahl der Unternehmen und der Vertragsgestaltung das ThürDSG zu beachten und den TLfD gem. § 8 Abs. 5 Satz 2 ThürDSG über die Beauftragung zu unterrichten haben. Ein direkter Hinweis darauf, dass gem. § 8 Abs. 6 Satz 1 ThürDSG mit schriftlichem Vertrag sicherzustellen ist, dass der Auftragnehmer die Bestimmungen des ThürDSG befolgt und sich der Kontrolle durch den TLfD unterwirft, wurde jedoch nicht in die Verfügung aufgenommen. Auch wurde „aus praktischen Erwägungen“ die Möglichkeit zugelassen, auf eine Verpflichtung einzelner Unternehmensmitarbeiter zugunsten einer Verpflichtung des Geschäftsführers zu verzichten, wenn gegenüber der Gemeinde erklärt wird, dass die Mitarbeiter über den Inhalt der Verpflichtung unterrichtet worden seien.

Ich habe gegenüber dem TFM gefordert, die Verpflichtung nicht auf die Geschäftsführer zu beschränken, sondern auf alle natürlichen Personen der beauftragten Unternehmen, die an Druck und Versand von Steuerkarten beteiligt sind, anzuwenden sowie in der Verfügung für das Jahr 2000 einen Hinweis auf die Kontrollbefugnis des TLfD gem. § 8 Abs. 6 Satz 1 ThürDSG aufzunehmen, da ansonsten die Kontrolltätigkeit des TLfD gegenüber der beauftragten Unternehmen nicht gewährleistet werden könne. In dem an die OFD gerichteten Erlass des TFM vom 15. Juli 1999 zum Lohnsteuerkartenausstellungsverfahren 2000 sind meine diesbezüglichen Forderungen berücksichtigt worden. Der Inhalt des Erlasses hat in einer Verfügung der OFD sowie in einem Merkblatt zur Ausstellung und Übermittlung der Lohnsteuerkarten 2000 für Gemeinden und Finanzämter seinen Niederschlag gefunden.

Gegenüber den Thüringer Kommunen habe ich auf die Forderungen aus § 8 ThürDSG hingewiesen und um Unterrichtung einer zur etwaigen Beauftragung von privaten Serviceunternehmen mit dem Druck und Versand von Lohnsteuerkarten gebeten.

9.12 Übersendung von Steuerunterlagen mittels Infobrief

Seitens einer Kommune wurde ich gebeten, zu beurteilen, ob der Versand von Mahnungen und Steuerbescheiden mittels der Versandform „Infobrief“ (1. TB 10.10) aus datenschutzrechtlicher Sicht zulässig ist. Bei der Versandform „Infobrief“ handelt es sich um das Angebot eines Unternehmens. Danach wird beim Versand einer Mindestanzahl von Briefen pro Sendung Preisnachlass gewährt. Zugleich muss der Kunde mit einer stichprobenweisen Öffnung von Briefen durch Mitarbeiter des Unternehmens zwecks Prüfung des Inhalts einverstanden sein. Da es sich bei Steuerbescheiden und Mahnungen um sensible personenbezogene Daten handelt, sind nach § 9 Abs. 3 ThürDSG bei der Verarbeitung personenbezogener Daten in nichtautomatisierten Dateien oder in Akten Maßnahmen zu treffen, die verhindern, dass Unbefugte auch beim Transport auf die Daten zugreifen können. Im Fall der Infobriefe ist durch die Möglichkeit der stichprobenweisen Öffnung der Zugriff von Mitarbeitern des Unternehmens, als Dritte, nicht verhindert. Die Versandform als Infobrief zur Versendung von Steuerdaten ist daher aus datenschutzrechtlicher Sicht als unzulässig zu bewerten.

9.13 Steuerliche Anerkennung von Auslandsgruppenreisen

Im Kreis der Datenschutzbeauftragten des Bundes und der Länder wurde im Berichtszeitraum die datenschutzrechtliche Problematik bei der Prüfung von Werbungskosten und Betriebsausgaben für Auslandsgruppenreisen diskutiert. Kosten einer Auslandsgruppenreise können steuerlich anrechenbar sein, wenn die Reise ausschließlich beruflichen bzw. betrieblichen Zwecken dient. Zur Beurteilung des Reisezwecks werden verschiedene Kriterien, wie bspw. der konkrete Veranstaltungsplan, die Mitreise von Familienangehörigen und die Homogenität des Teilnehmerkreises herangezogen. Auf meine diesbezügliche Anfrage teilte das TFM mit, dass auch in der Thüringer Finanzverwaltung die Homogenität des Teilnehmerkreises bewertet wird. Hierzu wird vom Steuerpflichtigen das Verzeichnis der Reiseteilnehmer (Namen und Anschriften) abgefordert. Bei Entscheidungen in Zweifelsfällen werden Kontrollmitteilungen mit Name und Anschrift der Mitreisenden an die

Wohnsitzfinanzämter der Mitreisenden übersandt, was zur Gleichmäßigkeit der Besteuerung beitrage.

Ich halte die Übermittlung von personenbezogenen Daten von Mitreisenden in Form von Kontrollmitteilungen für datenschutzrechtlich bedenklich, da hierbei die personenbezogenen Daten der in der Teilnehmerliste benannten Steuerpflichtigen an die jeweiligen Wohnsitzfinanzämter auch dann übersandt werden, wenn die Kosten der Gruppenreise nicht geltend gemacht werden. Ich habe das TFM darauf hingewiesen, dass nach meinem Kenntnisstand Teilnehmer einer Gruppenreise die Möglichkeit haben, gegenüber dem Reiseveranstalter die Nichtaufnahme ihrer personenbezogenen Daten in die Teilnehmerliste zu fordern. Im Hinblick auf diesen Umstand ist aus der Teilnehmerliste nicht mit Sicherheit auf die Homogenität des Teilnehmerkreises zu schließen.

9.14 Führung eines Fahrtenbuches durch Ärzte

Wie im 2. TB (9.6) berichtet, hatte ich dem TFM gegenüber die Auffassung vertreten, dass die vorgesehene Neuregelung, wonach Ärzte bei der Führung eines steuerlichen Fahrtenbuches zu verpflichten seien, neben Datum, Kilometerstand und Ort auch den Name und die Anschrift des besuchten Patienten aufzuzeichnen nach derzeitiger Rechtslage unzulässig ist. Seit Anfang 1999 ist diese Regelung in Kraft getreten. Bis dahin war statt des Namens und der Anschrift des Patienten lediglich die Eintragung „Patientenbesuch“ anzugeben.

Nach übereinstimmender Auffassung der DSB des Bundes und der Länder ist die Verpflichtung zur Mitteilung von Name und Anschrift der Patienten datenschutzrechtlich bedenklich und verstößt gegen das Auskunftsverweigerungsrecht gem. § 102 Abs. 1 Nr. 3 Buchstabe c AO. Danach steht Ärzten ein Auskunftsverweigerungsrecht über das zu, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist. Dies umfasst nicht allein Inhalte des Arzt-Patienten-Verhältnisses, sondern auch die Information über die Tatsache, dass der Arzt den Patienten aufgesucht hat. Diese Vorschrift dient der Wahrung der ärztlichen Schweigepflicht. Ein Verstoß hiergegen ist nach § 203 StGB strafbar. Dieser Rechtsstandpunkt wurde

gegenüber den BMF und den obersten Finanzbehörden der Länder vertreten, welche zunächst beabsichtigten, die Neuregelung unverändert beizubehalten.

Mittlerweile konnte auf Initiative des BfD eine Kompromisslösung mit dem BMF erzielt werden, wonach Name und Adresse des besuchten Patienten in einem vom Fahrtenbuch getrennt zu führenden Verzeichnis festgehalten werden. Die Finanzämter sollen dieses Verzeichnis nur dann einsehen, wenn Zweifel an der Richtigkeit oder Vollständigkeit der Eintragungen im Fahrtenbuch bestehen und diese Zweifel nicht mit anderen Mitteln auszuräumen sind.

9.15 Internes aus einer Rechnungsprüfungsstelle im Internet

Im Oktober 1999 war aus der Presse zu entnehmen, dass ein Abgeordneter des Thüringer Landtags einen Bericht der Rechnungsprüfer und verschiedene interne Unterlagen der Rechnungsprüfungsstelle im Internet veröffentlicht hatte. Dabei war in der Presse auch von datenschutzrechtlicher Relevanz gesprochen worden. Nach § 37 Abs. 1 ThürDSG kontrolliert der Landesbeauftragte für den Datenschutz bei allen öffentlichen Stellen die Einhaltung der Vorschriften dieses Gesetzes und anderer Rechtsvorschriften über den Datenschutz, wobei sich nach Abs. 2 die Kontrolle auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, erstreckt. Davon ausgenommen ist nach § 37 Abs. 4 ThürDSG neben den Gerichten auch der Landtag, die einer Kontrolle des Landesbeauftragten für den Datenschutz nur in so weit unterliegen, als sie in Verwaltungsangelegenheiten tätig sind. Wie der Landtag selbst, sind auch die Abgeordneten zu betrachten, deren Handeln einer datenschutzrechtlichen Prüfung durch den Landesbeauftragten für den Datenschutz nicht unterfällt. Die Veröffentlichung von internen Schriftstücken durch einen Abgeordneten im Internet ist nicht dem allgemeinen Verwaltungsbereich zuzuordnen, weshalb auch keine Zuständigkeit des TLfD vorlag.

Zuständig bin ich jedoch für alle öffentlichen Stellen des Freistaats Thüringen, so auch den Thüringer Rechnungshof und das von der Rechnungsprüfungsstelle geprüfte TMWAI, was die Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften und insbesondere die zu treffenden technischen und organisatorischen Maßnahmen

zur Sicherstellung des Datenschutzes angeht. Es stellte sich daher weiter die Frage, ob durch die Veröffentlichung im Internet das informationelle Selbstbestimmungsrecht von Beteiligten verletzt worden sein konnte. Ich habe deshalb den Thüringer Rechnungshof gebeten, mir die veröffentlichte Prüfmitteilung der Staatlichen Rechnungsprüfungsstelle zu übersenden, um angesichts meiner gesetzlichen Aufgabe zu prüfen, ob personenbezogene Daten in dem Schriftstück enthalten sind. Der Personenbezug ist mitunter nicht einfach festzustellen, da dies nicht allein davon abhängt, dass eine natürliche Person benannt wird, sondern auch Informationen, die geeignet sind, einen Personenbezug herzustellen, personenbezogene Daten darstellen können.

Die Durchsicht der Prüfmitteilung, die mir seitens des Rechnungshofs erst nach mehrmaligen Anschreiben zur Verfügung gestellt wurde, weil er davon ausgegangen war, dass darin keine personenbezogenen Daten enthalten sind, hat ergeben, dass sowohl personenbezogene als auch personenbeziehbare Daten zu entnehmen sind. Infolge dessen sind seitens der zuständigen Stelle ebenso wie beim Empfänger der Prüfmitteilung nach § 9 ThürDSG die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die Ausführung der datenschutzrechtlichen Vorschriften zu gewährleisten. Dies gilt sowohl für die Unterlagen in Papierform als auch bei der automatisierten Verarbeitung personenbezogener Daten. Der Thüringer Rechnungshof hat mir zwischenzeitlich teilweise die getroffenen organisatorischen und technischen Maßnahmen zum Schutz der personenbezogenen Daten mitgeteilt. Eine Stellungnahme des TMWAI steht noch aus, da der Ausgang eines staatsanwaltshaftlichen Ermittlungsverfahren abgewartet werden soll, was aber meiner Auffassung nach der erbetenen Stellungnahme nicht entgegen stehen kann.

10. Justiz

10.1 Fehlende bereichsspezifische Regelungen bei der Justiz - Beratungen zum Strafverfahrensänderungsgesetz (StVÄG)

Auch in diesem Berichtszeitraum sind die Lücken durch fehlende bereichsspezifische Regelungen im Bereich der Justiz immer noch nicht vollständig geschlossen (1. TB 10.1; 2. TB 10.2). In Anbetracht dessen, dass derzeit in allen Bereichen der Justiz im Zuge von Modernisierungsmaßnahmen umfassende Systeme der automatisierten Datenverarbeitung eingeführt werden und damit eine vollkommen neue Qualität der Datenverarbeitung im Justizbereich Einzug erhält, haben die Datenschutzbeauftragten des Bundes und der Länder mit der Entschließung der 56. Konferenz (Anlage 4) wiederum darauf hingewiesen, dass die Rechtsprechung der Bundesverfassungsgerichts zum so genannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Seit dem Volkszählungsurteil sind immerhin bereits 16 Jahre vergangen.

Nachdem der Gesetzentwurf für ein StVÄG 1996, mit dem wesentliche Lücken hätten geschlossen werden können, der Diskontinuität unterfallen war, liegt nunmehr als Bundestags-Drucksache 14/1484 vom 16.08.1999 wieder ein Gesetzentwurf zur Änderung und Ergänzung des Strafverfahrensrechts - StVÄG 1999 vor. Aus datenschutzrechtlicher Sicht enthält der nunmehr vorliegende Entwurf noch Verschlechterungen gegenüber dem Vorentwurf des StVÄG 1996. Zu meinen bereits im 2. TB (10.2) dargestellten Bedenken und Forderungen, die nach wie vor bestehen, hatte ich zu dem Gesetzentwurf mit Stand vom 14.01.1999 ergänzend Stellung genommen. Beispielsweise sollte eine Änderung aufgenommen werden, dass dem nicht anwaltlich vertretenen Beschuldigten ebenfalls Akteneinsicht, soweit dem nicht die dort genannten Umstände entgegenstehen, zu gewähren ist und nicht nur ein Recht auf Auskunft und Abschriften eingeräumt wird. Diese Forderung stützt sich auf eine Entscheidung des Europäischen Gerichtshofs für Menschenrechte vom 17. Februar 1997, wonach die Verweigerung der Akteneinsicht gegenüber einem nicht anwaltlich vertretenen Beschuldigten

Art. 6 Abs. 1 und 3 Europäische Menschenrechtskonvention (EMRK) verletzt. Darüber hinaus sollte aufgenommen werden, dass für nicht beschuldigte Personen in Anbetracht der Schwere des Eingriffs in das informationelle Selbstbestimmungsrecht im Rahmen der längerfristigen Observation eine Benachrichtigungspflicht aufgenommen wird. Eine im Entwurf des StVÄG 1996 enthaltene Verpflichtung zur Löschung von bereits bei der Polizei vorhandenen Daten sollte zur Sicherung der Zweckbindung beibehalten werden. Darüber hinaus sollten, soweit gemeinsame Dateien zulässig sein sollen, Regelungen zur datenschutzrechtlichen Verantwortlichkeit der beteiligten Stellen aufgenommen werden. Es bleibt abzuwarten, ob es in dieser Wahlperiode letztendlich zu den noch fehlenden Regelungen im Bereich der Justiz kommen wird.

10.2 Mitteilungen in Straf- und Zivilsachen (MiStra, MiZi)

Die aufgrund des Justizmitteilungsgesetzes zu ändernden Verwaltungsvorschriften - Mitteilungen in Strafsachen (MiStra) und Mitteilungen in Zivilsachen (MiZi) - sind fristgemäß zum 1. Juni 1998 in Kraft getreten. Die Änderungen der Verwaltungsvorschriften wurden seitens der Datenschutzbeauftragten des Bundes und der Länder intensiv begleitet. Eigens hierzu wurden Arbeitsgruppen eingesetzt, die die datenschutzrechtlichen Forderungen unter einigem Zeitdruck in eine gemeinsamen Stellungnahme zusammengestellt hatten. Diese Stellungnahme ist seitens der Datenschutzbeauftragten ggf. mit möglichen weiteren Forderungen und Anmerkungen den Justizressorts übersandt worden. Durch die Aufnahme verschiedener Änderungen haben beide Verwaltungsvorschriften aus meiner Sicht erfreulicherweise erhebliche datenschutzrechtliche Verbesserungen erfahren: In zahlreichen Fällen ist für die Anordnung bestimmter Mitteilungen zusätzlich ein geforderter ausdrücklicher Richter- oder Staatsanwaltsvorbehalt und die Benachrichtigung der Betroffenen aufgenommen worden. Einzelne Mitteilungspflichten wurden gestrichen, weil sie nicht erforderlich waren, z. B. in Strafsachen gegen Empfänger von Leistungen nach dem Bundesentschädigungsgesetz oder gegen Inhaber von Fischereischeinen sowie Mitteilungen über Namensänderungen an das Kraftfahrtbundesamt, weil die Bestimmungen einen zusätzlichen Meldeweg bedeutet hätten. Darüber hinaus sind bei weiteren Mitteilungen Ausnahmen von

der Mitteilungspflicht vorgesehen oder ausgedehnt und teilweise die Adressaten der Mitteilungen konkretisiert worden.

Die MiZi wurde darüber hinaus mit Wirkung zum 1. September 1999 erneut geändert, indem u. a. ein neuer Unterabschnitt Mitteilungen betreffend Angehörige rechtsberatender Berufe eingefügt wurde. Die vorgesehene Mitteilung an die Kammern zu Forderungsklagen gegen Angehörige rechtsberatender Berufe und den dazu ergangenen Entscheidungen oder geschlossenen Vergleichen habe ich unter dem Gesichtspunkt der Erforderlichkeit nicht für notwendig angesehen. Nicht jede Forderung, der sich Angehörige rechtsberatender Berufe ausgesetzt sehen, begründet schon den Verdacht, dass Vermögensverfall oder zumindest eine angespannte finanzielle Lage vorliegen muss. Die entsprechende Vorschrift wurde dahingehend ergänzt, dass sie hinsichtlich des Zwecks der Mitteilung konkretisiert wurde. Auch weiteren aus dem Kreis der Datenschutzbeauftragten geäußerten Bedenken wurden durch entsprechende Änderungen weitgehend Rechnung getragen.

10.3 Thüringer Gesetz zur Ausführung der Insolvenzordnung (ThürAGInsO)

Mit dem Thüringer Gesetz zur Ausführung der Insolvenzordnung wurde von der eingeräumten Kompetenz Gebrauch gemacht, zu bestimmen, welche Personen oder Stellen als geeignet für die Ausstellung der mit dem Antrag auf Eröffnung des Verbraucherinsolvenzverfahrens vorzulegenden Bescheinigungen über den erfolglosen Versuch einer außergerichtlichen Schuldenbereinigung mit den Gläubigern anzusehen sind. Durch das Gesetz kann die Beratung und Vertretung in Verbraucherinsolvenzverfahren künftig in nicht geringem Umfang auch von nicht-öffentlichen Stellen wahrgenommen werden. Da aber für nicht-öffentliche Stellen das Thüringer Datenschutzgesetz nicht anwendbar ist, kommt das Bundesdatenschutzgesetz zur Anwendung. Der Schutz der personenbezogenen Daten des Bundesdatenschutzgesetzes bezieht sich jedoch nur auf Dateien, sodass im Gesetzgebungsverfahren aus meiner Sicht sichergestellt werden musste, dass auch Daten, die nicht in oder aus Dateien verarbeitet werden, ebenfalls unter datenschutzrechtliche Vorschriften fallen. Es ist nämlich zu erwarten, dass personenbezo-

gene Daten durch die nicht-öffentlichen Stellen auch in Akten verarbeitet werden. Ich hatte daher die Einfügung eines Datenschutzparagraphen vorgeschlagen. Der daraufhin eingefügte § 6 „Datenschutz“ spricht zwar nur von „geeigneten Stellen nach § 1“, die geeigneten Personen nach § 5 des ThürAGInsO wurden nicht erwähnt. Zur Vermeidung etwaiger Auslegungsschwierigkeiten habe ich darauf hingewiesen, dass nach § 2 Abs. 4 BDSG auch natürliche Personen als nicht-öffentliche Stellen anzusehen sind. Auch wenn dies ausdrücklich nicht in dem Thüringer Gesetz zur Ausführung der Insolvenzordnung zum Ausdruck kommt. Zwischenzeitlich liegen auch die „Grundsätze für die Anerkennung von geeigneten Stellen im Verbraucherinsolvenzverfahren auf der Grundlage des ThürAGInsO“ des TMSG vor.

In § 7 ThürAGInsO ist vorgesehen, dass durch das Landesamt für Soziales und Familie den Beratungsstellen nach Maßgabe des Haushaltsplans auf Antrag Zuwendungen zu den anerkannten Personalkosten und den notwendigen Sachkosten gewährt werden. Näheres hierzu ist in der Richtlinie zur Förderung von Schuldner- und Verbraucherinsolvenzberatungsstellen im Freistaat Thüringen vom 19.02.1999 (ThürStAnz, S. 755) geregelt. In Nr. 7 der Richtlinie wird bestimmt, dass der Verwendungsnachweis aus einem zahlenmäßigen Nachweis der geförderten Personalkosten laut Formblatt und einem Tätigkeitsbericht der geförderten Beratungsstelle besteht. Auf meine Anfrage hin hat mir das Landesamt für Soziales und Familie bestätigt, dass im Verwendungsnachweis der geförderten Schuldnerberatungsstellen keine personenbezogenen Angaben der beratenen Schuldner oder deren Gläubiger erforderlich sind. Der Tätigkeitsbericht umfasst lediglich eine Statistik über die erfolgten Beratungen, die keine personenbezogene Daten der beratenen Schuldner oder deren Gläubiger enthält.

10.4 Akustische Wohnraumüberwachung und parlamentarische Kontrolle

Mit der Änderung von Art. 13 GG mit dem Gesetz zur Änderung des Grundgesetzes vom 26. März 1998 (BGBl. I S. 610), das am 1. April 1998 in Kraft getreten ist, sind die verfassungsrechtlichen Grundlagen für die akustische Wohnraumüberwachung (2. TB 10.8)

geschaffen worden. Nach Art. 13 Abs. 3 GG dürfen zur Strafverfolgung aufgrund richterlicher Anordnung technische Mittel zur akustischen Überwachung von Wohnungen, in denen der Beschuldigte sich vermutlich aufhält, eingesetzt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine durch Gesetz bestimmte besonders schwere Straftat begangen hat und die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre. Die befristete Anordnung hat durch einen mit drei Richtern besetzten Spruchkörper zu erfolgen. Bei Gefahr im Verzug kann sie auch durch einen einzelnen Richter getroffen werden. Insoweit ist dadurch teilweise den Forderungen der Datenschutzbeauftragten nachgekommen worden. Nach Art. 13 Abs. 4 GG ist der Einsatz technischer Mittel zur Überwachung von Wohnungen zur Gefahrenabwehr aufgrund richterlicher Anordnung bzw. bei Gefahr im Verzug durch eine andere gesetzlich bestimmte Stelle geregelt worden. Durch Art. 13 Abs. 5 GG findet auch der Einsatz technischer Mittel zum Schutz der bei einem Einsatz in Wohnungen tätigen Personen Berücksichtigung, der nicht von einer richterlichen Entscheidung abhängig ist, sondern von einer gesetzlich bestimmten Stelle angeordnet werden kann. Nach Art. 13 Abs. 6 GG ist eine jährliche Berichtspflicht der Bundesregierung über den genannten erfolgten Einsatz technischer Mittel eingeführt worden. Auf der Grundlage dieses Berichts übt ein vom Bundestag gewähltes Gremium die parlamentarische Kontrolle aus. Darüber hinaus haben die Länder eine gleichwertige parlamentarische Kontrolle zu gewährleisten.

Mit dem „Gesetz zur Verbesserung der Bekämpfung der organisierten Kriminalität“ vom 4. Mai 1998 (BGBl. I S. 845) liegt auch das zur Umsetzung erforderliche Ausführungsgesetz im Bereich der Strafverfolgung vor. In diesem Rahmen ist weitgehend den weiteren datenschutzrechtlichen Forderungen nachgekommen worden. Nach dem neugefassten § 100 c StPO darf das in einer Wohnung nicht-öffentlich gesprochene Wort des Beschuldigten abgehört und aufgezeichnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass er eine dort katalogmäßig aufgeführte Straftat begangen hat. Die in § 100 c Abs. 1 Nr. 3 StPO aufgeführten Katalogstraftaten umfassen neben Mord, Totschlag und Entführung beispielsweise auch Geldfälschung, Fälschung von Zahlungskarten und Vordrucken

für Euroschecks, Bandendiebstahl, schweren Raub, gewerbsmäßige Hehlerei, Geldwäsche, Bestechung und Bestechlichkeit. Der Einsatz technischer Mittel zur Überwachung ist nicht auf Wohnungen von Beschuldigten beschränkt, sondern darf auch in Wohnungen anderer Personen durchgeführt werden, wenn Tatsachen die Annahme rechtfertigen, dass der Beschuldigte sich in diesen Räumlichkeiten aufhält und die Maßnahme zur Erreichung des Strafverfolgungszwecks dringend geboten erscheint. Ausgenommen sind Wohnungen von Personen, denen ein Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht. Akustische Wohnraumüberwachung ist auch nicht gestattet, wenn zu erwarten ist, dass sämtliche aus der Maßnahme zu gewinnende Erkenntnisse einem Verwertungsverbot unterliegen, was bei Zeugnisverweigerungsberechtigten aus persönlichen Gründen und bei Berufshelfern zutrifft, wenn die Verwertung der Erkenntnisse unangemessen wäre. Dies dürfte allerdings überwiegend erst nach Durchführung des Eingriffs feststellbar sein.

Nach § 100 e Abs. 1 StPO in Umsetzung des Art. 13 Abs. 6 GG berichtet die Staatsanwaltschaft der jeweils zuständigen obersten Justizbehörde spätestens drei Monate nach Beendigung einer Maßnahme über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahme sowie über die erfolgte Benachrichtigung der Beteiligten oder die Gründe, aus denen die Benachrichtigung bislang unterblieben ist und den Zeitpunkt, in dem die Benachrichtigung voraussichtlich erfolgen kann. Nach Abs. 2 unterrichtet die Bundesregierung den Bundestag auf der Grundlage von Ländermitteilungen jährlich über die durchgeführten Maßnahmen der akustischen Wohnraumüberwachung. Dieses Verfahren zur parlamentarischen Kontrolle der weit reichenden Eingriffe in das Grundrecht auf Unverletzlichkeit der Wohnung dient nach dem Willen des Gesetzgebers der parlamentarischen Kontrolle der Normeffizienz (Evaluierung) und hebt sogleich die politische Kontrollfunktion der Parlamente gegenüber der Exekutive hervor. Es ersetzt zwar nicht die Überprüfung von Lauschangriffen durch die Gerichte und Datenschutzbeauftragten, hat aber gleichwohl eine grundrechtsichernde Bedeutung.

Zu Art. 13 Abs. 6 Satz 3 GG, der bestimmt, dass die Länder eine gleichwertige parlamentarische Kontrolle gewährleisten, haben einige Landesjustizverwaltungen, so auch das TMJE die Ansicht ver-

treten, Art. 13 Abs. 6 GG sehe eine Berichtspflicht über Lauschangriffe zu Strafverfolgungszwecken gegenüber den Landesparlamenten nicht vor. Dies hat die Datenschutzbeauftragten des Bundes und der Länder veranlasst, mit der Entschließung vom 17. Juni 1999 zu „Parlamentarische Kontrolle von Lauschangriffen in den Bundesländern“ (Anlage 13) Stellung zu beziehen. Sie vertreten die Auffassung, dass die Verfassung eine effektive parlamentarische Kontrolle von Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muss. Dazu gehört auch, dass große Lauschangriffe, die als repressive Maßnahmen zur Strafverfolgung durch Landesbehörden angeordnet werden, von einer parlamentarischen Kontrolle umfasst sind. Insoweit sollte deshalb durch Gesetz eine regelmäßige Berichtspflicht der Landesregierung für präventiv-polizeiliche (Gefahrenabwehr) und repressive (Strafverfolgung) Lauschangriffe gegenüber den Landesparlamenten vorgesehen werden.

Die neuen verfassungsrechtlichen Vorgaben machten auch eine Änderung des Landesrechts erforderlich. Das entsprechende Thüringer Gesetz zur Umsetzung des Artikel 13 des Grundgesetzes vom 27. Juli 1999 ist zwischenzeitlich in Kraft getreten (GVBl. S. 454). Durch Anpassungen des Polizeiaufgabengesetzes (PAG) und des Verfassungsschutzgesetzes (ThürVSG) wurden die vorgeschriebenen Richtervorbehalte zur Anordnung von Maßnahmen der akustischen Wohnraumüberwachungen umgesetzt. Als anordnenden Stellen bei Gefahr im Verzug (Art. 13 Abs. 4 GG) und beim Einsatz von Personenschutzsendern (Art. 13 Abs. 5 GG) wurde der Leiter der Polizeidirektion oder der Präsident des Landeskriminalamtes für den Bereich des PAG bzw. der Präsident des Landesamts für Verfassungsschutz oder die ihm nachgeordneten Abteilungsleiter für den Bereich des Verfassungsschutzgesetzes bestimmt. In eilbedürftigen Fällen des Einsatzes von Personenschutzsendern kann die Anordnungskompetenz auch auf einen bestellten Beauftragten der Polizeidirektion übertragen werden. Darüber hinaus wurde die parlamentarische Kontrolle des Einsatzes akustischer Wohnraumüberwachungen zum Zweck der Gefahrenabwehr in beiden Gesetzen aufgenommen. Hinsichtlich der im Gesetzentwurf eines Thüringer Gesetzes zur Umsetzung von Art. 13 GG (Drucksache 2/3712) vorgesehenen, auf den präventiven Bereich beschränkten parlamentarischen

Kontrolle hatte ich gegenüber der Landesregierung und im Parlament Stellung genommen und die Auffassung vertreten, dass Art. 13 Abs. 6 Satz 3 GG von den Ländern verlangt, eine gleichwertige parlamentarische Kontrolle wie im Bund zu gewährleisten, was demzufolge sowohl den präventiven als auch den repressiven Bereich betrifft. Meinem Vorschlag, eine Berichtspflicht der Landesregierung an den Landtag entsprechend § 100 Abs. 1 StPO über die durchgeführten Maßnahmen nach § 100 c Abs. 1 Nr. 3 StPO neben der Berichtspflicht an den Bundestag festzuschreiben, ist jedoch im Gesetzgebungsverfahren nicht gefolgt worden. Die parlamentarische Kontrolle nach Art. 13 Abs. 6 Satz 3 GG ist der Parlamentarischen Kontrollkommission übertragen worden.

10.5 Überwachung der Telekommunikation - Entwicklungen im Sicherheitsbereich - Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten

Im 2. TB (10.13) hatte ich über die Einführung von Berichtspflichten bei der Überwachung des Fernmeldeverkehrs im Freistaat Thüringen per Erlass des TMJE im Februar 1996 informiert. Nach den Übersichten für die Jahre 1997 und 1998 war zunächst 1997 ein Anstieg der Verfahren, in denen Maßnahmen nach §§ 100 a, 100 b StPO angeordnet wurden, um mehr als das Doppelte in Bezug auf 1996 zu verzeichnen. Auch die Anzahl der Betroffenen in dem Zeitraum war gestiegen. Dem gegenüber ist die Anzahl der Verfahren und der Betroffenen im Jahr 1998 geringfügig zurückgegangen. Es sollte dennoch darüber nachgedacht werden, eine gesetzliche Berichtspflicht ähnlich der bei der akustischen Wohnraumüberwachung (§ 100 e StPO) über Anlass, Verlauf, Ergebnis, Anzahl der Betroffenen und Kosten einzuführen, um sicherzustellen, dass Telefonüberwachungen nur durchgeführt werden, wenn sie sinnvoll sind und nicht zur Standardmaßnahme werden.

Die 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat aufgrund des Umstands, dass die Sicherheitsbehörden in der vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben, in einer Entschließung darauf hingewiesen, dass in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente fehlen

(Anlage 7). Die Datenschutzbeauftragten des Bundes und der Länder haben gegenüber dem Bundesgesetzgeber und der Bundesregierung die Erwartung zum Ausdruck gebracht, dass die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung). Auf meine Bitte um Meinungsäußerung zu der geforderten Evaluierung hat das TMJE Bedenken geäußert, da nahezu alle Eingriffsbefugnisse - ausgenommen bei Gefahr im Verzug - dem Richtervorbehalt unterliegen und die geforderte Evaluierung letztlich zu einer Kontrolle der richterlichen Tätigkeit führen würde, die mit den eindeutigen verfassungsrechtlichen Vorgaben im Hinblick auf die Unabhängigkeit der Gerichte nicht im Einklang stehen könne. Darüber hinaus ließe sich allein aus der Angabe der Anzahl der durchgeführten Maßnahmen noch kein Schluss auf die Erforderlichkeit und Wirksamkeit ziehen. Das Bundesministerium der Justiz hat zwischenzeitlich die Ausschreibung eines Forschungsvorhabens zum Thema „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO“ mit Datum vom 20. August 1999 veranlasst (Bundesanzeiger Nr. 163, Seite 15203). Durch die Untersuchung sollen empirisch gesicherte Erkenntnisse als Grundlage der Bewertung der Notwendigkeit und der Erfolgseignung der Ermittlungsmaßnahme gewonnen werden, was als erster Schritt zur Evaluierung dieser Eingriffsbefugnisse angesehen werden kann.

Bei der Überwachung der Telekommunikation geht es nicht nur um das gesprochene Wort, was landläufig unter der Telefonüberwachung verstanden wird. Immer mehr Bedeutung gewinnt auch der Zugriff auf Verbindungsdaten (angerufene Teilnehmer, Zeitpunkt und Dauer eines Gesprächs), die von Telekommunikationsanbietern vorzuhalten sind, um die Telekommunikationsüberwachung zu ermöglichen. § 12 des Gesetzes über Fernmeldeanlagen (FAG) erlaubt auch Zugriffe auf Verbindungsdaten in der Telekommunikation wegen unbedeutender Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation nach § 100 a StPO unzulässig wäre. Seine zeitliche Geltungsdauer war ursprünglich bis zum 31. Dezember 1997 befristet, jedoch durch das Begleitgesetz zum Telekommunikationsgesetz vom 17. Dezember 1997 bis 31. Dezember 1999 verlängert worden. Unter Berücksichtigung der fortgeschrittenen Digitaltechnik, der vollständigen Datenerfassung

und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen. § 12 FAG stammt aus dem Jahr 1920, als nur ein Bruchteil der Daten anfiel, auf welche jetzt auch infolge der Digitalisierung zugegriffen werden kann. Zudem legen die Gerichte die Vorschrift noch extensiv aus, indem sie teilweise sogar den Zugriff auf zukünftige Verbindungsdaten als gedeckt sehen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich daher mit der Entschließung der 58. Konferenz vom 07./08. Oktober 1999 (Anlage 17) entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG gewandt und statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der Grundrechte der Bürgerinnen und Bürger insbesondere des Rechts auf informationelle Selbstbestimmung gefordert. Mit dem Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des Gesetzes über Fernmeldeanlagen vom 20. Dezember 1999 (BGBl. I S. 2491) wurde die Verlängerung der Geltungsdauer des § 12 FAG bis 31. Dezember 2001 beschlossen.

10.6 Einsatz von Lügendetektoren im Strafverfahren

Durch aktuelle Entscheidungen des Bundesverfassungsgerichts und ein Verfahren vor dem Bundesgerichtshof hat die Frage der Zulässigkeit des Einsatzes von Polygraphen - von sog. Lügendetektoren - im Berichtszeitraum in der Presse viel Beachtung hervorgerufen. Der Einsatz eines Polygraphen greift intensiv in das Persönlichkeitsrecht des Betroffenen ein. Er misst und hält vegetative Erregungszustände fest, auf die der Betroffene keinen Einfluss hat. Das Prinzip des Polygraphen beruht auf der Messung unwillkürlicher körperlicher Reaktionen, die vom vegetativen Nervensystem ausgehen und daher willentlich nicht beeinflussbar sind. So wird der Blutdruck, die Bewegungen des Brustkorbs (Atmung), die Leitfähigkeit der Haut für elektrische Ströme (Aktivität der Schweißdrüsen) sowie die Verteilung des Blutes im Körper als Zeichen für Anspannung gemessen. Der Einsatz des Polygraphen ist Teil einer mehrstündigen Untersuchung, wobei die meiste Zeit vorbereitende Gespräche stattfinden.

Entscheidend ist, dass der betroffene Beschuldigte oder Verdächtige dem Einsatz des Lügendetektors zustimmt, denn ohne seine Einwilligung ist die Durchführung nicht möglich, da das Messergebnis unbrauchbar wäre.

Die Datenschutzbeauftragten des Bundes und der Länder erhielten die Gelegenheit, einer Demonstration des Polygraphen im Arbeitskreis Justiz. In der mit Spannung erwarteten Entscheidung hat der BGH am 17. Dezember 1998 (1 StR 156, 258/98) die polygraphische Untersuchungsmethode im strafgerichtlichen Verfahren als Beweismittel generell ausgeschlossen. Die Bundesrichter waren der Auffassung, dass bei einer freiwilligen Mitwirkung des Beschuldigten an der Durchführung eines solchen Verfahrens zwar kein Verstoß gegen die Menschenwürde und damit auch nicht gegen die informationelle Selbstbestimmung vorliege, sich die Ergebnisse eines Polygraphenverfahrens aber als beweisuntauglich erweisen, da es nach wissenschaftlicher Auffassung nicht möglich sei, eindeutige Zusammenhänge zwischen emotionalen Zuständen eines Menschen und hierfür spezifischen Reaktionsmustern im vegetativen Nervensystem zu erkennen.

10.7 Kontrollkompetenz des TLfD bei Gerichten

Im 2. TB (10.12) hatte ich dargelegt, dass das TMJE seinerzeit die Auffassung vertrat, meine Kontrollkompetenz könne sich nicht auf die gesamte zur Unterstützung der rechtspflegerischen Tätigkeit eingesetzten EDV beziehen. Ob beim Einsatz von automatisierten Verfahren, mittels derer auch Verwaltungstätigkeiten erledigt werden können, die Datensicherungsmaßnahmen gänzlich meiner Kontrolle entzogen werden, sobald auch Rechtspfleger oder Richter Zugriffe erhalten oder mit diesen in Verwaltungangelegenheiten eingesetzten Verfahren auch ein der Rechtspflegertätigkeit zuzuordnender Bereich erledigt werden könnte, ist nach wie vor umstritten. Auch ein mit dem TMJE im Berichtszeitraum geführtes Gespräch hat zu keiner befriedigenden Lösung geführt.

Mit der Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 zur Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

(Anlage 3) war die Forderung aufgegriffen worden, dass sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u. a. auch darauf erstreckt, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung. Daher wäre eine gesetzliche Klarstellung hilfreich, dass Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden. Damit wäre meines Erachtens geklärt, dass auch automatisierte Verfahren hinsichtlich der Datensicherheit der Kontrolle des TLfD unterliegen, auch wenn mit diesen Verfahren Tätigkeiten, die zweifellos der richterlichen Unabhängigkeit zuzuordnen sind, erledigt werden können. Dass die Bereiche, die der richterlichen Unabhängigkeit unterliegen, von der Kontrolle ausgenommen sind, ist selbstverständlich. Die Kontrolle der gesamten automatisierten Verfahren hinsichtlich der Datensicherheit wäre damit allerdings gewährleistet.

Seitens des TMJE wird hierzu jedoch die Auffassung vertreten, eine Gesetzesänderung im Sinne der zitierten Entschließung der 56. Konferenz der Datenschutzbeauftragten würde zur Klärung der Abgrenzungsfragen nichts beitragen können. Infolge dessen wird auch eine entsprechende Änderung des Thüringer Datenschutzgesetzes seitens des TMJE nicht unterstützt werden.

10.8 DNA-Analyse - Genetischer Fingerabdruck

Am 11. September 1998 ist das DNA-Identitätsfeststellungsgesetz in Kraft getreten (BGBl. I S. 2646). Nach dem damit eingefügten § 81 g Abs. 1 StPO dürfen einem Beschuldigten, der einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung verdächtig ist, Körperzellen entnommen und zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersucht werden, wenn Grund zur Annahme besteht, dass der Betroffene rückfällig werden wird. Nach § 2 DNA-Identitätsfeststellungsgesetz dürfen diese Maßnahmen auch durchgeführt werden, wenn der Betroffene wegen einer der in § 81 g Abs. 1 StPO ge-

nannten Straftaten rechtskräftig verurteilt oder nur wegen erwiesener oder nicht auszuschließender Schuldunfähigkeit, auf Geisteskrankheit beruhender Verhandlungsunfähigkeit oder fehlender oder nicht ausschliessbar fehlender Verantwortlichkeit nicht verurteilt worden ist und die entsprechende Eintragung im Bundeszentralregister oder Erziehungsregister noch nicht getilgt ist. § 81 f StPO, auf den § 81 g Abs. 3 StPO verweist, setzt hierfür die richterliche Anordnung zur Durchführung der Untersuchung voraus.

Auf meine Nachfrage hat mir das TIM mitgeteilt, dass im Ergebnis der Beratungen einer interministeriellen Arbeitsgruppe (TIM, TMJE, Generalstaatsanwaltschaft) für den Freistaat Thüringen verbindlich festgelegt wurde, dass bezüglich der Untersuchungsmaßnahme selbst in jedem Fall eine richterliche Anordnung erforderlich ist. Auf diese könne auch bei Einverständnis des Betroffenen nicht verzichtet werden. Eine etwaige Freiwilligkeit macht lediglich die richterliche Anordnung bezüglich der Entnahme des Probenmaterials selbst entbehrlich, nicht jedoch bezüglich der anschließenden Untersuchung des Materials. Gegen diese Vorgehensweise bestehen keine datenschutzrechtlichen Bedenken.

In Umsetzung des DNA-Identitätsfeststellungsgesetzes ist in der Dienstanweisung KAN (Kriminalaktennachweis) des Freistaats Thüringen festgelegt, dass die Fundstellen der über eine Person vorhandenen Kriminalakten nachgewiesen werden. In der Datei KAN-Bund des polizeilichen Informationssystems INPOL wird ein so genannter DNA-Merker gesetzt, sodass bei Aufruf einer bereits erfassten Person festgestellt werden kann, ob bereits eine DNA-Analyse vorliegt, um erneute Entnahmen von Proben und mehrfache molekulargenetische Untersuchungen zu vermeiden. Da eine allgemeine Recherche zu DNA-Merkern nicht möglich ist und in der Datei KAN-Bund nur Beschuldigte zu Straftaten von erheblicher Bedeutung eingestellt werden, wie mir das TIM mitgeteilt hat, habe ich dagegen keine datenschutzrechtlichen Bedenken.

10.9 Täter-Opfer-Ausgleich und Datenschutz

Nachdem der Bundesrat in seiner Stellungnahme zum Entwurf des StVAG 96 die Prüfung der Erforderlichkeit einer entsprechenden

gesetzlichen Grundlage zur Durchführung des Täter-Opfer-Ausgleichs angeregt hatte (2. TB 10.14), wurde dem Bundesrat ein Gesetzentwurf der Bundesregierung (Bundesratsdrucksache 325/99 vom 28. Mai 1999) vorgelegt. Zu diesem Gesetzentwurf haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer 58. Konferenz mit der Entschließung zu „Täter-Opfer-Ausgleich und Datenschutz“ (Anlage 20) Stellung genommen und Forderungen aufgestellt. Kernstück der datenschutzrechtlichen Überlegungen war die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben. Der Gesetzentwurf sah nämlich vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das hätte aber auch bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Auf meine Bitte um Mitteilung, inwieweit das datenschutzrechtliche Anliegen unterstützt werden kann, hatte mir das TJM zugesagt, im weiteren Gesetzgebungsverfahren auf die in der Entschließung zum Ausdruck gebrachte Rechtsauffassung hinzuweisen.

In dem zwischenzeitlich beschlossenen „Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des Gesetzes über Fernmeldeanlagen“ vom 20. Dezember 1999 (BGBl. I S. 2491) hat dies dazu geführt, dass nunmehr gegen den ausdrücklichen Willen des Verletzten eine Eignung des Verfahrens für einen möglichen Täter-Opfer-Ausgleich nicht angenommen werden darf.

10.10 Fußfessel - Elektronisch überwachter Hausarrest

Nachdem die Justizminister auf Ihrer Konferenz am 7. - 9. Juni 1999 beschlossen haben, den elektronisch überwachten Hausarrest für bestimmte Gruppen von Strafgefangenen als Modellversuch einzuführen, haben sich die Datenschutzbeauftragten des Bundes und der Länder mit der datenschutzrechtlichen Problematik befasst. Zunächst ist eine Gesetzesänderung notwendig, weil bislang nur Geldstrafen oder Freiheitsstrafen im Bereich des Erwachsenenstrafrechts verhängt werden können. Eine solche Gesetzesänderung liegt in Form

des Gesetzentwurfs des Bundesrates vor, wobei die rechtlich zu schaffende Möglichkeit zur Durchführung eines elektronisch überwachten Hausarrestes auf vier Jahre befristet sein soll. Danach sollen im Rahmen von Modellversuchen in Baden-Württemberg, Hamburg und Hessen Erfahrungen gesammelt werden. Datenschutzrechtlich problematisch sind folgende Punkte:

Der Straftäter könnte zum bloßen Objekt technischer Überwachung werden. Es bedarf einer zusätzlichen Überwachung in Form von Blut- und Urinkontrollen, die gesetzlich zugelassen und hinsichtlich der Zweckbindung bestimmt werden müsste. Familienangehörige der mit Fußfessel an das Haus gebundenen Personen müssten eine Einwilligung erteilen, denn auch für diese sind Einschnitte in das informationelle Selbstbestimmungsrecht zu erwarten.

Da Thüringen an dem Modellversuch nicht teilnehmen wird, wie aus der Antwort des Thüringer Justizministers auf eine mündliche Anfrage im Thüringer Landtag im Juli 1999 entnommen werden konnte, bleibt abzuwarten, welche Erkenntnisse sich aus den in den anderen Ländern stattfindenden Modellversuchen zur Lösung der datenschutzrechtlichen Problematik ergeben.

10.11 Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Schon im 1. TB (10.1) habe ich darauf hingewiesen, dass in den bis dahin bekannt gewordenen Entwürfen zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln bezüglich der Aufbewahrung von Akten und der Speicherung personenbezogener Daten in Dateien enthalten waren und die Datenschutzbeauftragten Forderungen nach konkreten gesetzlichen Regelungen in diesem Bereich erhoben hatten (1. TB Anlage 16). Zwischenzeitlich hat auch die Rechtsprechung festgestellt, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf (OLG Hamm mit Beschluss vom 17. September 1998) und der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei

(Beschluss des OLG Frankfurt am Main vom 16. August 1998). Dies haben die Datenschutzbeauftragten des Bundes und der Länder zum Anlass genommen, mit der Entschließung der 58. Konferenz zum Thema „Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften“ (Anlage 21) nochmals darauf hinzuweisen, dass sie es für dringend geboten halten, unverzüglich mit der Umsetzung dieser Aufgabe zu beginnen.

10.12 Weitergabe personenbezogener Daten an gemeinnützige Einrichtungen

Die Diskussion um die datenschutzrechtliche Problematik der Datenübermittlung im Zusammenhang mit der Entrichtung von Geldern an gemeinnützige Einrichtungen durch Beschuldigte bzw. Angeklagte (1. TB 10.7; 2. TB 10.15) hielt weiter an. Im Anschluss an den 2. TB war ich zunächst davon ausgegangen, dass die dort dargestellte Vorgehensweise zwischenzeitlich auch umgesetzt wurde. Im Oktober 1998 trat das TMJE an mich heran, um gesprächsweise neue Lösungsansätze zu erörtern. Dort bestand die Befürchtung, dass durch die angekündigte Wahlmöglichkeit, entweder an die Staatskasse zu deren Gunsten oder verbunden mit der Einwilligung zur Übermittlung der personenbezogenen Daten an gemeinnützige Einrichtungen zu bezahlen, den gemeinnützigen Einrichtungen ein nicht unerheblicher Teil der Zuwendung verloren gehen würde, weil sich die Betroffenen vorrangig für die erste Alternative entscheiden könnten. Ein konkreter Vorschlag seitens des TMJE steht allerdings immer noch aus.

10.13 Personendatenverwechslung - gleicher Name, gleicher Geburtstag

Ein Bürger hatte sich beim BfD darüber beschwert, dass er von Thüringer Justizbehörden im Rahmen von Strafverfahren mehrfach zur Zahlung von Strafen aufgefordert und zu Gerichtsverhandlungen geladen wurde. Als Grund dafür musste der Betroffene feststellen, dass er seinen Namen und seinen Geburtstag mit einem anderen teilt. Dies konnte er zunächst gegenüber einem Amtsgericht und einer Staatsanwaltschaft aufklären, zumal er einen anderen Geburtsort als der Gesuchte aufweisen konnte. Nach einem Umzug sah er sich

jedoch erneut einer identischen Zahlungsaufforderung ausgesetzt. Nachdem ich zuständigkeitshalber die Angelegenheit übernommen hatte, erhielt der Betroffene auch noch Zahlungsaufforderungen von Finanzämtern wegen Steuerrückständen. Im Rahmen der datenschutzrechtlichen Prüfung im Bereich der Strafverfolgung habe ich zwei Staatsanwaltschaften kontrolliert. Danach ergab sich Folgendes:

Die gesuchte Person war im Rahmen eines Strafverfahrens unter Angabe ihres Namens, Geburtstags und Geburtsorts und der letzten bekannten Adresse von einer Staatsanwaltschaft erstmals zur Aufenthaltsermittlung im INPOL ausgeschrieben worden. Gleichzeitig erfolgte die Niederlegung eines Suchvermerks im BZR. In der Folge wurde der Beschwerdeführer vom Bundesgrenzschutz auf einem Flughafen angesprochen. Ohne zu bemerken, dass er an einem anderen Ort als der Gesuchte geboren wurde, wurde die damalige Anschrift des Beschwerdeführers als Aufenthalt der gesuchten Person an die ausschreibende Staatsanwaltschaft mitgeteilt. Da man dort davon ausging, der Gesuchte sei nunmehr gefunden, erfolgte die Löschung der Ausschreibung, der Beschwerdeführer bekam die Zahlungsaufforderung. Dies hätte jedoch vermieden werden können, wenn die vorliegenden personenbezogenen Daten seitens der Staatsanwaltschaft auf die Richtigkeit überprüft worden wären, denn dann hätte die Abweichung hinsichtlich des Geburtsorts festgestellt werden können.

Nach Überprüfung des Hinweises des Beschwerdeführers, es handle sich um eine Verwechslung, wurde eine neue Ausschreibung zur Aufenthaltsermittlung veranlasst und ein neuer Suchvermerk im BZR niedergelegt. Dabei wurde allerdings als letzte bekannte Adresse zu dem Gesuchten versehentlich die Adresse des Beschwerdeführers angegeben. Kein Wunder, dass der Beschwerdeführer wieder „gefunden“ wurde und, obwohl die Personendatenverwechslung aktenkundig war, bekam er wiederum dieselbe Zahlungsaufforderung. Mit der erneuten Fahndungsausschreibung wurde der Beschwerdeführer mit einer Straftat in Verbindung gebracht, die er unstrittig nicht begangen hat. Durch die Ausschreibung im INPOL war er als gesuchter Straftäter für alle Polizeidienststellen und andere berechnigte Stellen abrufbar. Weiterhin war er Maßnahmen ausge-

setzt, die dem Gesuchten galten. Dies stellte eine erhebliche Beeinträchtigung seiner schutzwürdigen Belange dar.

Die mangelnde Sorgfalt bei der Verarbeitung personenbezogener Daten im Zusammenhang mit der Ausschreibung zur Aufenthaltsermittlung durch die Staatsanwaltschaft habe ich daher als groben datenschutzrechtlichen Verstoß gem. § 39 Abs. 1 ThürDSG beanstandet. Um zukünftig sicherzustellen, dass derartige Mängel bei der Verarbeitung und Nutzung personenbezogener Daten gerade in einem sensiblen Bereich wie einer Staatsanwaltschaft verhindert werden, habe ich gefordert, entsprechende Hinweise an die Mitarbeiter schriftlich festzulegen. Dies ist zwischenzeitlich sowohl seitens der betroffenen Staatsanwaltschaft als auch seitens der Generalstaatsanwaltschaft erfolgt. Auch die damit befasste Polizeidienststelle hat für die Zukunft durch entsprechende Belehrungen sichergestellt, dass künftig eine aufmerksamere Kontrolle von Fahndungsmitteilungen erfolgt.

Aus den Beschwerdeschreiben beigefügten Unterlagen hatte ich aus einer Ladung zur Gerichtsverhandlung den Hinweis auf eine andere Staatsanwaltschaft entnommen, bei der ich in der Folge Einsicht in den entsprechenden Ermittlungsvorgang nahm. Auch durch diese Staatsanwaltschaft war eine Personenfahndung zur Aufenthaltsermittlung des Gesuchten im INPOL und ein Suchvermerk im BZR veranlasst worden, nachdem eine Nachfrage beim Meldeamt zu dem Gesuchten ergeben hatte, dass dieser unbekannt verzogen und daher von Amts wegen abgemeldet worden war. Daraufhin wurde der Staatsanwaltschaft von einer Polizeidienststelle und vom BZR mitgeteilt, der Gesuchte sei nach Mitteilung der eingangs erwähnten Staatsanwaltschaft unter der Adresse des Beschwerdeführers wohnhaft. Mit Beschluss des Amtsgericht erhielt der Beschwerdeführer dann eine Ladung zur Hauptverhandlung in einer Strafsache. Aufgrund der eingesehenen Unterlagen konnte nicht festgestellt werden, dass seitens dieser Staatsanwaltschaft bei der Ausschreibung des Gesuchten und bei Auffinden des Beschwerdeführers datenschutzrechtliche Vorschriften verletzt worden wären. Aus den Schreiben der Polizeidienststelle und der Mitteilung des BZR ergaben sich für die Staatsanwaltschaft keine Hinweise auf eine mögliche Verwechslung. Allerdings stellt sich in diesem Zusammenhang

die Frage, ob seitens der Staatsanwaltschaft weiterer Handlungsbedarf gegenüber dem BZR bestand, nämlich diesem mitzuteilen, dass es sich bei der Adresse des Beschwerdeführers nicht um die Adresse des Gesuchten handelt. Dies erscheint im Hinblick darauf wichtig, weil auch andere Behörden den Inhalt der Erledigterklärung zu eventuellen weiteren bestehenden Suchvermerken seitens des BZR erhalten und es dadurch erneut zu Personendatenverwechslungen kommen könnte. Eine Stellungnahme hierzu seitens der Staatsanwaltschaft steht noch aus.

Die Tatsache, dass der Beschwerdeführer in dieser Angelegenheit trotz neuer Ausschreibung zur Aufenthaltsermittlung und einer Mitteilung des BZR unter Angabe seiner Adresse nicht erneut behelligt wurde, lässt annehmen, dass es hier nicht zu erneuten Verwechslungen kommen wird.

Ein für den Gesuchten zuständiges Finanzamt hatte ebenfalls versucht, seinen aktuellen Aufenthalt zu ermitteln. Das BZR teilte ihm mit, der Gesuchte sei unter der Adresse des Beschwerdeführer nach Mitteilung der eingangs erwähnten Staatsanwaltschaft wohnhaft. Obwohl das Finanzamt den Geburtsort des Gesuchten an das BZR übermittelt hatte, war in der Antwort kein Hinweis auf einen abweichenden Geburtsort enthalten. Die Überprüfung der mitgeteilten Meldedaten durch eine Melderegisteranfrage ergab für das Finanzamt ebenfalls keine Anhaltspunkte auf Abweichungen. Daraufhin erhielt der Beschwerdeführer die Zahlungsaufforderung zur Begleichung von Steuerrückständen. Zu dieser konnte der Beschwerdeführer wiederum klären, er sei nicht der Steuerpflichtige. Kurze Zeit darauf wurde er jedoch auch von seinem für den Wohnort zuständigen Finanzamt angeschrieben. Das lag daran, weil fast gleichzeitig mit der Absendung der Zahlungsaufforderung auch eine Abgabe an dieses Finanzamt erfolgt war. Aber auch dort ist zwischenzeitlich die Verwechslung bekannt. Seitens der Steuerverwaltung wurden nach Feststellung der Verwechslung die Daten des Beschwerdeführers gelöscht und das BZR auf den Umstand der Verwechslung hingewiesen.

Im Rahmen der Prüfung der Angelegenheit erhielt ich Kenntnis von verschiedenen BZR-Auskünften, aus denen nicht eindeutig hervorging, ob Eintragungen den Gesuchten oder den gleichnamigen Be-

schwerdeführer betreffen, da das Unterscheidungsmerkmal Geburtsort nicht angegeben war. Ich habe daher zuständigkeithalber an den BfD die Bitte um Prüfung gerichtet, damit der Beschwerdeführer zukünftig nicht weiteren Maßnahmen ausgesetzt wird, die dem Gesuchten gelten.

10.14 Strafverfahren gegen Ortsbürgermeister

Aus der Presse war zu entnehmen, dass eine Anklageschrift der Staatsanwaltschaft sich bereits bei einer Stadtverwaltung befand, obwohl der Betroffene sie selbst noch nicht vorliegen hatte. Ich habe dies zum Anlass genommen, Anfragen zu der Angelegenheit an die betroffene Staatsanwaltschaft und den betroffenen Oberbürgermeister zu richten. Eine Übersendung der Anklageschrift durch die Staatsanwaltschaft an den Oberbürgermeister als zuständigem Dienstvorgesetztem war zulässigerweise im Rahmen der gesetzlichen Regelungen nach Nr. 15 der Mitteilungen im Strafverfahren (MiStra) als „vertrauliche Personalsache“ erfolgt. Die Übermittlung personenbezogener Daten nach Nr. 15 MiStra erfolgen zu dem Zweck, die Einleitung möglicher dienstrechtlicher Maßnahmen durch die hierfür zuständigen Personen zu ermöglichen. Der Oberbürgermeister hat mir mitgeteilt, die Unterlagen seien vertraulich behandelt worden und nur den zuständigen mit der Angelegenheit befassten Beigeordneten zur Kenntnis gelangt.

Auch wenn übermittelte Unterlagen keinen Eingang in Personalakten finden und damit keine Personalaktendaten im herkömmlichen Sinne darstellen, handelt es sich um sensible personenbezogene Daten, die besonders gegen den Zugriff Unbefugter zu schützen sind. Anhaltspunkte dafür, dass dem nicht nachgekommen wurde, ergaben sich aus den Darlegungen des Oberbürgermeisters nicht. Für solche Fälle habe ich dem Oberbürgermeister jedoch darüber hinaus angeraten, vertrauliche Personaldaten nur dann zu kopieren, wenn sich hierfür eine besondere Erforderlichkeit ergibt. Soweit Kopien für unerlässlich betrachtet werden, sollte deren Anzahl und Empfänger auf dem Original notiert werden. Wie diese Anklageschrift oder Angaben hieraus im Kommunalwahlkampf in die Öffentlichkeit geraten sind, war jedoch nicht feststellbar.

10.15 Aktenbearbeitung durch Staatsanwälte zu Hause

Ein Landesbeauftragter für den Datenschutz war mit der Frage konfrontiert, wie die Beachtung datenschutzrechtlicher Vorschriften gewährleistet werden kann, wenn Staatsanwälte die ihnen zur Bearbeitung übertragenen Akten in ihre Privatwohnungen verbringen. Dies gab Anlass, im Kreise der Datenschutzbeauftragten, Regelungen über besondere technische und organisatorische Maßnahmen zur Datensicherung im häuslichen Bereich zu diskutieren. Es wurde einhellig festgestellt, dass jedenfalls zumindest Regelungen auf Verwaltungsebene für dieses Problemfeld erforderlich sind. Das TMJE hat mir hierzu mitgeteilt, die Einhaltung des Datenschutzrechts unterfalle den allgemeinen Dienstpflichten der Staatsanwälte, ohne dass es hierzu einer deklaratorischen Dienstanweisung bedürfe. Im Übrigen seien Verstöße gegen datenschutzrechtliche Bestimmungen im Zusammenhang mit der Mitnahme von Akten zur häuslichen Bearbeitung im Geschäftsbereich nicht feststellbar. Hinsichtlich des Richterbereichs wurde eine entsprechende Dienstanweisung als unzulässig angesehen, da damit in den verfassungsrechtlich geschützten Kernbereich richterlicher Tätigkeit eingreifen würde.

Die Verwaltungsvorschrift des Thüringer Ministeriums für Justiz und Europaangelegenheiten vom 19. Oktober 1995 (1518/1-10) - JMBL. 1995 Seite 69 ff. - enthält als Dienstanweisung für die Benutzung von Personalcomputern zu dienstlichen Zwecken unter 8. Hinweise zur Informationsverarbeitung außerhalb der Dienststelle. Diese beschränken sich darauf, dass durch geeignete Maßnahmen sicherzustellen ist, dass die Informationen keinen Dritten zugänglich sind, wenn eine Informationsverarbeitung außerhalb der Dienststelle bzw. am Heimarbeitsplatz erfolgt. Tragbare PC könnten leichter entwendet werden, entsprechende Gegenmaßnahmen seien durch die Anwender zu treffen. Dem kann allerdings nur deklaratorischer Charakter zukommen. Andere Länder haben bereits ausführliche Vorschriften, die differenzierte Forderungen aufstellen. So ist beispielsweise die Mitnahme von dienstlichen Akten anzuzeigen, damit jederzeit festgestellt werden kann, wo sich Akten befinden. Der Einsatz von privaten DV-Anlagen und damit die Informationsverarbeitung auch im häuslichen Bereich ist entweder der Behördenleitung anzuzeigen oder von deren Genehmigung abhängig, wobei

keine Unterscheidung zwischen Richtern, Staatsanwälten und Rechtspflegern zum Tragen kommt. Hinzu kommen konkrete Bestimmungen zur Aufbewahrung von Datenträgern, die gegen unbefugte Kenntnissnahme auch durch Familienmitglieder zu sichern sind.

10.16 Einsatz von EDV-Technik im Gerichtsvollzieherbüro

Vor Erlass der Verwaltungsvorschrift des TMJE vom 23.04.1999 zum Einsatz von EDV-Technik im Gerichtsvollzieherbüro (JMBL. 1999, S. 22 f) hat mir das TMJE die Möglichkeit gegeben, zu dem Entwurf der Neufassung Stellung zu nehmen. Da die Verwaltungsvorschrift vorsah, dass grundsätzlich von den Gerichtsvollziehern bei ihrer Geschäftstätigkeit nur solche Software eingesetzt werden darf, die durch das für Justiz zuständige Ministerium für den Einsatz in Thüringen zugelassen ist, habe ich angeregt, klarzustellen, dass zur Vereinfachung hier bereits eine datenschutzrechtliche Freigabe im Sinne von § 34 Abs. 2 ThürDSG mit der Zulassung vorliegt, da eine Prüfung hinsichtlich der Datenarten und der regelmäßigen Datenübermittlungen stattgefunden hat. Dem ist das TMJE gefolgt.

Die Regelung zur Aufbewahrung von Sicherungskopien an einem sicheren Ort wurde für die Praxis dahingehend konkretisiert, dass eine Aufbewahrung in einem Stahlschrank, soweit vorhanden, erfolgen soll.

Die in 5.2 Satz 2 vorgesehene Ausnahme, dass eine Verbindung des eingesetzten EDV-Systems mit anderen EDV-Systemen oder Kommunikationsnetzen zugelassen werden kann, sollte meines Erachtens noch mal überdacht werden, da mit der Verbindung besondere Risiken hinsichtlich der Datensicherheit entstehen. Seitens des TMJE wurde jedoch daran festgehalten, um die Möglichkeit zu eröffnen, zusätzliche EDV-Systeme etwa zur Abwicklung des Zahlungsverkehrs, einsetzen zu können.

10.17 Automatisiertes Verfahren SIJUS-Straf-StA

Zu dem im 2. TB (10.11.2) genannten Themenpapier „Datenschutzrechtliche Forderungen zum Einsatz von automatisierten staatsanwaltschaftlichen Informationssystemen“ hatte mir das TMJE als

Grundlage zu einem Meinungsaustausch mitgeteilt, die datenschutzrechtlichen Aspekte seien bereits weitgehend durch das bei den Thüringer Staatsanwaltschaften eingeführte Informationssystem berücksichtigt. Die Einrichtung automatisierter Informationssysteme erfordere wegen des schnellen Zugriffs auf sensible Daten von Beschuldigten und auch Dritten besondere Sorgfalt. Gerade auch die sich aus der Anwendung von SIJUS-Straf ergebenden datenschutzrechtlichen Probleme waren Gegenstand von Erörterungen unter den Anwenderländern.

Die Bund-Länder-Kommision zur Datenverarbeitung und Rationalisierung in der Justiz (BLK) hatte bereits in ihrer 62. Sitzung am 11. und 12. November 1997 eine Arbeitsgruppe damit beauftragt, eine Bewertung der in dem Themenpapier erhobenen Forderungen zum Einsatz von automatisierten staatsanwaltschaftlichen Informationssystemen vorzubereiten. Nach einem Zwischenbericht sieht es die Arbeitsgruppe als ihre Aufgabe an, die Forderungen der Datenschutzbeauftragten zu erörtern und daraus Empfehlungen zu erarbeiten, die bei Neuentwicklungen oder im Rahmen notwendiger Anpassungen und Umstellungen bestehender Verfahren realisiert werden sollen. Eine schlüssige abschließende Bewertung sei allerdings erst möglich, wenn alle wesentlichen Forderungen der Datenschutzbeauftragten durch die Arbeitsgruppe erörtert und im Zusammenhang soweit erforderlich unter Berücksichtigung der Europäischen Datenschutzrichtlinie und der Entschlüsse der Datenschutzbeauftragten beurteilt worden sind. Die BLK hat die Arbeitsgruppe gebeten, einen entsprechenden Schlussbericht bis zur Hauptsitzung 1999 vorzulegen, eine abschließende Stellungnahme liegt mir noch nicht vor.

10.18 Angemessener Datenschutz auch für Untersuchungsgefangene

Nach langer und intensiver Begleitung durch die Datenschutzbeauftragten des Bundes und der Länder ist das Strafvollzugsgesetz durch das Vierte Gesetz zur Änderung des Strafvollzugsänderungsgesetzes vom 26. August 1998 um datenschutzrechtliche Bestimmungen ergänzt worden. Es gilt nun, auf die möglichst datenschutzgerechte Umsetzung der Neuregelung, insbesondere hinsichtlich der gesetzli-

chen Regelungen zur Löschung und Vernichtung von Aktenteilen, zu achten, wobei das Gesetz von Höchstfristen ausgeht, sodass für sensiblere Teile in Verwaltungsvorschriften kürzere Fristen festgelegt werden sollten.

Mit dem Entwurf eines Gesetzes zur Regelung des Vollzugs der Untersuchungshaft (BR-Drucksache 249/99 vom 30. April 1999) hat die Bundesregierung die seit Jahren erhobene Forderung der Datenschutzbeauftragten nach einer bereichsspezifischen gesetzlichen Regelung aufgegriffen. Mit der Stellungnahme des Bundesrats zu diesem Gesetzentwurf (BR-Drucksache 249/99 Beschluss) vom 11. Juni 1999 wurde jedoch einseitig das staatliche Vollzugsinteresse betont und damit datenschutzrechtlichen Verbesserungen teilweise der Raum genommen. Die Datenschutzbeauftragten des Bundes und der Länder haben mit der Entschließung vom 16. August 1999 „Angemessener Datenschutz auch für Untersuchungsgefangene“ (Anlage 14) insbesondere zu den Problemkreisen der inhaltlichen Überwachung von Unterhaltung mit Besuchern und Briefen sowie den ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigern und Beschuldigten, zur Datenübermittlung an öffentliche Stelle außerhalb der Vollzugsanstalt und der Einschränkung des Auskunfts- und Akteneinsichtsrechts der Gefangenen im Hinblick auf den Zweck der Untersuchungshaft Stellung genommen. Die Untersuchungshaft muss einer anderen Sichtweise unterfallen als der Vollzug von Freiheitsstrafen von bereits Verurteilten, weil für Untersuchungshäftlinge immer noch die Unschuldsvermutung gilt. Diese Entschließung hatte ich dem TMJE mit der Bitte um Unterstützung der gestellten Anforderungen an einen angemessenen Datenschutz übersandt. Das TMJE hatte hierauf mitgeteilt, es sei bei etwaigen Stellungnahmen zum in Rede stehenden Gesetzentwurf gehalten, insbesondere vollzugliche und verfahrensrechtliche Belange zu berücksichtigen. Datenschutzrechtliche Aspekte würden unterstützt, soweit sie nicht den vorgenannten Belangen entgegenstehen. Insoweit sah sich das TMJE gehindert, der geäußerten Bitte um Unterstützung bei einer starken Berücksichtigung datenschutzrechtlicher Anforderungen beim weiteren Gesetzgebungsverfahren nachzukommen.

10.19 Erhebung von Besucherdaten in einer Justizvollzugsanstalt

Ein Gefangener hatte sich darüber beschwert, dass einem Familienangehörigen zum Zweck des Besuchs in der Justizvollzugsanstalt (JVA) Daten abverlangt werden, die nicht erforderlich seien. Auf dem hierzu seitens der JVA verwandten Formular war die Erhebung des Namens, der Anschrift, des Geburtstags, des Geburtsorts, der Staatsangehörigkeit und des Berufs des Besuchers, sowie eine pauschale Einverständniserklärung dazu, dass bei zuständigen Behörden Auskünfte eingeholt und der Verwertung der hierbei erlangten Erkenntnisse zugestimmt wird, vorgesehen.

Auf meine Anfrage hat das TJM dargelegt, dass die Erklärung des Besuchers eines Gefangenen zu seinen persönlichen Daten sowie seine Einverständniserklärung zur Einholung von Auskünften über seine Person bei den zuständigen Behörden in sicherheitssensiblen Justizvollzugsanstalten erforderlich ist, damit diese Anstalten prüfen können, ob Gründe für einen Besuchsverbot gem. § 25 Strafvollzugsgesetz vorliegen. Hierzu benötigt die Anstalt die Angaben zur Person des Besuchers, die eine eindeutige Identifizierung ermöglichen und auch aus dem Personalausweis entnommen werden können, wozu der Beruf nicht zählt.

Im Ergebnis wurde das Formular geändert. Es enthält nunmehr auch den Hinweis für den Besucher, dass - soweit im Einzelfall erforderlich - bei den konkret benannten zuständigen Behörden Auskünfte eingeholt werden können, damit geprüft werden kann, ob Gefahren für die Sicherheit oder Ordnung der Anstalt bestehen und bei Personen, die nicht Angehörige des Gefangenen sind, zu befürchten ist, dass sie einen schädlichen Einfluss auf den Gefangenen oder seine Eingliederung behindern würden. Darüber hinaus wird darauf hingewiesen, welche konkreten Einkünfte eingeholt werden können. Gegen das neugefasste Formular bestehen daher keine weiteren datenschutzrechtlichen Bedenken. Die verlangten Angaben sind erforderlich und auch ausreichend, um die im Einzelfall notwendige Prüfung zu ermöglichen.

10.20 Neufassung der Dienstordnung für Notare

Seit Oktober 1998 liegt ein Diskussionsentwurf über die Neufassung der Dienstordnung für Notare (DONot) vor, die das Niedersächsische Justizministerium federführend ausgearbeitet hat. Dieser enthält nähere Bestimmungen zur Amtsführung im Allgemeinen, der Führung von Büchern, Verzeichnissen, Akten, zum Kostenregister, zur Erstellung von Übersichten, zur Abwicklung von Urkundsgeschäften und der Verwahrungsgeschäfte sowie zur Herstellung der notariellen Urkunden, Prüfung der Amtsführung, zur automationsgestützten Führung der Bücher und Verzeichnisse und datenschutzrechtliche Regelungen. Zu einer länderübergreifenden Besprechung über die Neufassung habe ich gegenüber dem TMJE zu diesem Diskussionsentwurf Stellung genommen.

Der Landesbeauftragte für den Datenschutz Niedersachsen vertrat in den länderübergreifenden Besprechungen über die Neufassung die datenschutzrechtlichen Belange aller Datenschutzbeauftragten der Länder. Im Ergebnis liegt nunmehr ein Entwurf mit Stand Juni 1999 vor, der im Gegensatz zur vorherigen Fassung auch konkrete Aufbewahrungsbestimmungen und Regelungen zur Vernichtung nicht erforderlicher Zwischenausdrücke enthält. Die mit der automationsgestützten Führung von Büchern und Verzeichnissen verbundene datenschutzrechtliche Problematik sollte gesondert in einer Arbeitsgruppe erarbeitet werden und das Ergebnis noch Ende des Jahres 1999 in die nächste Fassung der DONot einfließen.

10.21 Auskunftersuchen öffentlicher Stellen bei der SCHUFA

Ausgelöst durch an verschiedene Datenschutzbeauftragte der Länder gerichtete Anfragen der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) haben sich die Datenschutzbeauftragten mit folgender Problematik beschäftigt:

Zunehmend richten Staatsanwaltschaften und Gerichte Auskunftersuchen zur Beauskunftung sämtlicher bekannter Informationen an die SCHUFA. Bei der SCHUFA werden z. B. Kreditkarten, Bankverbindungen, Girokonten, PKW-Finanzierungsinstitute und hierzu

„Positiv-“ und „Negativmerkmale“ gespeichert. Bei einem umfassenden Auskunftersuchen besteht die Gefahr, dass neben den Informationen, die für einzelne Strafverfahren oder auch zur Entscheidung über Anträge auf Prozesskostenhilfe erforderlich sind, auch Überschussinformationen, die für die zugrundeliegenden Sachverhalte nicht relevant sind, übermittelt werden. Auf der anderen Seite erhält die SCHUFA die Information, dass jemand mit einem Strafverfahren oder ähnlichem in Verbindung gebracht wird. Auf meine Nachfrage wurde mir seitens des TMJE mitgeteilt, dass strafrechtliche Ermittlungshandlungen grundsätzlich ihre Ermächtigungen in §§ 160, 161 StPO finden. Gesonderte Regelungen hierzu lägen nicht vor. In der Praxis könne bei einer Anfrage noch nicht abgesehen werden, ob nach Erhalt der Auskunft auch Überschussinformationen erlangt werden. Erst eine spätere Gesamtschau sämtlicher Ermittlungsergebnisse unter Berücksichtigung des konkreten Tatverdachtes lasse die Beurteilung der erlangten Informationen zu. Dies war nachvollziehbar. Im Bereich des Prozesskostenhilferechts kann im Rahmen des § 118 Abs. 2 Satz 2 ZPO von einer entsprechenden Anfrage Gebrauch gemacht werden. Jedoch wurde mir versichert, dass dabei die Anforderungen des Datenschutzes berücksichtigt werden. Insgesamt wird im Einzelfall zu prüfen sein, ob seitens der öffentlichen Stelle der SCHUFA im Rahmen von Auskunftersuchen auch nur die erforderlichen Grunddaten mitgeteilt werden und ob die Auskunft entsprechend eingeschränkt werden kann.

10.22 Datenträgeraustausch aus den bei den Amtsgerichten geführten Schuldnerverzeichnissen

Den Entwurf von „Datenübertragungsregeln für Datenübermittlung und Datenträgeraustausch aus den bei den Amtsgerichten geführten Schuldnerverzeichnissen“ (gem. § 915 d ZPO) - vorgelegt von der Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung (BLK) - erhielt ich mit der Gelegenheit zur Stellungnahme seitens des TMJE zur Kenntnis.

Im beim Vollstreckungsgericht geführten Schuldnerverzeichnis werden die Daten von Betroffenen gespeichert, die eine eidesstattliche Versicherung nach § 807 ZPO oder § 248 AO abgegeben haben

oder gegen die nach § 901 ZPO die Haft angeordnet ist. Der Entwurf regelt die Übertragung von Daten entsprechend der Abdrucke aus den Schuldnerverzeichnis nach §§ 915 d und 915 e ZPO in einer nur maschinell lesbaren Form durch Datenübermittlung oder Datenträgeraustausch im Rahmen der technischen Möglichkeiten an die Stellen, die diese Abdrucke laufend aufgrund einer Bewilligung nach Maßgabe der § 2 ff. SchuVVO beziehen. Das können Kamern oder auch Antragsteller sein, die die Abdrucke zur Errichtung und Führung zentraler bundesweiter oder regionaler Schuldnerverzeichnisse verwenden sowie Antragsteller mit berechtigtem Interesse, denen durch Einzelauskünfte nicht hinreichend Rechnung getragen werden kann.

Unter dem Kapitel Datenschutz im Entwurf der Datenübertragungsregeln ist festgelegt, die Vertraulichkeit und die Integrität der zu übermittelnden Daten sei durch Verschlüsselung sicherzustellen. Allerdings können beim Datenträgeraustausch Vertraulichkeit und Integrität auch auf andere Weise gewährleistet werden. Für die Datenübermittlung ist darüber hinaus unter Berücksichtigung der landesspezifischen Regelungen und Gegebenheiten ein genormter Kommunikationsdienst zu verwenden und eine Entscheidung über das zu benutzende Netz zu treffen. Hierzu habe ich darauf hingewiesen, dass bei der Auswahl des Netzes Gesichtspunkte der Datensicherung Berücksichtigung finden sollten.

Dieser Entwurf sollte nach Abstimmung mit den Landesjustizverwaltungen durch die BLK empfohlen werden. Es war angekündigt, sobald die technischen Voraussetzungen vorliegen und ein entsprechender Bedarf vorhanden ist, diesen auch für die Justizverwaltung in Thüringen zu erlassen.

11. Gesundheits- und Sozialdatenschutz

11.1 Gesundheitsreform 2000

Im Sommer 1999 wurde von der Bundesregierung der Entwurf eines Gesetzes zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 (GKV-Gesundheitsreform 2000) vorgelegt. Darin waren auch umfangreiche Änderungen bei der Verarbeitung von Sozialdaten der Versicherten vorgesehen. Ausweislich der allgemeinen Begründung unter Ziffer 12. (Verbesserung der Datentransparenz und

Datengrundlagen zur Steuerung der GKV) sollten die „Transparenz und Datengrundlagen als entscheidende Voraussetzungen zur Steuerung des Leistungs- und Ausgabengeschehens verbessert werden durch:

- eine verbesserte Bereitstellung der steuerungsrelevanten Daten in der gesetzlichen Krankenversicherung und
- eine kassenartenübergreifende Datenzusammenführung durch Arbeitsgemeinschaften der Krankenkassen bzw. ihrer Verbände für Steuerungsaufgaben im GKV-System sowie für die Gesundheitsberichtserstattung des Bundes und der Länder“.

So war insbesondere geplant, das bisherige Abrechnungsverfahren im ambulanten Bereich, das nur ausnahmsweise den Krankenkassen versichertenbezogene Abrechnungsdaten in die Hände gibt, zu Gunsten zentraler personenbezogener Abrechnungs- und Leistungsdatenbanken im Hoheitsbereich der Krankenkassen zu verändern. Dies hätte zu einer erheblichen Verschlechterung des bisher geltenden Datenschutzniveaus in diesem Bereich und einen Schritt hin zum „gläsernen Versicherten“ geführt. Aufgrund des Protestes der Datenschutzbeauftragten des Bundes und der Länder gegen die Errichtung von Sammlungen solch sensibler Daten, der in einer Entschließung vom 25. August 1999 zum Ausdruck kam (Anlage 13), sind im weiteren Gesetzgebungsverfahren unter Mitwirkung der Datenschutzbeauftragten Veränderungen dahingehend vorgenommen worden, dass sämtliche Abrechnungsdaten aller Leistungserbringer vor deren Weiterleitung an die Kassen zu Abrechnungszwecken von den geplanten Datenannahmestellen pseudonymisiert werden sollten, sodass die Kassen im Regelfall keine versichertenbezogenen Abrechnungsdaten mehr erhalten (Anlage 16). Die vom Bundestag verabschiedete Fassung des Gesetzentwurfs wurde vom Bundesrat abgelehnt. Ein daraufhin von der Bundesregierung im Vermittlungsverfahren vorgelegtes Teilgesetz enthielt demgegenüber nur noch kleine Veränderungen der Abrechnungsvorschriften in den §§ 284 ff. SGB V, sodass es auch nach Inkrafttreten der Gesundheitsreform 2000 zum 1. Januar 2000 beim bisherigen Abrechnungsverfahren und den damit verbundenen Datenflüssen verbleibt. Meine insoweit gegenüber dem TMSG gemachten Bedenken sind daher größtenteils gegenstandslos geworden.

Veränderungen gibt es lediglich bei der ambulanten ärztlichen Versorgung. So können die Krankenkassen nach § 65 a SGB V den Versicherten einen Bonus gewähren, wenn diese sich verpflichten, vertragsärztliche Leistungen außerhalb der hausärztlichen Versorgung nur auf Überweisung des von ihnen gewählten Hausarztes in Anspruch zu nehmen. Gleiches gilt nach § 140 g SGB V für die freiwillige Teilnahme an der „integrierten Versorgung“ von mindestens einem Jahr. Darüber hinaus sieht § 73 Abs. 1 b SGB V vor, dass der gewählte Hausarzt mit schriftlicher Einwilligung des Versicherten, die dieser widerrufen kann, bei mitbehandelnden Ärzten oder Leistungserbringern Behandlungsdaten und Befunde des Versicherten zum Zweck der Dokumentation und weiteren Behandlung erheben darf. Damit korrespondiert die in § 73 Abs. 1 b Satz 2 SGB V vorgesehene Pflicht der mitbehandelnden Ärzte und Leistungserbringer, den Versicherten nach dem von ihm gewählten Hausarzt zu fragen und diesem mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, die erforderlichen Behandlungsdaten zu übermitteln. In diesem Zusammenhang ist auch die im § 140 a SGB V eingeführte „integrierte Versorgung“ zu sehen, an der der Versicherte wiederum freiwillig teilnehmen kann. Gegenüber den ursprünglich unbestimmt formulierten Zugriffsmöglichkeiten auf Befunddaten innerhalb der „integrierten Versorgung“ konnten die Datenschutzbeauftragten erreichen, dass einschränkende Zugriffsvoraussetzungen in § 140 a Abs. 2 Satz 2 SGB V aufgenommen wurden. Ein mitbehandelnder Arzt oder Leistungserbringer darf danach auf die innerhalb der integrierten Versorgung (z. B. Praxisnetz) gemeinsam geführte Dokumentation nur dann zugreifen, wenn der Versicherte ihm gegenüber seine Einwilligung erteilt hat, die Information für den konkret anstehenden Behandlungsfall genutzt werden soll und der Leistungserbringer zu dem Personenkreis gehört, der nach § 203 StGB zur Geheimhaltung verpflichtet ist. Mit diesen Regelungen will der Gesetzgeber sowohl die hausärztliche Versorgung verbessern wie auch die Zusammenschlüsse von Ärzten in sog. Praxisnetzen (integrierte Versorgung) fördern.

11.2 Erstes Gesetz zur Änderung des Medizinproduktegesetzes - versteckte Sozialdatenschutzänderung

Bereits im 2. TB (5.2.7) habe ich über die Voraussetzungen berichtet, unter denen Sozialleistungsträger nach § 68 SGB X Sozialdaten an die Polizei und Strafverfolgungsbehörden übermitteln dürfen. Dabei hatte ich die Auffassung vertreten, dass im Sozialamt unter dem Begriff der derzeitigen Anschrift auch der momentane Aufenthalt eines Sozialhilfeempfängers verstanden werden kann. In ihrer Stellungnahme zu meinem 2. TB hat die Landesregierung in diesem Zusammenhang zu Bedenken gegeben, dass im Interesse einer vertrauensvollen Zusammenarbeit zwischen Sozialämtern und den dort vorsprechenden Hilfeempfängern der Eindruck vermieden werden sollte, als ob die Sozialämter Instrumente oder gar selbst Teil der Strafverfolgung seien.

Über die von mir noch akzeptierte Interpretation des § 68 SGB X ging eine Gesetzesänderung Mitte 1998 hinaus. Ganz überraschend und ohne Beteiligung des für den Sozialdatenschutz zuständigen Sozialausschusses hatte der Bundestag im Rahmen der Beratungen zum 1. Gesetz zur Änderung des Medizinproduktegesetzes auf Vorschlag des Gesundheitsausschusses eine Änderung von § 68 SGB X beschlossen, wonach neben der derzeitigen Anschrift des Betroffenen von dem Sozialleistungsträger auf Ersuchen der Polizei auch sein derzeitiger oder zukünftiger Aufenthalt übermittelt werden darf. Damit wurde nicht nur für den Bereich der Sozialhilfe sondern für alle Sozialleistungsträger (z. B. auch Krankenkassen oder Jugendämter) eine Verschlechterung des Sozialdatenschutzes bei Anfragen von Polizei und Strafverfolgungsbehörden bewirkt. Ich habe mich daraufhin an das TMSG mit der Bitte gewandt, im Bundesratsverfahren wenigstens eine Beschränkung auf solche mutmaßlichen Straftäter vorzunehmen, die per Haftbefehl gesucht werden. Eine Änderung im Bundesratsverfahren ist aber nicht mehr erfolgt. Nach Inkrafttreten der Regelung habe ich gegenüber dem TMSG zum Ausdruck gebracht, dass die erweiterten Übermittlungsregelungen in § 68 SGB X von den Sozialleistungsträgern in der Praxis restriktiv gehandhabt werden sollten. Da eine Übermittlung nach dem Wortlaut des neuen § 68 SGB X nur auf Ersuchen im Einzelfall zulässig ist, sind meines Erachtens Regelanfragen oder die Führung von

Fahndungslisten bei den Sozialleistungsträgern nicht zulässig. Im Rahmen eines Beratungsgesprächs eines Sozialamtes zu dieser Problematik habe ich diese Auffassung ebenfalls vertreten. Es wird daher zu beobachten sein, in welcher Weise diese neuen Übermittlungsmöglichkeiten von den Sozialleistungsträgern genutzt werden.

11.3 Verordnung über die Gesundheitsuntersuchung von Asylbewerbern nach § 62 Abs. 1 AsylVfG

Nach § 62 Abs. 1 Asylverfahrensgesetz (AsylVfG) sind Ausländer, die in einer Aufnahmeeinrichtung oder Gemeinschaftsunterkunft wohnen, verpflichtet, eine ärztliche Untersuchung auf übertragbare Krankheiten zu dulden. Die oberste Landesgesundheitsbehörde hat danach den Umfang der Untersuchung und den untersuchenden Arzt zu bestimmen. Den hierzu vorgesehenen Entwurf einer Verordnung über die Gesundheitsuntersuchung von Asylbewerbern nach § 62 Abs. 1 AsylVfG hat mir das TMSG zur Stellungnahme vorgelegt. Darin war u. a. vorgesehen, dass Asylbewerbern die Gelegenheit zu einer freiwilligen Untersuchung auf AIDS und Hepatitis B zu geben ist. Vor dem Hintergrund der Vorschrift des § 62 Abs. 2 AsylVfG, wonach das Ergebnis der Gesundheitsuntersuchung der für die Unterbringung zuständigen Behörde mitzuteilen ist, hätte dies dazu geführt, dass neben der nach § 3 Abs. 1 Nr. 13 BSeuchG meldepflichtigen Hepatitis B-Erkrankung auch ein positiver AIDS-Test aus einer freiwilligen Untersuchung der Unterbringungsbehörde übermittelt worden wäre, obwohl selbst nach dem BSeuchG keine Meldepflicht besteht, sondern aufgrund der Laborberichtsverordnung lediglich eine anonymisierte Mitteilung an das Robert-Koch-Institut vorgesehen ist. Auf meine Anregung hin hat das TMSG die entsprechende Regelung dahingehend ergänzt, dass eine Mitteilung des Ergebnisses der freiwilligen Untersuchung auf AIDS nach § 62 Abs. 2 AsylVfG der vorherigen Einwilligung des Ausländers bedarf. Zu differenzieren ist aber bei einem freiwilligen Test auf Hepatitis B. Weil hier eine Meldepflicht besteht, darf auch eine Übermittlung des Ergebnisses ohne Einwilligung des Betroffenen erfolgen. Dem TMSG habe ich empfohlen, dass die untersuchenden Ärzte die Betroffenen vor der Untersuchung auf diese Übermittlungsmöglichkeit hinweisen. Die vorgenommenen Ergänzungen betreffen allerdings nur die freiwilligen Untersuchungen. Sofern sich im Rahmen

der Pflichtuntersuchung im Einzelfall Anhaltspunkte für eine AIDS- oder Hepatitis B-Erkrankung ergeben, darf das Ergebnis eines entsprechenden Tests der Unterbringungsbehörde zur Ergreifung evtl. notwendiger Maßnahmen mitgeteilt werden.

11.4 Thüringer Schiedsstellenverordnung nach § 78 g SGB VIII

Mit Wirkung zum 01.01.1999 wurden mit den §§ 78 a bis 78 g Regelungen in das SGB VIII aufgenommen, wonach zwischen den Trägern der öffentlichen Jugendhilfe und den Trägern der Einrichtung oder seinem Verband Vereinbarungen über Leistungsangebote, Entgelte und Qualitätsentwicklung der Jugendhilfe abgeschlossen werden können. Sofern es zu Streitigkeiten zwischen den Vertragspartnern kommen sollte, sieht § 78 g SGB VIII in Anlehnung an § 94 BSHG die Einrichtung einer Schiedsstelle vor. Nach § 78 g Abs. 4 SGB VIII werden die Landesregierungen ermächtigt, durch Rechtsverordnungen näheres über das Verfahren und die Geschäftsführung zu regeln. Vom TMSG wurde mir der Entwurf der entsprechenden Rechtsverordnung zur datenschutzrechtlichen Prüfung vorgelegt.

In § 13 war lediglich vorgesehen, dass sich die Schiedsstelle eine Geschäftsordnung geben kann. Obwohl im Rahmen des Schiedsverfahrens regelmäßig keine personenbezogenen Daten von Jugendlichen verarbeitet werden, können dennoch nach § 9 Abs. 3 der Verordnung Zeugen und Sachverständige hinzugezogen werden, über die nach § 9 Abs. 6 personenbezogene Aufzeichnungen im Rahmen der Niederschrift erfolgen. Zudem ist denkbar, dass im Rahmen von Streitigkeiten zu Vereinbarungen über Inhalt, Umfang und Qualität der Leistungsangebote auch beispielsweise die Qualifikation von Mitarbeitern der Einrichtungen zum Gegenstand der Beratungen werden können, was ebenfalls eine Verarbeitung personenbezogener Daten darstellen würde. Daher waren entsprechende organisatorische Maßnahmen vorzusehen, die sicherstellen, dass von diesen personenbezogenen Daten keine Unbefugten Kenntnisse erhalten können. Das betrifft sowohl die Frage, in welchem Umfang den Mitgliedern der Schiedsstellen Unterlagen mit personenbezogenem Inhalt übergeben werden wie auch die Frage, was mit diesen Unter-

lagen nach Ausscheiden der Mitglieder geschieht. Zudem sollte der Umgang mit personenbezogenen Daten in der Geschäftsstelle geregelt werden. Ich habe daher dem TMSG vorgeschlagen, in § 13 Abs. 1 die verpflichtende Erstellung einer Geschäftsordnung vorzusehen, in der diese Verfahrensregelungen beim Umgang mit personenbezogenen Daten zu regeln sind. Dem ist das Ministerium gefolgt. Die Thüringer Verordnung über die Schiedsstelle nach § 78 g SGB VIII (ThürSchiedsVO-SGB VIII) vom 28.01.1999 (GVBl. S. 206f.) ist am 28.02.1999 in Kraft getreten.

11.5 Regelung der Berufsausübung Thüringer Hebammen und Entbindungspfleger

Bislang war durch Bundesrecht nur das Berufsbild und die Ausbildung zur Hebamme und zum Entbindungspfleger geregelt. Bei der Neuregelung zur Berufsausübung in einem Thüringer Hebammengesetz vom 29. September 1998 (GVBl. S. 286) und einer Thüringer Berufsordnung für Hebammen- und Entbindungspfleger vom 24. November 1998 (GVBl. S. 417 f) habe ich mich im Gesetzgebungsverfahren beteiligt. Der Gesetzentwurf sah in § 2 Abs. 2 als Zulassungsvoraussetzung zur Aufnahme der freiberuflichen Tätigkeit u. a. vor, ein polizeiliches Führungszeugnis vorzulegen. Die Terminologie des Bundeszentralregistergesetzes (BZRG) sieht jedoch ein „polizeiliches“ Führungszeugnis nicht mehr vor. Entweder handelt es sich um ein Führungszeugnis nach § 30 Abs. 1 BZRG (sog. „Privatführungszeugnis“) oder aber einen Nachweis darüber, dass ein Führungszeugnis zur Vorlage bei einer Behörde nach § 30 Abs. 5 BZRG (sog. Behördenführungszeugnis) beantragt wurde. Dabei werden in einem Behördenführungszeugnis u. a. auch Eintragungen über Entscheidungen von Verwaltungsbehörden sowie Entscheidungen aufgenommen, bei denen der Betreffende wegen Schuldunfähigkeit nicht verurteilt wurde. In den Ausschussberatungen wurde von den Vertretern des TMSG vorgetragen, dass es sich bei dem Hebammenberuf um einen Beruf handle, der ein hohes Maß an Zuverlässigkeit erfordere, weshalb das zulassende Gesundheitsamt ein Behördenführungszeugnis benötige. Gegenüber dem federführenden Ausschuss für Arbeitsmarkt und Gesundheit habe ich daraufhin eine Änderung in § 2 Abs. 2 vorgeschlagen, die der Terminologie des BZRG angepasst ist. Danach wird mit dem Zulas-

sungsantrag eine Erklärung des Bewerbers bzw. der Bewerberin gefordert, dass ein Führungszeugnis gem. § 30 Abs. 5 BZRG zur Vorlage beim zuständigen Gesundheitsamt beantragt wurde.

Darüber hinaus hatte ich vorgeschlagen, in § 1 Abs. 3 des Gesetzes Regelungen über die Pflicht der Hebammen- bzw. des Entbindungspflegers zur Verschwiegenheit zu treffen. Das TMSG hat mir daraufhin einen bereits erstellten Entwurf einer Berufsordnung für Hebammen- und Entbindungspfleger vorgelegt, der die Verschwiegenheitspflichten der Hebammen und Entbindungspfleger nur sehr allgemein enthielt. Meinen Vorschlägen, diese Regelungen an die Vorschriften zur Schweigepflicht und zur Dokumentationspflicht der Ärzte in der ärztlichen Berufsordnung anzupassen hat das TMSG weitgehend entsprochen, sodass eine ausdrückliche Regelung im Gesetz nicht angezeigt war.

11.6 Neufassung der Berufsordnungen der Landesärzte- und Landeszahnärztekammer Thüringen

Im Nachgang zu der auf dem 100. Deutschen Ärztetag 1997 in Eisenach beschlossenen Musterberufsordnung für die deutschen Ärztinnen und Ärzte haben auch die Landesärztekammer und Landeszahnärztekammer Thüringen ihre Berufsordnungen den neueren Entwicklungen angepasst. Vom TMSG wurde mir Gelegenheit gegeben, zu den Entwürfen aus datenschutzrechtlicher Sicht Stellung zu nehmen. Hierbei waren zwei Fragestellungen von besonderem Interesse. Zum einen war es die in § 10 Abs. 2 Berufsordnung der Landesärztekammer und § 6 Abs. 4 Berufsordnung der Landeszahnärztekammer Thüringen vorgesehene Ausnahme des Einsichtsrecht des Patienten in diejenigen Teile der Krankenunterlagen, welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten. Der von mir vorgeschlagenen Beschränkung dieser Ausnahmever schrift auf solche Fälle, bei denen es nach Prüfung des Einzelfalls Anhaltspunkte dafür gibt, dass der Patient durch die Gewährung der Akteneinsicht gesundheitlichen Schaden erleiden könnte, ist wohl letztlich auch im Hinblick auf die wortgleiche Formulierung der Musterberufsordnung nicht entsprochen worden.

Der zweite Bereich betrifft die in § 10 Abs. 4 Berufsordnung der Landesärztekammer Thüringen und § 4 Abs. 5 Berufsordnung der Landeszahnärztekammer Thüringen geregelte Verfahrensweise bei der Praxisaufgabe bzw. Praxisübergabe hinsichtlich der ärztlichen Aufzeichnungen. Dort ist wie in den bisher geltenden Berufsordnungen vorgesehen, dass sich der Arzt oder Zahnarzt, dem bei einer Praxisaufgabe oder Praxisübergabe zahn-/ärztliche Aufzeichnungen über Patienten in Obhut gegeben werden, verpflichtet, diese Aufzeichnungen getrennt von den übrigen Unterlagen unter Verschluss zu halten und sie nur mit Einwilligung des Patienten einzusehen oder weiterzugeben. In diesem Zusammenhang habe ich das TMSG für den praktischen Vollzug einer Praxisübergabe oder -aufgabe darauf hingewiesen, dass die Übergabe der Patientenakte an den Praxisnachfolger in der Regel des ausdrücklichen Einverständnisses des Patienten bedarf. Andernfalls wäre das informationelle Selbstbestimmungsrecht der Patienten und die ärztliche Schweigepflicht verletzt. Zur Erlangung einer Einwilligung wird es deshalb für erforderlich angesehen, dass die Patienten vor Weitergabe ihrer Akten an den übernehmenden Arzt oder Zahnarzt in geeigneter Weise informiert werden.

Dem TMSG als zuständiger Rechtsaufsichtsbehörde habe ich mitgeteilt, dass keine Einwände gegen die vorliegenden Entwürfe der Berufsordnungen aus datenschutzrechtlicher Sicht bestehen.

11.7 Telemedizin: Das vernetzte Arzt-Patienten-Verhältnis

In den vergangenen Jahren hat auch im Gesundheitswesen der Einsatz von Informations- und Telekommunikationstechnologie zugenommen. Durch die neuen Medien haben sich vielfältige Anwendungsmöglichkeiten ergeben, die sowohl die medizinische Versorgung der Patienten verbessern helfen als auch die Kosten im Gesundheitswesen verringern können. Diesen neuen Chancen der Verbesserung der medizinischen Versorgung stehen allerdings auch Risiken für das Recht auf informationelle Selbstbestimmung des Patienten gegenüber, weil es sich bei den der medizinischen Behandlung und Abrechnung zugrundeliegenden personenbezogenen Daten mit um die sensibelsten Daten handelt, die einen Menschen betreffen können. Der mögliche Einsatz telemedizinischer Anwen-

dungen ist breit gestreut. Er reicht von der Teleinformation, d. h. das Zur-Verfügung-Stellen von allgemeiner medizinischer Information in Datennetzen zum Abruf sowohl für Patienten als auch für die Ärzte, über die Telekonsultation oder -diagnostik, die Telebehandlung bis hin zur zentralen oder dezentralen ärztlichen Dokumentation, die im Rahmen von Gesundheits- und Praxisnetzen von einer Vielzahl von Beteiligten am Gesundheitswesen abgerufen werden können.

Die Rechtsgrundlagen, die für die Erhebung, Verarbeitung und Nutzung dieser medizinischen Informationen in elektronischer Form anzuwenden sind, unterscheiden sich - zumindest derzeit - nicht von denjenigen, die für die herkömmliche Kommunikation unter den Ärzten sowie zwischen Ärzten und Dritten in Schrift und Sprache gelten. So ist die ärztliche Schweigepflicht in den Berufsordnungen der Ärzte normiert. Über § 203 StGB wird eine Schweigepflichtsverletzung unter Strafe gestellt, dem Arzt in den Prozessordnungen ein Zeugnisverweigerungsrecht über den Inhalt der Behandlung mit dem Patienten eingeräumt sowie in § 97 StPO den Strafverfolgungsbehörden verboten, diese Unterlagen zu beschlagnahmen, sofern sie sich im Gewahrsam des Arztes befinden. Grundlage zur Erhebung und Dokumentation von Gesundheitsdaten ist das Behandlungsverhältnis mit dem Patienten. Soweit öffentliche Stellen für ihre Aufgabenerfüllung Gesundheitsdaten erheben, verarbeiten und nutzen gelten die Vorschriften, des Sozialgesetzbuches, des ThürKHG oder des ThürDSG als Auffangnorm. Der Einsatz von Telekommunikation und Informatik bei telemedizinischen Anwendungen hat jedoch zur Folge, dass besondere Vorkehrungen zur Einhaltung dieser gesetzlichen Voraussetzungen beim Umgang mit den Patientendaten getroffen werden müssen.

Praxisnetze und elektronische Patientenakte

Im Berichtszeitraum wurde ich zum Teil durch Beratungsanfragen von Unternehmen, im Rahmen meiner Kontrolltätigkeit, aber auch durch die Diskussion unter den Datenschutzbeauftragten des Bundes und der Länder insbesondere mit der datenschutzrechtlichen Bewertung von Praxisnetzen sowie der Einrichtung von zentralen oder dezentralen elektronischen Krankenakten konfrontiert, wobei sich die meisten Anwendungen in einer mehr oder weniger weit fortge-

schriftlichen Planungs- oder Durchführungsphase befinden. So hat die KV Thüringen auf der Grundlage von § 73 a SGB V mit einer Krankenkasse einen Strukturvertrag abgeschlossen, der die Errichtung von Praxisnetzen zum Gegenstand hatte. Ziel des Vertrages sollte sein, die Qualität der Patientenversorgung dadurch zu verbessern, dass Überweisungen nur an Ärzte innerhalb des Praxisnetzes erfolgen und ein Erfahrungsaustausch der Ärzte zu kostengünstigen Behandlungsmethoden, preiswerten Arzneien und anderen kostendämpfenden Möglichkeiten stattfinden kann. Ein elektronischer Austausch von Informationen oder gar eine gemeinsam geführte Patientendokumentation war hier noch nicht vorgesehen.

Elektronischer Arztbrief

Als eine erste Stufe der informationstechnischen Zusammenarbeit ist bei solchen Projekten denkbar, dass neben dem Austausch allgemeiner medizinischer Information der bisherige Informationsaustausch über den Arztbrief durch einen E-Mail-Versand ersetzt wird. Dies setzt wie beim herkömmlichen Versand zunächst die Einwilligung des Patienten zur Weiterleitung der medizinischen Information an einen mitbehandelnden Arzt voraus. Beim Versand elektronischer Post über Netze oder gar das Internet bestehen große Gefahren für die Wahrung der Vertraulichkeit, für die Unverfälschtheit (Integrität) sowie für die eindeutige Zuordnung der Urheberschaft der Nachricht (Authentizität). Um sicherzustellen, dass in allen Phasen der Kommunikation die Vertraulichkeit der Nachricht gewahrt bleibt, ist eine sichere kryptographische Verschlüsselung zwingend erforderlich, die denselben Schutz vor unbefugter Kenntnisnahme wie bei Versendung eines herkömmlichen Arztbriefes gewährleistet. Eine weniger sichere kryptographische Verschlüsselung birgt die Gefahr, dass eine im Netz von Unbefugten abgefangene Nachricht mit sensiblen Gesundheitsdaten zwar heute noch nicht entschlüsselt werden kann, dies aber bei fortschreitender Entwicklung der Technik in einigen Jahren ohne weiteres möglich sein könnte. Für den Patienten vielleicht sogar lebenswichtig ist aber auch die Integrität und Authentizität der Nachricht. Elektronische Daten können in Datennetzen ohne weiteres unbemerkt verfälscht werden, was u. U. ernste Konsequenzen für den Patienten haben könnte. Nach dem derzeitigen Stand der Technik ist die Gewährleistung der Integrität und Authentizität elektronischer Dokumente nur mit einer digitalen Signatur

möglich, die eindeutig den Urheber und die Unversehrtheit des Dokuments ausweist. Selbstverständlich gelten diese grundsätzlichen Datensicherungsanforderungen auch für den Zugriff auf elektronische Patientenakten.

Elektronische Patientenakte

Besondere rechtliche und technische Probleme werfen jedoch solche medizinische Netze auf, bei denen eine Vielzahl von Ärzten nicht nur elektronisch miteinander kommunizieren, sondern die medizinischen Informationen über einen Patienten in einer sog. elektronischen Patientenakte gespeichert werden, auf die sämtliche an einem bestimmten Gesundheitsnetz beteiligten Ärzte Zugriff erhalten sollen. Dabei sind zwei unterschiedliche Modelle denkbar, die unter der Voraussetzung, dass alle Beteiligten vernetzt sind, realisiert werden können. Zum einen ist dies die zentrale Speicherung beispielsweise beim Hausarzt oder einer zentralen Servicestelle. Zum anderen die dezentrale Speicherung bei den Netzbeteiligten (z. B. Ärzte, Krankenhäuser), wobei den übrigen Netzteilnehmern Zugriffsrechte auf diese Daten eingeräumt werden (virtuelle elektronische Patientenakte). Durch die Einführung derartiger elektronischer Patientenakten mit der Zugriffsmöglichkeit einer Vielzahl von Ärzten wird eine neue Qualität in diesem Bereich geschaffen. Es wird an den bislang geltenden Grundaussagen der ärztlichen Schweigepflicht gerüttelt, wonach die im Rahmen der Behandlung anfallenden Daten ausschließlich dem Arzt und dem Patienten bekannt gegeben werden dürfen. Ausnahmen hiervon sind nur durch eine gesetzliche Regelung oder mit der Einwilligung des Patienten zulässig. Obwohl der Gesetzgeber eine engere Zusammenarbeit der Ärzte insbesondere zur Einsparung teurer Doppeluntersuchungen im Gesundheitsreformgesetz 2000 fordert, hat er den Zugriff auf eine gemeinsame ärztliche Dokumentation im Rahmen von „Integrierten Versorgung“ (z. B. Praxisnetze) in § 140 a Abs. 2 SGB V nicht gesetzlich zugelassen, sondern auch hier von der Einwilligung des Patienten abhängig gemacht (11.1). Die praktische Umsetzung der rechtlichen Voraussetzung einer Einwilligung wirft unter den hierbei gegebenen technischen Bedingungen und der Teilnahme einer Vielzahl von Ärzten eine Reihe datenschutzrechtlicher Fragen auf:

– Zentrale Datenhaltung

Die Einwilligung des Betroffenen hat zunächst sicher das Ziel, die Selbstbestimmung des Patienten hinsichtlich der Verarbeitung seiner Patientendaten zu verwirklichen. Aufgrund der gesetzten äußeren Rahmenbedingungen ist damit vielfach aber auch der Verzicht von Rechtspositionen des Patienten verbunden. Je gewichtiger demnach die Rechte für den Betroffenen sind, auf die er verzichtet, desto wichtiger wird eine Aufklärung durch den Arzt über die Folgen der Einwilligung. Hierzu zählt auch die Aufklärung darüber, welche Folgen eine zentrale Datenhaltung z. B. beim Hausarzt hat. Allein die Tatsache, dass alle relevanten Gesundheitsdaten über einen längeren Zeitraum (ggf. auf Lebenszeit) an einer zentralen Stelle konzentriert sind, führt bereits zu einem objektiven Gefährdungspotenzial, das bei einer dezentralen Speicherung nicht gegeben ist. Dieses Gefährdungspotenzial ergibt sich zum einen daraus, dass durch das Eindringen nur eines Unbefugten (z. B. aus dem Netz) auf den zentralen Speicher auf ein Vielfaches an Gesundheitsdaten zugegriffen und evtl. manipuliert werden kann, als das bei einer dezentralen Speicherung möglich ist. Aber auch die Möglichkeit, dass nachträglich Rechtsvorschriften erlassen werden, die eine Verwendung der zentral gespeicherten Daten zu anderen Zwecken (z. B. Gesundheitsberichterstattung, Forschung etc.) erlauben, kann eine solche objektive Gefährdungssituation darstellen, weil der Betroffene u. U. seine Einwilligung zu einer zentralen Speicherung der Gesundheitsdaten nicht erteilt hätte, wenn er bereits bei der Einwilligung zur Teilnahme am Praxisnetz von dieser Möglichkeit Kenntnis gehabt hätte. Beim Einholen der Einwilligungserklärung vom Patienten zur Anlage einer zentralen elektronischen Patientenakte muss dieser deshalb auf den Umfang und die Tragweite der Speicherung hingewiesen werden.

– Beschlagnahmefreiheit

Das Gefährdungspotenzial für die Wahrung des Patientengeheimnisses bei einer zentralen elektronischen Patientenakte wird weiter für den Fall erhöht, dass die zentrale Speicherung nicht beim Hausarzt, sondern bei einer außerhalb des ärztlichen Bereiches liegenden Stelle (z. B. Servicestelle) erfolgt. Dabei ist es

ohne Bedeutung, ob diese Servicestelle nur Hilfsfunktionen bei der Aktenführung der elektronischen Patientenakte erfüllt. Nach § 97 StPO sind nämlich nur solche ärztliche Aufzeichnungen von der Beschlagnahme durch die Strafverfolgungsbehörden ausgeschlossen, die sich im Gewahrsam des Arztes oder einer Krankenanstalt befinden. Sofern dies nicht der Fall ist, würde die Rechtsposition des Patienten, der seine Einwilligung zur Anlage einer zentralen elektronischen Patientenakte gibt, im Vergleich zu der herkömmlichen Dokumentation wesentlich verschlechtert. Auch darauf müsste der Patient bei Einholung der Einwilligung hingewiesen werden. Allerdings hielte ich eine derartige Einschränkung der Patientenrechte nicht mehr für angemessen. Daher sollte bei zentraler Datenspeicherung diese in der Obhut eines behandelnden Arztes erfolgen. Für den Fall, dass die Daten auf einem zentralen Server außerhalb der Arztpraxis oder des Krankenhauses vollständig kryptographisch verschlüsselt abgelegt werden und ausschließlich der zeugnisverweigerungsrechtliche Arzt die Möglichkeit zur Entschlüsselung hat, könnte möglicherweise der Beschlagnahmeschutz auf technischem Wege erhalten bleiben.

- **Einzeleinwilligung zur Speicherung/Zugriffsbeschränkungen**
Bei den Voraussetzungen für eine wirksame Einwilligung ist zwischen dem Modell einer virtuellen dezentralen elektronischen Patientenakte und einer zentralen elektronischen Patientenakte zu unterscheiden. Bei einer zentralen elektronischen Patientenakte muss im Gegensatz zur virtuellen elektronischen Patientenakte, bei der die jeweilige medizinische Dokumentation auf den Rechnern der beteiligten Ärzte verbleibt und nur auf Anforderung übermittelt wird, bereits zur Anlage der Akte von den am Netz beteiligten Ärzten ein Datensatz an die zentrale Datei übermittelt werden. Schon diese Übermittlung bedarf einer Einwilligung des Patienten, z. B. nach § 27 Abs. 3 ThürKHG bedarf es für eine wirksame Einwilligung des Betroffenen in eine Datenerhebung, -verarbeitung oder -nutzung im Regelfall einer ausdrücklichen schriftlichen Erklärung, nachdem zuvor der Betroffene über den konkreten Zweck und Umfang der Datenverarbeitung sowie über die Freiwilligkeit der Einwilligung und eventuelle Folgen der Verweigerung informiert worden ist. Pauschale Einwilligungser-

klärungen, wonach sich der Patient mit der Speicherung sämtlicher Behandlungsdaten, die bei den am Praxisnetz beteiligten Ärzten über ihn vorhanden sind, in der elektronischen Patientenakte einverstanden erklärt, werden dem nicht gerecht. Wenn jedoch - wie dies bei ärztlichen Behandlungen über einen längeren Zeitraum der Fall ist - der Umfang und der Kreis der Empfänger der zu übermittelnden Daten auch nicht annähernd absehbar sind oder eine Fragestellung erst zukünftig auftaucht, stößt die Einwilligung an ihre Grenzen. Für weitere Übermittlungsfälle muss eine erneute Einzeleinwilligung mit den dann für die dortige Entscheidung notwendigen Informationen über den Zweck und die Datenflüsse eingeholt werden. Für das Anlegen einer zentralen automatisierten Patientenakte bedarf es daher in jedem konkreten Behandlungsfall der ausdrücklichen Einwilligung des Patienten, welche Daten in die elektronische Patientenakte eingestellt werden sollen. Dabei sollte es dem Patienten ermöglicht werden, dass er bestimmte Daten von vornherein nur dem Zugriff eines Teils der ihn behandelnden Ärzte eröffnet.

– Einzeleinwilligung für Abrufe

Diese Voraussetzungen gelten selbstverständlich auch für die Einwilligung zum Abruf von Daten aus der elektronischen Patientenakte, wobei hier auch die virtuelle elektronische Patientenakte einbezogen ist. Ebenso wie bei der herkömmlichen Verfahrensweise, dass der Arzt seinen Patienten in der Sprechstunde um seine Einwilligung bittet, bei einem mitbehandelnden Arzt bestimmte Befunde anzufordern, muss der Patient jedem einzelnen Abruf aus der elektronischen Patientenakte zustimmen. Wegen des großen Umfangs hochsensibler Daten bedarf es dazu gesteigerter technischer Vorkehrungen, um Abrufe ohne Vorliegen einer entsprechenden Einwilligung technisch auszuschließen. Dies könnte beispielsweise dadurch erfolgen, dass der Patient zur Autorisierung des Zugriffs ein Auslesen seiner Krankenversicherten(chip-)karte als Zugriffsberechtigung durch den Arzt ermöglicht. Will der behandelnde Arzt im Interesse einer verbesserten Behandlung des Patienten durch die Nutzung von Daten mitbehandelnder Ärzte vermeiden, dass der Patient pauschal eine Einwilligung in den Abruf aus der elektronischen Krankenakte verweigert, sollte das System so ausgestaltet sein, dass der Pati-

ent dem behandelnden Arzt in der konkreten Behandlungssituation differenzierte Abrufmöglichkeiten einräumen kann. Dies ist beispielsweise dann von Bedeutung, wenn der Patient bei Einholung einer Zweitmeinung dem betreffenden Arzt nicht die in der Erstuntersuchung gestellten Diagnosen zugänglich machen will. Sind die Zugriffsrechte nach dem Alles-oder-Nichts-Prinzip eingerichtet und will der Patient die Informationen der vorherigen Konsultation eines anderen Arztes nicht offenbaren, bleibt ihm nur die Möglichkeit einem Abruf aus der elektronischen Patientenakte generell nicht zuzustimmen. Die Frage differenzierter Zugriffsrechte auf medizinische Informationen wurde bereits im Rahmen der Diskussion um medizinische Patientenchipkarten (1. TB 11.10.2; 2. TB 11.13) erörtert. Von Seiten der Ärzte wurde dabei die These vertreten, dass ein Vertrauensverhältnis zwischen Arzt und Patient dann beendet sei, wenn der Patient dem Arzt Angaben verweigere. Dem ist aber entgegenzuhalten, dass bei objektiver Betrachtung durchaus ein großer Teil fachärztlicher Dokumentationen für die Behandlung eines anderen Facharztes irrelevant ist. Sofern dies doch der Fall sein sollte, wird der Arzt seinen Patienten überzeugen, ihm den erforderlichen Zugriff auf den Teil der elektronischen Patientenakte zu gewähren, der vom betreffenden Facharzt eingestellt wurde.

– Notfallzugriff

Eine wirksame Einwilligung kann jedoch nur dann abgegeben werden, wenn der Patient hierzu körperlich und geistig in der Lage ist. Dies kann in medizinischen Notfallsituationen, z. B. durch Bewusstlosigkeit ausgeschlossen sein. Sofern die Zugriffsberechtigung technisch an das Einlesen der Chipkarte gekoppelt würde, könnte auch im Fall des Vergessens der Chipkarte kein Abruf aus der elektronischen Patientenakte erfolgen, obwohl möglicherweise eine dringende medizinische Notwendigkeit dafür besteht. Ebenso wie bei den Patientenchipkarten (2. TB 11.13) wird für solche Fälle diskutiert, dass der beteiligte Arzt im Netz einen Notfallzugriff z. B. durch Eingabe des Namens oder des Geburtsdatums eingeräumt bekommt. Dabei müssten jedoch die erfolgten Zugriffe auf die Patientendaten umfassend protokolliert werden, um die erfolgten Zugriffe für den Patienten transparent zu machen.

– Sicherung der Auskunftsrechte

Aufgrund der komplexen Struktur derartiger elektronischer Patientenakten ist es für die vom Patienten in den jeweiligen Behandlungssituationen abverlangte Einwilligungsentscheidungen erforderlich, dass dieser beispielsweise von seinem Hausarzt jederzeit Auskunft über den Inhalt der gespeicherten Informationen und die bereits erfolgten Abrufe erhalten kann.

Die aufgezeigten Problemfelder stellen jedoch nur einen Ausschnitt der Schwierigkeiten dar, die es zur Sicherung des informationellen Selbstbestimmungsrechts des Patienten beim Einsatz telemedizinischer Anwendungen zu überwinden gilt. Wegen der dynamischen Entwicklung auf diesem Gebiet, werden mich diese Fragestellungen wohl auch zukünftig weiter beschäftigen.

11.8 Umgang der Landesärztekammer mit Einkommensnachweisen zur Berechnung des Kammerbeitrags

Die Landesärztekammer hatte eine Änderung ihrer Beitragsordnung ab dem Jahr 1996 dahingehend beschlossen, dass der Arzt zum Nachweis der Selbsteinstufung seiner Einkünfte aus ärztlicher Tätigkeit eine Kopie des Einkommenssteuerbescheids oder eine Bestätigung des Steuerberaters für das Vorvorjahr (also 1996 für das Jahr 1994) der Kammer vorzulegen hat (1. TB 11.11.1). Die Beitragsordnung sieht weiterhin vor, dass diese Nachweise nach der Prüfung der Selbsteinstufung und Eingang des Beitrages von der Ärztekammer vernichtet werden. In einer Eingabe äußerte ein Arzt Zweifel daran, ob die Steuerbescheide tatsächlich von der Landesärztekammer nach Beitragseingang vernichtet werden, weil er und auch viele seiner Kollegen im Jahr 1998 von der Landesärztekammer eine Aufforderung erhalten hatten, Beiträge für das Jahr 1995 nachzuzahlen. Für 1995 galten jedoch nach der alten Beitragsordnung als Bemessungsgrundlage für die Beitragserhebung noch die Einkünfte aus ärztlicher Tätigkeit aus dem Vorjahr (also ebenfalls 1994), die von den Ärzten im Rahmen einer Selbsteinstufung der Kammer anzugeben waren, ohne dass diese durch Nachweise (wie z. B. den Einkommenssteuerbescheid) belegt werden mussten. Der betreffende Arzt hatte nun die Vermutung, dass der

Einkommenssteuerbescheid für das Jahr 1994, den er zur Beitragsveranlagung für das Jahr 1996 der Kammer vorgelegt hatte, entgegen den ausdrücklichen Regelungen der Beitragsordnung vernichtet wurde, sondern im Jahr 1998 für eine Nacherhebung der Beiträge für das Jahr 1995 verwendet worden war.

Eine daraufhin von mir durchgeführte Kontrolle bei der Landesärztekammer hat diese Vermutung nicht bestätigt. Alle Nachweise für die Beitragserhebung waren von der Landesärztekammer nach Beitragseingang entsprechend der Regelungen der Beitragsordnung vernichtet worden. Die Beitragsnachforderungen für das Jahr 1995 waren der Landesärztekammer auf Grund des Übergangs von dem alten zum neuen Beitragsverfahren möglich: Nach Prüfung der Einkünfte aus ärztlicher Tätigkeit im Vorvorjahr wurden die einzelnen Ärzte in Beitragsstufen von jeweils 10.000 DM Jahreseinkommen eingestuft und der entsprechende Jahresbeitrag festgesetzt. Eine Speicherung des exakten Jahreseinkommens erfolgt nicht. Die Höhe der gezahlten Beiträge werden für die Dauer von 4 Jahren gespeichert, da innerhalb dieses Zeitraums noch Ansprüche aus der Beitragszahlung gerichtlich geltend gemacht werden können. Dadurch, dass für die Jahre 1995 und 1996 auf Grund der Veränderung des Beitragsberechnungsverfahrens die Bemessungsgrundlage jeweils das Jahr 1994 war, war es der Kammer bei einer Überprüfung im Jahre 1998 möglich, Rückschlüsse auf die Größenordnung des Einkommens im Jahr 1994 zu ziehen und damit auch eine unkorrekte Selbsteinschätzung des Jahres 1995 festzustellen. Datenschutzrechtlich hält sich die Nutzung der Beitragsdaten aus dem Jahr 1996 zur Überprüfung der Beitragsfestsetzung für das Jahr 1995 im Rahmen des § 20 Abs. 1 ThürDSG, da auch die Daten der Selbsteinstufung im Jahr 1995 zum Zweck der Beitragsfestsetzung und des Beitragsinzugs erhoben und gespeichert worden sind.

Bei der Kontrolle musste ich allerdings feststellen, dass weder für die automatisiert verarbeiteten personenbezogenen Daten noch für das Schriftgut Regelungen über die Aufbewahrungsdauer existieren. So waren insbesondere die Beitragsdaten ab dem Jahr 1992 gespeichert. Da es nach Angaben der Landesärztekammer in der Vergangenheit in zahlreichen Fällen auch eine Rückerstattung von zu viel gezahlten Kammerbeträgen gab, habe ich bis zum Erlass entspre-

chender Regelungen durch die Landesärztekammer gegen die weitere Speicherung der Daten keine Bedenken erhoben. Darüber hinaus waren die datenschutzrechtlichen Freigaben für die im Einsatz befindlichen automatisierten Verfahren erst kurz vor meiner Kontrolle erteilt worden. Die zu erstellenden Anlagen- und Verfahrensverzeichnisse sowie die Datenschutzregistermeldungen waren an einigen Stellen überarbeitungsbedürftig. Obwohl nach Ziffer 34.2 VVThürDSG den der Aufsicht des Landes unterliegenden Körperschaften lediglich die Bestellung eines behördeninternen Datenschutzbeauftragten empfohlen wird, zeigten die festgestellten Defizite, dass ein solcher durchaus erforderlich ist. Auf meine Empfehlung hin hat die Landesärztekammer zwischenzeitlich eine behördeninterne Datenschutzbeauftragte bestellt.

11.9 Wiederaufgefundene Kurierpost eines Klinikums

Die Presse berichtete über einen Vorgang, dass Briefe eines Klinikums, darunter auch ärztliche Gutachten, Krankenfunde und Abrechnungen, die den jeweiligen Empfängern zugestellt werden sollten, in einem Baggersee entdeckt worden seien. Eine von der Polizei eingesetzte Taucherstaffel sei zur Suche nach den Briefen eingesetzt worden.

Daraufhin wurde umgehend das betreffende Klinikum zum Sachverhalt und insbesondere zu den Modalitäten beim Versand von Schriftstücken, die der ärztlichen Schweigepflicht unterliegen, befragt.

Das Klinikum beantwortete kurzfristig die aufgeworfenen Fragen. Es bestätigte den Umstand, dass über 2000 Briefe als vermisst angesehen werden. Es berichtete weiter, dass Grundlage der Beförderung ein schriftlicher Vertrag mit einem Postdienstunternehmen sei. Dieses Unternehmen hatte allerdings auch ein Subunternehmen teilweise mit der Beförderung von Briefdienstleistungen beauftragt, obwohl dafür keine Zustimmung des Klinikums eingeholt wurde. Das Klinikum hat daraufhin den abgeschlossenen Beförderungsvertrag gekündigt. Weiter wurden alle Organisationseinheiten des Klinikums angewiesen, sämtliche, im fraglichen Zeitraum bearbeitete Post zu überprüfen und gegebenenfalls erneut, durch nunmehr die Deutsche Post AG, zu versenden.

Die wiederaufgefundenen Briefe seien nahezu alle nicht geöffnet gewesen, hat das Klinikum informiert. Gegebenenfalls noch nicht zugestellte Briefsendungen an die Empfänger wurden nachgeholt, damit die Rechte der Betroffenen aus dem Vorkommnis nicht weiter beeinträchtigt werden.

11.10 Einsichtsrecht in Patientenunterlagen

Auch im vergangenen Berichtszeitraum bin ich aufgrund von Eingaben mit dem Auskunftsbegehren in Krankenunterlagen beschäftigt gewesen (2. TB 11.12). Die Besonderheit in einem Fall lag darin, dass der Petent vorgetragen hat, es seien Unterlagen in seiner Krankenakte gefälscht worden. Dabei handelte es sich um mehrere Aufenthalte in den Psychiatrischen Abteilungen mehrerer ehemaliger Bezirkskrankenhäuser in den 70er und 80er Jahren. Die daraufhin erfolgte Überprüfung in einem Landesfachkrankenhaus, das als Nachfolgeeinrichtung die Unterlagen aufbewahrt, hat keinerlei Anhaltspunkte für eine Manipulation der Unterlagen ergeben. Ebenso hat sich seine gleichfalls vorgetragene Vermutung, dass Unterlagen, die beim Landesamt für Rehabilitation und Wiedergutmachung zur Bearbeitung seines Rehabilitierungsantrags wegen in den ehemaligen Bezirkskrankenhäusern erlittenen Schädigungen gespeichert sind, gefälscht worden seien, nach meiner Kontrolle vor Ort nicht bestätigt. Obwohl sich der Petent mehr von meiner Überprüfung erhofft hatte, konnte ich ihm in dieser Angelegenheit nur insoweit helfen, dass er vom Krankenhaus zugesagt bekam, jederzeit selbst oder durch einen Bevollmächtigten Einblick in die Krankenunterlagen zu erhalten. Allgemein ist aufgrund der bearbeiteten Eingaben festzustellen, dass von Krankenhäusern in Thüringen soweit wie möglich den Patienten Einsicht in ihre Unterlagen gewährt wird.

11.11 Patientenakten nach Umzug gefunden

Von der örtlichen Presse wurde ich unterrichtet, dass in einem geräumten ehemaligen Krankenhaus nach dessen Umzug in einen Neubau Patientenunterlagen gefunden worden seien. Besucher hatten diese anlässlich einer zweitägigen Verkaufsaktion für zurückgelassenes altes Mobiliar in den bisherigen Klinikräumen entdeckt und der Presse übergeben.

Wie mir von den Verantwortlichen versichert wurde, waren zum Zeitpunkt des Verkaufs ausschließlich Räume zugänglich, die altes zum Verkauf bestimmtes Mobiliar enthielten. Durch eine Vielzahl von Aufsichtspersonal sei gewährleistet gewesen, dass die wenigen verschlossenen Räume, in denen sich noch ältere Patientenakte sowie Röntgenaufnahmen befanden, nicht betreten werden konnten. Der Anfangsverdacht seitens der Klinikleitung, dass in diese Archivräume eingebrochen worden sei und die Patientenunterlagen von dort stammten, bestätigte sich aufgrund des Inhaltes und der Form der von der Presse übergebenen Unterlagen nicht. Davon konnte ich mich auch anlässlich meiner unverzüglich vor Ort durchgeführten Kontrolle überzeugen, bei der kein Bezug zu den noch in den Archivräumen lagernden Patientenakten festzustellen war. Statt dessen ließen die wenigen aus verschiedenen Arbeitsbereichen aufgefundenen unterschiedlichen Einzelschriftstücke und Notizen aufgrund ihres Inhaltes, der Form und Qualität eher darauf schließen, dass nach dem Umzug vor der Freigabe der Räume für die Öffentlichkeit nicht sorgfältig geprüft worden war, ob nicht dort in, unter oder hinter Möbelstücken (insbesondere Schränken und Regalen) noch einzelne Schriftstücke (insbesondere Altpapier mit Patientendaten) verblieben waren.

Als eine wesentliche Ursache für die unzureichende Kontrolle müssen die dazu fehlenden Regelungen in den Umzugsmaßnahmenplänen des Klinikums angesehen werden. Obwohl eine Vielzahl schriftlicher Festlegungen zu den einzelnen Umzugsschritten und -maßnahmen getroffen worden waren, fehlten konkrete Regelungen zum Datenschutz. Selbstverständlich hat eine medizinische Einrichtung bei einem Umzug in erster Linie dem Wohl der Patienten besonderes Augenmerk zu schenken. Gleichwohl trägt sie aber auch die Verantwortung für die durchgängige Gewährleistung der ärztlichen Schweigepflicht. Insoweit bedurfte es entsprechender schriftlicher Festlegungen in den Umzugskonzeptionen zu den Einzelmaßnahmen, zu Verantwortlichkeiten, zu Protokollierungs- und Kontrollpflichten.

Dass offensichtlich die technischen und organisatorischen Maßnahmen zur Datensicherung während des gesamten Umzugs nicht ausreichten, um zu gewährleisten, dass Patientenunterlagen nicht in unbefugte Hände gelangen, war gem. § 39 ThürDSG zu beanstan-

den. Gleichzeitig wurde vom Klinikum gefordert, baldmöglichst die noch im ehemaligen Krankenhauskomplex verbliebenen alten Patientenunterlagen in das Patientenarchiv unter Festlegung geeigneter Maßnahmen, die dabei einen Zugriff Unbefugter ausschließen, zu überführen, was zwischenzeitlich erfolgte.

11.12 Umgang mit Patientenakten aus ehemaligen Polikliniken

In meinen vorangegangenen Tätigkeitsberichten (1. TB 11.3.1; 2. TB 5.2.9) hatte ich bereits ausführlich über die Probleme beim Umgang mit Patientenakten ehemaliger Polikliniken berichtet. Aufgrund der ärztlichen Berufsordnungen sind alle Ärzte verpflichtet, ihre Aufzeichnungen mindestens zehn Jahre nach Abschluss der Behandlung aufzubewahren, soweit nicht spezialgesetzliche Vorschriften eine längere Aufbewahrungsdauer vorschreiben. Dies betrifft im besonderen Maße Aufzeichnungen über Röntgenbehandlungen sowie über medizinische Maßnahmen, die den Bestimmungen der Strahlenschutzverordnung unterfallen. Für diese Unterlagen gilt eine Aufbewahrungsfrist von 30 Jahren. Ungeachtet dessen ist vor einer Vernichtung von Aufzeichnungen zu bedenken, dass eine mögliche Haftung wegen Vertragsverletzung oder deliktischen Handelns nach den Vorschriften des BGB erst nach 30 Jahren verjährt, weshalb sich aus der Sicht des Arztes empfiehlt, bei Behandlungsunterlagen bis zu diesem Zeitpunkt von einer Vernichtung Abstand zu nehmen, um für den Arzt in einem möglichen Haftungsprozess nachteilige Folgen bei der Beweislastverteilung zwischen Arzt und Patienten zu vermeiden.

Mit den „Gemeinsamen Hinweisen und Empfehlungen des Thüringer Ministeriums für Soziales und Gesundheit und des Thüringer Innenministeriums zur Aufbewahrung und Nutzung von Patientenunterlagen aus Gesundheitseinrichtungen der ehemaligen DDR“ aus dem Jahr 1996 war den Kommunen eine datenschutzgerechte Anleitung zur weiteren Verwahrung der Altakten aus ehemaligen Polikliniken gegeben worden. Wegen der besonderen Sensibilität der Daten habe ich im Berichtszeitraum die praktische Umsetzung dieser Regelungen mehrfach kontrolliert.

In zwei Landkreisen gab es dabei keinerlei Anlass für Beanstandungen. Die Unterlagen werden dort in Verantwortung der jeweiligen Gesundheitsämter ordnungsgemäß, übersichtlich und vor unbefugtem Zugriff Dritter sicher verwahrt. Klärungsbedürftig waren lediglich noch Festlegungen zur Datensicherheit bei Havariefällen sowie bei Reinigungsarbeiten durch Fremdfirmen. Ich habe diesbezüglich darauf hingewiesen, dass in jedem Fall durch geeignete Maßnahmen (z. B. durch verschlossene Behältnisse oder durch eine entsprechende Beaufsichtigung) eine unbefugte Kenntnisnahme der Patientendaten durch Dritte auszuschließen ist.

In einem Gesundheitsamt hatten bisher gleichfalls die räumlichen Bedingungen, wie auch die Regelungen zum Umgang mit den Patientenakten den datenschutzrechtlichen Anforderungen im Sinne des vorgenannten Erlasses entsprochen. Da aber nach dem Eigentümerwechsel die Lagerräume nur noch befristet zur Verfügung standen, hatte man entgegen meiner auf Anfrage gegebenen Empfehlungen (2. TB 11.10) damit begonnen, die Patientenakten der ehemaligen Polikliniken zur Mikroverfilmung vorzubereiten, mit der Absicht, die Originalakten später zu vernichten.

Bei meiner Prüfung vor Ort gemeinsam mit der Rechtsaufsichtsbehörde stellte sich zudem heraus, dass die Stadt zur Durchführung dieser Tätigkeiten eine nicht-öffentliche Stelle beauftragt hatte. Dadurch war eine Dienst- und Fachaufsicht über die Bearbeiter seitens des Amtsarztes nicht mehr gegeben, was einem Verstoß gegen die Einhaltung der ärztlichen Schweigepflicht gem. § 203 StGB gleichkam und von mir gem. § 39 Abs. 1 ThürDSG beanstandet wurde. Darüber hinaus wurde aber auch die Erforderlichkeit der Mikroverfilmung aus datenschutzrechtlicher Sicht in Frage gestellt, da zwangsläufig im Rahmen der Vorbereitung und Durchführung der Verfilmung durch die jeweiligen Bearbeiter Kenntnis vom Inhalt jeder einzelnen Patientenakte genommen wird, was bei einer ausschließlichen Verwahrung nicht notwendig wäre. Andererseits konnte die Mikroverfilmung aber nicht automatisch zur anschließenden Vernichtung der Originalakten führen, da Mikrofilmen bei einer eventuellen gerichtlichen Auseinandersetzung die notwendige Beweiskraft möglicherweise fehlt.

Zur Behebung meiner Beanstandung erfolgte unverzüglich in Abstimmung mit den zuständigen Stellen die Übernahme der bisher bei der GmbH beschäftigten Arbeitskräfte durch die Stadtverwaltung, sodass von diesem Zeitpunkt an die Aufgaben nur noch von Mitarbeitern der Stadtverwaltung wahrgenommen wurden. Dennoch hielt man zunächst an der Fortführung der Mikroverfilmung fest, bis auch die obersten Aufsichtsbehörden für Kommunales und Gesundheitswesen sowie das Justizministerium auf Anfragen die von mir und der Kommunalaufsicht bereits geäußerten Bedenken zur vorzeitigen Vernichtung der Originale bestätigten und zum Ausdruck brachten, dass im Interesse der betroffenen Patienten und auch der Verwaltung selbst von einer Vernichtung der Originalunterlagen vor Ablauf der Aufbewahrungsfristen abgesehen werden sollte. Um nach der Einstellung der Mikroverfilmung dennoch baldmöglichst den Aktenbestand verringern zu können, wurde von der Stadt festgelegt, eine patientenaktenbezogene Finddatei mit dem jeweils letzten in der Patientenakte eingetragenen Behandlungsdatum zu erstellen, die es ermöglicht, sukzessive die Einzelakten mit Ablauf der Aufbewahrungsfrist auszusondern und zu vernichten.

11.13 Umfang der Einsicht in Krankenunterlagen durch Kassen und MDK

Im Anschluss an die im 2. TB (11.23) dargestellte Thematik, wonach im Rahmen der Abrechnung der Krankenhausleistungen mit den Krankenkassen auch nach Abschluss der Krankenhausbehandlung eine Übersendung von Krankenhausunterlagen (z. B. Operations- und Krankenhausentlassungsberichte) im Einzelfall zur Überprüfung des Vorliegens von Voraussetzungen, Art und Umfang der Leistung von § 275 Abs. 1 Satz 1 Nr. 1 SGB V gedeckt ist, wurde unter den Datenschutzbeauftragten die Frage erörtert, ob dies im Einzelfall auch zur Überprüfung der konkret in Ansatz gebrachten Abrechnungsart (Fallpauschale, Sonderentgelt oder Pflegesatz) zulässig ist. Die Zuordnung von erbrachten Krankenhausleistungen zu Sonderentgelten, Fallpauschalen oder Pflegesätzen ist im Einzelfall ohne ärztlichen Sachverstand und Kenntnis von weiteren Umständen der Behandlung aus der Behandlungsakte allein anhand der nach § 301 SGB V den Krankenkassen übermittelten Angaben vielfach nicht zweifelsfrei möglich. Ich gehe daher davon aus, dass in diesen Ein-

zelfallen auch der MDK zur Prüfung der Zuordnung der Abrechnungsart von den Krankenkassen nach § 275 Abs. 1 Satz 1 Nr. 1 SGB V beauftragt werden kann. Auch hier gilt, wie bereits im 2. TB (11.23) dargestellt, dass für eine derartige Überprüfung konkrete Anhaltspunkte vorliegen müssen und eine flächendeckende Überprüfung oder gar eine Überprüfung, um erst Material für Pflegesatzverhandlungen zu gewinnen, unzulässig wäre.

Der MDK Thüringen hat mich auf eine Praxis hingewiesen, wonach Thüringer Krankenhäuser mitunter die Übersendung von Krankenunterlagen an Medizinische Dienste anderer Bundesländer, die von den dortigen Krankenkassen ihrer in Thüringen behandelten Versicherten beauftragt wurden, mit der Begründung verweigert haben, dass es eine ausschließliche „örtliche Zuständigkeit“ des MDK Thüringen für die Krankenhäuser in Thüringen gebe. Der MDK Thüringen ist demgegenüber der Auffassung, dass aus § 275 Abs. 1 SGB V keine örtliche Zuständigkeit ableitbar sei. Er geht davon aus, dass der MDK auch Unterlagen von Krankenhäusern anderer Bundesländer anfordern kann, um Gutachten im Auftrag der Krankenkasse des Versicherten zu erstellen. Zu dieser Fragestellung habe ich mich an den BfD mit der Bitte gewandt, eine Klärung mit dem Bundesministerium für Gesundheit herbeizuführen. Dieses hat daraufhin mitgeteilt, dass § 278 SGB V allein die Frage regelt, wer Träger der Medizinischen Dienste ist. Die fachliche Zuständigkeit des MDK ergebe sich vielmehr aus seiner Aufgabenbeschreibung in § 275 ff. SGB V. Nicht der Leistungserbringer, sondern der Versicherte der Krankenkasse bildet demnach den Anknüpfungspunkt für die Zuständigkeit der Medizinischen Dienste. Dies bedeute, dass der MDK eines anderen Bundeslandes berechtigt ist, sofern die Voraussetzungen des § 275 SGB V vorliegen, für die Versicherten der dortigen Krankenkassen von einem Krankenhaus in Thüringen Krankenunterlagen anzufordern. Der MDK Thüringen, dem ich diese Stellungnahme zugeleitet habe, hat mir im Nachgang mitgeteilt, dass der überwiegende Teil der Medizinischen Dienste in Deutschland ebenfalls die Auffassung vertreten, dass eine örtliche Zuständigkeit nicht verbindlich vorgegeben sei.

Schließlich wurde unter den Datenschutzbeauftragten auch die Frage erörtert, unter welchen Voraussetzungen die von manchen Kranken-

kassen praktizierte Verfahrensweise, von den Versicherten Einwilligungserklärungen zur Übersendung von Krankenhausentlassungsberichten an die Krankenkassen zu verlangen, als zulässig anzusehen ist. Dabei ging es um solche Fallkonstellationen, bei denen die Krankenkassen sich mit Einwilligung des Versicherten Krankenhausentlassungsberichte vorlegen lassen, um prüfen zu können, ob eine Beauftragung des MDK nach § 275 Abs. 1 SGB V erforderlich ist. Bei dieser Frage gehe ich davon aus, dass zur Prüfung, ob eine Beauftragung des MDK erfolgen soll, die Kassen keine medizinischen Daten anfordern dürfen. Das ergibt sich bereits aus § 276 Abs. 2 Satz 1 letzter Halbsatz SGB V, wonach die Krankenkassen in den Fällen der Beauftragung des MDK mit der Begutachtung nach § 275 Nr. 1 bis 3 SGB V keine Patientendaten bei den Leistungserbringern zur Vorlage an die Kassen, sondern nur direkt an dem MDK verlangen dürfen. Dies ist auch folgerichtig, da den Kassen regelmäßig der notwendige medizinische Sachverstand fehlen dürfte, der aber gerade beim MDK für die Kassen vorgehalten wird. Grundlage für Anhaltspunkte, die zu einer Begutachtung führen können, sind daher die Angaben nach § 301 SGB V. Sofern sich die Kassen - auch ggf. unter beratender Hinzuziehung des MDK nach § 275 Abs. 4 SGB V - nicht sicher sind, ob die Voraussetzungen von § 275 Abs. 1 SGB V vorliegen, könnte ggf. der MDK - mit Einwilligung des Versicherten - weitere Unterlagen anfordern, um diese Vorprüfung vorzunehmen.

11.14 Modellvorhaben nach § 63 SGB V zur Optimierung der Diabetesversorgung

Durch das 2. GKV-Neuordnungsgesetz vom 23. Juni 1997 (BGBl. I. S. 1520) wurde mit Wirkung ab 1. Juli 1997 für die Kassen und ihre Verbände die Möglichkeit eröffnet, zur Verbesserung der Qualität und der Wirtschaftlichkeit der Versorgung Modellvorhaben zur Weiterentwicklung der Verfahrens-, Organisations-, Finanzierungs- und Vergütungsformen der Leistungserbringer nach § 64 SGB V zu vereinbaren. Eine solche Vereinbarung über eine strukturierte und qualitätsgesicherte ambulante Versorgung von Patienten mit Diabetes mellitus hat die KV Thüringen mit der AOK Thüringen Anfang 1998 geschlossen und mir im Nachgang zur datenschutzrechtlichen Bewertung vorgelegt. Die Verbesserung der Qualität der Diabetiker-versorgung soll danach durch verbesserte, regelmäßige Schulungen

sowie durch die zwingende Überweisung bzw. Rücküberweisung der Versicherten zwischen Hausarzt und diabetologischer Schwerpunktpraxis (SPP) bei Über- oder Unterschreiten bestimmter klinischer und paraklinischer Parameter (z. B. Laborwerte, bei Schwangerschaften, bei auftretenden Komplikationen etc.) erreicht werden. Im Einzelnen war folgende Verfahrensweise geplant und auch teilweise schon realisiert: Die an dem Modellvorhaben freiwillig teilnehmenden Vertragsärzte bekommen bei Einhaltung der Schulungsaufträge und Überweisungskriterien (z. B. Überweisung an SPP bei Überschreitung bestimmter Laborwerte) für diese Leistungen innerhalb des Modellversuchs zusätzliche Vergütungen in Form von modellspezifischen Abrechnungsnummern, die mit einer bestimmten Punktzahl von der KV mit der AOK Thüringen vereinbart wurden. Um diese zusätzlichen Abrechnungsnummern vergüten zu können, wurde in Zusammenarbeit mit einem Hochschulinstitut ein Controllingverfahren entwickelt, mit dem auf der Grundlage von regelmäßig von den teilnehmenden Ärzten zu dokumentierenden klinischen Werten überprüft werden kann, ob die vorgegebenen Behandlungskriterien eingehalten sind und damit eine Zusatzvergütung erfolgen kann oder nicht. Diese Anamnese- und Befunddaten werden vom teilnehmenden Arzt ohne Einwilligung des Betroffenen auf einem Dokumentationsbogen vierteljährlich der eigens hierzu bei der KV Thüringen eingerichteten Vertrauensstelle mitgeteilt. Dort werden die Belege auf EDV erfasst und durch ein kryptographisches Verschlüsselungsverfahren so pseudonymisiert, dass weder die Identität des Arztes noch die des Patienten erkennbar ist. Diese Angaben werden dann in der Controllingstelle anhand der festgelegten Kriterien auf eine Abrechenbarkeit im Rahmen des Modellversuchs überprüft. Vor der Vergütung an die einzelnen Ärzte wird das Controllingergebnis, das ausschließlich die Tatsache enthält, ob die Kriterien eingehalten sind (oder nicht) einschließlich der entsprechenden Begründung, nach der Zuordnung in der Vertrauensstelle zu Arzt und Versichertem der Abrechnungsstelle bekannt gegeben. Es hat sich allerdings im Lauf der Einführung des Verfahrens herausgestellt, dass die Einhaltung der Überweisungskriterien unter Umständen erst nach mehreren Quartalen festgestellt werden kann. Daher erfolgte die Zahlung der modellspezifischen Abrechnungsnummern an alle teilnehmenden Ärzte unter Vorbehalt. Die Zahlungen können

dann von der KV Thüringen innerhalb eines Jahres bei Nichteinhaltung der Kriterien von den Ärzten zurückgefordert werden.

Meine datenschutzrechtliche Überprüfung des Verfahrens hat an zwei Stellen gravierende Mängel ergeben, die ich formell nach § 39 ThürDSG beanstanden musste. Es handelte sich dabei um die fehlende Rechtsgrundlage für eine Erhebung der Anamnese- und Befunddaten durch die KV Thüringen ohne die Einwilligung der beteiligten Patienten sowie die nicht ausreichende räumliche und organisatorische Trennung der Vertrauensstelle von der Abrechnungsstelle bei der KV Thüringen. Eine gesetzliche Offenbarungsbefugnis der teilnehmenden Ärzte war der Vorschrift des § 63 SGB V nicht zu entnehmen, da § 63 SGB V keine Abweichung von den datenschutzrechtlichen Vorschriften des zehnten Kapitel (§§ 284 bis 305 SGB V) vorsieht. Die Beteiligung am Modellvorhaben durch die Versicherten ist freiwillig. Damit waren die von der KV Thüringen ohne eine entsprechende Einwilligung der Versicherten entgegengekommenen Meldungen unter Verletzung datenschutzrechtlicher Vorschriften erfolgt. Nach meiner Beanstandung hat die KV Thüringen alle bereits vorliegenden Meldungen den teilnehmenden Ärzten zurückgegeben und diesen eine Einverständniserklärung samt einer Patienteninformation, in der über Zweck und Umfang der Einwilligung informiert wird, übergeben. Die teilnehmenden Ärzte wurden verpflichtet, nur diejenigen Dokumentationsbögen (erneut) an die KV Thüringen zu übersenden, bei denen die jeweiligen Patienten nach Aufklärung eine entsprechende schriftliche Einwilligung erteilt haben, die der Arzt zu seinen Akten zu nehmen hat. Der Arzt hat dies gegenüber der KV Thüringen durch eine entsprechende Sammelerklärung zu bestätigen. Außerdem wurde diese Verfahrensweise in die Vereinbarung zwischen KV Thüringen und AOK Thüringen verbindlich aufgenommen.

Bei einer späteren Kontrolle in der KV Thüringen hinsichtlich der Einhaltung der vereinbarten Verfahrensweise stellte sich heraus, dass die eingehenden Dokumentationsbögen nicht in einer räumlich und organisatorisch von der Abrechnungsstelle getrennten Organisationseinheit in die EDV erfasst wurden, sondern dass dies von Mitarbeitern der Abrechnungsstelle im Bereich derselben erfolgte. Im Hinblick darauf, dass die Versicherten im Rahmen der Einholung

ihrer schriftlichen Einwilligung auf dem Informationsblatt ausdrücklich darauf hingewiesen worden sind, dass die Daten vollständig in der Vertrauensstelle anonymisiert und eine Identifikation eines Patienten außerhalb der Vertrauensstelle ausgeschlossen ist, kann sich die Zulässigkeit der Verarbeitung personenbezogener Daten auch nur auf die Vertrauensstelle erstrecken, weshalb ich die Erhebung und Verarbeitung dieser Daten in der Abrechnungsstelle formell nach § 39 ThürDSG beanstandet habe. Ebenfalls beanstandet habe ich die Tatsache, dass entgegen § 34 ThürDSG das Verfahren zur automatisierten Verarbeitung der Daten noch nicht freigegeben war. Die Freigabe und die Erstellung des Anlagen- und Verfahrensverzeichnisses ist zwischenzeitlich erfolgt. Darüber hinaus hat die KV Thüringen nunmehr mitgeteilt, dass durch organisatorische Maßnahmen sichergestellt ist, dass die Erfassung der Dokumentationsbögen ausschließlich in der Vertrauens- und Controllingstelle erfolgt.

Die Pseudonymisierung erfolgt auf einem Rechner in der Vertrauensstelle der KV Thüringen, bei dem die den Arzt und Patienten identifizierenden Angaben mit einem kryptographischen Verfahren verschlüsselt werden. Zugang zu diesem Verfahren haben nur die Mitarbeiter der Vertrauensstelle bei der KV Thüringen über PIN-gesicherte Chipkarten. Des Weiteren wurde aufgrund meiner Forderung im Datenschutz- und Datenflusskonzept nunmehr eindeutig festgestellt, dass der AOK Thüringen lediglich zahlenmäßig mitgeteilt wird, bei wie vielen Fällen die modellspezifische Abrechnungsnummer gerechtfertigt abgerechnet wurde und bei welchen nicht. Gegen diese Verfahrensweise und die Übermittlung von anonymisierten Daten an das Universitätsinstitut zur wissenschaftlichen Auswertung des Vorhabens habe ich keine Bedenken geäußert.

Wie mir bekannt geworden ist, plant der AOK Bundesverband dieses Controllingverfahren auch auf andere Bundesländer zu übertragen. Um die mit einer Einwilligung verbundenen Schwierigkeiten zu umgehen, wird derzeit erwogen, die Pseudonymisierung bereits beim teilnehmenden Arzt durchzuführen, sodass keine versichertenbezogenen Anamnese- und Befunddaten an die KV Thüringen übermittelt werden. Ergebnisse hierzu sind mir allerdings noch nicht bekannt.

11.15 Kontrolle bei der Kassenärztlichen Vereinigung Thüringen (KVT)

Bei der im Berichtszeitraum durchgeführten Kontrolle in der KVT habe ich einige Mängel festgestellt, die zu beanstanden waren. So wurde die gesamte Datenverarbeitung zur Abrechnung mit den Leistungserbringern nicht von der KVT selbst durchgeführt, sondern bereits im Jahre 1991 war die Kassenärztliche Vereinigung Hessen hiermit beauftragt worden. Nach den Vorschriften des § 80 SGB X ist dies zwar grundsätzlich möglich, doch müssen hierbei zwischen den Vertragspartnern konkrete Regelungen getroffen werden, die sicherstellen, dass der Auftraggeber (hier die KVT) als verantwortliche Stelle die notwendigen Weisungen und Datenschutzmaßnahmen vorgibt. Dem gegenüber enthielt die Vereinbarung lediglich die Aussage, dass sich die Kassenärztliche Vereinigung Hessen verpflichtet, die jeweils gültigen Bestimmungen des Datenschutzes für die KVT zu gewährleisten. Dies entsprach nicht den Voraussetzungen von § 80 Abs. 2 SGB X, wonach der Auftrag schriftlich zu erteilen ist und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Darüber hinaus besteht die Besonderheit, dass es sich bei dem Auftragnehmer um eine außerhalb Thüringens liegende Stelle handelt, auf die die Vorschriften über die Datenschutzkontrolle des ThürDSG nicht anwendbar sind. Daher war die KVT verpflichtet, vertraglich mit der KV Hessen die Kontrollmöglichkeit des TLfD sicherzustellen. Auf meine Forderung hin erfolgte zwischenzeitlich eine entsprechende Ergänzung des Vertrags zwischen der KV Thüringen und der KV Hessen.

Darüber hinaus waren weder für das Lohn- und Gehaltsprogramm, die Datenverarbeitung durch die zentrale Telefonanlage noch hinsichtlich der Abrechnungsverfahren mit den Leistungserbringern datenschutzrechtliche Freigaben durch die KV Thüringen erfolgt. Zudem lagen nur zum Teil Anlagen- und Verfahrensverzeichnisse vor, die auch in einigen Bereichen überarbeitungsbedürftig waren. Diese Freigaben wurden im Nachgang der Kontrolle nachgeholt und entsprechende Anlagen- und Verfahrensverzeichnisse bzw. Registermeldungen von der KV Thüringen erarbeitet. Schließlich musste ich auch die Verfahrensweise bei der Vernichtung von personenbe-

zogenem Aktenmaterial beanstanden. Hierzu waren in jeder Abteilung in sog. Raucherräumen Sammelbehälter als „Blaue Mülltonne“ aus Kunststoff aufgestellt, die den vielfach verwendeten Mülltonnen ähneln. Der Deckel war verschlossen hatte allerdings einen derart breiten Einwurfschlitz, dass es ohne weiteres möglich war, durch Hineingreifen sensibles Aktenmaterial herauszunehmen. Die KV Thüringen hat daraufhin die Einwurfschlitze mit Vorrichtungen versehen, die ein unbefugtes Eingreifen unmöglich machen.

11.16 Durchführung des Psychotherapeutengesetzes

Bei der Umsetzung des am 1. Januar 1999 in Kraft getretenen Gesetzes über die Berufe des psychologischen Psychotherapeuten und des Kinder- und Jugendlichenpsychotherapeuten vom 16.06.1998 (BGBl. I. S. 1311 ff. - PsychThG) stellte sich die Frage, wie die Psychotherapeuten im Rahmen der von ihnen beantragten Approbation den Nachweis über erbrachte Therapiestunden erbringen können, ohne dass sie hierbei ihre Schweigepflicht gegenüber den Patienten verletzen. Hintergrund war die Übergangsvorschrift von § 12 Abs. 3 und 4 PsychThG, wonach bereits praktizierende Psychotherapeuten eine Approbation erlangen können, wenn sie den Nachweis über eine bestimmte Anzahl von Stunden erbrachter Psychotherapieleistungen führen können. Unproblematisch war dies bei solchen Fällen, in denen die geleisteten Therapiestunden von Kostenträgern wie gesetzlichen Krankenkassen, privaten Krankenversicherungen oder Beihilfestellen erstattet wurden. Für diese Fälle genügte zur Nachweisführung eine Bestätigung des Kostenträgers über die Anzahl der abgerechneten und geleisteten Therapiestunden ohne Angabe der Patienten.

Problematisch wäre es jedoch dann, wenn die Antragsteller Nachweise über Therapien von Selbstzahlern bei der Zulassungsbehörde in der Form einreichen, die die Person der behandelten Patienten erkennen ließ. Dies würde eine Verletzung der Schweigepflicht des Psychologen nach § 203 StGB darstellen. Im Kreise der Datenschutzbeauftragten besteht die Auffassung, dass die in § 12 Abs. 3 und 4 PsychThG vorgesehene Nachweisführung durch den Antragsteller keine Offenbarungsbefugnis im Sinne des § 203 Abs. 1 StGB darstellt. Vom TLVwA, das für Thüringen die zuständige Approba-

tionsbehörde ist, habe ich die vorgesehenen Antragsunterlagen zur Approbation als psychologischer Psychotherapeut bzw. Kinder- und Jugendlichenpsychotherapeut angefordert. Obwohl mir von dort mitgeteilt wurde, dass in Thüringen nur solche Therapiestunden anerkannt würden, die durch einen Kostenträger (gesetzliche Krankenkasse, private Krankenversicherung oder Beihilfefestsetzungsstelle) erstattet worden sind, war in den Antragsunterlagen auch auf die Möglichkeit hingewiesen, wonach eine Nachweisführung im Einzelfall durch Eigenbelegung ausreichen kann. Daraus könnte jedoch der Antragsteller den Schluss ziehen, dass er zur Vorlage von Einzelabrechnungen seiner Patienten berechtigt oder gar verpflichtet ist. Auf meine Aufforderung hin hat das TLVwA die Antragsformulare mit einem Hinweis versehen, dass eine patientenbezogene Nachweisführung von Therapien aus datenschutzrechtlichen Gründen nur mit anonymisierten Belegen erfolgen darf. Antragsteller, die bereits die alten Antragsformulare übersandt bekommen hatten, wurden im Rahmen der weiteren Antragsbearbeitung auf die anonymisierte Vorlage von Nachweisen hingewiesen. Mit Inkrafttreten des PsychThG wurden auch die Vorschriften des § 95 Abs. 10 bis 13 SGB V zur Ermächtigung/Zulassung von Psychotherapeuten eingefügt. Danach entscheidet der Zulassungsausschuss bei der Kassenärztlichen Vereinigung über die Ermächtigung/Zulassung von Psychotherapeuten. § 95 Abs. 11 SGB V setzt ebenso wie bei der Approbation den Nachweis einer bestimmten Anzahl von dokumentierten Behandlungsstunden voraus. Meine Nachfrage bei der Kassenärztlichen Vereinigung Thüringen hat ergeben, dass hier ausschließlich Nachweise von Kostenträgern (gesetzliche Krankenkassen, private Krankenversicherungen, Beihilfefestsetzungsstellen) verwendet werden, die keine Zuordnung zu den jeweiligen Patienten ermöglichen.

11.17 Beitritt der AOK Thüringen zur ARGE-Mitte

Bereits im 2. TB (11.17) habe ich über die datenschutzrechtlichen Probleme berichtet, die mit einer Auslagerung der Datenverarbeitung der AOK Thüringen auf einen privaten Auftragnehmer verbunden sind. Nachdem die AOK Thüringen zunächst das damals beauftragte Rechenzentrum in die eigene Organisation der AOK Thüringen eingegliedert hat, ist der Konzentrationsprozess in diesem Be-

reich weiter fortgeschritten. Mit Wirkung vom 1. Juli 1998 ist die AOK Thüringen der Arbeitsgemeinschaft AOK Rechenzentrum Mitte (ARGE-Mitte) beigetreten. Dabei handelt es sich um eine Arbeitsgemeinschaft nach § 219 Abs. 3 SGB V mit der ausschließlichen Zweckbestimmung, ein Rechenzentrum für die beteiligten AOK'n aus Hessen, Rheinland-Pfalz, dem Saarland und nun auch Thüringen bereitzustellen. Der Sitz der Arbeitsgemeinschaft befindet sich in Hessen, sodass primär für die datenschutzrechtliche Kontrolle dieser Arbeitsgemeinschaft der Hessische Datenschutzbeauftragte zuständig ist. Sofern die ARGE-Mitte Sozialdaten der AOK Thüringen im Auftrag nach § 80 SGB X verarbeitet, gehe ich jedoch davon aus, dass sich die ARGE-Mitte als Auftragnehmer gegenüber der AOK Thüringen verpflichtet, sich nach § 8 Abs. 6 ThürDSG vertraglich meiner Kontrolle zu unterwerfen, um sicherzustellen, dass mir eine datenschutzrechtliche Kontrolle über die von der AOK Thüringen automatisiert verarbeiteten Sozialdaten möglich bleibt. Obwohl die Möglichkeit für mich, bei der ARGE-Mitte eine datenschutzrechtliche Kontrolle durchzuführen, von den Beteiligten nicht bestritten wurde, sind bislang die vertraglichen Regelungen zwischen der AOK Thüringen und der ARGE-Mitte noch nicht um einen entsprechenden Passus ergänzt worden. Die AOK Thüringen geht davon aus, dass mein Kontrollrecht jedenfalls dadurch gewährleistet sei, dass ich sozusagen in Begleitung des Auftraggebers, hier also der AOK Thüringen, die datenschutzrechtlichen Vorkehrungen im Rechenzentrum der ARGE-Mitte überprüfen kann. Bei dieser Problematik geht es mir ausschließlich darum, dass meine Kontrollzuständigkeit gegenüber der AOK Thüringen uneingeschränkt erhalten bleibt.

11.18 Von der Chipkarte verfolgt

Im Berichtszeitraum wurde ich mehrfach von Bürgern eingeschaltet, die von ihrem Wahlrecht einer gesetzlichen Krankenversicherung Gebrauch gemacht hatten bzw. deren Versicherungspflicht durch Aufnahme einer selbständigen Tätigkeit endete, die jedoch einige Zeit später einen Brief von ihrer früheren Krankenkasse erhalten haben, in dem sie als „neues Mitglied“ der Kasse begrüßt wurden und dem gleichzeitig eine Krankenversichertenkarte beilag. Die Betroffenen, die teilweise schon jahrelang keinerlei Kontakt zu der

betreffenden Krankenkasse mehr hatten, vermuteten nun, dass mit ihren personenbezogenen Daten bei der Kasse nicht ordnungsgemäß umgegangen wurde. Meine Überprüfung hat ergeben, dass es sich um solche Fälle gehandelt hat, in denen die Krankenkasse als Einzugsstelle des Gesamtsozialversicherungsbeitrags tätig geworden ist. Nach den Vorschriften der § 28 ff. SGB IV i. V. m. der Datenerfassungs- und Datenübermittlungsverordnung (DEÜV) hat die Krankenkasse als Einzugsstelle die Pflicht, den Beitragssatz festzulegen sowie den jeweiligen Sozialversicherungsträgern die erforderlichen Daten und Gelder zu übermitteln. Sofern die Kasse vom Versicherten gewählt ist, darf sie in diesem Zusammenhang auch die auf sie entfallenden Krankenversicherungsbeiträge einbehalten. In einem Fall hatte nach dem Versicherungswechsel der Arbeitgeber diese Veränderung der Einzugsstelle nicht mitgeteilt, in einem anderen Fall wurde aufgrund einer Betriebsprüfung Jahre nach dem Ende der Versicherung die Betriebsnummer des Arbeitgebers korrigiert.

In allen Fällen hat sich die Krankenkasse eines hierfür von ihrem Bundesverband entwickelten EDV-Verfahrens bedient. Dieses war so programmiert, dass auch bei Korrekturen von Daten des Beitragsinzugs eine Neuanschuldung zur Krankenversicherung erfolgt, wobei automatisch ein Begrüßungsschreiben erstellt sowie eine Krankenversichertenkarte ausgestellt wird. Für die Fälle, in denen ausschließlich Korrekturen am Beitragskonto vorgenommen werden, ohne dass es zu einer tatsächlichen Neuanschuldung (sonst wird von einer sog. „Interimsmeldung“ gesprochen) kommt, muss der jeweilige Sachbearbeiter manuell die Ausstellung und den Versand einer neuen Chipkarte unterdrücken. Da es sich um ein bundesweit einheitliches Verfahren handelt und damit der Programmieraufwand nicht unerheblich ist, hat die Krankenkasse in einer Dienstanweisung, die jedem Sachbearbeiter vorliegt, ausdrücklich auf die manuelle Unterdrückung der Ausstellung einer Versichertenkarte im Fall von rückwirkenden Änderungen im Beitragskonto hingewiesen. Bei den überprüften Fällen ist dies jedoch aus Unachtsamkeit der betreffenden Kassenmitarbeiter unterblieben. Ich habe die Krankenkasse aufgefordert, bei ihrem Bundesverband nachdrücklich auf eine Programmänderung hinzuwirken, die eine automatische Unterdrückung der Ausstellung der Versichertenkarte bei rückwirkenden Korrekturen vorsieht. Dies wurde veranlasst. Aufgrund der Vorfälle hat die

Krankenkasse zudem die zuständigen Mitarbeiter nochmals ausdrücklich auf eine sorgfältige Prüfung der Kartenneuausstellung bei Korrekturen in den Beitragskonten bis zur technischen Lösung des Problems hingewiesen.

11.19 Veränderter ICD-10-Code im Abrechnungsverfahren

Die Pflicht zur Anwendung des ICD-10-Codes war aufgrund der öffentlichen Diskussion im Jahr 1996 durch eine Vereinbarung der Kassenärztlichen Bundesvereinigung sowie den Spitzenverbänden der Krankenkassen und der Deutschen Krankenhausgesellschaft für zwei Jahre ausgesetzt worden, um den Katalog umfassend zu überarbeiten (2. TB 11.18.2). Hauptkritikpunkte aus datenschutzrechtlicher Sicht waren die Tatsache, dass häufig vorkommende Diagnosen teilweise zu wenig Aufschlüsselungen aufwiesen und andererseits seltene, zum Teil nur in tropischen Gegenden vorkommende Krankheiten, sehr detailliert aufgeführt wurden. Darüber hinaus enthielten einige Schlüssel keine Diagnosen im engeren Sinne, sondern Rückschlüsse auf bestimmte Verhaltens- und Lebensweisen als Ursachen von Krankheiten. Schließlich wurde der Schlüssel den praktischen Anforderungen auch deshalb nicht gerecht, weil keine Differenzierungen z. B. hinsichtlich einer Verdachtsdiagnose oder einer Ausschlussdiagnose möglich waren und so möglicherweise ein verkürztes und damit falsches Bild von der abgerechneten Behandlung des Patienten entstehen konnte. Durch Bekanntmachung vom 24. Juni 1999 im Bundesanzeiger (Nr. 124, vom 8. Juli 1999, Seite 10985) des Bundesministeriums für Gesundheit wurde nunmehr eine Fassung des ICD-10-Codes (sog. ICD-10-SGB) mit Wirkung vom 1. Januar 2000 in Kraft gesetzt, die die datenschutzrechtlichen Kritikpunkte weitgehend berücksichtigt. Mit dem gleichzeitig in Kraft getretenen Gesundheitsreformgesetz 2000 ist in § 295 Abs. 1 Satz 3 SGB V und § 301 Abs. 2 SGB V die Ermächtigung geschaffen worden, wonach das BMG das Deutsche Institut für medizinische Dokumentation und Information (DIMI) beauftragen kann, den Schlüssel um Zusatzkennzeichen zu ergänzen. Zu der Frage, ob und in welcher Form eine bundeseinheitliche Anwendung des ICD-10-SGB auch tatsächlich erfolgt, liegen mir bislang keine Erkenntnisse vor.

11.20 Telefonische Beauskunftung von Sozialdaten

Im Rahmen einer Eingabe war ich auch mit der Frage befasst, unter welchen Voraussetzungen telefonische Auskünfte über Sozialdaten an die Betroffenen erteilt werden dürfen. Dabei geht es vor allem darum, wie ausgeschlossen werden kann, dass ein Anrufer unter Vorspiegelung einer falschen Identität sich die Auskunft von Sozialdaten Dritter erschleicht. Von einer Krankenkasse wurde mir in diesem Zusammenhang deren Dienstanweisung zum Schutz der Sozialdaten vorgelegt und mitgeteilt, dass Mitarbeiter der Kasse, die telefonische Auskünfte an Versicherte geben, in der Dienstanweisung darauf hingewiesen werden, die eindeutige Identität des telefonisch Anfragenden festzustellen. Darüber hinaus würden sensible Sozialdaten über Erkrankungen, Diagnosen, Zahlungsvorgänge oder Kontoverbindungen grundsätzlich nicht telefonisch offenbart. Zudem sei festgelegt, dass für den Fall, dass im Zusammenhang mit der telefonischen Anfrage der Anrufende nicht zweifelsfrei identifiziert werden kann, aus Sicherheitsgründen die Möglichkeit des Rückrufes genutzt werden soll oder der Anrufer gebeten wird, zwecks Klärung der Angelegenheit in der zuständigen Geschäftsstelle vorzusprechen. Diese mir gegenüber geschilderte Verfahrensweise fand zwar meine Zustimmung, doch war dies nur andeutungsweise in der Dienstanweisung geregelt. Insbesondere die Regelung, dass bei Zweifeln an der Identität des Betroffenen von der Möglichkeit des Rückrufs Gebrauch gemacht werden soll, war nicht enthalten. Gerade bei telefonischen Auskünften ist wegen den sehr eingeschränkten Kontrollmöglichkeiten der Identität des Anrufenden großer Wert drauf zu legen, dass die Mitarbeiter entsprechend unterwiesen sind und dies auch nachvollziehbar dokumentiert ist. Die Kasse hat mir daraufhin zugesagt, bei der nächsten Änderung der Dienstanweisung eine entsprechende Ergänzung vorzunehmen.

11.21 Führung der Pflegedokumentation bei häuslicher Pflege

Im Rahmen des Gedankenaustausches unter den Datenschutzbeauftragten des Bundes und der Länder wurde die Frage erörtert, unter welchen Voraussetzungen die Pflegekasse Einsicht in die vom Pflegedienst geführte Pflegedokumentation nehmen kann. Ich habe dies zum Anlass genommen, um bei einer Pflegekasse die dortige Ver-

fahrensweise in Erfahrung zu bringen. Zur Durchführung sowohl der vollstationären wie auch der teilstationären Pflege und der Kurzzeitpflege haben die Landesverbände der Pflegekassen mit den Vereinigungen der Träger der stationären Pflegeeinrichtungen Rahmenverträge nach § 75 Abs. 1 SGB XI geschlossen. Darin ist einerseits festgelegt, dass die Pflegeeinrichtung eine Pflegedokumentation sachgerecht und kontinuierlich zu führen hat, die u. a. die Pflegeanamnese, die Pflegeplanung, den Pflegebericht, Angaben über den Einsatz von Pflegehilfsmitteln und Angaben über durchgeführte Pflegeleistungen beinhaltet. Darüber hinaus hat die Pflegeeinrichtung die von ihr erbrachten Pflegeleistungen in einem Leistungsnachweis als Bestandteil der Pflegedokumentation aufzuzeichnen. Im Rahmen der Abrechnungen mit den Pflegekassen sind nur diese Leistungsnachweise vorzulegen. Dies ist auch sachgerecht, da im SGB XI den Pflegekassen keine Zuständigkeit zur Prüfung der Pflegebedürftigkeit oder der Einhaltung von Qualitätssicherungskriterien zukommt, da dies in den §§ 18 und 80 SGB XI allein dem MDK aufgrund seines Sachverständes übertragen ist und die Angaben zur Pflegeanamnese zum Teil sehr sensitive Angaben über den Betroffenen enthalten.

Die Pflegekasse hat mir mitgeteilt, dass im Rahmen der Abrechnungen bei Unstimmigkeiten des Leistungsnachweises die betroffenen Pflegedienste zur Abgabe einer kurzen Stellungnahme zur Frage der Pflegesituation des Pflegebedürftigen unter Einwilligung des Pflegebedürftigen aufgefordert werden. Anstatt dieser kurzen Stellungnahme würden Pflegedienste häufig den Pflegekassen eine Kopie der Pflegedokumentation übersenden. Damit werden jedoch der Pflegekasse eine Vielzahl von sensiblen Daten von den Pflegediensten übermittelt, obwohl letztlich nur einzelne Angaben überprüft werden müssen. Es würden hierdurch auch die Vorschriften umgangen, wonach zur Überprüfung der medizinischen Notwendigkeit von Pflegeleistungen grundsätzlich der MDK einzuschalten ist. Daher habe ich die Pflegekasse aufgefordert, ihre Verfahrensweise zu verändern. Diese hatte mitgeteilt, dass zukünftig der Pflegeantrag so geändert werden soll, dass nur unter bestimmten Voraussetzungen mit Einwilligung des Pflegebedürftigen die Pflegedokumentation von Beratern der Pflegekasse, an die sich der Pflegeversicherte selbst gewandt hat, eingesehen werden können. Somit gehe ich da-

von aus, dass eine Einsichtnahme in Pflegedokumentationen zur Klärung von Abrechnungsunterlagen durch die Pflegekasse künftig nicht mehr erfolgen.

11.22 Kontrolle bei der LVA Thüringen

Bereits im 2. TB (11.29) habe ich über die gegenseitige Beauftragung der Träger der gesetzlichen Rentenversicherung mit der Versichertenbetreuung berichtet und dabei auf die erforderlichen technischen und organisatorischen Maßnahmen hingewiesen, die ein unberechtigtes Aufrufen von Daten der bei den gesetzlichen Rentenversicherungsträgern in Deutschland gespeicherten Daten verhindern sollen. Dort habe ich auch über die von der LVA Thüringen getroffenen Dienstanweisungen berichtet, die diese Maßnahmen absichern sollen. Die Umsetzung dieser Schutzmaßnahmen habe ich jetzt vor Ort kontrolliert und zudem auch die Zugriffsmöglichkeiten innerhalb der LVA Thüringen auf die Versichertenkonten untersucht.

Bundesweites Zugriffsverfahren

Die Prüfung hat ergeben, dass im Rahmen des Zugriffs auf Versichertendaten anderer Rentenversicherer zum Zwecke der Beratung der Versicherten die von mir geforderten Maßnahmen alle auch in der Praxis umgesetzt wurden. Ein wichtiger Punkt war hier zunächst, dass der Kreis der Mitarbeiter der LVA Thüringen, die Zugriffsrechte auf die Daten aller gesetzlich rentenversicherten Personen in Deutschland erhalten, auf das unbedingt erforderliche Maß beschränkt wurde. Insgesamt haben etwa 70 Sachbearbeiter bei der LVA Thüringen ein solches Zugriffsrecht, bei dem sie auf einige Stammdaten wie die Versichertennummer und Adressen sowie auf die jeweiligen Versichertenkonten zugreifen können. Diese Mitarbeiter sind in so genannten Auskunft- und Beratungsstellen tätig, bei denen zwischen zwei und drei Mitarbeiter Zugriffe zu Beratungszwecken durchführen. Die Einrichtung dieser Zugriffsrechte erfolgt auf schriftliche Anweisung des jeweiligen Referatsleiters, wobei dem behördeninternen Datenschutzbeauftragten ein Mitspracherecht dergestalt eingeräumt wird, dass bei Verweigerung seiner Zustimmung die Entscheidung über die Einrichtung des konkreten Zugriffsrechts dem Geschäftsführer der LVA vorbehalten ist. Der Auskunftssuchende hat in der Auskunft- und Beratungsstelle nach

Feststellung seiner Identität durch einen Lichtbildausweis einen Antrag auf Auskunft und Beratung zu unterschreiben, in dem der Mitarbeiter der LVA Datum, Name, Vorname und Rentenversicherungsträger sowie den Anlass der Auskunft einzutragen und durch seine Unterschrift zu bestätigen hat. Der Auskunftssuchende hat dann die Möglichkeit, sich die Rentenauskunft am Bildschirm anzeigen und vom Bearbeiter erläutern zu lassen und/oder einen Ausdruck mitzunehmen. In jedem Fall wird im Versichertenkonto des zuständigen Rentenversicherungsträgers ein Datenschlüssel abgelegt, mit dem der Zeitpunkt und der zugreifende Rentenversicherungsträger protokolliert wird. Zudem werden bei der LVA in einer Kontrolldatei die Versichertennummer, Datum und Uhrzeit des Zugriffs sowie Referat und zugreifender Sachbearbeiter aufgezeichnet. Die schriftlichen Auskunftsanträge werden für sechs Monate aufbewahrt, sodass der behördeninterne Datenschutzbeauftragte in die Lage versetzt wird, durch einen Vergleich der Anträge mit den protokollierten Nutzungen eine mögliche missbräuchliche Nutzung des Verfahrens festzustellen. Eine derartige Kontrolle wurde bereits durch den behördeninternen Datenschutzbeauftragten der LVA Thüringen vorgenommen, bei der keine Anhaltspunkte für unzulässige Zugriffe festgestellt worden seien.

Einer im Rahmen der Kontrolle vorgelegten Übersicht des Verbands Deutscher Rentenversicherungsträger (VDR) war zu entnehmen, dass die Versicherten durchaus von dieser Serviceleistung Gebrauch machen. So wurden innerhalb eines bestimmten Monats bundesweit in etwa 31.000 Fällen Auskünfte vom nicht zuständigen Rentenversicherungsträger erteilt. Dabei spielten die Zugriffe von Mitarbeitern der LVA Thüringen auf Daten anderer Rentenversicherungsträger (etwa 100) und solcher auf die Datenbestände der LVA Thüringen (etwa 600) nur eine untergeordnete Rolle. Obwohl durchaus angemessene Vorkehrungen der LVA Thüringen getroffen wurden, um zu verhindern, dass Mitarbeiter der LVA Thüringen ohne dienstlichen Anlass z. B. aus Neugier und damit unbefugt auf die Millionen von Datensätzen zugreifen können, besteht der beste Schutz hiergegen darin, dass ein solcher Zugriff technisch erst überhaupt nicht möglich gemacht wird. Dies tritt mit dem Grundgedanken des Dialogisierungsverfahrens in Konflikt, den Versicherten bei allen Geschäftsstellen der Rentenversicherungsträger in Deutschland die

Möglichkeit zu eröffnen, entsprechende Auskünfte zu erhalten. Es dürfte jedoch eine Vielzahl von Versicherten geben, die im Verlauf ihres Berufslebens niemals den Rentenversicherungsträger gewechselt haben und für die daher eine solche Serviceleistung überhaupt nie in Betracht kommen wird. Eine technische Möglichkeit, einzelne Versichertenkonten vom Zugriff im Rahmen des Dialogisierungsverfahrens auszuschließen, war zum Zeitpunkt der Kontrolle nicht gegeben. Zwischenzeitlich wurde vom VDR, der für die programmtechnische Umsetzung des Verfahrens verantwortlich ist, auf Betreiben mehrerer Datenschutzbeauftragter eine solche technische Sperre des Zugriffs auf derartige Konten ermöglicht. Von der LVA Thüringen wurde mir mitgeteilt, dass nunmehr seit Anfang 1999 diejenigen Versicherten, die diesen Service nicht in Anspruch nehmen wollen, durch eine Erklärung bei der LVA Thüringen erreichen können, dass grundsätzlich keine Mitarbeiter anderer Rentenversicherungsträger auf ihr Versichertenkonto zugreifen können. Dadurch hat es nunmehr der Versicherte in der Hand, ob er von jeder Geschäftsstelle vom Rentenversicherungsträger in Deutschland derartige Auskünfte erhalten kann oder ob er hierauf verzichtet und damit zugleich den Kreis der potentiell Zugriffsberechtigten auf seine Daten erheblich einschränkt.

LVA-internes Verfahren

Bei den Zugriffsrechten auf die Versichertendaten innerhalb der LVA Thüringen stellt sich eine ähnliche Problematik, wenngleich es sich hier nicht um eine Auftragsdatenverarbeitung handelt, sondern um eine Nutzung der Daten innerhalb eines Sozialleistungsträgers. Auf die Daten der ca. 1,5 Millionen Versicherten haben von den etwa 1500 Beschäftigten ca. $\frac{3}{4}$ einen lesenden Zugriff auf die in einem vernetzten Verfahren gespeicherten Daten. Der Grund für diese weit gehenden Zugriffsrechte liegt darin, dass bei der Bearbeitung eines Rentenvorgangs sehr häufig auf Versichertenkonten von bei der LVA Thüringen versicherten Familienangehörigen zugegriffen werden muss. Nach Nr. 5 der Anlage zu § 78 a SGB X sind die Sozialleistungsträger verpflichtet, Maßnahmen zu treffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (sog. Zugriffskontrolle). Hierbei trifft die speichernde Stelle auch die Pflicht, die Zu-

griffsrechte nicht umfassender einzurichten als für die Aufgabenerfüllung erforderlich. Wenn jedoch aus den oben genannten Gründen ein sehr großer Kreis jedenfalls lesenden Zugriff auf alle Versichertenaten der LVA Thüringen eingeräumt bekommt, so müssen zusätzliche organisatorische Maßnahmen ergriffen werden, um eine missbräuchliche Nutzung durch Mitarbeiter der LVA Thüringen zu verhindern. Daher habe ich von der LVA Thüringen gefordert, dies zukünftig bei der Weiterentwicklung der Softwarelösungen dergestalt einzubeziehen, dass die technischen Zugriffsmöglichkeiten dem erforderlichen Umfang angepasst werden können. Bis dahin sollten die lesenden Zugriffe zumindest stichprobenartig protokolliert und ausgewertet werden.

In meiner Forderung wurde ich im Nachgang der Kontrolle durch eine Eingabe bestärkt. Darin hat sich der frühere Ehemann einer Mitarbeiterin der LVA Thüringen bei mir darüber beschwert, dass seine frühere Ehefrau sinngemäß zum Ausdruck gebracht habe, sie sei jederzeit über dessen Bruttoeinkommen informiert, da diese Angaben in der EDV eingespielt seien und sie aufgrund ihrer Arbeit als Sachbearbeiterin Zugriff auf diese Daten habe. Dies habe ich zum Anlass genommen, bei der LVA Thüringen nochmals die stichprobenartigen Protokollierungen der lesenden Zugriffe einzufordern. Von dort wurde mir mitgeteilt, dass die lesenden Zugriffe der Sachbearbeiter durch den behördeninternen Datenschutzbeauftragten stichprobenartig protokolliert und ausgewertet werden. Die Überprüfung des konkreten Falles hat anhand der Auswertung von Protokollaufzeichnungen keine unberechtigten Zugriffe der Mitarbeiterin ergeben. Darüber hinaus wurde diese Mitarbeiterin im Speziellen sowie alle Mitarbeiter der LVA Thüringen über die Möglichkeit der Protokollierung und Prüfung der lesenden Zugriffe informiert und gleichzeitig darauf hingewiesen, dass ein Zugriff auf Versichertenaten ausschließlich im Zusammenhang mit der Sachbearbeitung zulässig ist. Den behördeninternen Datenschutzbeauftragten der LVA habe ich aufgefordert, diese konkrete Mitarbeiterin in die zukünftigen Stichprobenkontrollen einzubeziehen.

Telearbeit bei Betriebs- und Einzugsstellenprüfung

Im Rahmen der Kontrolle der automatisierten Datenverarbeitung der LVA Thüringen wurde ich auch mit der Durchführung von Telear-

beit (15.13) im Bereich der Betriebs- und Einzugsstellenprüfung durch Mitarbeiter der LVA Thüringen konfrontiert. Das noch in der Aufbauphase stehende Projekt sah vor, dass den Mitarbeitern der Einzugsstellen und Betriebsprüfung über eine ISDN-Leitung die für die Betriebsprüfungen erforderlichen Daten auf einen von der LVA Thüringen zur Verfügung gestellten PC überspielt werden sollte. Hierbei war zunächst nicht vorgesehen, die Daten zu verschlüsseln. Obwohl die Sicherheit bei ISDN-Wählleitungen höher einzuschätzen ist als bei Internetverbindungen, habe ich die LVA aufgefordert, wegen der Sensibilität der Daten diese nur verschlüsselt zu übertragen. Zur Durchführung der Telearbeit wurde zwischen der LVA Thüringen und dem dortigen Personalrat eine Dienstvereinbarung abgeschlossen. Darin sind ausreichende organisatorische Maßnahmen hinsichtlich der Datensicherheit und des Datenschutzes bei Telearbeitsplätzen getroffen, wie z. B. die verschlüsselte Speicherung der Daten oder den Einsatz von Passworten etc..

11.23 Sozialhilfedatenabgleich

Seit dem 1. Januar 1998 ist die Sozialhilfedatenabgleichsverordnung in Kraft, die regelmäßige Abgleiche der Daten der Sozialhilfeträger mit denen der Bundesanstalt für Arbeit und den Trägern der gesetzlichen Unfall- und Rentenversicherungen Daten über erbrachte Sozialleistungen ermöglicht, um eventuell missbräuchliche Inanspruchnahme von Sozialleistungen zu entdecken. Bereits im Verfahren zum Erlass der Rechtsverordnung habe ich Zweifel daran geäußert, ob der regelmäßige Abgleich der Daten aller Sozialhilfeempfänger noch als verhältnismäßig anzusehen ist (2. TB 11.3), weil bislang keinerlei verlässliche Zahlen dazu vorlagen, dass ein massenhafter Missbrauch seitens der Sozialhilfeempfänger festzustellen war. Das Bundesgesundheitsministerium hat sich dieser Frage auf Drängen des BfD angenommen und ein Sozialforschungsinstitut mit der erfolgskontrollierenden Begleitung der Einführung des Sozialhilfedatenabgleichs beauftragt. Ergebnisse hierzu liegen noch nicht vor.

Ich habe mich bei einem Sozialhilfeträger, der als einziger Thüringer Stelle in diese Begleitforschung einbezogen ist, über den Umsetzungsstand der Sozialhilfedatenabgleichsverordnung informiert. Vor der Durchführung des erstmaligen Datenabgleiches hat der Sozialhil-

feträger durch Pressemitteilungen und im Sozialamt ausgehängte Informationsblätter die Sozialhilfeempfänger auf den bevorstehenden Datenabgleich hingewiesen und diesen die Möglichkeit gegeben, eventuell „vergessene“ Angaben unverzüglich nachholen zu können, ohne dass Strafanzeige erstattet wird. Wegen technischer Schwierigkeiten konnte der Sozialhilfeträger am Datenabgleich für das 1. Quartal 1998 nicht teilnehmen. Der Datenabgleich für das 2. Quartal 1998 hat ergeben, dass ein sehr geringer Anteil von Treffermeldungen von der Datenstelle des Verbandes der Rentenversicherungsträger (VDR) zurückgemeldet wurde. Von etwa 9.000 Anfragedatensätzen waren nur etwa 280 Treffer, was etwa einer Quote von 3 % entspricht. Da allgemein bekannt ist, dass die Datei über geringfügige Beschäftigte beim VDR vielfach deshalb unkorrekte Angaben enthält, weil Arbeitgeber ihre geringfügigen Beschäftigungsverhältnisse oft nicht abmelden, nachdem diese beendet wurden, hat der Sozialhilfeträger aus datenschutzrechtlicher Sicht die richtige Verfahrensweise gewählt: Bevor zur Aufdeckung möglicher Missbrauchsfälle an Dritte herangetreten wird, und damit möglicherweise die Betroffenen zu Unrecht dem Verdacht ausgesetzt werden, sie hätten Sozialleistungen missbräuchlich in Anspruch genommen, werden mit allen Betroffenen zunächst Anhörungen durchgeführt, bei der sich in vielen Fällen die Treffer durch objektive Gegebenheiten erklären lassen (wie z. B. ein zwischenzeitlich beendetes, aber noch nicht beim VDR gemeldetes geringfügiges Beschäftigungsverhältnis). Damit verringerte sich der Anteil der tatsächlichen Missbrauchsfälle noch erheblich, sodass bereits jetzt davon ausgegangen werden kann, dass ein massenhafter Missbrauch von Sozialleistungen, der in der Diskussion zur Schaffung der Rechtsgrundlagen der Sozialhilfedatenabgleichsverordnung beschworen wurde, wohl nicht feststellbar ist. Was die Verhältnismäßigkeit des Eingriffs aber auch den Aufwand, den die Sozialämter betreiben, um diesen Datenabgleich durchzuführen, im Vergleich zur tatsächlich festgestellten Höhe von missbräuchlich in Anspruch genommenen Sozialleistungen anlangt, bleibt das Ergebnis der bundesweiten Begleitforschung abzuwarten.

11.24 Zusätzlicher Datenaustausch bei Sozialleistungen

Eine Arbeitsgruppe der Arbeits- und Sozialministerkonferenz von Bund und Ländern (ASMK) hat im Jahre 1998 Vorschläge erarbeitet, inwieweit ein zusätzlicher Datenaustausch bei Sozialleistungen zum effektiveren Mitteleinsatz und zur Verhinderung von Sozialleistungsmissbrauch eingeführt werden könnte. Zu diesem umfangreichen Änderungsvorschlägen hat die Konferenz der Datenschutzbeauftragten von Bund und Ländern in einer EntschlieÙung vom 20. Oktober 1997 darauf hingewiesen, dass bei den gemachten Vorschlägen Einschränkungen des Sozialdatenschutzes nur dann in Betracht kommen, wenn sie tatsächlich erforderlich und verhältnismäßig sind, sowie die Datenflüsse für den Bürger transparent bleiben (2. TB 11.2). Zwischenzeitlich sind einige dieser Vorschläge bereits in Form von Gesetzesänderungen umgesetzt worden. So wurde beispielsweise mit Wirkung zum 1. Januar 1998 durch das Erste SGB III Änderungsgesetz ein neuer § 67 e SGB X eingefügt, der es der Bundesanstalt für Arbeit und der Bundeszollverwaltung erlaubt, bei ihren Außenprüfungen auch bestimmte für andere Leistungsträger wichtige Daten mitzuerheben und dem zuständigen Leistungsträger zu übermitteln. Eine weiter gehende Reaktion der Arbeitsgruppe der ASMK auf die von den Datenschutzbeauftragten vorgebrachten Bedenken gegen die Vorschläge liegt bislang nicht vor. Allerdings hat das Bundesministerium für Arbeit und Sozialordnung erfreulicherweise in einer Stellungnahme an die Arbeitsgruppe in zahlreichen Punkten die Einschätzung der DSB bezüglich einer fehlenden Erforderlichkeit der vorgesehenen Datenaustausche geteilt. Die Datenschutzbeauftragten haben erklärt, dass sie auch weiterhin ihr Gesprächsangebot zu den Vorschlägen aufrechterhalten. Gegenüber dem TMSG habe ich nochmals betont, dass ich die Auffassung des BfD, wonach regelmäßige Datenabgleiche in der öffentlichen Verwaltung einer speziellen gesetzlichen Ermächtigungsgrundlage bedürfen, nachdrücklich von mir unterstützt wird. Bevor weitere regelmäßige Datenabgleichsverfahren eingeführt werden oder gar eine für den Bereich der sozialen Sicherung allgemeine Ermächtigungsgrundlage für regelmäßige Datenabgleiche geschaffen wird, sollten die Erfahrungen mit den bereits existieren-

den Datenabgleichsverfahren einer eingehenden Analyse unterzogen werden (11.23).

12. Statistik

12.1 Volkszählung 2001

Volkszählungen sind sowohl national wie auch international das Fundament der amtlichen und nicht amtlichen Statistik. Sie zeichnen ein in sich abgeschlossenes aber vielseitig verwendbares Gesamtbild der Gesellschaft, des Staates und der Wirtschaft. In der Vergangenheit wurden Volkszählungen stets in Form von Primärerhebungen unmittelbar beim Bürger in größeren Zeitabständen durchgeführt. In den dazwischen liegenden Zeiträumen erfolgte eine Fortschreibung der Daten aufgrund laufender statistischer Berichterstattungen sowie durch Stichprobenerhebungen (z. B. Mikrozensus, Gebäude- und Wohnungszählung). Auf der Grundlage einer EU-Leitlinie aus dem Jahr 1997 ist beabsichtigt, im Jahr 2001 im Gemeinschaftsgebiet der EU Volkszählungen durchzuführen. Aus Kosten- und Akzeptanzgründen hatte aber bereits 1996 die Bundesregierung einen Methodenwechsel dahingehend beschlossen, dass künftige Zensen weitgehend als Sekundärerhebungen durch die Nutzung und Zusammenführung von Daten vorhandener Register durchgeführt werden sollen. Unter diesem Aspekt werden der EU für die gemeinschaftliche Zählung im Jahr 2001 im Wesentlichen nur fortgeschriebene Bevölkerungszahlen gemeldet und gegenwärtig geprüft, in welcher Form, in welchem Umfang und welcher Auswertungstiefe in den kommenden Jahren in der Bundesrepublik eine Volkszählung durchgeführt werden soll. Dazu liegen zwei Modelle zur Diskussion vor. Das sog. Bundesmodell stützt sich im Wesentlichen auf nur drei Quellen (Einwohnermelderegister, Dateien und Statistiken zur Erwerbstätigkeit, Ergebnisse des Mikrozensus), während das sog. Ländermodell eine zusätzliche primärstatistische Gebäude- und Wohnungszählung sowie Ergänzungsstichproben im erwerbstätigen Bereich vorsieht. Entsprechend dieser unterschiedlichen Datenbasis ist die Ergebniserstellung beim Ländermodell wesentlich umfangreicher und in einer tieferen Gliederung (bis auf Kreis- und Gemeindeebene) möglich, während das Bundesmodell vor allem den Anforderungen der EU für Ländervergleiche entspricht. Aus der Sicht des Datenschut-

zes ist insoweit zwangsläufig der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen beim Ländermodell aufgrund des umfangreicheren Datenfonds und der vorgesehenen Verknüpfungen der Daten gegenüber dem Bundesmodell weitaus größer. Unabhängig davon, für welches Modell man sich entscheiden wird, bedarf es in jedem Fall normenklarer gesetzlicher Vorgaben zum Verfahren sowie insbesondere auch zu den technischen und organisatorischen Maßnahmen, die die Trennung von Statistik und Verwaltungsvollzug bei einem künftigen Zensus durchgängig, d. h. beginnend mit der Erhebung oder Zusammenführung von Registern (z. B. bei der Klärung von Widersprüchen) bis zur Veröffentlichung der Ergebnisse gewährleistet. Gegenwärtig laufen die Vorbereitungen einer Testerhebung zur Gewinnung von Erkenntnissen über die Qualität der zur Nutzung vorgesehenen Register (z. B. der Melderegister im Hinblick auf Mehrfachfälle oder Fehlbestände und deren Korrekturmöglichkeiten), zur Prüfung von Verfahren zur effektiven Gebäude- und Wohnungszählung, zur Haushaltsgenerierung sowie zur Zusammenführung der Register. Positiv ist in diesem Zusammenhang das Bemühen der Verantwortlichen sowohl auf Bundes- wie auch auf Landesebene hinsichtlich einer frühstmöglichen Einbeziehung der Datenschutzbeauftragten zur Beurteilung datenschutzrechtlicher Fragen zu bewerten. Insoweit habe und werde ich auch weiterhin im Rahmen meiner Möglichkeiten dieses Vorhaben kritisch aber auch konstruktiv begleiten.

12.2 Umsetzung des Hochbaustatistikgesetzes

Mit Inkrafttreten des Gesetzes über die Statistik der Bautätigkeiten im Hochbau und der Fortschreibung des Wohnungsbestandes (Hochbaustatistikgesetz) vom 1. Januar 1999 verloren die bisherigen Regelungen zur Durchführung der Statistik der Bautätigkeit und der Fortschreibung des Gebäudebestandes vom 27. Juli 1998 ihre Gültigkeit. In Umsetzung der bis Ende 1998 gültigen Rechtsvorschriften waren in Thüringen wie auch in vielen anderen Bundesländern die Bauherren auf der Grundlage von Verwaltungsvorschriften zur Abgabe ihrer Erhebungsbögen bei den Gemeinden bzw. Aufsichtsbehörden zur Weiterleitung an das zuständige Landesamt für Statistik verpflichtet. Diese Verfahrensweise war in der Vergangenheit bereits von Datenschutzbeauftragten kritisiert worden, da dadurch ohne

eine entsprechende Rechtsgrundlage die Trennung zwischen Statistik und Verwaltungsvollzug durchbrochen wurde. Im nunmehr geltenden Hochbaustatistikgesetz ist die Auskunftspflicht neu geregelt. Danach sind die Bauaufsichtsbehörden, die Bauherren und die mit der Baubetreuung Beauftragten sowie die Gemeinden und Gemeindeverbände zur Auskunft verpflichtet. Desweiteren werden die Landesregierungen ermächtigt, durch Rechtsverordnung näheres zur Auskunftspflicht zu bestimmen. In der Gesetzesbegründung heißt es dazu, dass die Vorschrift die Auskunftspflicht festlegt und allgemein die infrage kommenden Auskunftspflichtigen benennt und die Länder ihren bauordnungsrechtlichen Verhältnissen entsprechend spezifische Regelungen schaffen werden, um eine vollständige Erfassung der Erhebungseinheiten und der Erhebungsmerkmale sicherzustellen. Die Auskunftspflicht besteht, soweit vom Gesetzgeber nichts weiteres bestimmt ist, nach dem Bundesstatistikgesetz ausschließlich gegenüber den mit der Bundesstatistik amtlich betrauten Stellen. Dies ist in Thüringen nach dem Thüringer Statistikgesetz das TLS. Die Einrichtung zusätzlicher Erhebungsstellen, die im Übrigen zur Gewährleistung des Statistikgeheimnisses vom Verwaltungsvollzug zu trennen sind, ist nach dem Gesetz für die Durchführung der Hochbaustatistik nicht vorgesehen. Insoweit ist die Vorgabe eines Informationsweges, die den Bauherren verpflichtet, seinen Erhebungsbogen bei der Bauaufsichtsbehörde zur Weiterleitung an das TLS abzugeben ebenso wie eine Vorschrift, die die Gemeinde anweist ihre Meldung über die Bauaufsichtsbehörde an das TLS zu übergeben, ein Verstoß gegen das Trennungsgebot zwischen Verwaltungsvollzug und Statistik. Gerade durch die Neuregelung im Hochbaustatistikgesetz, wonach auch die Zulässigkeit einer Übermittlung von Einzeldaten von den statistischen Ämtern der Länder an die Gemeinden und Gemeindeverbände auf statistische Stellen beschränkt wird, wenn dort durch Landesgesetz eine Trennung dieser Stellen von anderen kommunalen Verwaltungen sichergestellt ist und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist, unterstreicht die Forderung des Gesetzgebers nach einer vollständigen Trennung von Verwaltung und Statistik bei dieser Erhebung. Dies ist aber bei dem gegenwärtig in Thüringen noch praktizierten Verfahren nicht gewährleistet. Nach wie vor wird auf der Grundlage eines Erlasses des TIM aus dem Jahre 1992 in Umsetzung der nur bis Ende 1998 gültigen Rechtsvorschriften die Erhe-

bung der Daten von den Bauherren und Gemeinden über die Untere Bauaufsichtsbehörde geleitet. Die bisherige Argumentation, dass die Baubehörden dadurch keine weiteren Daten der Bauherren zur Kenntnis erhalten, als die ihnen ohnehin aus den Bauantragsunterlagen bekannten, bestätigten sich bei einer Kontrolle nicht, wobei auch, wenn die Bauaufsichtsbehörden keinerlei zusätzliche Informationen erhalten würden, nach meiner Auffassung eine Verknüpfung der Statistikbögen mit dem Bauantrag derart, dass ohne deren Abgabe keine Bearbeitung des Bauantrags erfolgt, unzulässig sein dürfte. Aufgrund der Feststellung, dass die Bauaufsichtsbehörden tatsächlich ohne Rechtsgrundlagen die Funktion von Erhebungsstellen wahrnehmen, indem von ihnen nicht nur der Einzug, sondern auch die Kontrolle sowie die Klärung von Rückfragen mit den Auskunftspflichtigen wahrgenommen wird und sie dabei Informationen erhalten, die über die ihnen im Rahmen ihrer originären Aufgabenerfüllung vorliegenden Daten hinausgehen, habe ich das zuständige Ministerium um eine alsbaldige Neuregelung gebeten. In der mir vorliegenden Stellungnahme wurde ich zwischenzeitlich darüber informiert, dass mit Blick auf die statistik- und datenschutzrechtliche Problematik eine Änderung des Erhebungsweges mit dem Ziel der Einhaltung des Trennungsgebotes zwischen Verwaltungsvollzug und Statistik vorgesehen ist und die dazu notwendigen Abstimmungen mit den beteiligten Stellen bereits veranlasst sind.

12.3 Was haben statistische Einzeldaten mit einer „Windhose“ zu tun?

Auf einem Sportplatz in Göttingen war von Passanten beobachtet worden, wie von einem benachbarten Recyclingbetrieb durch eine Windhose aufgewirbeltes Altpapier auf den Sportplatz getragen wurde. Beim genauen hinsehen stellte sich heraus, dass darunter auch eine Unterlage des TLS mit Personenbezug war. Die Lokalpresse schaltete sich ein und fragte beim TLS nach, wie diese Unterlagen nach Göttingen gelangt sind. Daraufhin informierte mich das TLS sofort über den Vorfall.

Bei einem Kontrollbesuch im TLS stellte sich heraus, dass zur Vernichtung im Keller des TLS bereitgestellte Einzelbögen der Bevölkerungsstatistik (Zählkarten über Geburten, Eheschließungen etc.)

versehentlich den Mitarbeitern eines Recyclingbetriebes mitgegeben worden waren, als diese gewöhnliches Altpapier ohne personenbezogenen Inhalt abholten. Die Mitarbeiter des Recyclingbetriebes brauchten keine Veranlassung zu besonderen Sicherheitsmaßnahmen zu haben, mussten sie doch davon ausgehen, Altpapier ohne personenbezogenen Inhalt entgegengenommen zu haben. Wäre nicht die so genannte „Windhose“ in Göttingen aufgetreten, so wäre dieses Versehen überhaupt nicht aufgefallen und die Unterlagen wären ohne Aufsehen recycelt worden. Dies ist wohl auch mit dem übrigen Teil des personenbezogenen Schriftguts geschehen, da im Ergebnis der Nachforschungen der Polizei außer dem von Passanten gefundenen Zählblatt über die Bevölkerungsstatistik keine weiteren personenbezogenen Unterlagen des TLS aufgefunden wurden und das Entsorgungsunternehmen versichert hat, den Rest der Ladung ordnungsgemäß vernichtet zu haben. Obwohl die organisatorischen Regelungen des TLS vorsahen, dass personenbezogenes Schriftgut getrennt vom übrigen Altpapier zu entsorgen ist, konnte es zu der Verwechslung kommen, weil in dem Lagerraum sowohl personenbezogenes Schriftgut als auch gewöhnliches Altpapier zum Abtransport lagerte. Trotz der Tatsache, dass nachweislich nur ein Zählbogen aus der Bevölkerungsstatistik aufgefunden wurde, war der Vorfall als ein Verstoß gegen die Geheimhaltungsvorschrift des § 16 Abs. 1 BStatG i. V. m. § 9 Abs. 3 ThürDSG zu bewerten, den ich gegenüber dem TLS beanstandet habe. Das TLS hat unverzüglich die Konsequenzen aus dem Vorfall gezogen, indem die Entsorgung jeglichen Altpapiers - ob mit personenbezogenem Inhalt oder nicht - im TLS durch eigene Mitarbeiter mit einem Aktenvernichter durchgeführt wird. Der Fall zeigt anschaulich, dass die besten datenschutzrechtlichen Vorkehrungen innerhalb einer Stelle untauglich werden können, wenn die Überwachung der Daten bis zur nachweislichen und vollständigen Vernichtung nicht sichergestellt ist.

12.4 Erhebung von Daten zur Durchführung vorbereitender Untersuchungen im Zusammenhang mit städtebaulichen Sanierungsmaßnahmen

Zur Beurteilung der Sanierungsbedürftigkeit von Stadtgebieten sowie zur Vorbereitung und Durchführung der Sanierung dürfen nach dem Baugesetzbuch von den Eigentümern und Bewohnern der be-

troffenen Grundstücke personenbezogene Daten mit Auskunftspflicht über ihre persönlichen Lebensumstände im wirtschaftlichen und sozialen Bereich, namentlich über die Berufs-, Erwerbs- und Familienverhältnisse, das Lebensalter, die Wohnbedürfnisse, die sozialen Verpflichtungen sowie über die örtlichen Bindungen erhoben werden. Voraussetzung ist lediglich der Beschluss der Gemeinde über den Beginn vorbereitender Untersuchungen zur Festlegung eines Sanierungsgebietes. Obwohl die Daten nicht zur Regelung von Einzelfällen, sondern regelmäßig zur statistischen Aufbereitung und Auswertung erhoben werden, finden für sie die Vorschriften über Kommunalstatistiken keine Anwendung. Dennoch unterliegen die Daten einer ausdrücklichen Zweckbindung und dürfen nach dem Willen des Gesetzgebers mit einer Ausnahme (der Übermittlung an Finanzbehörden zur Besteuerung) nur für Zwecke der Sanierung verwendet werden.

Während die Durchführung einer Statistik im Kommunalbereich einer Satzung bedarf, in der die Erhebungs- und Hilfsmerkmale konkret benannt werden müssen, ist es bei obigen Untersuchungen Aufgabe der Baubehörde die für die Beurteilung der Sanierung notwendigen und geeigneten Datenarten über die Lebensumstände der Eigentümer und Bewohner zu bestimmen. Wie ich feststellen musste, führt dies mitunter zu Anfragen und Eingaben, da von den Baubehörden die im Baugesetzbuch enthaltenen Vorgaben zum zulässigen Umfang der Datenerhebung teilweise auch sehr weit ausgelegt werden, was zu Unverständnis bei den Betroffenen führt. In jedem Fall ist aber zu beachten, dass der Umfang der Erhebung von Daten für die vorbereitenden Untersuchungen eines künftigen Sanierungsgebietes für den Betroffenen eindeutig erkennbar und eine Vermischung mit anderen Erhebungen ausgeschlossen wird. Dies war von einer Stadt nicht beachtet worden. Da neben den Untersuchungen für das Sanierungsgebiet zeitgleich auf der Grundlage einer Satzung auch eine statistische Erhebung über kommunale und soziale Fragen im Stadtgebiet durchgeführt wurde, hatte man, da ein Teil der Fragen im Statistikbogen durchaus auch für Sanierungsfragen von Interesse waren, den Bewohnern im vorgesehenen Sanierungsgebiet kurzerhand beide Bögen zugesandt. In dem Anschreiben wurde dabei unter Hinweis auf die Auskunftspflicht lediglich darüber informiert, dass die Fragebögen zu vorbereitenden Untersuchungen des vorgesehenen Sanierungsgebietes erhoben werden. Ungeachtet

dessen, dass damit gegen die Festlegung in der Statistiksatzung bezüglich des vorgesehenen Stichprobenumfangs verstoßen wurde, entstand bei den Befragten der Eindruck, dass sich ihre Auskunftspflicht nach dem Baugesetzbuch gleichfalls auf die statistische Erhebung bezog, die jedoch nach Satzung ohne Auskunftspflicht vorgesehen war. Mehrere Bürger hatten sich deshalb an mich gewandt, mit der Bitte um eine Prüfung der Rechtmäßigkeit der Erhebung. Im Ergebnis dessen wurden alle betroffenen Einwohner unverzüglich in einem Rundschreiben über den tatsächlichen Sachverhalt informiert und gebeten, den Statistikbogen nicht zurückzusenden und eigenverantwortlich zu vernichten. Die in die Stichprobe für die Statistik einbezogenen Haushalte erhielten erst nach Abgabe der Fragebögen für die vorbereitenden Untersuchungen des vorgesehenen Sanierungsgebietes den für die Statistik bestimmten Erhebungsbogen, sodass weitere Missverständnisse ausgeschlossen werden konnten.

13. Bildung, Wissenschaft und Forschung

13.1 Datenerhebungen für schulärztliche Untersuchungen

In den beiden vorangegangenen Tätigkeitsberichten (1. TB 13.1; 2. TB 13.1) hatte ich bereits auf die noch ausstehende Verordnung zur Schulgesundheitspflege hingewiesen. Dies ist auch insoweit bedauerlich, da insbesondere mit den Vorsorgeuntersuchungen gegenwärtige oder zu erwartende Gesundheits- oder Entwicklungsstörungen der Kinder frühzeitig erkannt und behandelt werden sollen und die mit den Untersuchungen verbundenen Datenerhebungen ausschließlich auf das Wohl der Kinder gerichtet sind. Da aber für öffentliche Stellen beim Umgang mit personenbezogenen Daten das Verbotsprinzip mit Erlaubnisvorbehalt gilt, können die Daten, soweit nicht in Rechtsvorschriften entsprechende Regelungen aufgenommen sind, nur mit Zustimmung der Betroffenen erhoben werden. Anfragen zu Problemen der schulärztlichen Untersuchungen zeigen, dass in diesem Bereich durchaus ein Bedürfnis nach Rechtssicherheit bei allen Beteiligten besteht. Es wäre deshalb zu wünschen, dass hier durch die noch vorhandene Verordnungslücke geschlossen wird. Praktische Fragen ergeben sich aus datenschutzrechtlicher Sicht im Bereich der Schulgesundheitspflege vor allem bei der Erhebung von Daten bei bzw. im Vorfeld schulärztlicher Untersuchungen.

gen, weil Unsicherheiten darüber bestehen, ob und in welchem Umfang es sich um „Pflichtuntersuchungen“ handelt und inwieweit die Eltern gegenüber dem Schularzt zur Auskunftserteilung verpflichtet sind. Aufgrund der fehlenden konkreten Regelungen zur Schulgesundheitspflege werden gegenwärtig im Vorfeld von Untersuchungen Daten zum sozialen Umfeld des Schülers, über seine überstandenen Krankheiten und gesundheitliche Störungen bei den Eltern auf freiwilliger Grundlage mittels Fragebögen erhoben. Mitunter werden aber die Betroffenen über die Freiwilligkeit nicht ausdrücklich informiert. Bezüglich des Umfangs der Datenerhebung ist desweiteren der Erforderlichkeitsgrundsatz zu beachten, wobei aufgrund der Vielfalt der Einflussfaktoren auf die Gesundheit und die körperliche und geistige Entwicklung der Kinder die Grenzen dafür mitunter schwer erkennbar sind. Es ist deshalb im besonderen Maße notwendig, die zu erhebenden Daten sorgfältig auszuwählen und die Notwendigkeit den Betroffenen unter Hinweis auf die Zweckbindung der Daten und ihre Vertraulichkeit zu erläutern. Dass fehlende Informationen und Hinweise auch zu Misstrauen führen können, zeigte sich in einem Fall, wo sich Eltern durch den Inhalt des Fragebogens „kontrolliert“ fühlten. Ihnen waren im Vorfeld der jährlich in einer Förderschule durchgeführten Untersuchungen stets die gleichen Fragebögen mit den gleichen Fragen (Angaben zu den Eltern und Geschwistern, überstandene Krankheiten) worden ohne einen Hinweis übergeben, dass die Angaben zur Aktualisierung der beim Schularzt vorliegenden Schülerakte vorgesehen und deshalb nur die Veränderungen seit der letzten Untersuchung mitzuteilen sind. Gemeinsam mit dem zuständigen Gesundheitsamt konnte hier durch geringfügige Ergänzung im Erhebungsbogen die bestehenden Missverständnisse ausgeräumt werden.

13.2 Datenschutz bei Chroniken und Jahrbüchern von Schulen

Eine Schule erkundigte sich bei mir, inwieweit es datenschutzrechtlich zulässig wäre, im Jahrbuch der Schule eine Liste der Lehrer mit Vor- und Zunamen sowie von Klassenlisten, bei denen die Schüler ebenfalls mit Vor- und Zunamen genannt werden sollten, abzudrucken. Ich machte die Schule darauf aufmerksam, dass eine Veröffentlichung personenbezogener Daten der Schüler und Lehrer nach

§ 57 Abs. 6 Thüringer Schulgesetz (ThürSchulG) nur zulässig ist, sofern der Veröffentlichung nicht widersprochen wird. Auf das Recht der Betroffenen, der Aufnahme ihrer Daten zu widersprechen, ist dabei „in geeigneter Weise“ hinzuweisen. Der unbestimmte Rechtsbegriff „in geeigneter Weise“ ist dahingehend zu interpretieren, dass der Betroffene nicht im Einzelnen auf die Widerspruchsmöglichkeit hinzuweisen ist, sondern es ausreicht, dies in einer allgemeinen Form, z. B. in ortsüblicher Weise, durchzuführen.

13.3 Listen über Teilnahme am Religionsunterricht

In einer Eingabe informierte mich ein Bürger darüber, dass ein Schulamts von den Schulen im Zuständigkeitsbereich regelmäßig Listen anfordert, auf denen die Namen aller Schüler aufgeführt sind, die am Religionsunterricht teilnehmen. Nach Auskunft durch das Schulamts erfolgte die Anforderung solcher Listen lediglich einmalig und auch nur für das Fach Katholische Religionslehre. Das Schulamts wäre koordinierend tätig geworden, da für ein Schulfach mindestens eine Zahl von 8 Schülern zusammenkommen müsse und in manchen Schulen nur 1-2 Schüler vorhanden sind, die an diesem Schulfach teilnehmen. Die Listen seien zwischenzeitlich vernichtet worden. Ich habe dem Schulamts abschließend mitgeteilt, dass es für die Zusammenstellung von Unterrichtsgruppen ausgereicht hätte, von den Schulen lediglich statistisches Zahlenmaterial über die Klassenstufe und Anzahl der Schüler zu erheben.

13.4 Klassentreff Agentur

Eine Firma, deren Geschäftsidee darin liegt, bundesweit Klassentreffen von ehemaligen Schülern zu organisieren, fragte bei mir an, ob die Anwendung des sog. Adressmittlungsverfahren (1. TB 5.2.5, 13.3.1) aus datenschutzrechtlicher Sicht zulässig ist. Ich habe der Firma mitgeteilt, dass gegen das Verfahren grundsätzlich keine datenschutzrechtlichen Bedenken bestehen. Eine Verpflichtung der Schulen, die von der Firma übergebenen und zuvor frankierten Kuverts mit der zuletzt bekannten Adresse zu versehen und zu verschicken besteht allerdings nicht. Datenschutzrechtliche Bedenken hatte ich jedoch insoweit, als die Klassentreff Agentur auf den Kuverts ihren Absender angeben wollte und nicht den der Schule. Hier-

durch hätte die Gefahr bestanden, dass alle unzustellbaren Briefe an die Agentur zurückgegangen wären und diese damit auf Umwegen die Namen und früheren Anschriften der ehemaligen Schüler erfahren hätte. Mit diesen früheren Anschriften wäre es nämlich nach § 32 Abs. 1 ThürMeldeG möglich gewesen, bei den Meldebehörden Auskunft über die aktuellen Adressen zu erlangen. Zur Vermeidung von Irritationen bei den Adressaten habe ich die Klassentreff Agentur zusätzlich gebeten, den Kuverts eine Erläuterung zum Adressmittlungsverfahren beizufügen.

13.5 Hochschulchipkarte „THOSKA“

Nachdem einige Hochschulen in anderen Bundesländern bereits erste Erfahrungen mit der Umstellung vom herkömmlichen Studentenausweis auf eine Studentenchipkarte gemacht haben, stehen die Planungen der Thüringer Hochschulen zur Einführung einer solchen Chipkarte unmittelbar vor ihrem Abschluss, wobei zunächst eine Hochschule das Projekt erproben soll. Die ursprüngliche Einführung einer einheitlichen Thüringer Hochschul- und Studentenwerkskarte (THOSKA) war für das Wintersemester 1998/99 geplant. Der Termin ließ sich aber aufgrund der zahlreichen organisatorischen Schwierigkeiten nicht halten, sodass nunmehr eine Einführung für die erste Jahreshälfte 2000 vorgesehen ist. Die Chipkarte soll eine multifunktionale Anwendungsmöglichkeit erlauben. Neben der bekannten Ausweisfunktion sollen die Studenten an hierfür eingerichteten Terminals die über sie gespeicherten Daten abrufen können und Zugriffs- und Zugangsberechtigungen (Bestellung und Ausleihe Bibliothek, Zugang zu Netzen und DV-Verfahren, Zutritt zu gesicherten Räumen, Zufahrt zu Parkflächen usw.) erhalten. Zusätzlich soll die Karte eine Geldbörsenfunktion beinhalten, mit der wiederkehrende Leistungen (Kopierkosten, Mensaverpflegung, Semestergebühren usw.) vom Studenten bargeldlos beglichen werden können. Darüber hinaus soll die Chipkarte auch für die Bediensteten der Hochschulen für ein Zeiterfassungssystem genutzt werden. Um bestimmte Vorgänge auszulösen, muss zusätzlich zur THOSKA eine persönliche PIN eingegeben werden. Auf diese Weise soll bei Verlust der Karte ein Missbrauch weitgehend ausgeschlossen werden. Geplant ist auf dem Chip nur diejenigen Daten zu speichern, die auch sichtbar auf dem Plastikkörper aufgedruckt sind. Da eine spezi-

elle Rechtsgrundlage für die Verarbeitung von Studentendaten mittels Chipkarte bzw. bei Benutzung der Karte nicht vorhanden ist, gehe ich davon aus, dass die Nutzung nur auf freiwilliger Basis erfolgen darf und auch die möglichen Anwendungen von den Betroffenen ebenfalls freiwillig ausgewählt werden können. Für Studierende, die sich gegen die THOSKA entscheiden, dürfen keine Nachteile entstehen, die über die durch die Chipkarte bedingten Erleichterungen hinausgehen. Die Betroffenen sind spätestens mit der Einwilligung über Art, Umfang, Zweck und Beteiligte der Datenverarbeitung umfassend aufzuklären. Auch mit der Einführung auf freiwilliger Basis sind zahlreiche Rechts- und Verwaltungsvorschriften, z. B. die Immatrikulationsordnungen, anzupassen. Datenschutzrechtliche Bedenken habe ich gegen eine ursprünglich geplante, aktive Datenänderung an den Selbstbedienungsterminals durch den Studierenden bzw. den Mitarbeiter geäußert. Hiermit wäre nicht mehr die speichernde Stelle, sondern der Betroffene verantwortlich für die Speicherung seiner personenbezogenen Daten. Es muss systemseitig sichergestellt werden, dass keine Änderung des Datenbestandes durch den Studierenden oder den Mitarbeiter möglich ist. Als Lösung habe ich vorgeschlagen, dass dem Betroffenen ein Mailsystem zur Verfügung gestellt wird, mit dem er seine Änderungswünsche der Hochschulverwaltung zur Vorbereitung von Verwaltungsvorgängen übermitteln kann. Zu den für die Anwendung erforderlichen Hintergrundsystemen kann ich mich erst äußern, wenn ein konkretes Konzept vorliegt. In jedem Fall sind die erforderlichen technischen und organisatorischen Maßnahmen gem. § 9 ThürDSG zu treffen. In den Überlegungen zur Novellierung der Datenschutzgesetze ist eine Normierung zum Einsatz von Chipkarten geplant. Bislang ist dies z. B. in § 8 Abs. 2 Hessisches Datenschutzgesetz bereits umgesetzt worden. Ich werde mich dafür einsetzen, dass dies auch in der Novelle zum ThürDSG Berücksichtigung finden wird.

13.6 Automatisiertes Buchentleihverfahren in Universitätsbibliotheken

In der Bibliothek einer Hochschule wurde die bis dahin übliche manuelle Ausleihverbuchung durch ein automatisiertes System ersetzt. Bei einer Ausleihe werden dabei die auf den Büchern sowie

auf der neuen Bibliothekskarte aufgebrachten Balkencodes elektronisch abgelesen und verbucht. Vorteil dieses Systems ist die schnelle Verbuchungsgeschwindigkeit. In einer Eingabe wurde mir die Frage gestellt, was sich hinter einem solchen Strichcode verbirgt und ob es möglich ist, die gespeicherten Daten in unzulässiger Weise zu verarbeiten oder zu nutzen. In der Antwort habe ich darauf hingewiesen, dass jedem umgangssprachlichen Zeichen eine bestimmte Strichkombination zugeordnet ist. Der Balkencode der Bibliothekskarte stellt eine zehnstellige codierte Nummer dar. Die ersten vier Ziffern sind die Identifikationsnummer der Hochschulbibliothek, die nachfolgenden fünf Ziffern sind dem Kartenbesitzer zugeordnet und bei der letzten Ziffer handelt es sich um eine Prüfziffer. Da das Verfahren selbst ordnungsgemäß freigegeben und zum Datenschutzregister gemeldet worden war, haben darüber hinaus keine Anhaltspunkte bestanden, von einer unzulässigen Verarbeitung oder Nutzung der verbuchten Daten auszugehen. Datenschutzrechtliche Probleme waren allerdings im Zusammenhang mit der in Fernleihe im länderübergreifenden Bibliothekenverbund eingesetzten Software festzustellen, da diese zunächst nur einen unverschlüsselten Zugriff im Internet ermöglichte. Somit konnte nicht ausgeschlossen werden, dass Unbefugte personenbezogene Daten von Entleihern zur Kenntnis nehmen. Ich hatte mich beim TMWFK dafür eingesetzt, dass Thüringen im Bibliothekenverbund auf eine schnellstmögliche Einführung eines Verschlüsselungssystems dringt und bis dahin, soweit noch nicht erfolgt, alle Nutzer auf die unverschlüsselte Datenübertragung und die damit verbundenen Risiken hinzuweisen sind. Zwischenzeitlich wurde ich darüber unterrichtet, dass eine Verschlüsselung aller über das Internet übertragenen Informationen im Zusammenhang mit der Buchausleihe nunmehr möglich ist.

13.7 Internationaler Schülervergleich (OECD-Studie „PISA“)

Die OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) wird künftig in 32 Industriestaaten der Welt eine internationale Schulleistungsstudie durchführen, mit dem erklärten Ziel, Indikatoren für das Wissen, die Fähigkeiten und die Fertigkeiten von 15-jährigen Schülern in den Bereichen Leseverständnis, Mathematik und Naturwissenschaften auf einer verlässlichen und

national repräsentativen Basis in Zeitreihen den Verantwortlichen zur Verfügung zu stellen. Die Erhebungen sollen im Jahr 2000 beginnen und alle drei Jahre mit jeweils wechselnden thematischen Schwerpunkten fortgeführt werden. Auf der Grundlage einer Vereinbarung zwischen dem Bundesministerium für Bildung und Forschung und der ständigen Konferenz der Kultusminister der Länder beteiligt sich auch die Bundesrepublik an diesem Programm. Die Betreuung wurde im Auftrag der Kultusministerkonferenz einem Konsortium unter Federführung des Max-Planck-Instituts für Bildungsforschung in Berlin übertragen. Im Vorfeld der künftigen Leistungsvergleiche fanden 1999 in ausgewählten Schulen dazu entsprechende Tests statt. Die Übersendung der Prozedurbeschreibungen, der Informationsschreiben an die Betroffenen sowie der Erhebungsbögen erfolgte dabei an die Kultusverwaltungen so spät und teilweise unvollständig, dass mir wie auch den anderen Datenschutzbeauftragten der Länder trotz der guten Zusammenarbeit mit dem TKM für eine umfassende datenschutzrechtliche Bewertung nur unzureichend Zeit verblieb. Die daraufhin erfolgten kurzfristigen und wenig koordinierten Verfahrens- und Textänderungen in den Unterlagen führten zwar dazu, dass dem Projekt insgesamt seitens der Datenschutzbeauftragten zugestimmt werden konnte, jedoch in Detailfragen keine allseitig befriedigenden Lösungen erreicht wurden. Im Ergebnis des Tests erfolgte deshalb Ende des Jahres nochmals eine gemeinsame Beratung der Datenschutzbeauftragten der Länder mit den Verantwortlichen der Studie auf Bundesebene, um die noch vorhandenen datenschutzrechtlichen Probleme einer einvernehmlichen Lösung zuzuführen. Schwerpunkte waren dabei insbesondere die Fragen zur Gewährleistung der Vertraulichkeit während der gesamten Dauer der Studie, die Notwendigkeit einer umfassenden Aufklärung der Betroffenen, die Sicherung der freiwilligen Teilnahme und des Nachweises durch deren schriftliche Einwilligung. Die in diesem Zusammenhang von mir eingebrachten Änderungs- und Ergänzungsvorschläge hatten zuvor im Rahmen einer Abstimmung bereits die Zustimmung des TKM gefunden, sodass aus der Sicht des Datenschutzes nach Umsetzung aller Hinweise der Durchführung der Studie ab 2000 in Thüringen nichts mehr im Wege stehen dürfte.

13.8 Studenten als Forscher

Es ist durchaus üblich, dass Studenten z. B. in den Fachrichtungen Bauwesen (bei der Bauplanung und Sanierung) oder im sozialwissenschaftlichen Bereich im Rahmen ihrer Ausbildung Seminararbeiten übertragen bekommen, die die Erhebung (z. B. durch Umfragen), die Verarbeitung und Nutzung personenbezogener Daten erforderlich machen. Sowohl von den Bildungseinrichtungen wie auch von den Studenten selbst wird dabei häufig übersehen, dass soweit dies im Auftrag der Hochschule erfolgt, die für öffentliche Stellen geltenden datenschutzrechtlichen Bestimmungen zu beachten sind. Danach ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn dies ein Gesetz oder eine andere Rechtsvorschrift erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Da regelmäßig aufgrund fehlender Vorschriften im wissenschaftlichen Bereich nur eine Erhebung auf freiwilliger Grundlage in Betracht kommt, muss der Betroffene bei der Einholung seiner Einwilligung darüber sowie über den Zweck der Speicherung und eine vorgesehene Übermittlung hingewiesen werden. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand dann vor, wenn der Forschungszweck erheblich beeinträchtigt werden würde. In diesem Fall sind die Gründe dafür schriftlich festzuhalten. Bei der Festlegung der Erhebungsmerkmale gilt auch im wissenschaftlichen Bereich der Erforderlichkeitsgrundsatz. Dass hierbei aber mitunter zunächst auch Daten erhoben werden, bei denen sich erst im Rahmen der Auswertung herausstellt, dass der Forschungszweck auch erreicht werden konnte, ohne deren Kenntnis, muss sicher hingenommen werden. Dennoch ist der Wissenschaftler (oder Student im Rahmen einer wissenschaftlichen Arbeit) verpflichtet, die Notwendigkeit für die Erhebung der einzelnen Merkmale zu begründen. Dass er die Daten nur für den Forschungszweck verwenden darf, den er gegenüber den Betroffenen genannt hat, d. h. für den die Daten erhoben wurden, müsste selbstverständlich sein, ebenso wie der vertrauliche Umgang mit den Daten und ihre vor unbefugter Kenntnisnahme sichere Verwahrung. Zu beachten gilt ferner, dass personenbezogene Daten, die für wissenschaftliche Zwecke erhoben

wurden, zu anonymisieren sind, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Hilfsmerkmale gesondert zu speichern, mit denen die Einzelangaben einer bestimmten oder bestimmbar Person noch zugeordnet werden können.

Leider zeigen immer wieder Hinweise aus dem Kreis Betroffener, dass nicht jeder Student über die notwendige Sensibilität beim Umgang mit personenbezogenen Daten verfügt, was sich in Unkenntnis datenschutzrechtlicher Bestimmungen, der Missachtung von Aufklärungs- und Hinweispflichten bei der Erhebung personenbezogener Daten gegenüber den Betroffenen, den fehlenden eigenen „Vorgaben“ zur Anonymisierung und Vernichtung der Daten sowie in einer Verfahrensweise, die nicht in jedem Fall den Zugang Unbefugter ausschließt, äußert. In den mir bekannt gewordenen Fällen habe ich deshalb bei den Verantwortlichen die Einhaltung der datenschutzrechtlichen Bestimmungen eingefordert und gebeten, bei der künftigen Vergabe von Forschungsaufträgen, bei denen eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten erforderlich ist, die Studenten nachdrücklich über die einschlägigen datenschutzrechtlichen Vorgaben zu unterrichten. Ungeachtet dessen sollten aber nach meiner Auffassung auch die Datenschutzbeauftragten der Bildungseinrichtungen dieser Problematik verstärkt Beachtung schenken.

14. Wirtschaft, Verkehr, Wohnungswesen, Umwelt

14.1 „Schwarze Listen“ bei der Handwerkskammer

Durch mehrere Zeitungsartikel wurde ich darauf aufmerksam, dass eine Thüringer Handwerkskammer beabsichtigte, über private Auftraggeber, die ihre Rechnungen bei erbrachten Leistungen nicht beglichen haben, eine „Schwarze Liste“ zu erstellen. Zugang zu dieser Liste sollten alle Kammermitglieder erhalten.

Auf meine Anfrage begründete die Handwerkskammer ihr Vorhaben damit, dass sie im Rahmen ihrer Tätigkeit zur Förderung der wirtschaftlichen Interessen des Handwerks nach der Handwerksordnung und der Einrichtung von Vermittlungsstellen zur Beilegung von Streitigkeiten zwischen Handwerkern und ihren Auftraggebern in

den Besitz vielseitiger Informationen über die Rechtsverhältnisse Dritter gelangt. Als „privat-wirtschaftliche Dienstleistung“ wollte man nunmehr diese Kenntnisse bei Informations- und Beratungsgesprächen bzw. in Stellungnahmen gegenüber den Mitgliedern verwenden. So wurde insbesondere als Möglichkeit der Verwertung auch in Betracht gezogen, bei der Prüfung von Vertragsangeboten eines in anderen Beratungsfällen bereits auffällig gewordenen Auftraggebers den betroffenen Handwerker zu weiter gehenden rechtlichen Absicherungen zu raten. Die Nutzung der Erkenntnisse sollte dabei nicht im Ermessen des Mitarbeiters der Handwerkskammer liegen, sondern würde dann als dessen Rechtspflicht im Rahmen einer fachkundigen Beratung angesehen werden. Darüber hinaus sollten aber auch Erkenntnisse aus Einzelvorgängen bei konkreten Anfragen den Mitgliedsbetrieben im Rahmen einer individuellen Beratung zur Verfügung gestellt werden. Eine Veröffentlichung außerhalb der Handwerkskammer und ihrer Mitglieder war nicht vorgesehen.

Dieser Rechtsauffassung konnte ich mich nicht anschließen. Zunächst bedurfte es einer Klarstellung dahingehend, dass die Handwerkskammern in Thüringen in ihrer Gesamtheit als Körperschaften des öffentlichen Rechts den Vorschriften des Thüringer Datenschutzgesetzes für den öffentlichen Bereich unterliegen, auch wenn die Datenerhebung im Einzelfall nicht zur Erfüllung hoheitlicher Aufgaben erfolgt. Insoweit bedarf es stets zur Erhebung und Verarbeitung personenbezogener Daten einer Rechtsvorschrift oder der Einwilligung der Betroffenen. Was die Übermittlung von Daten an Stellen außerhalb des öffentlichen Bereichs anbelangt, ist zu beachten, dass die Verarbeitung und Nutzung der Daten nur zulässig ist, wenn es zur Aufgabenerfüllung der Handwerkskammer erforderlich ist und im Rahmen des jeweiligen Beratungsvorganges erfolgt, für den die Daten erhoben worden sind. Ansonsten muss in jedem Einzelfall geprüft werden, ob ein berechtigtes Interesse des Empfängers an der Kenntnis der zu übermittelnden Daten und kein schutzwürdiges Interesse des Betroffenen an dem Ausschluss der Übermittlung vorliegt. Im weiteren ist der Betroffene von der Handwerkskammer von der Übermittlung zu unterrichten (§ 22 Abs. 3 ThürDSG).

Im Ergebnis der Prüfung gelangte ich deshalb zu der Rechtsauffassung, der sich auch das TMWI anschloss, dass aus der Sicht des Datenschutzes die Erstellung und Nutzung einer „Schwarzen Liste“ mangels einer Rechtsgrundlage unzulässig ist.

14.2 Datenübermittlungen durch das Finanzamt an Kammern

Im Berichtszeitraum hatten mehrere Bürger bei mir angefragt, ob es zulässig ist, wenn die Finanzämter an Kammern (Handwerkskammer, Industrie- und Handelskammer) bestimmte Steuerdaten zur Festsetzung von Kammerbeiträgen übermitteln. Ich habe allen Petenten hierzu mitgeteilt, dass die Finanzbehörden nach § 31 Abs. 1 AO berechtigt sind, Körperschaften des öffentlichen Rechts die zur Festsetzung von Kammerbeiträgen erforderlichen Besteuerungsgrundlagen mitzuteilen. Diese gesetzlich zugelassene Durchbrechung des Steuergeheimnisses wird in den Kammergesetzen ausdrücklich wiederholt (§ 113 Abs. 2 S. 3 Handwerksordnung, § 9 Abs. 2 IHK Gesetz).

14.3 Formular zur Energiebelieferung zu umfangreich

In einer Eingabe wurde mir ein Anmeldeformular zum Bezug von Strom und Erdgas mit der Bitte um eine datenschutzrechtliche Prüfung vorgelegt. Nicht für das Vertragsverhältnis zwischen den Kunden und dem Energieversorgungsunternehmen erforderlich erschien mir dabei das Erheben des Ausstellungsdatums, der ausstellenden Dienststelle sowie der ID-Nummer des Personalausweises, des Namens und der Adresse des Arbeitgebers, der Namen und Adressen weiterer Haushaltsmitglieder sowie deren Arbeitgeber. Das Unternehmen hatte daraufhin den Antragsbogen in der Weise überarbeitet, dass die Daten zum Personalausweis und zu den Arbeitgebern der Haushaltsmitglieder entfallen sind, die Angaben über den Arbeitgeber des Vertragspartners und dessen Anschrift als freiwillig gekennzeichnet werden und der Antragsteller aus Gründen der Transparenz darauf hingewiesen wird, dass seine Daten nur im Rahmen des Vertragsverhältnisses verarbeitet werden. Gegen den geänderten Fragebogen bestanden keine datenschutzrechtlichen Bedenken mehr. Die nicht erforderlichen Daten auf den bereits aus-

gefüllten, alten Anmeldebögen wurden gesperrt, da eine umfassende Löschung dieser Daten nur mit unverhältnismäßig hohem Aufwand möglich gewesen wäre. Auf Antrag von Betroffenen konnten diese sowie die nunmehr als freiwillig gekennzeichneten Daten auf den alten Anmeldebögen gelöscht, d. h. unkenntlich gemacht werden.

14.4 Neuerungen im Straßenverkehrsrecht

Zum 01.01.1999 ist das Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze vom 24.04.1998 (BGBl. I, 747) in Kraft getreten. Auf die datenschutzrechtlichen Bedenken, die sich aus der Änderung ergeben, hatte ich im 2. TB (14.7) bereits hingewiesen. Unverändert geblieben ist grundsätzlich die Führung des Verkehrszentralregisters (VZR). In das vom Kraftfahrt-Bundesamt (KBA) in Flensburg geführte VZR werden außer den bisherigen Negativdaten, wie Verkehrsstraftaten und bestimmte Ordnungswidrigkeiten, die Punktbewertung, Fahrverbote, Entziehungen, nunmehr auch Entscheidungen ausländischer Gerichte und Behörden über die Aberkennung der Fahrerlaubnis in dem entsprechenden Land gespeichert. Die gespeicherten Daten dürfen an eine große Anzahl von Stellen übermittelt werden, soweit dies zur Erfüllung der Aufgaben dieser Stellen erforderlich ist. Außer den örtlichen Fahrerlaubnisbehörden, den Bußgeld- und Polizeibehörden, soweit sie für die Verfolgung von Verkehrsordnungswidrigkeiten zuständig sind, sind das auch das Bundeskriminalamt, der Bundesgrenzschutz sowie mit diesen Aufgaben betraute Stellen der Zollverwaltung und die Zollfahndungsstellen, die Polizeibehörden der Länder und die Zentrale Militärkraftstelle (§ 61 Abs. 3 u. 4 FeV). Dies gilt nunmehr auch für die Übermittlung an zuständige Stellen anderer Staaten, dadurch nicht schutzwürdige Interessen des Betroffenen beeinträchtigt werden, insbesondere wenn im Empfängerland kein angemessener Datenschutzstandard gewährleistet ist (§ 30 Abs. 7 StVG). Der Abruf im automatisierten Verfahren ist unter bestimmten Bedingungen ebenfalls möglich. Getilgt werden die Eintragungen je nach Schwere des Delikts nach Ablauf von zwei bis zehn Jahren. Der Betroffene erhält auf Antrag unentgeltlich Auskunft über die zu seiner Person gespeicherten Daten (§ 30 Abs. 8 StVG).

Das KBA führt zusätzlich seit dem 01.01.1999 das neu errichtete Zentrale Fahrerlaubnisregister (ZFER). Hierin werden die "positiven" Fahrerlaubnisdaten, z. B. Namen, Vornamen, Tag und Ort der Geburt, die Klassen der erteilten Fahrerlaubnis sowie die erteilende Behörde, der Tag des Beginns und des Ablaufs der Probezeit, Auflagen, Beschränkungen, Hinweise auf Eintragungen im VZR usw., mit Ausnahme der Anschrift des Betroffenen, für über 50 Millionen deutsche Fahrerlaubnisinhaber gespeichert. Diese Daten waren bisher ausschließlich bei den örtlichen Fahrerlaubnisbehörden gespeichert. Durch die Änderungen des Straßenverkehrsrechts sind nun alle Fahrerlaubnisbehörden verpflichtet, die "positiven" Fahrerlaubnisdaten an das KBA zu übermitteln. Die dort gespeicherten Daten werden zur Übermittlung an die gleichen Stellen wie oben für das VZR beschrieben, bereitgehalten. Wenn die Fahrerlaubnis erloschen ist, sind die im ZFER gespeicherten Daten zu löschen. Auch hier ist die Auskunft über die eigenen gespeicherten Daten auf Antrag unentgeltlich zu erteilen (§ 58 StVG). Die Abrufe im automatisierten Verfahren durch die hierzu berechtigten Stellen sind wie zuvor durch das KBA zu protokollieren. Durften diese Protokolldaten aber bisher nur für Zwecke der Datenschutzkontrolle verwendet werden, so können diese Daten jetzt sowohl aus dem VZR als auch aus dem ZFER von den Strafverfolgungsbehörden zur Aufklärung oder Verhütung von schwer wiegenden Straftaten gegen Leib, Leben oder Freiheit einer Person verwendet werden. Die Protokolldaten sind nunmehr sechs statt drei Monate aufzubewahren. Weiterhin sind den Führerscheinakten beigeheftete Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse nach spätestens zehn Jahren zu vernichten (§ 2 Abs. 9 StVG), es sei denn, die Unterlagen stehen im Zusammenhang mit Eintragungen im VZR oder ZFER und sind nach den Bestimmungen für diese Register zu einem späteren Zeitpunkt zu tilgen oder zu löschen. Die Fahrerlaubnisbehörde ist allerdings hierzu nur verpflichtet, wenn die Akte bei anderer Gelegenheit benötigt wird. Die Überprüfung der Akten muss jedoch spätestens bis zum 1. Januar 2014 durchgeführt werden (§ 65 Abs. 1 StVG).

Mit den Änderungen im StVG ist am 1. Januar 1999 die Fahrerlaubnis-Verordnung (FeV) in Kraft getreten. Hierin ist die zunächst im Regierungsentwurf vorgesehene Regelung, wonach der Betroffene

vor Übersendung seiner Fahrerlaubnisunterlagen an die Gutachterstelle Gelegenheit erhält, in diese Einblick zu nehmen, auf Beschluss des Bundesrates nicht mehr enthalten. Ebenfalls sind nach § 11 Abs. 6 S. 4 FeV nunmehr die "vollständigen" Fahrerlaubnisunterlagen an die untersuchende Stelle zu übersenden und nicht, wie im Entwurf zunächst vorgesehen, die "erforderlichen" Unterlagen.

14.5 Kontrollen in Führerscheinstellen

Da örtliche Fahrerlaubnisregister längstens bis zum 31.12.2005 geführt werden dürfen und der BfD mir darüber hinaus mitgeteilt hatte, dass sich bei der Übermittlung der Fahrerlaubnisdaten durch die örtlichen Fahrerlaubnisbehörden an das ZFER (14.5) Anlaufschwierigkeiten ergeben, nahm ich das zum Anlass, die Führerscheinstellen zweier Landkreise einer datenschutzrechtlichen Prüfung zu unterziehen, wobei ich den Schwerpunkt darauf setzte, mir ein Bild davon zu machen, wie sich die Übermittlung der Fahrerlaubnisdaten an das ZFER vollzieht. In einer der Führerscheinstellen musste ich dabei feststellen, dass der Datenaustausch mit dem KBA in Flensburg auf eine Gesellschaft mit Sitz außerhalb Thüringens übertragen wurde und der Landkreis, entgegen den Bestimmungen des § 8 Abs. 6 ThürDSG nicht seiner Verpflichtung nachkam, vertraglich sicherzustellen, dass die Gesellschaft als Auftragnehmer die Bestimmungen des ThürDSG befolgt und sich meiner Kontrolle entsprechend der §§ 37 bis 40 ThürDSG unterwirft. Dies habe ich beanstandet. Weiterhin war zum Kontrollzeitpunkt zu dem von der Fahrerlaubnisbehörde zur automatisierten Verarbeitung der Führerscheindaten genutzten Verfahren keine schriftliche Freigabe nach § 34 Abs. 2 ThürDSG erfolgt. Zusätzlich war das Verfahren weder in dem von der Stelle zu führenden Anlagen- und Verfahrensverzeichnis enthalten noch zum Datenschutzregister gemeldet. Das Versäumte wurde von der Stelle nachgeholt. Darüber hinaus waren aus datenschutzrechtlicher Sicht verschiedene, nicht ausreichend getroffene technische und organisatorische Maßnahmen zu kritisieren, indem z. B. die Zugriffsrechte nicht dokumentiert waren.

In der anderen Führerscheinstelle waren offensichtlich aufgrund meiner Kontrollankündigung zu dem dort in der Anwendung befindlichen Verfahren zur automatisierten Verarbeitung der Fahrer-

laubnisdaten eine schriftliche Freigabe sowie eine Datenschutzregistermeldung erstellt worden. Wie bereits bei der ersten Führerscheinstelle von mir festgestellt wurde, bestanden auch in diesem Fall datenschutzrechtliche Bedenken gegen die vergebenen Zugriffsrechte. So hatten mehr Personen Zugriff auf das Verfahren, als dies zur Aufgabenerfüllung erforderlich war. Außerdem konnte nicht nachvollzogen werden, welche Zugriffsrechte an wen, zu welchem Zeitpunkt erteilt bzw. entzogen wurden. Noch während der Kontrolle wurden unzulässige Zugriffsrechte gesperrt und die Einrichtung von Protokollierungen zugesagt. Insgesamt stellte ich im Zusammenhang mit der Erst- bzw. Neuerteilung von Fahrerlaubnissen bei beiden Führerscheinstellen die folgenden Datenübermittlungen fest:

Die Verfahrensweise der bei der Beantragung einer Fahrerlaubnis erforderlichen Prüfungen ist in beiden Führerscheinstellen gleich. Anfragen der Fahrerlaubnisbehörde, ob Eintragungen im Bundeszentralregister (BZR) bzw. im Verkehrszentralregister (VZR) über den Antragsteller vorliegen, erfolgen zunächst auf elektronischem Weg. Wird von den Registerbehörden elektronisch eine „0“ zurückübertragen, so liegen keine Eintragungen vor. Übertragen diese jedoch eine „1“, so ist eine entsprechende Eintragung vorhanden, die auf dem Postweg an die Fahrerlaubnisbehörde übersandt wird. Im Falle des BZR ist dies ein Führungszeugnis, beim VZR sind dies z. B. Eintragungen von Mitteilungen der Staatsanwaltschaft über Verkehrsstraftaten oder schwere Verkehrsordnungswidrigkeiten. Wenn keine Gründe, die gegen die Erteilung der Fahrerlaubnis sprechen, vorliegen, ergeht an die Bundesdruckerei in Berlin der Auftrag zur Herstellung eines Führerscheins, wobei die erforderlichen Daten sowie das Lichtbild beigelegt werden. Nach der Fertigstellung wird der Führerschein an die Fahrerlaubnisbehörde gesendet. Dort wird der Führerschein auf die Richtigkeit der Daten überprüft und an die prüfende Organisation (TÜV, Dekra, usw.) mit einem Prüfauftrag und der Mitteilung über die ausbildende Fahrschule übersendet. Nach bestandener Prüfung versieht die Prüfstelle den Führerschein mit dem Datum des Prüfungstags und händigt ihn an den Betroffenen aus. Die Fahrerlaubnisbehörde bekommt von der Prüforganisation hierüber eine Mitteilung, die dies daraufhin an das Fahrerlaubnisregister des KBA meldet und somit die zweijährige Probezeit be-

ginnt. An das KBA gemeldete Bußgeldtatbestände werden an die örtliche Fahrerlaubnisbehörde übermittelt, die dem Betroffenen bestimmte Auflagen erteilen kann, z. B. zukünftig die Verlängerung der Probezeit auf 4 Jahre.

Ist einem Betroffenen die Fahrerlaubnis entzogen worden, etwa durch die Mitteilung des KBA, dass ein bestimmter Punktestand erreicht wurde oder die Mitteilung des Gerichts über die Entziehung des Führerscheins durch Strafbefehl oder Urteil, muss dieser die Neuerteilung einer Fahrerlaubnis beantragen. Diese Neuerteilung kann die örtliche Behörde von bestimmten Anforderungen, z. B. der Vorlage eines MPU-Gutachtens abhängig machen. Hierbei werden die vollständigen Fahrerlaubnisakten an den vom Betroffenen ausgewählten Gutachter verschickt. Nach Erstellung des Gutachtens übersendet die Gutachterstelle das Gutachten an den Betroffenen und dieser entscheidet dann darüber, ob er es an die Fahrerlaubnisbehörde übergibt. Wird das Gutachten nicht vorgelegt, ist in der Regel eine Wiedererteilung der Fahrerlaubnis ausgeschlossen. Liegen die Unterlagen hingegen vor, muss sich die Fahrerlaubnisbehörde ein Bild darüber machen, ob eine Neuerteilung gerechtfertigt ist oder nach einer weiteren Wartezeit die Erstellung eines neuen MPU-Gutachtens verlangt wird.

Da bislang nur die Fahrerlaubnisdaten von laufenden Vorgängen an das ZFER übermittelt wurden, ist damit zu rechnen, dass voraussichtlich bis zur endgültigen Auflösung der örtlichen Fahrerlaubnisregister noch einige Zeit vergehen wird. Ich werde den jeweiligen Stand und die Verfahrensweise der Datenübermittlungen von den Thüringer Fahrerlaubnisbehörden an das ZFER weiterhin begleiten.

14.6 Sonderparkausweis mit zu vielen Daten

In einer Eingabe hat sich der Inhaber einer Sonderparkerlaubnis an mich gewandt, mit der Frage, weshalb er verpflichtet ist, bei der Benutzung eines Behindertenparkplatzes jedem zu offenbaren, dass er (unter Angabe seines Namens und der Anschrift) schwergebehindert ist und über einen befristeten Sonderparkausweis für sein Kfz verfügt. Hintergrund dafür ist die in der Straßenverkehrsordnung enthaltene Vorschrift, dass Fahrzeuge mit dem Zusatzschild

„(Rollstuhlfahrersymbol) mit Parkausweis-Nr. ...“ vom Halteverbot ausgenommen werden, wenn der Parkausweis gut lesbar im Fahrzeug ausgelegt wird. Von dem im konkreten Fall für die Ausstellung von Sonderparkausweisen zuständigen Ordnungsamt waren auf der Vorderseite der bundesweit einheitlichen Auslegekarte (Sonderparkgenehmigung) an der für die Eintragung des Namens der Genehmigungsbehörde vorgesehenen Stelle auch der Name des Inhabers der Sondergenehmigung und dessen Anschrift eingetragen worden.

Auf meine Nachfrage beim Ordnungsamt konnte mir für diese Verfahrensweise weder eine spezialgesetzliche Regelung noch eine Erforderlichkeit für die „Veröffentlichung“ genannt werden, da bei Kontrollen durch Ordnungskräfte eine Kenntnis dieser Daten vor Ort nicht notwendig ist, um zu prüfen, ob eine Ausnahmegenehmigung für das betreffende Fahrzeug zurecht besteht. Insoweit war die Pflicht zur Offenbarung der Angaben zur Person im Sinne des ThürDSG als eine unzulässige Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs zu betrachten. Von der für die in diesen Fragen zuständigen oberen Verkehrsbehörde in Thüringen wurde meine Rechtsauffassung bestätigt. Um gleichartige Verstöße gegen datenschutzrechtliche Bestimmungen in anderen Kreisen und Gemeinden auszuschließen, wurden alle Straßenverkehrsbehörden des Freistaats angewiesen, künftig personenidentifizierende Daten, soweit keine besonderen Gründe dem entgegenstehen, nur auf der Rückseite der Auslegekarte zu vermerken. Gründe für eine Eintragung der Personaldaten auf der Vorderseite wären dabei insbesondere Auslandsfahrten in andere europäische Länder (Mitgliedsstaaten der CEMT), da dies dort als verbindliche Voraussetzung für die Anerkennung von Sonderparkgenehmigungen gilt, worüber selbstverständlich die Schwergebehinderten bei ihrer Antragstellung zu informieren sind.

14.7 Kfz-Zulassung via Internet?

Zur Entlastung der Zulassungsstellen und der damit erhofften Verkürzung der Wartezeiten für den Bürger bestehen bei einigen Gebietskörperschaften Überlegungen, Zulassungsvorgänge zukünftig Autohäusern zu übertragen. Für die Umsetzung dieses Vorhabens sind grundsätzlich zwei Möglichkeiten denkbar: Zum einen können

die Autohäuser, wie bisher schon üblich, die Zulassungsformalitäten für ihre Kunden erledigen, mit dem Unterschied, dass die Autohausmitarbeiter nicht mehr persönlich bei der Zulassungsstelle erscheinen müssen, sondern die relevanten Kundendaten per Internet direkt in einen Computer der Zulassungsstelle eingeben. Die weiteren Verfahrensschritte werden dann in der Zulassungsstelle erledigt. Zum anderen handeln die Autohäuser als beliebene Unternehmer und übernehmen damit hoheitliche Aufgaben der öffentlichen Verwaltung. Sie erledigen also nicht nur die Zulassungsformalitäten, sondern übernehmen zusätzlich das Bedrucken und Bestempeln der Fahrzeugbriefe und Scheine, lassen die Kennzeichen herstellen und versehen sie mit den notwendigen Plaketten. Lediglich der Original-Zulassungsantrag, die Bestätigung des Halters über die Aushändigung der Fahrzeugpapiere und ggf. die Original-Versicherungsbestätigung würde per Post an die Zulassungsstelle verschickt werden, die diese Unterlagen verwaltet.

Aus datenschutzrechtlicher Sicht bestehen gegen die erste Alternative keine grundsätzlichen Bedenken. Es muss aber sichergestellt bleiben, dass das Kfz vom Halter selbst bei einer Zulassungsstelle angemeldet werden kann, Dritte nicht auf den Echtdatenbestand der Zulassungsbehörde zugreifen können, nur eine Dateneingabe ermöglicht wird, auf andere gespeicherte Daten nicht zugegriffen werden kann, eine Identifizierung und Authentifizierung der Zugriffsberechtigten sichergestellt ist, eine Protokollierung der Eingaben zu Nachweiszwecken erfolgt, die Übertragung an die Zulassungsstellen verschlüsselt vorgenommen und schließlich die Autohäuser und Zulassungsdienste in ihrem eigenen Bereich verpflichtet werden, geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit zu treffen.

Hingegen halte ich eine Übertragung der Aufgaben der Zulassungsstellen an Private aus Datenschutzgründen für sehr bedenklich. Es würde eine große Anzahl von privaten speichernden Stellen entstehen, deren Personal entsprechend zu schulen und die Zuverlässigkeit zu überprüfen wäre. Den Autohäusern müssten ggf. Zugriffe auf Dateien anderer öffentlicher Stellen (z. B. Meldeämter, KBA) eingeräumt werden. Schließlich könnte dies eine Signalwirkung für die Übertragung sonstiger hoheitlicher Tätigkeiten der öffentlichen

Verwaltung auf Private ausüben, sodass eine unübersehbare Anzahl von privaten speichernden Stellen entstehen würde und kein Überblick mehr zu erhalten wäre, wer über den Betroffenen wann wo welche Daten gespeichert hat und wie diese weiter verarbeitet werden. Das TMWI hat mich auf Anfrage in meiner Auffassung bestätigt und eine Aufgabenübertragung auf private Unternehmer in Form einer Beleihung abgelehnt. Zwischenzeitlich ist mir bekannt geworden, dass in einem Landkreis eines anderen Bundeslandes bereits ein Konzept zur Kfz-Zulassung über das Internet erstellt und testweise umgesetzt wurde. Es handelt sich hierbei um die von mir oben beschriebene erste Möglichkeit, die grundsätzlich datenschutzrechtlich unproblematisch ist, wenn die erforderlichen technischen und organisatorischen Maßnahmen umgesetzt werden.

14.8 Adressveröffentlichung von Einspruchsführern

Ein Bürger machte mich darauf aufmerksam, dass in der öffentlichen Bekanntmachung einer Stadt im Zusammenhang mit Anregungen im Bauleitplanverfahren die Namen und Adressen von Einspruchsführern veröffentlicht wurden. Ich teilte der Stadtverwaltung daraufhin mit, dass mir eine spezialgesetzliche Grundlage, die diese Übermittlung erlaubt, nicht bekannt ist. Auch nach § 22 Abs. 1 ThürDSG konnte ich keine Zulässigkeit der Übermittlung feststellen, da im vorliegenden Fall das Recht auf informationelle Selbstbestimmung das Interesse der Öffentlichkeit an der Kenntnis der Daten überwiegt. Eine Einwilligung der betroffenen Bürger lag ebenfalls nicht vor. Der Einwand der Stadtverwaltung, dass die Einspruchsführer aktiv an der öffentlichen Sitzung teilgenommen hätten und von den anwesenden Bürgern ohnehin wahrgenommen worden wären, konnte ich nicht gelten lassen. Es besteht nämlich ein qualitativer Unterschied, ob diese Daten an eine nicht näher bekannte Öffentlichkeit übermittelt werden oder nur derjenige sie wahrnehmen kann, der selbst aktiv an der öffentlichen Sitzung teilnimmt. Der Betroffene hat ein schutzwürdiges Interesse daran, dass seine personenbezogenen Daten nicht über die Maßen hinaus "breit gestreut" werden. Die Stadtverwaltung hatte mir schließlich zugesagt, zukünftig keine Namen und Adressen von Einspruchsführern in ihrem Amtsblatt zu veröffentlichen.

14.9 Aushang von Mieterlisten durch Wohnungsbaugesellschaft

Im Jahre 1998 erreichten mich mehrere Beschwerden von Bürgern, die sich dagegen wandten, dass in ihren Wohnhäusern öffentlich Listen zum Aushang gebracht wurden, auf denen für jede Wohnung der Name des Mieters und die Anzahl der jeweils mit ihm gemeinsam wohnenden Personen angegeben waren. Auf Nachfrage teilte mir daraufhin die Eigentümerin der Gebäude, eine öffentliche Wohnungsbaugesellschaft mit, dass sie dem Wunsch vieler Mieter folgend, die Betriebskosten nicht entsprechend der Wohnungsgröße, sondern nach der Anzahl der in den Wohnungen lebenden Personen umlegen möchte. Aufgrund der Vielzahl der Wohnungen und der Tatsache, dass nur unvollständige bzw. nicht aktuelle Übersichten zur Anzahl der Bewohner zur Verfügung standen, sollten mit dem öffentlichen Aushang die Bewohner veranlasst werden, die Richtigkeit ihrer Angaben zu prüfen und ggf. zu berichtigen. Darüber hinaus war auch eine „gesellschaftliche Kontrolle“ durch Nachbarn beabsichtigt, indem diese gleichfalls der Wohnungsbaugesellschaft Hinweise auf „falsche“ Personenzahlen geben sollten.

Bei der Beurteilung der Verfahrensweise ist aus datenschutzrechtlicher Sicht zu berücksichtigen, dass es sich bei der besagten Wohnungsbaugesellschaft um eine öffentliche Stelle handelt, die am Wettbewerb teilnimmt. Diese darf, entsprechend den Bestimmungen des Bundesdatenschutzgesetzes personenbezogene Daten zur Wahrnehmung ihrer berechtigter Interessen an Dritte übermitteln, wenn kein Grund zur Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder der Nutzung überwiegen. Geht man zunächst davon aus, dass ein berechtigtes Interesse zur ordnungsgemäßen Umlegung der Gebühren im Rahmen der Betriebskostenabrechnung besteht, bedarf es im weiteren einer Prüfung, ob dafür eine Veröffentlichung der Daten zwingend erforderlich und verhältnismäßig ist bzw. ob und welche schutzwürdigen Interessen der Betroffenen einem öffentlichen Aushang der Daten entgegenstehen.

Zweck der Maßnahme sollte nach Angaben der Wohnungsbaugesellschaft die Erhebung der tatsächlichen Zahl der Bewohner in den

einzelnen Wohnungen sein. Dazu bedarf es grundsätzlich keiner Datenübermittlung an Dritte, da es regelmäßig möglich ist, diese Wohnungsbelegungsdaten beim Betroffenen selbst durch Angestellte der Wohnungsbaugesellschaft, wie Hausmeister, durch Aufträge (z. B. im Rahmen der Ablesung von Wasseruhren oder Heizmessgeräten) oder in Schriftform erheben zu können. Nur wenn dies zu keinem Ergebnis führt oder Anhaltspunkte für falsche Angaben durch die Betroffenen vorliegen, erscheint eine Befragung von Nachbarn im Einzelfall gerechtfertigt, wobei auch dann keine Notwendigkeit besteht, diesen die der Gesellschaft bekannte Zahl der Bewohner bekannt zu geben. In jedem Fall muss aber die Übermittlung der Daten an unbeteiligte Dritte (z. B. Besucher des Hauses) ausgeschlossen werden. Sie verbietet sich bereits deshalb weil schutzwürdige Interessen der Betroffenen dem entgegenstehen. Zur Beurteilung der Schutzwürdigkeit ist dabei nicht nur das Bekanntwerden der persönlichen Verhältnisse der Mieter (z. B. allein stehend), sondern insbesondere auch die möglichen Folgen für die Betroffenen zu betrachten. Hierbei sind sowohl objektive als auch subjektive Aspekte zu berücksichtigen. Schutzwürdig sind in jedem Fall Daten, wenn aus objektiver Sicht unter Zugrundelegung der durchschnittlichen Verhältnisse Nachteile für den Betroffenen möglich sind. Inwieweit es sich dabei um Nachteile wirtschaftlicher, sozialer oder persönlicher Art handelt, ist unerheblich. Insoweit kann ein schutzwürdiges Interesse allein dadurch begründet werden, dass Unbefugte die Informationen über die Anzahl der Bewohner (z. B. bei Alleinstehenden) zu kriminellen Handlungen benutzen könnten. Ebenso ist im konkreten Fall nicht auszuschließen, dass die Informationen zu begründeten oder unbegründeten Vorbehalten oder Misstrauen gegenüber anderen Mietern führen können, wenn z. B. durch die Veröffentlichung nicht aktueller Daten der Eindruck entsteht, dass der Betroffene durch bewusste Falschangaben seinen Anteil an den Betriebskosten ungerechtfertigt reduzieren möchte.

Aus den vorgenannten Gründen habe ich der Wohnungsgesellschaft mitgeteilt, dass ich den öffentlichen Aushang von Mieterdaten für unzulässig erachte und diese aufgefordert, künftig davon Abstand zu nehmen.

14.10 Datenübermittlungen an Zweckverbände

Immer wieder erreichen den TLfD Fragen oder Eingaben von Bürgern zum Umfang der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zur Berechnung kommunaler Gebühren und Abgaben. Ein Schwerpunkt bildet dabei neben dem Abfallbereich insbesondere auch die Wasser- und Abwasserentsorgung. Bei der näheren Betrachtung stellt man häufig fest, dass (wie auch unter 14.13 im Abfallbereich ausführlich beschrieben) die jeweiligen Satzungen nicht normenklar und für den Bürger verständlich sind oder Regelungen enthalten, die sich in der Praxis nicht oder nur teilweise umsetzen lassen. Dies betrifft im Wasser- und Abwasserbereich z. B. auch die Nutzung von Einwohnermeldedaten, deren regelmäßige Übermittlung an Zweckverbände mangels entsprechender gesetzlicher Grundlage unzulässig ist. Dennoch werden häufig unter Verweis auf die Amtshilfe Meldebehörden aufgefordert, den Zweckverbänden regelmäßig Meldedaten und ihre Veränderungen mitzuteilen. Ungeachtet der Tatsache, dass mitunter entsprechende konkrete Vorschriften zur Erhebung von Meldedaten in den Satzungen fehlen, stellt sich bei näheren Prüfungen meist heraus, dass keine personenbezogenen sondern nur statistische Daten, insbesondere zur Anzahl der Bewohner je Grundstück für die Gebührenberechnung und -veranlagung benötigt werden.

Im Interesse des Datenschutzes wäre es deshalb wünschenswert, wenn bei der Erarbeitung der Satzungen stets neben einer Prüfung der rechtlichen Zulässigkeit von Datenerhebungen auch deren praktische Umsetzung untersucht werden würde und die Ergebnisse normenklar in den Satzung Aufnahme fänden.

Im Rahmen einer Eingabenbearbeitung befasste ich mich auch mit der Bereitstellung von Grundstücksdaten aus dem automatisierten Liegenschaftsbuch zur Berechnung und Veranlagung von Wasser- und Abwassergebühren. Dazu werden auf der Grundlage einer Mustervereinbarung zwischen dem Nutzer und der Thüringer Kataster- und Vermessungsverwaltung Verträge abgeschlossen, die auch besondere Regelungen zum Datenschutz enthalten. Im Rahmen meiner Prüfung musste ich aber feststellen, dass das im Einsatz befindliche

Programm keine Selektion der Daten zuließ, sodass jeder Empfänger den gleichen Datensatz erhält, gleichgültig, ob er zur Aufgabenerfüllung nach der jeweiligen Satzung vollständig oder nur in Teilen benötigt wird. Da bisher auch seitens der Nutzer keine weiteren Differenzierungswünsche an die dafür zuständige oberste Landesbehörde herangetragen worden waren, erhalten gegenwärtig alle Zweckverbände Angaben zur konkreten Lage der Grundstücke, zu den Nutzungsarten und Flächengrößen sowie Daten über die Eigentümer unter Berücksichtigung der Rechtsverhältnisse untereinander. Erst mit der Entwicklung eines neuen Programmes wird es ab Mitte 2000 möglich sein, entsprechende Selektionen einzelner Daten je Grundstück vornehmen zu können.

Zur Gewährleistung des Datenschutzes habe ich deshalb das TIM gebeten, die Nutzer des automatisierten Liegenschaftsbuches unter Verweis auf die gegenwärtigen Unzulänglichkeiten des Programms hinsichtlich der fehlenden Selektionsmöglichkeiten nachdrücklich darauf hinzuweisen, dass sie nur zur Erhebung, Verarbeitung und Nutzung der Daten berechtigt sind, die entsprechend ihrer konkreten Satzung zur Aufgabenerfüllung benötigt werden. Soweit deshalb in den übermittelten Datensätze darüber hinausgehende Angaben enthalten sind, gelten diese im Sinne des Thüringer Datenschutzgesetzes als gesperrt. Eine Übernahme dieser Daten in eigene Verfahren sowie ihre Verarbeitung und Nutzung ist daher unzulässig.

14.11 Datenverarbeitung bei der Abfallgebührenberechnung

Mehrfache Anfragen und Eingaben zu Problemen der Datenerhebung bei der Abfallentsorgung, worüber ich in meinem 2. TB (14.18) bereits ausführlich berichtet habe, gaben mir Anlass, im abgelaufenen Berichtszeitraum die Erhebungsverfahren sowie den Umgang mit personenbezogenen Daten in verschiedenen Abfallbehörden, Abfallwirtschaftsbetrieben bzw. Zweckverbänden zu kontrollieren. Dabei habe ich im Ergebnis in drei überprüften Landkreisen festgestellt, dass um das Ziel, ein Optimum an Müllvermeidung, Mülltrennung und Gebührengerechtigkeit zu erreichen, die unterschiedlichsten Verfahren und Gebührenmaßstäbe und -berechnungen angewandt werden, der Verwaltungsaufwand und der Umfang der Datenerhebungen aber mit steigendem Bemühen nach immer mehr

Gebührengerechtigkeit (nach dem Verursacherprinzip) zwangsläufig zunimmt.

Die wenigsten datenschutzrechtlichen Probleme waren dort festzustellen, wo die Gebührenberechnung nur grundstücksbezogen erfolgt und eine mengenunabhängige Grundgebühr nach der Anzahl der unter einer Anschrift wohnhaft gemeldeten Personen berechnet und erhoben wird. Hierfür bedarf es lediglich einer personenbezogenen Datenerhebung der Anschlusspflichtigen, d. h. der Grundstückseigentümer oder der ihnen gleichgestellte Erbbauberechtigte, Nießbraucher, Wohnungseigentümer und sonstigen zur Nutzung eines Grundstücks dinglich Berechtigten. Die dafür notwendigen Daten werden auf der Grundlage der Abgabenordnung von den für die Verwaltung der Grundsteuer zuständigen Behörden oder von den zuständigen Katasterbehörden nach dem Thüringer Katastergesetz angefordert. Des Weiteren werden zur Berechnung der mengenunabhängigen Grundgebühren lediglich die Anzahl der auf den bewohnten Grundstücken gemeldeten Personen benötigt, deren Übermittlung nach der ersten Thüringer Meldedatenübermittlungsverordnung vorgesehen ist. Soweit sich im Rahmen der Gebührenveranlagung ergibt, dass diese Anzahl nicht der tatsächlichen Zahl der Bewohner entspricht und deshalb die Grundstückseigentümer Widerspruch einlegen, muss dies zwischen dem Anschlusspflichtigen bzw. Wohnungsgeber, der Melde- sowie der Abfallbehörde geklärt werden. Dadurch wird gleichzeitig erreicht, dass mögliche Differenzen einzelfallbezogen auch zur Aktualisierung der Melderegister führen, ohne dass datenschutzrechtliche Bestimmungen verletzt werden. Tests zur erzeugerbezogenen Gebührenveranlagung durch die Benutzung von Müllschleusen hatten zu einer Zunahme der illegalen Entsorgungen bzw. zur Erhöhung der Grundgebühren aufgrund steigender Fixkosten geführt, sodass in diesem Landkreis an dem bisherigen Verfahren festgehalten und auch künftig auf die Einführung von Müllschleusen verzichtet werden soll.

In den beiden anderen kontrollierten Landkreisen wurde mit der Argumentation, dass eine Müllvermeidung und -reduzierung sowie eine Gebührengerechtigkeit nur erreicht werden könne, wenn der einzelne Haushalt gegenüber der Abfallbehörde als Gebührenpflichtiger bestimmt sei, eine haushaltsbezogene Datenerhebung und eine

entsprechende Meldepflicht der Haushalte festlege. Dass dabei bereits die Definition des Haushaltes zu Problemen führen kann, habe ich bereits ausführlich in meinem 2. TB (14.18) erörtert. In dem kontrollierten Landkreis hatten die fehlende Normenklarheit zum Umfang der Datenerhebung und zur Auskunftspflicht der Anschluss-, Benutzungs- und Gebührenpflichtigen zur Verunsicherung der Betroffenen und die teilweise nicht erforderliche sowie die Doppelerhebung von Daten zu Beschwerden und Verärgerung geführt. Die Ursachen dafür lagen darin, dass alle Haushalte auskunftspflichtig waren, aber nur ein Teil der Haushalte ihre mengenunabhängige Grundgebühr nach der Satzung unmittelbar bei der Abfallbehörde zu entrichten hatten (Eigentümer und Nutzer von Müllschleusen), während die übrigen „Mieterhaushalte“ die Müllgebühren im Rahmen der Betriebskostenzahlung gegenüber dem Vermieter zahlten. Darüber hinaus wurde der „gelbe Sack“ mit einer haushaltsbezogenen Registriernummer versehen. Im Ergebnis der Kontrolle wurden deshalb die Regelungen dahingehend konkretisiert, dass die Datenerhebung nur noch bei Personen erfolgt, die zur Gebührenzahlung unmittelbar herangezogen werden und der Umfang der Datenerhebung auf das erforderliche Maß beschränkt wurde.

In diesem Landkreis wird die behältervolumenbezogene Grundgebühr nach der Anzahl der Benutzungspflichtigen (Anzahl der Hausbewohner/Anzahl der Haushaltsangehörigen bzw. Bewohner einer Wohnung bei eigenem Abfallbehälter oder bei Schleusennutzung) berechnet wird. Somit beschränkte sich die Notwendigkeit der Datenerhebung auf die Anschlusspflichtigen bzw. die Benutzungspflichtigen, soweit diese ihre Abfallgebühren unmittelbar gegenüber der Abfallbehörde entrichten. In einem dritten Landkreis erhält demgegenüber den Bescheid für mengenunabhängige Grundgebühr jeder einzelne Privathaushalt, berechnet auf der Grundlage der Zahl der gemeinsam lebenden und wirtschaftenden Personen, während der Anschlusspflichtige nur noch die aufkommensabhängige Abfallgebühr entrichtet und ggf. auf die Mieter umlegt. Problematisch ist die Umsetzung dessen, was als „Haushalt“ definiert ist. Haushalt sind danach nämlich berechnete Personen, die alleine oder gemeinsam mit anderen eine selbständig bewirtschaftete oder in sich abgeschlossene Wohneinheit auf einem Grundstück nutzen. In der Praxis stellt sich letztlich heraus, dass die nach der Satzung auskunfts-

pflichtigen Haushalte nur bedingt ihrer Meldepflicht nachkommen, insbesondere wenn sich eine mengenunabhängige Gebührenerhöhung abzeichnet.

Deshalb wurde nach Möglichkeiten gesucht, die fehlenden Informationen - entgegen der Satzung - durch andere Quellen zu gewinnen. Im vorliegenden Fall wurden die Meldebehörden aufgefordert, jede natürliche oder räumliche Bevölkerungsbewegung personenbezogen, d. h. jeden Zu- oder Wegzug sowie jede Geburt und jeden Tod eines Einwohners der Abfallgebührenstelle namentlich mitzuteilen. Dies ist jedoch auf der Grundlage der geltenden melderechtlichen Bestimmungen in Thüringen unzulässig. Regelmäßige Datenübermittlungen sind in Thüringen nur erlaubt, wenn dafür eine konkrete Rechtsvorschrift vorliegt. Im Rahmen der Verabschiedung der ersten Meldedatenübermittlungsverordnung war um den Erfordernissen der Abfallbehörden zu entsprechen (s. o.) lediglich eine Vorschrift aufgenommen worden, dass den Landratsämtern regelmäßig die Anzahl der auf einzelnen Grundstücken wohnenden Personen mitgeteilt werden. Da die Melderegister ohnehin keine Angaben über Haushalte enthalten, war auf eine weiter gehende Regelung verzichtet worden, um zu vermeiden, dass in den Landkreisen zweite Melderegister eingerichtet werden.

Im kontrollierten Landkreis war dennoch diese regelmäßige Datenübermittlung erfolgt, mit dem Ziel der Aktualisierung der Datei der Gebührenpflichtigen. Dazu wurden die Einzeldaten „Haushalten“ zugeordnet, indem - soweit nicht von den Betroffenen eine Veränderung vorliegt, bei der sich die Übermittlung vom Meldeamt erübrigt - dies fiktiv anhand von plausiblen Hinweisen (wie Namensgleichheit), im Ergebnis weiterer Auskunftersuchen (im Regelfall als Rückfrage beim Betroffenen) oder nach eingelegten Widersprüchen gegen Gebührenbescheide erfolgt. Ich habe darauf hingewiesen, das Verfahren entsprechend der gesetzlichen Vorgaben zu verändern und darauf hingewiesen, dass aufgrund meiner Erkenntnisse meinen Anregungen bei der Neubekanntmachung des Thüringer Abfallwirtschafts- und Altlastengesetzes dahingehend gefolgt wurde, dass künftig die öffentlich-rechtlichen Entsorgungsträger verpflichtet sind, zur Durchsetzung ihrer Aufgaben nach dem Kreislaufwirtschafts- und Abfallgesetzes in Ihren Satzungen zu bestimmen, bei

welchen Personen oder Stellen welche personenbezogenen Daten erhoben werden sollen und bereits in der Erarbeitungsphase für entsprechende Satzungen die notwendigen Prüfungen der Datenquellen und Entscheidungen getroffen werden.

14.12 Auskunftserteilungen zu Prüfungen nach dem Landwirtschaftsanpassungsgesetz

Nach der Wende 1989 sind die ehemaligen Landwirtschaftlichen Produktionsgenossenschaften (LPG) den sozialen und ökologischen Bedingungen der Marktwirtschaft angepasst worden. Im Zuge des Umstrukturierungsprozesses kam es verschiedentlich zu Vermögensauseinandersetzungen zwischen den Rechtsnachfolgern der LPG und ehemaligen LPG-Mitgliedern. In § 70 Abs. 3 Landwirtschaftsanpassungsgesetz (LwAnpG) ist ein Prüfverfahren vorgesehen, welches die oberste Landesbehörde ermächtigt, sofern ihr Anhaltspunkte für ein gesetzwidriges Verhalten bei der Geschäftsführung der LPG vorliegen, Prüfungen vorzunehmen. In der Eingabe eines Bürgers teilte mir dieser mit, dass das TMLNU keine Auskünfte aus Gutachten, die anlässlich von Prüfungen nach § 70 Abs. 3 LwAnpG erstellt wurden, an beteiligte ehemalige LPG-Mitglieder erteilt. Die Mitteilung von Ergebnissen solcher Prüfungen sei aber notwendig, um bestehende Ansprüche zu prüfen und durchsetzen zu können. Ich bat daraufhin das TMLNU um eine Stellungnahme zu der Frage, welche Gründe gegen die Einsicht oder Auskunft durch ehemalige LPG-Mitglieder in die erstellten Gutachten bestehen. Gleichfalls wies ich darauf hin, dass nach meinem Kenntnisstand in Sachsen die Ergebnisse einer Überprüfung allen ehemaligen LPG-Mitgliedern bekannt gemacht werden. Nach Ansicht des TMLNU seien die Prüfungsverfahren in Sachsen und Thüringen nicht zu vergleichen. Während in Sachsen diese Prüfungen von externen Gutachtern (i. d. R. Wirtschaftsprüfer) im Auftrag des Landwirtschaftsministeriums durchgeführt werden, würde das TMLNU aus Kostengründen die Kontrollen nur mit eigenem Personal auf der Grundlage von Beschwerden immer unter dem Gesichtspunkt der vom Beschwerdeführer vorgetragenen Sachverhalte durchführen. Die jeweiligen Beschwerdeführer hätten nach der Prüfung durch das TMLNU ein individuelles Antwortschreiben erhalten. Im Gegensatz zu den sächsischen Gutachten, die die durchgeführte Vermögensauseinanderset-

zung wohl generell bewerten würden und es deshalb für jeden Betroffenen möglich sei, seine Individualrechte daraus herzuleiten, wären die Thüringer Prüfergebnisse hierfür ungeeignet. Soweit sich das begehrte Einsichtsrecht auf betriebliche Unterlagen (Bilanzen, Mitgliederlisten, Umwandlungsbeschlüsse, usw.) beziehe, bestünde für alle LPG-Mitglieder nach gefestigter BGH-Rechtsprechung die Möglichkeit, dies im Unternehmen wahrzunehmen. Aus diesem Grund sei es nicht nachvollziehbar, warum diese betrieblichen Unterlagen im TMLNU und nicht im Unternehmen eingesehen werden sollen.

Im Ergebnis konnte ich das TMLNU davon überzeugen, dass zumindest aus datenschutzrechtlichen Gründen eine Auskunft bzw. Einsichtnahme in die Unterlagen nicht unzulässig ist. Da die in § 22 Abs. 1 ThürDSG genannten Zulässigkeitsvoraussetzungen vorliegen, steht die Auskunftserteilung bzw. die Möglichkeit der Einsichtnahme im pflichtgemäßen Ermessen des TMLNU.

14.13 Kontrolle eines Amtes für Arbeitsschutz

Die Ämter für Arbeitsschutz, die im Geschäftsbereich des TMSFG dem Landesamt für Soziales und Familie (LASF) nachgeordnet sind, nehmen als Gewerbeaufsichtsbehörden Aufgaben zur Überwachung der Einhaltung arbeitsrechtlicher Vorschriften wahr. Dies reicht von der Gerätesicherheit über Gefahrstoffschutz, Jugendschutz bis hin zur Einhaltung von Lenkzeiten durch LKW- und Busfahrer. Bei Verstößen werden Bußgelder verhängt, was auch eine Erhebung und entsprechende Verarbeitung von personenbezogenen Daten mit sich bringt. Bei einer Kontrolle in einem Amt für Arbeitsschutz war festzustellen, dass neben ordnungsgemäß freigegebenen Verfahren zwei automatisierte Verfahren im Einsatz waren, für die keine Freigabe nach § 34 Abs. 2 ThürDSG vorlag. Die Begründung dafür war: Weil keinerlei Ausdrücke oder Übermittlung an andere Stellen aus dem Verfahren erfolgten, so die Stelle, sei man davon ausgegangen, dass es sich nicht um den Einsatz eines automatisierten Verfahrens handelte, mit dem personenbezogene Daten verarbeitet werden (§ 34 Abs. 2 ThürDSG). Dem habe ich entgegengehalten, dass der Verarbeitungsbegriff des § 3 Abs. 3 ThürDSG auch bereits das Speichern

von personenbezogenen Daten umfasst und es daher nicht darauf ankommt, ob die Daten ausgedruckt oder übermittelt werden. Nach meiner Beanstandung hat das hierfür zuständige LASF auf Antrag des Amtes die Verfahren freigegeben. Gleichzeitig wurden Anlagen- und Verfahrensverzeichnisse erstellt und Meldungen zum Datenschutzregister erstattet.

Geringfügige Verstöße z. B. gegen die vorgeschriebenen Ruhezeiten durch LKW-Fahrer werden - wie beim Falschparken auch - vom Amt für Arbeitsschutz mit einer Verwarnung und dem damit verbundenen Verwarnungsgeld geahndet. Wird das Verwarnungsgeld bezahlt, so ist ohne Feststellung von Schuld oder Unschuld an dem Verstoß die Sache erledigt. Wird nicht gezahlt, so werden zur Prüfung der Einleitung eines Bußgeldverfahrens mit einem Anhörungsbogen Angaben vom Fahrzeugführer zur Person und zur Sache erhoben. Die Angaben zur Sache sind freiwillig, d. h. es muss sich niemand selbst belasten. Demgegenüber ist der Betroffene verpflichtet, Angaben zur Person zu machen. Das vom Amt für Arbeitsschutz verwendete Formular enthielt zwar den Hinweis, dass Angaben zur Person in jedem Fall zu machen sind und der Betroffene sich nicht zur Sache äußern braucht. Allerdings war unter der Überschrift „weitere Angaben zur Person“ u. a. nach den wirtschaftlichen Verhältnissen gefragt. Ein Hinweis darauf, ob diese Angaben freiwillig oder aufgrund einer gesetzlichen Verpflichtung abgefragt werden, fehlte auf dem Formular. Vom Amt für Arbeitsschutz wurde das Fragen nach diesen Angaben damit begründet, dass schlechte wirtschaftliche Verhältnisse des Betroffenen bei der Bemessung der Höhe eines Bußgeldes zu dessen Gunsten berücksichtigt werden können. Das leuchtet zwar ein, gleichwohl muss dem Betroffenen die Wahl gelassen werden, ob er sich darauf berufen will. Daher habe ich der Stelle empfohlen, das Formular so umzuarbeiten, dass für den Betroffenen unzweifelhaft erkennbar ist, zu welchen Angaben er verpflichtet ist und welche er freiwillig machen kann.

15. Technischer und organisatorischer Datenschutz

15.1 Der Schritt in die Informationsgesellschaft

Die Informations- und Kommunikationswirtschaft gehört weltweit zu den dynamischsten Wirtschaftsbereichen. Dies ist ein nicht unwesentlicher Beleg für den derzeitigen Wandel von der Industriegesellschaft hin zu einer Informationsgesellschaft. Durch den Ausbau der Telekommunikationsinfrastruktur in den neuen Ländern besaßen Anfang 1998 nahezu alle privaten Haushalte mindestens ein stationäres Telefon. Eine statistische Erhebung durch das Thüringer Landesamt für Statistik ergab weiterhin, das derzeit von den Thüringer Haushalten ca. 32 % einen Anrufbeantworter, ca. 36 % einen PC und 9 % ein Faxgerät besitzen. Auch die Thüringer Wirtschaftszweige Herstellung von Büromaschinen, Datenverarbeitungsgeräten, usw. konnten im 1. Halbjahr 1999 eine hohe Umsatzproduktivität erzielen.

Die Informationsgesellschaft wird zu neuen Formen der Zusammenarbeit führen, wobei sich auch die Arbeitswelt der Mitarbeiter ändern wird. Schon heute sind Vertriebsmitarbeiter und Kundenbetreuer oft so genannte Teleworker. Mittlerweile ist eine junge Generation mit dem Internet und mit den neuen Technologien der IuK aufgewachsen. Für sie gehört deren Einsatz zur Normalität. Das Nutzen öffentlicher Netze, wie des Internet, ermöglichen eine schnelle und kostengünstige Datenübertragung. Diese Verbindungen weisen jedoch, wie bekannt, Schwachstellen und Risiken auf. So genannte Virtual Private Networks (VPN), welche eine verschlüsselte und zumeist auch komprimierte Datenübertragung über offene Netze ermöglichen, können in naher Zukunft im Hinblick auf die Sicherheit der zu übertragenden Daten einen nicht unwesentlichen Beitrag leisten. Insbesondere wird der Einsatz mobiler Kleingeräte in den nächsten Jahren rasant zunehmen. In Aussicht steht ein neuer Mobilfunkstandard mit der Bezeichnung Universal Mobile Telekommunikationssystem (UMTS). Die Einführung des UMTS-Standards, der für das Jahr 2002 vorgesehen ist, macht einen Datentransfer mit der hundert- bis zweihundertfachen Geschwindigkeit des heutigen Globalsystem for Mobile Communications-Standard (GSM) möglich. Durch die Entwicklung einer speziellen Technologie (Replikations-

mechanismen) können die Daten auf den mobilen Geräten mit zentral vorgehaltenen Daten abgeglichen werden. Mobiltelefone, mit denen man auch E-Mail versenden sowie im Internet surfen kann und auf denen datenbankgestützte Anwendungen laufen, werden zum Standard.

Neue Entwicklungen zeichnen sich auch bei Chipkarten ab. Während bei herkömmlichen Mikroprozessorkarten die einmal festgelegte Logik im Nachhinein nicht mehr verändert werden kann, bieten jetzt so genannte intelligente Mikroprozessorkarten die Möglichkeit, dass die Kartenbesitzer sich aus einem breiten Angebot verschiedener Anwendungen eine persönliche maßgeschneiderte Chipkarte zusammenstellen können, wobei neueste Applikationen auch per Internet oder an speziellen Automaten aufgespielt werden können. Die Hersteller werben damit, dass es für die Zusammenstellung beliebiger Kombinationen fast keine Grenzen gibt.

In großen Handelskonzernen sind derzeit so genannte Data-Warehouse-Lösungen im Aufbau, in denen Verkaufs-, aber auch Lieferdaten und Bestände für jeden Artikel und jede Filiale tagesgenau festgehalten werden. Permanent laufende Auswertungsprogramme sorgen u. a. auch dafür, dass das Kaufverhalten der Konsumenten erfasst wird und ermöglichen den Händlern bei systematischer Auswertung Rückschlüsse über das Einkaufsverhalten von Kunden.

Stand am Anfang des Internets nur eine Präsentation von Informationen an, kam inzwischen die Interaktivität mit dem jeweiligen Interessenten hinzu. Derzeit steht der Schritt von der Interaktivität zur Individualisierung insbesondere bei der Präsentation von Dienstleistungen und Produkten im World Wide Web (WWW) an. Jeder Besucher bekommt dabei ein für ihn maßgeschneidertes Informationsangebot angezeigt. Dazu können demographische Daten aus dem Data-Warehouse sowie Benutzerprofile und Kundendaten zu einem komplexen Verhaltensmuster generiert werden.

Mit diesen Entwicklungen sind auch Fragen des Datenschutzes und der Datensicherheit verbunden. Die Sicherheit von Daten selbst ist zu einer wirtschaftspolitischen Größe geworden. Informationen werden selbst zu einem begehrten Rohstoff. Allein für den europäischen Markt gehen Schätzungen davon aus, dass im Jahre 2005 mehr als 24 Milliarden Dollar an Sicherheitssoftware umgesetzt werden. 1998 waren es nur 1,1 Milliarden Dollar.

Für viele Unternehmen und Behörden wird die Vernetzung und Online-Datenübertragung als der Schlüssel für eine effektive Realisierung ihrer Aufgaben angesehen. Die Absicherung des eigenen Netzes gegenüber öffentlichen Netzen und die unversehrte sowie vertrauliche Übertragung von schutzwürdigen Daten über letztere stehen im Mittelpunkt hiermit verbundener sicherheitstechnischer Anforderungen und Maßnahmen. Ausgehend von den konkreten Bedrohungen sind geeignete Schutzmaßnahmen festzulegen. Hierzu zählen u. a. der Einsatz von Firewallsystemen, Verschlüsselungssoftware, Virens Scanner und die Realisierung von physischer Datensicherung, Zugangs- und Zugriffsschutz auf PC und Server sowie das Einrichten von Protokollierungsfunktionen und Monitoring. Die hierfür erforderlichen Aufwendungen können auch durch die gezielte Entwicklung und Anwendung datenschutzfreundlicher Technologien reduziert werden.

15.2 Einsatz von Informationstechnik in der Landesverwaltung

Die Thüringer Landesverwaltung weist einen hohen Anteil an Informationstechnik (IT) aus. So wird im Gesamtplan für 1998 bis 2000, der jährlich entsprechend der Zuarbeiten der Ressorts vom TIM erstellt wird, ausgewiesen, dass sich der Ausstattungsgrad der Arbeitsplätze mit IT (Terminals, Arbeitsplatzcomputer und Workstations) von 44 % im Jahre 1996 auf 80 % im Jahre 2000 erhöhen wird. Pro vorhandenen Büroarbeitsplatz werden im Jahr zwischen 2000 und 2500 DM (ohne Personalkosten) für IT ausgegeben. Im Jahr 1998 waren 532 Server und 145 Mehrplatzrechner in ca. 440 Lokalnets eingebunden. Durchschnittlich sind an jedem Server 19 Clients und an jedem Mehrplatzrechner 24 Terminals angeschlossen. Zu verzeichnen ist eine Tendenz zum zunehmenden Einsatz von Client-Serversystemen. Zurzeit dominiert noch bei Server- und Mehrplatzrechnern das Betriebssystem UNIX. Es zeichnet sich allerdings eine Zunahme von Rechnersystemen ab, die mit dem Betriebssystem Windows-NT-Server ausgestattet sind. So werden planmäßig im Jahre 2000 etwa 42 % der eingesetzten Server gegenüber 27 % im Jahre 1997 das Betriebssystem NT einsetzen. Die Zahl der vernetzten IT-Arbeitsplätze hat einen Anteil von ca. 79 % ge-

messen an der Gesamtanzahl der IT-Arbeitsplätze. Im Jahre 2000 wird sich dieser Anteil auf 94 % erhöhen. Bezüglich der eingesetzten Bürostandardsoftware sind die Textverarbeitung (91 % der APC) und die Tabellenkalkulation (86 % der APC) bestimmend. Im Jahr 2000 werden ca. ein Drittel der an vernetzten Arbeitsplatzcomputer tätigen Bediensteten die modernen elektronischen Kommunikationsdienste nutzen. Insbesondere die elektronische Kommunikation über das CN zeigt eine stark ansteigende Tendenz.

15.3 Das Corporate Network (CN) der Landesverwaltung

Das Corporate Network (CN) der Landesverwaltung bildet die Grundlage für die Kommunikation der Landesbehörden des Freistaats Thüringen untereinander. Über den hier eingerichteten zentralen Anschluss an das Internet werden weitere Kommunikationspartner erreicht.

Schon in den vergangenen Berichtszeiträumen (1. TB 15.5.1; 2. TB 15.2) nahm ich zum CN aus datenschutzrechtlicher Sicht Stellung. Hier sind u. a. auch grundsätzliche Anforderungen aus der Sicht des Datenschutzes beim Aufbau und Betrieb des CN dargelegt. Eine wesentliche Forderung stellt die Erarbeitung eines Sicherheitskonzeptes für den Betrieb des CN dar. Das TIM als verantwortliches Ressort sagte die Erarbeitung eines solchen Konzeptes zu. Im April 1998 wurde mir ein erster, noch nicht vollständiger Entwurf des Sicherheitskonzeptes zugeleitet, der entsprechend der Vorgehensweise nach dem IT-Sicherheitshandbuch des BSI erstellt worden ist und aus meiner Sicht auch eine fundierte Basis für das IT-Sicherheitskonzept bildet. Ungeachtet dessen ergaben sich aus datenschutzrechtlicher Sicht jedoch noch offene Fragen. So wurde zum Beispiel auf personenbezogene Daten nur marginal eingegangen. Ich teilte dem TIM mit, dass nach den datenschutzrechtlichen Vorschriften auch der Schutz personenbezogener Daten umfassend in den Entwurf einzubeziehen ist. Hierzu unterbreitete ich entsprechende Vorschläge. Im Entwurf werden durchweg die gängigen Sicherheitsfunktionen Vertraulichkeit, Integrität und Verfügbarkeit als Schutzziele herangezogen. Das Kriterium Verbindlichkeit, dass heißt inwieweit Daten einem Urheber zugeordnet werden können, fand keine Berücksichtigung. Die Verbindlichkeit ist jedoch für den zunehmenden elektronischen Nachrichtenaustausch ein wichtiger

Aspekt und sollte deshalb in die Bedrohungs- und Risikoanalyse einbezogen werden. Für das Stadium des Nutzbetriebes empfahl ich ein ressortübergreifendes zentrales Sicherheitsgremium einzurichten und unterbreitete für dessen Aufgaben diesbezügliche Vorschläge. Verbindlich sollte geregelt werden, dass eine Stelle an das CN nur angeschlossen wird, wenn diese über ein entsprechendes IT-Sicherheitskonzept verfügt. Bezüglich des geplanten Remote-Zugriffs, d. h. einen Zugriff von außerhalb des CN auf dessen Ressourcen, vertrat ich die Auffassung, dass ein solcher Zugang nur eingerichtet werden kann, wenn ein Zugriff Unbefugter nach dem derzeitigen Stand der Technik ausgeschlossen werden kann. Zum Einsatz von Protokollierungsfunktionen enthielt der vorliegende Entwurf keine konkreten Aussagen. Da insbesondere Firewalls über umfangreiche Protokollierungsfunktionen verfügen, bedarf es hierzu konkreter Regelungen.

Derzeit wird das CN schon von einer großen Anzahl von öffentlichen Stellen genutzt. Das eingesetzte Sicherheitssystem besteht u. a. aus einem mehrstufigen Firewall-System, welches den zentralen Übergang zum Internet bildet und die hierfür erforderlichen Schutzmaßnahmen realisiert. In das Sicherheitssystem können KryptoBoxen implementiert werden. Mit dem Einsatz dieser Boxen erfolgt eine Leitungsverschlüsselung, sodass der Datenverkehr zwischen zwei Boxen zwangsläufig verschlüsselt wird. Damit wurden auch datenschutzrechtlichen Forderungen entsprochen. Für den Zugang seitens der Einrichtungen der Landesverwaltung stehen ausgehend von deren Sicherheitsbedarf sechs Zugangsvarianten zur Auswahl. Die Entscheidung, welche der sechs Zugangsvarianten in den anzuschließenden Lokationen zum Einsatz kommt, wird anhand vorgegebener Kriterien gemeinsam zwischen dem jeweiligen Ressort, dem Netzbetreiber und dem TIM getroffen. Durch den kombinierten Einsatz einer Firewall und KryptoBoxen können angeschlossene Stellen nachzeitigem Erkenntnisstand ein hohes Sicherheitsniveau erzielen.

Obwohl nach Auskunft des TIM alle Maßnahmen, die zur Sicherheit des CN im IMA-IT sukzessiv beschlossen und von dem TLRZ/Systemhaus als Netzbetreiber im Wesentlichen umgesetzt wurden, fehlt nach wie vor ein verbindliches Sicherheitskonzept für

eine zielgerichtete und transparente Sicherheitspolitik zum Betreiben des CN, welches vor der Aufnahme des Benutzerbetriebes vorliegen sollte. Durch die zumeist einzeln im IMA-IT beschlossenen Sicherheitsmaßnahmen ist die sicherheitstechnische Gesamtkonzeption derzeit nur schwer nachvollziehbar. Das TIM teilte mir mit, dass an der Fertigstellung des IT-Sicherheitskonzeptes intensiv gearbeitet wird, meine Hinweise und Empfehlungen berücksichtigt wurden und noch beabsichtigt ist, das Thema "Digitale Signatur im CN" in den Entwurf einzubinden. Ich teilte daraufhin dem TIM mit, dass ich es in Anbetracht dessen nicht mehr für tragbar ansehe, ein so zentrales und relevantes Kommunikationsnetz, welches alle Ressorts und eine Vielzahl öffentlicher Stellen für ihre Kommunikation und diesbezügliche Anwendungen nutzen, ohne ein verbindliches Sicherheitskonzept zu betreiben. Weitere anstehende Themen könnten im Zuge der sowieso erforderlichen regelmäßigen Aktualisierungen in ein in Kraft gesetztes Sicherheitskonzept eingearbeitet werden. Inzwischen teilte mir das TIM mit, dass eine Fertigstellung der überarbeiteten Fassung des CN-Sicherheitskonzeptes für die achte Kalenderwoche des Jahres 2000 vorgesehen ist und der Komplex „Digitale Signatur“ gesondert bearbeitet wird.

Über das CN können auch die angeschlossenen Einrichtungen (Landtag, Landes- und Bundesdienststellen) miteinander zum Nulltarif sprachlich kommunizieren. Alle Gespräche die von außerhalb in das CN eingehen sowie die innerhalb des CN zwischen den angeschlossenen Einrichtungen geführt werden, werden über eine zentrale TK-Anlage vermittelt (2. TB 15.2.2). Für den Betrieb dieser TK-Anlage habe ich eine Betriebsordnung gefordert. Diese wurde vom TIM erarbeitet. Darin ist u. a. festgelegt, dass das Sicherheitskonzept für die zentrale TK-Anlage in das Sicherheitskonzept des CN eingebunden und die Konfiguration der zentralen TK-Vermittlungsanlage durch einen Revisor überprüft wird. Ich bat das TIM darum, das Sicherheitskonzept der zentralen TK-Anlage ebenfalls zeitnah zu vervollständigen. Da das Sicherheitskonzept der TK-Anlage nun unmittelbar in den Entwurf für das IT-Sicherheitskonzept des CN eingeflossen ist und mir bisher keine Information vorliegt, ob und wann dieses in Kraft gesetzt wurde, muss ich davon ausgehen, dass auch für die TK-Anlage kein verbindliches IT-Sicherheitskonzept in Kraft gesetzt ist. Offen ist die

Durchführung von Revisionen, d. h. eine Kontrolle des Ist- und Soll-Zustandes der TK-Anlage, welche einen wesentlichen und unverzichtbaren Beitrag zur Sicherheit der TK-Anlage in Bezug auf eventuelle Manipulationen darstellt. Ich muss deshalb weiterhin davon ausgehen, dass bisher solch eine Revision nicht stattgefunden hat. Auf meine diesbezügliche Bitte an das TIM um eine konkrete Stellungnahme hierzu, erhielt ich keine befriedigende Antwort. Das TIM teilte mir lediglich mit, dass das fachlich qualifizierte Personal bis zum heutigen Tag noch nicht zur Verfügung steht und im Zuge der momentanen Planungen zur Erweiterung der Nutzungsmöglichkeiten des CN auch für die Revisionstätigkeiten konkrete Vorschläge unterbreitet werden.

15.4 Konzentration der Rechenzentren der Landesverwaltung

Im August 1997 entschied die Landesregierung durch Kabinettsbeschluss, die Rechenzentren der Landesverwaltung zu einem Rechenzentrum mit Standort in der Landeshauptstadt Erfurt zusammenzufassen. Hiervon sind alle fünf Rechenzentren der Landesverwaltung betroffen, die mit Großrechnern ausgestattet sind. Im Einzelnen handelt es sich dabei um das

- Thüringer Landesrechenzentrum (TLRZ),
- Rechenzentrum des Landeskriminalamtes (LKA),
- Rechenzentrum der Bußgeldstelle (ZBS),
- Oberfinanzdirektion (OFD) - Rechenzentrum der Steuerverwaltung,
- Oberfinanzdirektion - Rechenzentrum der Zentralen Gehaltsstelle (ZG).

Für einen eventuellen Katastrophenfall wird ein Ausweichbetrieb im jetzigen ZG-Rechenzentrum der Oberfinanzdirektion in Suhl organisiert. Das neue Rechenzentrum, für das auch ein Neubau vorgesehen ist, um die derzeit verteilten Standorte zu konzentrieren, wird unter dem Namen "Zentrum für Informationsverarbeitung der Thüringer Landesverwaltung" (ZIV) geführt und ist der OFD zugeordnet. Für alle Landesbehörden, die Großrechnerverfahren einsetzen, besteht hinsichtlich des ZIV Benutzerzwang. Das ZIV ist zuständig für die Datenverarbeitung auf Großrechnern einschließlich der Ausdrucker-

stellung der Ergebnisdaten für alle Stellen des Landes, soweit diese Großrechnerleistungen in Anspruch nehmen. Die bestehende Fachaufsicht der einzelnen Ressorts für ihre auf dem Großrechnersystem ablaufenden EDV-Verfahren und -Programme wird von der Zusammenlegung nicht berührt. Auch die Bereiche Anwendungsprogrammierung und Verfahrensbetreuung verbleiben in der Zuständigkeit der Ressorts.

Im Rahmen dieses Konzentrationsprozesses wird das TLRZ in ein Systemhaus für Softwareentwicklung, -pflege und -betreuung, zunächst in die Rechtsform eines Landesbetriebes, umgewandelt. Inzwischen wurde gemäß einer Vereinbarung zwischen dem Thüringer Innenministerium und dem Thüringer Finanzministerium zum 01.01.1999 die Überleitung des kompletten Leistungsspektrums des bisherigen TLRZ-Rechenzentrumsbetriebs in das ZIV vorgenommen. Abweichend von den anderen Großrechnern, die unter dem Betriebssystem BS2000 arbeiten, wird auf dem ehemaligen Großrechner des TLRZ das Betriebssystem MVS eingesetzt. Auf diesem Rechner werden unter der Verfahrensbetreuung des TLRZ/Systemhaus zahlreiche Verfahren der Landes- und Kommunalverwaltung abgearbeitet.

Mit der Errichtung des ZIV sind auch originäre datenschutzrechtliche und sicherheitstechnische Fragen betroffen. Das Rechenzentrum der OFD-ZG, der OFD-Steuerverwaltung, das Rechenzentrum des LKA und das Rechenzentrum des TLRZ wurden von mir in den vergangenen Zeiträumen auf die Einhaltung der Vorschriften des ThürDSG kontrolliert, wobei insbesondere die seitens der Einrichtung ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen gem. § 9 ThürDSG geprüft wurden. Durch die Einrichtung des ZIV bedienen sich jetzt die betroffenen Stellen zur Erledigung ihrer Aufgaben anstatt, wie bisher eines eigenen Rechenzentrums, eines gemeinsamen Rechenzentrums. Damit liegt im Sinne von § 8 ThürDSG Auftragsdatenverarbeitung vor. Gem. § 8 Abs. 3 ThürDSG darf der Auftragnehmer, in diesem Fall das ZIV, die personenbezogenen Daten nur im Rahmen der Weisungen des jeweiligen Auftraggebers verarbeiten. Letzterer bleibt nach § 8 Abs. 1 ThürDSG weiterhin für die Einhaltung der Vorschriften des ThürDSG und anderer Vorschriften über den Datenschutz verantwortlich. Eine Besonderheit in diesem Zusammenhang liegt beim

TLRZ vor, das bislang selbst Auftragsdatenverarbeitung für Landes- und kommunale Stellen ausgeführt hat, aber jetzt die rechentechnischen Leistungen dazu nicht mehr selbst erbringen kann und hierfür das ZIV nutzt.

Die gemeinsame Abarbeitung von Verfahren mit teilweise sehr sensiblen Daten, die im Verantwortungsbereich unterschiedlicher Stellen liegen, bspw. der OFD-Steuerverwaltung und des LKA auf einem Rechnersystem, erfordern zusätzliche Sicherheitsmaßnahmen gegenüber der bisherigen Verfahrensabarbeitung. Insbesondere sind Vorkehrungen zu treffen, die eine sichere Abschottung von Verfahren und Daten der Stellen untereinander gewährleisten. Aus datenschutzrechtlicher Sicht muss hierbei die Absicherung der Vertraulichkeit, der Integrität und der Verfügbarkeit der Daten im Mittelpunkt der sicherheitstechnischen Betrachtungen stehen. Die OFD teilte mir Mitte 1998 mit, dass mit der Zusammenführung der fünf Rechenzentren externe Fachberatung in Anspruch genommen und auch ein IT-Sicherheitskonzept erarbeitet wird. So wurden im Auftrag der OFD eine Studie zu "Anforderungen an das neue Rechenzentrum" sowie Projektaufträge zur Organisationsstruktur und zum technischen Betriebskonzept des ZIV erstellt, deren Ergebnisse mir zwischenzeitlich vorliegen. Die von mir hierzu gegebenen Hinweise und Empfehlungen zu datenschutzrechtlichen und sicherheitstechnischen Sachverhalten werden von der OFD berücksichtigt.

In der Studie "Anforderungen an das neue Rechenzentrum" werden ausgehend von möglichen Bedrohungen die generellen Schutzziele und Anforderungen sowie sicherheitstechnische Maßnahmen für die Infrastruktur des neuen Rechenzentrums dargelegt. Konkrete Anforderungen und Maßnahmen sind u. a. für Sicherheitssysteme wie beispielsweise Gefahrenmeldeanlage, Einbruchmeldeanlage, Außensicherung und Innenüberwachung, Zutrittskontrollanlage, Wasserwarnsystem, Brandmeldeanlage sowie zu Feuerlöschsystemen aufgezeigt. Desweiteren werden detaillierte Ausführungen zur Sicherheitsorganisation unterbreitet.

Im August 1999 erhielt ich auf meine Anforderung vom TFM das Konzept zur Organisationsstruktur und das technische Grobkonzept/Betriebskonzept für das ZIV. Weiterhin wurde mir der Entwurf

für eine Geschäftsordnung für den Anwenderbeirat des ZIV übergeben. Der Anwenderbeirat stellt als ressortunabhängiges Gremium die Interessenvertretung aller Anwender des ZIV dar. Im Anwenderbeirat sind auch das TLRZ/Systemhaus und das ZIV vertreten. Aufgabe des Anwenderbeirats ist die Koordinierung des IT-Einsatzes des ZIV und die Festlegung langfristiger Strategien zur Fortentwicklung des ZIV aufzuzeigen. Der Anwenderbeirat besitzt das Recht, weitere beratende Mitglieder im Bedarfsfall für die Sitzungen zu benennen, wobei beispielhaft der TLfD aufgeführt ist. Diese Regelung wird von mir begrüßt, da hiermit die unmittelbare Möglichkeit gegeben ist, schon in einem frühzeitigen Stadium auf datenschutzrechtliche Anforderungen hinzuweisen und entsprechende Lösungsvorschläge zu unterbreiten.

In dem technischen Grobkonzept/Betriebskonzept werden datenschutzrechtliche Fragen nur insofern behandelt, als hier Grundsätze für die Regelung der Verantwortlichkeiten zwischen ZIV und Anwender im Hinblick auf Datenschutz und Sicherheit der Informationsverarbeitung dargelegt sind. So sind Festlegungen zur Erteilung der datenschutzrechtlichen Auflagen, zur Kontrolle des physischen Zugangs zu den Servicestandorten und zum Zugriffsschutz aufgeführt.

In dem Grobkonzept zur Organisationsstruktur des ZIV sind in einem Unterpunkt grundsätzliche Ausführungen zur Erstellung des IT-Sicherheitskonzeptes enthalten. Das aufgezeigte Vorgehen orientiert sich am IT-Sicherheitshandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Damit ist eine Vorgehensweise festgelegt, die ich schon im 1. TB 15.3 dargelegt habe und von mir auch im vorliegenden Fall als angemessen angesehen wird.

In einer Gesprächsrunde, an der die Verantwortlichen des TFM und der OFD für das ZIV sowie die Bearbeiter des Sicherheitskonzeptes von Seiten des beauftragten Unternehmens teilnahmen, erörterte ich noch einmal die mit der Gründung des ZIV zu beachtenden datenschutzrechtlichen Fragen. Seitens der Verantwortlichen wurden die Vorgehensweise, die bisherigen Aktivitäten und die bisher erreichten Ergebnisse dargelegt. Die externen Berater, welche das IT-Sicherheitskonzept erarbeiten, erläuterten dessen Zielstellungen, die Vorgehensweise und in einer ersten Übersicht auch inhaltliche Aspekte des Konzeptes. Die seitens der Gesprächsteilnehmer darge-

legten Ziele und inhaltlichen Darstellungen zu dem derzeit erarbeiteten IT-Sicherheitskonzept stehen in Übereinstimmung mit den datenschutzrechtlichen Anforderungen. Das IT-Sicherheitskonzept zielt u. a. auf die Bereitstellung isolierter Umgebungen für jeden Kunden und revisionssicherer IT-Dienstleistungen ab. Für alle Verfahren ist vorgesehen ausgehend von einer Schutzbedarfsanalyse die Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit zu beschreiben und die zu ihrer Gewährleistung erforderlichen technischen und organisatorischen Maßnahmen im Zusammenhang darzustellen. Für Verfahren mit einem hohen Schutzbedarf wird zusätzlich eine Bedrohungs- und Risikoanalyse durchgeführt. Desweiteren ist vorgesehen, die Kommunikationsverbindungen über das Corporate Network generell zu verschlüsseln. Es wurde vereinbart, dass das IT-Sicherheitskonzept nach Fertigstellung dem TLfD kurzfristig zur Prüfung bereitgestellt wird.

In der anschließenden Diskussion wurden u. a. auch Fragen zur Auftragsdatenverarbeitung gem. § 8 ThürDSG besprochen. Dabei wies ich darauf hin, dass das ZIV als Auftragnehmer gem. § 8 Abs. 2 ThürDSG seine Kunden auch über alle Dienstleistungen informieren muss, die im Auftrag des ZIV durch Fremdfirmen im Unterauftragsverhältnis ausgeführt werden und als Vertragsgegenstand eine Verarbeitung o. g. personenbezogener Daten beinhaltet. Dies erachte ich als erforderlich, damit die Auftraggeber ihren gesetzlichen Verpflichtungen gem. § 8 ThürDSG umfassend nachkommen können.

15.5 Projekt TESTA - Länderübergreifende Kommunikation

Mit dem Projekt TESTA (Trans European Services for Telematics between Administrations) wird die Vernetzung von Standorten der öffentlichen Verwaltung der EU-Länder für Datenkommunikation ausgeführt. Da zwischenzeitlich alle Länder der Bundesrepublik über eigene in sich geschlossene Landesnetze (Corporate Network CN, 1. TB 15.5.1; 2. TB 15.2, 15.3) verfügen, besteht seitens der Einrichtungen des Bundes und der Länder einschließlich deren Landesvertretungen ein starkes Interesse an einer kostengünstigen länderübergreifenden Kommunikation auf Basis eines so genannten Overlay-Netzes. Hierfür wurde zunächst im Rahmen des Projektes TESTA EUROPA das TESTA-Deutschland Netz als ein in sich geschlossenes Intranet des Bundes, der Bundesländer und künftig

auch der Kommunalverwaltungen konzipiert. TESTA Deutschland erhält Zugang zu TESTA Europa, sodass neben der Kommunikation der öffentlichen Einrichtungen in Deutschland untereinander auch eine solche im europäischen Maßstab ermöglicht wird. Vorerst ist das Overlay-Netz nur für die Datenkommunikation vorgesehen. Die Möglichkeit hierüber auch zukünftig die Sprachkommunikation zu realisieren wurde offen gehalten.

Für die Gesamtkonzeption und die Nutzung von TESTA ist der KoopA-ADV (Kooperationsausschuss Automatisierte Datenverarbeitung Bund, Länder, Kommunaler Bereich) verantwortlich. Das Land Thüringen vertreten durch das TIM hat die Projektsteuerung übernommen. Im Auftrag des KoopA-ADV hat der Freistaat Thüringen einen in diesem Ausschuss abgestimmten Rahmenvertrag zur Realisierung und zum Betrieb dieses TESTA-Netzes mit der Deutschen Telekom AG abgeschlossen. Inhalt des Vertrages ist die Bereitstellung eines bundesweiten Intranets für die Einrichtungen der öffentlichen Verwaltung. Neben allen Bundesländern, ihren nachgeordneten Einrichtungen sowie den Landesvertretungen beim Bund sind auch der Bund, seine nachgeordneten Einrichtungen und auch der kommunale Bereich berechtigt, diesem Vertrag beizutreten. Bis dato sind dem Rahmenvertrag alle Bundesländer und der Bund beigetreten.

Schon in meinem 1. TB (15.6) habe auf die Sicherheitsrisiken für die Verarbeitung von Daten hingewiesen, die mit der zunehmenden Vernetzung von Computern verbunden sind. Aus datenschutzrechtlicher Sicht ist besonders relevant, ob für das Projekt ein Sicherheitskonzept vorhanden ist und inwieweit Sicherheitsvorkehrungen für die zu übertragenden Daten getroffen wurden bzw. vorgesehen sind, um insbesondere einen Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit dieser Daten vorzubeugen. Auf meine Anforderung zur Bereitstellung der erforderlichen Unterlagen wurde mir vom TIM der o. g. Rahmenvertrag zur Verfügung gestellt.

In dem Rahmenvertrag - weitere Unterlagen standen mir vorerst nicht zur Verfügung - sind technische und organisatorische Maßnahmen zur Datensicherheit ausgehend von den möglichen Bedrohungen nicht explizit aufgeführt. Anhand dieser Unterlage konnte

ich mir jedoch einen ersten Überblick zu TESTA verschaffen. So arbeitet TESTA auf der Grundlage des paketorientierten Datenübertragungsdienstes Frame Relay, einer speziellen und weiterentwickelten Variante des bekannten X.25 Protokolls. TESTA nutzt die vorhandenen Netzressourcen der Deutschen Telekom, die auch durch eine Tochterfirma die erforderliche Netzadministration durchführt. Im Netz werden die Datenpakete mittels spezieller Netzknoten (Router) übertragen. Die jeweiligen Landesnetze sind über sog. Gateways, das sind spezielle Rechner, welche für die erforderliche Kompatibilität zwischen den jeweiligen Landesnetzen und TESTA sorgen, an TESTA angeschlossen. Jedes Bundesland stellt nur einen gesicherten zentralen Zugang zum TESTA-Netz bereit. Der zentrale Übergang bspw. für das Land Thüringen erfolgt über eine mehrstufige Firewall, welche das Landesnetz mittels spezieller Hard- und Software gegenüber dem Overlay-Netz absichert. In der ersten Ausbaustufe von TESTA stehen den Nutzern als Dienste u. a. E-Mail sowie bei entsprechender Berechtigung der Zugriff auf die JURIS-Datenbank (Juristisches Auskunftssystem) in Saarbrücken zur Verfügung.

Um nähere Informationen über die Sicherheitsvorkehrungen von TESTA zu erhalten, wandte ich mich erneut an das TIM. Von diesem wurde ausgeführt, dass TESTA hoch gesicherte Verwaltungsnetze verbindet und selbst gut gesichert ist. Die Netzzugänge der Kommunikationspartner sind über feste virtuelle Verbindungen zu einem Virtuellen Privaten Netzwerk (VPN) zusammengeschaltet. Die Netzverbindungen werden durch DLCI (Data Link Control Identifier) vor unerlaubten Zugriffen von außerhalb des VPN geschützt. Es handelt sich hierbei um ein Kennzeichnungsfeld zur Identifizierung einer Frame-Relay Verbindung. Weiterhin werden im TESTA-Netz IP-Adressen (Netzknoten- und Rechneradressen) verwendet, die nicht im Internet geroutet werden. Auch die in den Ländern intern verwendeten IP-Adressen werden in den Zugangsknoten des TESTA-Netzes umgesetzt und sind somit hier nicht bekannt. Damit wird Angriffen auf die internen Netzknoten und Rechner vorgebeugt. Vorgesehen sei auch, ein hardwarebasiertes kryptographische Verfahren zur Leitungsverschlüsselung einzusetzen. Gedacht ist an eine symmetrische Verschlüsselung der Datenpakete bei ihrer Übertragung im TESTA-Netz, und zwar beginnend vom je-

weiligen TESTA-Eingangsknoten bis zum entsprechenden Ausgangsknoten. In diesem Zusammenhang wurde jedoch erwähnt, dass für die Umsetzung dieser Leitungsverchlüsselung erhebliche praktische Probleme gesehen werden, insbesondere für das Management der Kryptoboxen. Insofern sei der Einsatz der Leitungsverchlüsselung noch offen. Ich vertrat gegenüber dem TIM die Auffassung, dass aus datenschutzrechtlicher Sicht eine Leitungsverchlüsselung für die Absicherung der Vertraulichkeit der Daten während der Übertragung im TESTA-Netz außerordentlich bedeutsam ist. Mit dieser würde nämlich unabhängig vom Kenntnisstand des jeweiligen Nutzers sowie seiner eingesetzten Software eine automatische und obligatorische Verschlüsselung der Datenpakete erfolgen. Da für die Übertragung sensibler Daten auch eine Verschlüsselung auf Anwendungsebene (Ende-zu-Ende-Verschlüsselung) erforderlich ist, muss TESTA hierfür offen sein. Im Hinblick auf den Einsatz der digitalen Signatur (2. TB 15.7.5), sollte auch geprüft werden, inwieweit für TESTA eine zentrale Zertifizierungsstelle zum Schlüsselmanagement (Trust-Center) aufgebaut werden sollte. Auch ein Sicherheitskonzept, in welchem u. a. die grundlegenden Sicherheitsmaßnahmen nachvollziehbar für die Nutzer von TESTA aufgezeigt sind, halte ich für einen datenschutzgerechten Betrieb erforderlich. Ich bat das TIM, sich beim KoopA-ADV für die Realisierung dieser Forderungen, die auch in Übereinstimmung mit dem AK-Technik der Datenschutzbeauftragten des Bundes und der Länder stehen, einzusetzen.

Das TIM teilte mir mit, dass sich der KoopA-ADV intensiv mit den Sicherheitsanforderungen an das TESTA-Netz beschäftigt hat. Eine Arbeitsgruppe des KoopA-ADV wurde beauftragt, die entsprechenden Vorleistungen zur Einführung der Leitungsverchlüsselung zu schaffen und hierzu ein Pflichtenheft zu erstellen. An einem Sicherheitskonzept wird gearbeitet. Für die Einrichtung eines Trust-Center wird derzeit kein zwingender Zusammenhang mit TESTA gesehen, hierfür wären insbesondere die Aktivitäten und Erfahrungen des Bundes für das Pilotprojekt SPHINX im Rahmen des Informationsverbundes Bonn-Berlin von Bedeutung. Die obige Entscheidung des KoopA-ADV leistet somit im Sinne des Datenschutzes einen wesentlichen Beitrag für einen Grundschutz gegen den Verlust der Vertraulichkeit der über das TESTA-Netz übertragenen Daten.

15.6 Technische und organisatorische Kontrolltätigkeit

15.6.1 Zum Ablauf einer Kontrolle

Bei der Vorbereitung und Durchführung einer solchen Kontrolle zeigte sich immer wieder, dass nicht wenige öffentliche Stellen über das Ziel und den Ablauf einer solchen Kontrolle keine ausreichende Vorstellung hatten. Nachfolgend deshalb einige grundsätzliche Ausführungen hierzu.

§ 9 ThürDSG bestimmt, dass öffentliche Stellen, die personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen haben, welche erforderlich sind, um die Ausführungen der Vorschriften des Thüringer Datenschutzgesetzes und anderer Vorschriften des Datenschutzes zu gewährleisten. Diese Verpflichtung zur Durchführung von Maßnahmen gilt sowohl für die automatisierte als auch für die nicht-automatisierte Datenverarbeitung. Im Rahmen der Kontrolle vor Ort wird festgestellt, inwieweit die ergriffenen technischen und organisatorischen Maßnahmen der öffentlichen Stelle in ihrer Gesamtheit und unter Beachtung des Grundsatzes der Angemessenheit die o. g. Zielstellung erfüllen. Insbesondere wird geprüft, inwieweit die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Authentizität der zu verarbeitenden personenbezogenen Daten sowie die Nachvollziehbarkeit der Verarbeitung gewährleistet ist. Nachvollziehbarkeit bezieht sich darauf, ob festgestellt werden kann, wer, wann, welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit) und inwieweit die Verfahrensweisen vollständig und aktuell dokumentiert sind (Transparenz). Unter Beachtung der vorhandenen Infrastruktur sowie der eingesetzten Hard-, System- und Anwendungssoftware wird im konkreten Fall festgestellt, ob die gem. § 9 Abs. 2 ThürDSG zu ergreifenden Sicherheitsmaßnahmen (1. TB 15.2) im Sinne der o. g. Zielstellung hinreichend vollzogen sind. Einbezogen sind in diese Prüfung auch erforderliche organisatorische Regelungen. In Anbetracht der fortschreitenden Vernetzung von EDV-Systemen werden zunehmend auch die getroffenen Maßnahmen zur Absicherung der lokalen Netze bzw. Intranets in die Kontrolle einbezogen. In Vorbereitung der Prüfung werden von der zu kontrollierenden Stelle i. d. R. die jeweils aussagekräftigen Unterlagen hierzu

angefordert. Im Ergebnis der Kontrolle erhält die öffentliche Stelle grundsätzlich einen Kontrollbericht. Der Bericht enthält den festgestellten Sachverhalt, dessen datenschutzrechtliche Würdigung sowie Forderungen, Empfehlungen und Hinweise zur Abstellung eventuell vorgefundener datenschutzrechtlicher oder sicherheitstechnischer Mängel. Über die Kontrolltätigkeit und hieraus folgende Erkenntnisse informiere ich regelmäßig im Rahmen meiner Tätigkeitsberichte (1. TB 15.14; 2. TB 15.4).

15.6.2 Feststellungen und Hinweise im Rahmen der Kontrolltätigkeit

Die Mehrzahl der von mir kontrollierten Stellen hatten gem. § 9 ThürDSG hinreichende technische und organisatorische Sicherheitsmaßnahmen zum Schutz der zu verarbeitenden personenbezogenen Daten ergriffen. Obwohl ich hier auch im Einzelfall bei der Kontrolle Schwachstellen feststellen musste, waren diese aufgrund der insgesamt getroffenen Maßnahmen jedoch nicht wesentlich, um den erzielten Schutzeffekt zu beeinträchtigen und wurden zumeist kurzfristig behoben. Insgesamt konnte ich feststellen, dass sicher auch aufgrund meiner Informationstätigkeit, die datenschutzrechtlichen Anforderungen an Sicherheitsmaßnahmen bewusster und auch gezielter unter Beachtung der Sensibilität der personenbezogenen Daten vorgenommen wurden. Allerdings stellte ich auch in diesem Berichtszeitraum wieder datenschutzrechtliche Unzulänglichkeiten im Ergebnis durchgeführter Kontrollen fest, über die ich weitestgehend auch schon in vorhergehenden Tätigkeitszeiträumen berichtete. Solche datenschutzrechtlichen Probleme und Feststellungen im Zuge der Kontrolltätigkeit waren insbesondere, dass

- keine datenschutzrechtliche Freigabe des eingesetzten Verfahrens gem. § 34 Abs. 2 ThürDSG vorlag,
- Datenschutzregistermeldungen unvollständig oder gar nicht vorlagen,
- kein Anlagen und Verfahrensverzeichnis nach § 10 ThürDSG vorhanden war,
- Verträge zur Datenverarbeitung im Auftrag nicht den Regelungen des § 8 ThürDSG entsprachen,

- Login-Prozeduren nicht den Anforderungen genügten, wobei insbesondere keine ausreichende Limitierung fehlerhafter Login-Versuche erfolgte,
- statt einer benutzerbezogenen Identifikation und Authentifikation Gruppenkennungen eingesetzt wurden,
- keine Passwortregelungen vorhanden waren,
- elementare Sicherheitsmechanismen wie Boot-Passwortschutz nicht ergriffen und Diskettenlaufwerke nicht gesperrt wurden,
- unzulässige Zugriffsrechte eingerichtet waren sowie
- eine unzureichende Protokollierung erfolgte.

Gem. § 9 Abs. 1 ThürDSG haben die öffentlichen Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des ThürDSG zu gewährleisten. Die Verantwortung hierfür liegt bei der jeweiligen öffentlichen Stelle. Gefordert sind aber auch die behördlichen Datenschutzbeauftragten und IT-Verantwortlichen, um künftig diese Unzulänglichkeiten vermeiden zu helfen. Hinweise und Empfehlungen zu den aufgezeigten Feststellungen gab es meinerseits bereits in den bisherigen Tätigkeitsberichten (1. TB 15.2, 15.6, 15.8, 15.12, 15.14; 2. TB 15.4).

15.6.3 Kontrolle im TIM

Das Abhandenkommen von zwei Computern im TIM mit teilweise sehr sensiblen Daten im Zuge des Umzugs der Behörde habe ich als schwer wiegenden Verstoß gegen datenschutzrechtliche Bestimmungen, insbesondere gegen § 9 Abs. 2 ThürDSG, gewertet und eine Beanstandung gegenüber dem TIM ausgesprochen. Im Ergebnis der durchgeführten Kontrollbesuche im TIM wurde auf Mängel und Schwachstellen beim Umzug mit personenbezogenen Daten hingewiesen und in diesem Zusammenhang datenschutzrechtliche Forderungen erhoben und Empfehlungen gegeben. In der Stellungnahme des TIM wurden umfangreiche Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit angekündigt. So gehörten bspw. zu diesen Maßnahmen die Überarbeitung der Konzeption für die Sicherheit des Gebäudes, objektsichernde Maßnahmen, die technische Überwachung, das Inkrafttreten einer Dienstanweisung zur

Gewährleistung von Datenschutz und Datensicherheit, von Leitblättern zur Regelung bei Störanfällen sowie eines Sicherheitsleitfadens (SLF) für PC Technik. Ich habe die bereits eingeleiteten technischen und organisatorischen Maßnahmen als geeignet angesehen, ein entsprechendes Datenschutzniveau zu sichern. Gleichzeitig habe ich angekündigt, die Umsetzung dieser Maßnahmen auch zu kontrollieren.

Im Zuge der öffentlichen Diskussion zu dieser Problematik gab es verstärkte Nachfragen anderer Behörden in Thüringen zu datenschutzrechtlichen Empfehlungen und Hinweisen in Vorbereitung und Durchführung von Behördenumzügen. Eine Handreichung dazu habe ich zusammengestellt (Anlage 23), die im Übrigen auch in der Zeitschrift Datenschutz und Datensicherheit (DuD) im Heft 11 des Jahres 1998 unter dem Thema „Umzugsrichtlinien“ veröffentlicht worden ist.

Bei den erneuten Kontrollbesuchen im TIM im Jahre 1999 überprüfte ich die infrastrukturellen Maßnahmen zur Absicherung des zentralen Rechnerraumes, die Nutzerverwaltung für den Server, die vergebenen Benutzereigenschaften, die eingestellten Richtlinien für Konten sowie Überwachungsrichtlinien und erteilte Freigabeberechtigungen für logische Laufwerke der Server, von Clients, Drucker etc.. In zwei Fachbereichen kontrollierte ich die für PC ergriffenen Sicherheitsmaßnahmen. Im Ergebnis wurde festgestellt, dass nicht alle Maßnahmen des „SLF“ umgesetzt waren. Bspw. waren entgegen den im SLF vorgegebenen Maßnahmen auf den kontrollierten PC's keine Boot-Passworte aktiviert und bei einem PC das Diskettenlaufwerk nicht gesperrt. Meiner Empfehlung, aus Sicherheitsgründen die Systemadministrator-Kennung umzubenennen und jedem Administrator eine eigene Kennung zuzuordnen, um seine Aktivitäten ggf. nachzuvollziehen, wurde nachgekommen. Bei der Überarbeitung des SLF wurden meine Empfehlungen berücksichtigt, was die Protokollauswertung der Überwachungsrichtlinien und Handlungsanweisungen zur Verfahrensweise bei festgestellten Sicherheitsverstößen betrifft. Konkrete Vorgaben wurden auch gemacht, was die Nachweisführung für vergebene Zugriffsrechte, die Passworthandhabung im Vertretungsfall und die Aufbewahrung der Protokolldateien betrifft. Der Empfehlung, einen IT-Geheimsschutzbeauftragten zu bestellen wollte das TIM ebenfalls

nachkommen. Weiter wurden im Berichtszeitraum auch Richtlinien zur technischen Sicherung und Bewachung von Verschlusssachen (VS-Sicherungsrichtlinien - VSSR) in Kraft gesetzt.

Ich habe dem TIM mitgeteilt, dass ich meine datenschutzrechtlichen Forderungen als erfüllt und den Kontrollvorgang als abgeschlossen ansehe.

15.6.4 Kontrolle der Oberfinanzdirektion (OFD)

Die Kontrolle hatte das Ziel, die automatisierte Verarbeitung personenbezogener Daten in dem Rechenzentrum (RZ) der OFD einschließlich des vorhandenen technischen und organisatorischen Umfeldes unter Beachtung der nach § 9 ThürDSG geforderten Maßnahmen zu überprüfen. Dabei wurden sowohl sachbereichsübergreifende Aspekte der IT-Sicherheit als auch die konkrete Umsetzung bzw. Realisierung von verfahrensbezogenen Sicherheitsmechanismen einbezogen.

Beanstanden musste ich den Einsatz des Zutrittskontrollsystems, des Zeiterfassungssystems und die Sprachkommunikation, mit denen personenbezogene Daten verarbeitet wurden, ohne entsprechende datenschutzrechtliche Freigaben nach § 34 Abs. 2 ThürDSG. Hinzu kam, dass das Zutrittskontrollsystem als auch die Sprachkommunikation von Dritten betrieben wurde, was eine Auftragsdatenverarbeitung darstellt. Darüber hinaus wurden Daten aus dem Zutrittskontrollsystem zur Verarbeitung im Zeiterfassungssystem genutzt, was von der Arbeitszeit- Dienstvereinbarung nicht vorgesehen war. Diese datenschutzrechtlichen Mängel sind zwischenzeitlich behoben.

Im Rahmen der Kontrolle wurde insbesondere das Verfahren „Integriertes Automatisiertes Besteuerungsverfahren“ (IABV) geprüft. Das System IABV wurde in den Siebziger- und Achtzigerjahren in Bayern entwickelt und wird auch in anderen Bundesländern eingesetzt. Es dient der Erfassung und Verarbeitung personenbezogener Daten zur Erstellung von Steuerbescheiden, Informationen für das Auskunftsverfahren sowie von Listen und Statistiken durch die Finanzämter und wird zentral im RZ der OFD eingesetzt. Dabei erfolgt

zwischen der OFD und den einzelnen Finanzämtern ein ständiger Datenaustausch.

Aus datenschutzrechtlicher Sicht sind auf Grund der Sensibilität der Daten im Steuerbereich die mit IABV verarbeitet werden, diese gemäß dem empfohlenen Schutzstufenkonzept des TLfD dem hohen Schutzbedarf -Stufe 2- zuzuordnen (1. TB 15.3). Die Zugangs- und Zugriffskontrolle für die Mitarbeiter in den Finanzämtern auf die zentral im RZ gespeicherten Daten ist hinreichend. Jeder Mitarbeiter wird eindeutig identifiziert und muss sich durch ein selbst vergebenes Passwort authentisieren. Die Aktivitäten beim schreibenden Zugriff auf die Daten werden nachvollziehbar protokolliert.

Bemängeln musste ich allerdings, dass von Seiten der Programmierer, Verfahrensbetreuer und Administratoren des OFD-Rechenzentrums der Steuerverwaltung nur mit gruppenbezogenen Kennungen auf den Großrechner (HOST) der OFD zugegriffen werden kann. Eine benutzerbezogene Identifikation und Authentifikation ist somit nicht möglich. Weiterhin musste ich feststellen, dass insgesamt die vorhandenen Protokollierungen unzureichend waren. Um in beiden Fällen den datenschutzrechtlichen Forderungen gerecht zu werden, würden nach Aussagen der OFD umfangreiche und komplexe Korrekturen erforderlich sein, die mit einem gewissen Risiko für die Funktionalität des Systems verbunden sind. Im Hinblick auf die bevorstehende Ablösung des Systems IABV durch das System FISCUS habe ich es deshalb als vertretbar angesehen, eine solche Systemanpassung nicht mehr durchzuführen.

Die Übertragung der Daten von den Finanzämtern an das Rechenzentrum der OFD erfolgte zum Zeitpunkt der Kontrolle unverschlüsselt über ein sternförmiges Standleitungsnetz, welches von der Telekom der OFD in Form einer geschlossenen Benutzergruppe zur Verfügung gestellt wurde. Auch wenn mit geschlossenen Benutzergruppen gearbeitet wird, kann nicht ausgeschlossen werden, dass über vermittelnde Netzknoten oder Leitungen Einblick in die Daten durch Unbefugte genommen werden kann und auch Manipulationen hierbei möglich sind. Nur durch den ergänzenden Einsatz kryptographischer Verfahren lassen sich die Vertraulichkeit und die Integrität der Daten von IABV wirksam schützen (2. TB 15.7). Nach Angaben des Thüringer Finanzministeriums werden inzwischen alle Daten der

Steuerverwaltung durch den Einsatz von Kryptoboxen nur in verschlüsselter Form über das CN, zwischen dem Zentrum für Informationsverarbeitung der Thüringer Landesverwaltung -ZIV- (15.4) und den Finanzämtern übertragen.

Bei der Fernwartung wurde empfohlen, zukünftig sichere Identifikations- und Authentifikationsverfahren einzusetzen, die mit Einmalpasswörtern auf Basis einer asymmetrischen Verschlüsselung arbeiten, um so Risiken wie z. B. Verlust der Vertraulichkeit, den Verlust der Integrität der vorgehaltenen Daten und dem Verlust der Verfügbarkeit des Systems zu begegnen.

15.6.5 Kontrolle im Thüringer Landesverwaltungsamt

Das Thüringer Landesverwaltungsamt (TLVwA) wurde im vorhergehenden Berichtszeitraum bereits einer datenschutzrechtlichen Kontrolle unterzogen. Die damals bemängelten technischen und organisatorischen Unzulänglichkeiten auf dem Gebiet des Datenschutzes insbesondere bei der Anwendung der automatisierten Datenverarbeitung wurden nach Angaben des TLVwA zwischenzeitlich behoben (2. TB 5.1.9). Das bis Ende 1997 zugesagte IT-Sicherheitskonzept des TLVwA stand allerdings auch nach Ablauf dieses Termins weiterhin aus. In Anbetracht der zentralen Funktion des Landesverwaltungsamtes sowie der Vielzahl der hier eingesetzten IT-Geräte und automatisierten Verfahren besteht die Erforderlichkeit zur Erstellung dieses IT-Sicherheitskonzeptes. Mit Schreiben vom Dezember 1998 teilte mir das TLVwA mit, dass das IT-Sicherheitskonzept fertig gestellt wurde. Obwohl ich das TLVwA mehrfach bat, dass nunmehr erstellte IT-Sicherheitskonzept mir zur Verfügung zu stellen, wurde dem nicht entsprochen.

Ich sah es deshalb als geboten an, mich kurzfristig im Rahmen eines Kontrollbesuches über das IT-Sicherheitskonzept und die Umsetzung der geforderten Maßnahmen vor Ort zu informieren. Im Rahmen des Kontrollbesuches wurde mir das seit Dezember 1998 in Kraft getretene Sicherheitskonzept übergeben. Dieses weist bezogen auf jeden PC-Arbeitsplatz und für Server detaillierte Sicherheitsmaßnahmen auf. Die Maßnahmen wurden auf der Basis des IT-Grundschutzhandbuch des BSI festgelegt. Meine Anregungen zur weiteren Umsetzung des IT-Sicherheitskonzeptes und zu einer Spe-

zifizierung der Sicherheitsmaßnahmen gemäß dem von mir empfohlenen Schutzstufenkonzept (1. TB 15.3) wurden vom TLVwA aufgegriffen.

Im Zuge dieser Kontrolle musste ich die noch nicht erfolgte Überarbeitung der Datenschutzordnung sowie die verbindliche Festlegung der Leistungsmerkmale der TK-Anlage anmahnen. Zwischenzeitlich liegen mir hierzu diesbezüglich überarbeitete Entwürfe des TLVwA vor.

In einem kontrollierten Fachreferat, welches über ein eigenes lokales Netz verfügt und somit auch Administrationsarbeiten wahrnimmt, stellte ich eine nicht ausreichend nachvollziehbare Rechtevergabe für die Mitarbeiter fest. Meine Hinweise zur Beseitigung dieses Mangels wurden inzwischen realisiert. In die Kontrolle wurden auch die vorhandenen rechnerseitigen Anbindungen an das öffentliche Netz einbezogen.

15.7 Elektronische Kommunikation in der Landesverwaltung

Im Staatsanzeiger Nr. 43/1999 veröffentlichte das TIM „Gemeinsame Regeln zur Nutzung der elektronischen Post in den Ministerien und der Staatskanzlei gem. § 45 und § 46 der ThürGGO“. Dieser Regelung ist zu entnehmen, dass alle Ministerien und die Staatskanzlei die Elektronische Post (E-Mail) als Kommunikationsmittel zur Beschleunigung und Vereinfachung von Verwaltungsvorgängen zu nutzen haben, soweit keine technischen, rechtlichen oder wirtschaftlichen Gründe dem entgegenstehen. Sie regelt den Empfang und Versand elektronischer Dokumente und bildet die Grundlage für ressortinterne Regelungen. Es heißt hier u. a.:

Personenbezogene Daten, die zur Sicherstellung eines ordnungsgemäßen E-Mail-Betriebes erhoben und gespeichert werden (Protokolldaten), unterliegen der Zweckbindung nach § 20 Abs. 4 ThürDSG. Eine Auswertung solcher Daten darf nicht zu einer Leistungs- und Verhaltenskontrolle der Bediensteten herangezogen werden. Für den behördeneigenen Mail-Server sind Sicherheitsmechanismen zu ergreifen, die eine Zutritts-, Zugangs- und Zugriffskontrolle gewährleisten. Weiterhin sind alle E-Mails auf eventuelle

Schadfunktionen (Viren) zu prüfen. In die Erarbeitung der gemeinsamen Regeln zur Nutzung der elektronischen Post wurde ich frühzeitig mit einbezogen. Meine Hinweise und Empfehlungen hierzu wurden berücksichtigt.

Die elektronische Übermittlung von Dokumenten mit personenbezogenen Daten wird durch diese Regelung nicht erlaubt. Bis zum Vorliegen einer gesonderten verbindlichen Verfahrensweise mit der die Vertraulichkeit, Unversehrtheit und Authentizität der übermittelten Daten gewährleistet werden kann, ist auf die elektronische Übermittlung solcher Daten zu verzichten.

15.8 Internetnutzung durch öffentliche Stellen

Zu der Nutzung des Internets durch die öffentliche Verwaltung als Darstellungs- und Informationsmedium sind auch datenschutzrechtliche Anforderungen zu beachten. In meinen vorherigen Tätigkeitsberichten wies ich bereits auf die Probleme beim Anschluss von Netzen der öffentlichen Verwaltung an das Internet (1. TB 15.13) und auf Datenspuren beim Zugriff auf Web-Server hin (2. TB 15.13).

Im Laufe dieses Berichtszeitraumes wurde ich mehrfach um Hinweise bezüglich datenschutzfreundlicher Anforderungen an die Gestaltung von Angeboten öffentlicher Stellen und Internet-Zugängen gebeten (4.6). Einen wesentlichen Bestandteil nimmt dabei die Veröffentlichung personenbezogener Daten in Internet-Angeboten und die Protokollierung von Verbindungsdaten ein:

Die Nutzung des Internets als Darstellungsmedium durch die öffentliche Stelle, ist meistens eine Selbstdarstellung gekoppelt mit gewünschter Kontaktaufnahme mit Bürgerinnen und Bürgern. Personenbezogene Daten können dabei in vielfältiger Weise erfasst, verarbeitet oder genutzt werden. Bei der Bewertung der Daten muss man unterscheiden zwischen den Daten, die im Internet veröffentlicht werden sollen (Inhaltsdaten) und den Daten, die mit der Inanspruchnahme einer solchen Darstellung anfallen (Verbindungsdaten). Bei der Präsentation im Internet besteht zunehmend das Bedürfnis neben der öffentlichen Stelle auch Personen vorzustellen z. B. mit Name, Funktionsbezeichnung, Zuständigkeit, Telefon- und

Zimmer-Nr., Foto, Adresse, Parteizugehörigkeit, Mitgliedschaft in Gremien, Vereinen und Verbänden.

Hierbei handelt es sich um eine Übermittlung personenbezogener Daten an eine nicht näher bekannte Öffentlichkeit in ihrer weitreichendsten Form. Wenn keine spezialgesetzliche Regelung eine solche Veröffentlichung erlaubt, ist diese nur nach § 22 ThürDSG i. V. m. § 20 ThürDSG zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und der Betroffene hierin eingewilligt hat.

Weiterhin bedarf es einer datenschutzrechtlichen Freigabe gem. § 34 Abs. 2 ThürDSG und einer entsprechenden Datenschutzregistermeldung nach § 3 ThürDSRegVO. Dies gilt auch für wesentliche Änderungen des Angebotes, dessen Struktur laufend überwacht werden sollte. Wird die Einrichtung und der Betrieb solch einer Präsentation nicht selbst durch die öffentliche Stelle, sondern durch andere Personen oder Stellen wahrgenommen, bleibt sie gem. § 8 ThürDSG weiterhin für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Nach § 8 Abs. 2 ThürDSG hat dabei die öffentliche Stelle die Auftragsdatenverarbeitung entsprechend vertraglich sicherzustellen.

Die beim Nutzen einer Präsentation im Internet vorhandenen Verbindungsdaten fallen entweder unter das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG) oder den Mediendienstestaatsvertrag (MDStV). Nach § 2 Abs. 2 TDG liegt z. B. ein Teledienst vor, bei Angeboten zur Information oder Kommunikation (soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht) und z. B. bei Angeboten von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit. Dementsprechend sind bei den Zugriffen in und aus dem Internet für die anfallenden Verbindungsdaten wie z. B. statische oder dynamische IP-Adresse, Rechnername, E-Mail-Adresse, die Seite, von der aus auf die neue Seite zugegriffen wurde, das Zugriffsziel sowie der Zugriffszeitpunkt die Regelungen des TDG und des TDDSG zu beachten.

Der Wunsch, Verbindungsdaten zum Zwecke der Missbrauchsbekämpfung oder Störungsabwehr so weit wie möglich auszuwerten

und gegebenenfalls zu speichern, erfordert nicht unabdingbar die Speicherung personenbezogener Benutzerdaten. Dies geht auch anonymisiert oder pseudonymisiert, wie dies im Übrigen vom Grundsatz her seitens des Gesetzgebers im § 4 TDDSG vorgesehen ist. Die anfallenden personenbezogenen Daten über den Ablauf des Abrufs oder Zugriffs oder der sonstigen Nutzung sind unmittelbar nach deren Beendigung zu löschen, soweit nicht eine längere Speicherung für Abrechnungszwecke erforderlich ist.

Gem. § 3 Abs. 5 TDDSG ist weiterhin der Nutzer vor der Erhebung über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer vor Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

Aus datenschutzrechtlicher Sicht gibt es bei der Nutzung des Internet als Informations- und Kommunikationsmittel durch die öffentliche Stelle keine grundsätzlichen Bedenken gegen eine Protokollierung anfallender personenbezogener Daten von Nutzern im erforderlichen Umfang, wenn der Zugang zum Internet ausschließlich für dienstliche Zwecke bereitgestellt wurde.

Vor der Bereitstellung des Internetzuganges empfehle ich der öffentlichen Stelle, den Bedarf hierfür generell und im Einzelfall auf Erforderlichkeit entsprechend der Aufgabenstellung für ihre Bediensteten zu überprüfen, um so u. a. die Gefahr eingeschleuster Ausspä- und Schadfunktionen so gering wie möglich zu halten.

Wenn beim Zugang zum Internet auch die private Nutzung eingeräumt wurde, bedarf es auch für die Datei, die zu Abrechnungszwecken erstellt wird, einer datenschutzrechtlichen Freigabe nach § 34 Abs. 2 ThürDSG, einer entsprechenden Datenschutzregistrierung nach § 3 ThürDSRegVO und der Beteiligung des Personals nach § 74 ThürPersVG.

Für jeden Nutzer sollte u. a. transparent festgelegt werden, welche Daten protokolliert werden, wer auf diese nach welchem Modus einen kontrollierenden Zugriff besitzt und wie lange die Protokolldaten vorgehalten werden. Aus datenschutzrechtlicher Sicht ist be-

denklich, wenn ausschließlich dem Administrator die Einsicht ohne jegliche Einschränkungen in das Protokoll vorbehalten ist. Für solche Einsichtnahmen sollten Modalitäten vorgegeben werden und in der Regel nach dem Vier-Augen-Prinzip verfahren werden. Dabei könnten der behördliche Datenschutzbeauftragte, der jeweilige Vorgesetzte und Personalratsmitglieder beteiligt sein.

15.9 Eckpunkte der Deutschen Kryptopolitik als wirksames Mittel zur Gewährleistung von Datenschutz und Datensicherheit

Unbestritten stellt die Verschlüsselung von Daten (2. TB 15.7.2, 15.7.4) die derzeit wirksamste Maßnahme dar, um die Vertraulichkeit der Informationen zu gewährleisten. In den letzten Jahren wurde in der Öffentlichkeit heftig diskutiert, inwieweit das Recht eines Jeden, seine Informationen zu verschlüsseln, eingeschränkt werden sollte, um den Belangen der inneren Sicherheit Genüge zu leisten. Diese Debatte wurde unter dem Begriff Kryptokontroverse geführt (2. TB 15.7.6). Sowohl von Seiten der Datenschützer als auch der Wirtschaft wurde immer wieder darauf hingewiesen, dass für das Vertrauen der Anwender beim Einsatz von kryptographischen Verfahren eine staatliche Kryptopolitik wichtig ist, die den Schutz ihrer Daten und damit den Nutzer in den Vordergrund stellt. Eine solche Politik muss nicht nur für eine weite Verbreitung starker kryptographischer Verfahren eintreten, sondern sie muss auch zur Entwicklung des notwendigen Sicherheitsbewusstseins der Nutzer beitragen. Die Bundesregierung hat jetzt mit ihrer Entschließung "Eckpunkte der Deutschen Kryptopolitik" vom 02.06.1999 verdeutlicht, dass sie nicht beabsichtigt, die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken und dass sie in der Anwendung einer sicheren Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürger sieht. Die Datenschutzbeauftragten des Bundes und der Länder begrüßen ausdrücklich diese Position der Bundesregierung. Auf der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08.10.1999 in Rostock wurde hierzu eine Entschließung (Anlage 19) unter dem Thema "Eckpunkte der Deutschen Kryptopolitik - ein Schritt in die richtige Richtung" verabschiedet. Die Datenschutzbeauftragten fordern hier u. a. die öffentlichen Stellen auf, mit gutem Beispiel vor-

anzugehen und kryptographische Verfahren zum Schutz personenbezogener Daten häufiger als bisher einzusetzen. Sie heben hervor, dass künftig Kryptographie der Standard in der Informations- und Kommunikationstechnik werden muss. In einer diesbezüglichen Information an die obersten Landesbehörden wies ich darauf hin, dass entsprechende Verschlüsselungsverfahren auf den Markt angeboten und verstärkt solche Verfahren eingesetzt werden sollten, um die Vertraulichkeit und Integrität von Daten sowohl für ihre Speicherung als auch während ihrer Übermittlungen in Netzen, die sich der Kontrolle der Einrichtung entziehen, abzusichern. Diese Thematik war auch Tagungsordnungspunkt im IMA-IT mit einem Fachvortrag zur Verschlüsselung und Digitalen Signatur sowie einer anschließenden positiven Diskussion zum verstärkten Einsatz solcher Verfahren in der Thüringer Landesverwaltung.

15.10 Datenschutz durch Technik-Einsatz transparenter Hard- und Software

Schon mehrfach äußerten sich die Datenschutzbeauftragten des Bundes und der Länder zur Entwicklung und zur Erforderlichkeit des Einsatzes von datenschutzfreundlichen Technologien. Darunter werden Verfahren und Technologien der Informations- und Kommunikationstechnik verstanden, die sich u. a. am Grundsatz der Datenvermeidung orientieren und deren Verfahrensabläufe und Verarbeitungsvorgänge nachvollziehbar sind (2. TB 15.6). Letzteres ist für Benutzer, welche gängige Hard- und Software für ihre Datenverarbeitung einsetzen insofern wichtig, als diese ihr gesetzliches Recht auf informationelle Selbstbestimmung nur wahrnehmen können, wenn auch die Nachvollziehbarkeit (Transparenz) der hier ablaufenden automatisierten Verfahren gewahrt ist. Transparenz ist aber auch bedeutsam für die Benutzerakzeptanz. So zeigt insbesondere die Praxis, dass eingesetzte Technologien und Verfahren von den Benutzern langfristig nur akzeptiert werden, wenn diese Vertrauen in die eingesetzten automatisierten Systeme besitzen. Auch hierfür sind transparente Verfahrensabläufe eine wichtige Voraussetzung.

Dass die zurzeit eingesetzten Informationstechnologien den Anspruch an Transparenz bei weitem nicht erfüllen, zeigt insbesondere

die öffentliche Diskussion bei der Nutzung des Internet. Selbst geschulte und erfahrene Benutzer von Diensten und Technologien des Internet können die hiermit verbundenen Risiken für die Sicherheit des eigenen Computers aber auch auf das Hinterlassen von persönlichen Spuren beim Surfen im Netz nur schwer durchschauen (2. TB 15.13). Von Transparenz kann hier keine Rede sein. Um die Risiken für personenbezogene Daten bei der Nutzung moderner Informations- und Kommunikationstechnologien weitestgehend auszuschließen sind, auch insbesondere die Anbieter von Tele- und Mediendiensten sowie die Hersteller und Anbieter von IuK-Technik gefordert. Sie sollten als Verbündete der Benutzer diese in ihrem Bestreben nach mehr Datensicherheit verstärkt unterstützen. Neben der Bereitstellung von Technologien und Hilfsmitteln für einen verbesserten Schutz der Daten ist deren Transparenz ein gewichtiger Aspekt. Mögliche mit der Nutzung dieser neuen Technologien noch verbundenen Risiken sind aufzuzeigen, um auch dem Benutzer entsprechende Maßnahmen zu seinem Selbstschutz zu ermöglichen.

Die Datenschutzbeauftragten des Bundes und der Länder nahmen die in der Öffentlichkeit geführte Diskussion über die Ausstattung des Pentium III-Prozessors der Firma INTEL mit einer Seriennummer zum Anlass, um noch einmal grundsätzlich auf die bei der Nutzung moderner Informations- und Kommunikationstechnik hiermit verbundenen Gefahren, insbesondere durch fehlende Transparenz, für die Anonymität der Benutzer aufmerksam zu machen. Die auf dem Prozessor eingetragene Seriennummer kennzeichnet diesen bzw. den PC eindeutig, und war als eine Identifikation bei online Transaktionen des Benutzers vorgesehen, indem seitens der kontaktierten Stelle die Nummer durch spezielle Software ausgelesen werden kann. Da bei solchen online Kontakten der Benutzer in bestimmten Fällen durchaus auch Name und Anschrift offenbaren könnte, wäre somit das Erstellen von Benutzerprofilen möglich. In ihrer Entschließung vom 25./26. März 1999 unter dem Thema "Transparente Hard- und Software" forderten die Datenschutzbeauftragten anlässlich ihrer 57. Konferenz in Schwerin (Anlage 12) die Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können. Sie wiesen daraufhin,

dass den Erfordernissen des Datenschutzes nur dann ausreichend Rechnung getragen wird, wenn zum Schutz der Privatheit transparente und in eigener Verantwortung der Anwender bedienbare Sicherheitsfunktionen zur Verfügung stehen. Den Anwendern empfehlen die Datenschutzbeauftragten, nur Produkte einzusetzen, welche diese Forderungen erfüllen.

15.11 Die elektronische Geldbörse

Bereits im Herbst 1995 forderte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, bei elektronischen Geldbörsen den elektronischen Zahlungsverkehr anonym zu gestalten (1. TB 15.15.3). Die Datenschutzbeauftragten forderten erneut auf ihrer 55. Konferenz im März 1998 (Anlage 2) die Kartenherausgeber und die Kreditwirtschaft auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten - so genannte White Cards - anzubieten. Die Anwendung ist dabei so zu gestalten, dass ein Karten- und damit personenbezogenes Clearing nicht erfolgt. Auch der Gesetzgeber wird aufgerufen, sicherzustellen, dass auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

15.12 Das Jahr 2000 Problem

Wer kennt nicht noch die über Medien veröffentlichten Meldungen zum Jahr 2000-Problem. Auch die öffentliche Verwaltung war von diesem Problem unmittelbar betroffen. Aus datenschutzrechtlicher Sicht ergaben sich durch den Jahrtausendwechsel insbesondere Gefährdungen für die Verfügbarkeit und Integrität der Daten. Sollte es bei personenbezogenen Daten durch das Jahr 2000-Problem zu Datenfälschungen gekommen sein, so haben öffentliche Stellen gem. §§ 14 bis 16 ThürDSG diese zu berichtigen, zu sperren oder zu löschen.

Für die fehlerfreie Datumsermittlung gehörte neben dem Test auf die Jahr-2000-Fähigkeit auch die richtige Berechnung der Schaltjahre und eine korrekte Umwandlung der Zeitdaten in serielle Datums- und Textformate. In nicht wenigen Fällen war auch eine Analyse des Programmquellcodes unabdingbar. Viele Hard- und Softwarefirmen

stellten zumindestens für ihre neuesten Produkte Analyseprogramme und Dateien zur Fehlerbehebung zur Verfügung.

Der Thüringer Interministerielle Ausschuss-Informationstechnik (IMA-IT) beschäftigte sich seit Anfang 1998 mit der Problematik der Jahr-2000-Umstellung. Die Koordinierung der Jahr-2000-Vorbereitung im Bereich der Informations- und Kommunikationstechnik wurde durch das TIM wahrgenommen, welches dem Thüringer Kabinett entsprechend berichtete. Diese Berichterstattungen beruhten auf der Basis eines Fragenkataloges der in Verbindung mit einem einheitlichen Bewertungsstichtag der IT-Objekte von jedem Ressort auszufüllen war.

Dem im Juli 1999 an das Kabinett übergebenen Bericht war zu entnehmen, das sämtliche Ressorts und die nachgeordneten Bereiche bis Mitte November 1999, alle diesbezüglichen Anpassungs- und Umstellungsarbeiten sicherzustellen hatten. Es wurde eingeschätzt, dass sich zwei Drittel der betroffenen IT-Objekte in der Anpassungs- bzw. Umstellungsphase befanden. Kritische Situationen bis zum Datumswechsel wurden in keinem Ressort gesehen. Die Großrechnerverfahren waren von den zuständigen Ressorts TFM und TIM bei der Datumsumstellung zu betreuen. Das Corporate Network der Landesregierung war hinsichtlich der Jahr-2000-Festigkeit überprüft worden. Die ressortübergreifenden Dienste (Mailing, Intranet-Anwendungen, Internet-Zugang) des Corporate Network der Landesverwaltung einschließlich der Kommunikationsstruktur waren durch das TLRZ als Netzbetreiber Jahr-2000-fähig zu gestalten. Das Thüringer Finanzministerium stellte einen Leitfaden „Auswirkungen der Datumsumstellung zur Jahrtausendwende in technischen Ausrüstungen der Elektrotechnik / Hinweise zur Verfahrensweise“ zur Verfügung, der auch relevante aktive Komponenten wie Telefonanlagen und Zeiterfassungssysteme berücksichtigte.

15.13 Datenschutzrechtliche Aspekte bei der Einrichtung von Telearbeitsplätzen

Mit Telearbeit wird eine Arbeitsform bezeichnet, die mit einer gewissen Regelmäßigkeit, unter Nutzung von Informations- und Kommunikationstechniken, außerhalb der Daten verarbeitenden Stelle (Behörde, Firma) erfolgt. Dabei kann der Telearbeiter sowohl

von einem festen Arbeitsplatz (häuslicher Bereich, Bürogemeinschaft) und/oder mit Hilfe mobiler Technik an nahezu jedem beliebigen Ort (Vertriebs-, Kundenservice) seine Arbeit verrichten. Die modernen Informations- und Kommunikationstechniken gestatten nunmehr den Einsatz von Telearbeit auf breiter Ebene, indem sie den hierfür erforderlichen ortsunabhängigen und unmittelbaren Zugriff auf entfernt gespeicherte Daten ermöglichen. In dem Aktionsprogramm der Bundesregierung "Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts" wird hervorgehoben, dass die Nachfrage nach Telearbeit durch Arbeitnehmer groß ist und gleichzeitig bemängelt, dass es bisher erst rund 800.000 Telearbeitsplätze in Deutschland gibt, wobei dem ein Gesamtvolumen von 2 bis 4 Millionen möglichen Telearbeitsplätzen gegenübersteht. Die nachfolgenden Ausführungen beschränken sich auf die Telearbeit im Rahmen eines Arbeits- oder Dienstverhältnisses. Werden dagegen Teledienstleistungen von rechtlich selbständigen Unternehmen oder Personen durchgeführt, so gelten je nach Art der Dienstleistung entweder die Vorschriften zur Auftragsdatenverarbeitung oder aber zur Datenübermittlung, wobei auch hier besondere technische und organisatorische Maßnahmen insbesondere bei der Übertragung personenbezogener Daten über Computernetze erforderlich sind.

Ein typischer Telearbeitsplatz ist mit einem PC einschließlich peripherer Geräte wie bspw. Drucker, Scanner, Fax ausgestattet, wobei der PC über Modem oder ISDN-Karte an die zentrale Informationstechnik der Daten verarbeitenden Stelle angebunden ist. Auf dem PC ist außer dem Betriebssystem, Anwendungs- und Kommunikationssoftware sowie im erforderlichen Maße Schutzsoftware installiert.

Das Einrichten von Telearbeitsplätzen kann sowohl für den Arbeitgeber/Dienstherrn aus wirtschaftlichen Gründen sowie situationsbedingt auch für den Mitarbeiter vorteilhaft sein. Neben arbeitsrechtlichen und sozialen Gesichtspunkten müssen, wenn personenbezogene Daten im Rahmen von Telearbeit erhoben, verarbeitet oder genutzt werden, auch datenschutzrechtliche und sicherheitstechnische Aspekte bei der Planung und dem Betrieb von Telearbeitsplätzen beachtet werden. Aus datenschutzrechtlicher Sicht ergeben sich hierbei Gefahren für das Persönlichkeitsrecht Betroffener, die unmittelbar damit zusammenhängen, dass jetzt auch große Datenmen-

gen außerhalb der zumeist geschützten betrieblichen oder behördlichen IT-Infrastruktur verarbeitet und vorgehalten werden. Ein möglicher Missbrauch dieser Daten, indem bspw. gegen ihre Zweckbindung verstoßen wird, ist an dem entfernten Arbeitsplatz nahezu leicht möglich. Auch bei öffentlichen Stellen in Thüringen war feststellbar, dass schon Telearbeitsplätze eingerichtet waren. Zudem gibt es Anfragen an meine Dienststelle, welche datenschutzrechtlichen Aspekte bei der Telearbeit zu beachten sind.

Die gesetzlichen Grundlagen zur Verarbeitung personenbezogener Daten bilden das Bundesdatenschutzgesetz (BDSG) und für die öffentlichen Stellen des Freistaats Thüringen das Thüringer Datenschutzgesetz (ThürDSG), sofern keine spezialgesetzlichen Regelungen vorliegen. Aufgrund der Anbindung des Telearbeiters per Telekommunikation an den Betrieb bzw. die Dienststelle könnten auch die bereichsspezifischen Datenschutzvorschriften des Telekommunikationsgesetzes (TKG) und des Teledienstedatenschutzgesetzes (TDDG) zur Anwendung kommen. Dies würde aber voraussetzen, dass die Telekommunikationsbeziehungen des Telearbeiters zu seinem Arbeitgeber/Dienstherrn in die Anwendungsbereiche des TKG bzw. Teledienstegesetzes (TDG) fallen. Wegen des Abhängigkeitsverhältnisses von seinem Arbeitgeber/Dienstherrn ist der Telearbeiter nicht als Dritter anzusehen, der sich gegenüber seinem Arbeitgeber/Dienstherrn auf das Fernmeldegeheimnis berufen und den Inhalt der Telekommunikation und damit der erbrachten Telearbeit verschweigen kann. Auf das Ergebnis der Telearbeit hat der Arbeitgeber/Dienstherr im Rahmen des Arbeits-/Dienstverhältnisses gerade Anspruch. Daher fehlt es nach § 3 Nr. 5 TKG bereits an einem nachhaltigen Angebot von Telekommunikation für Dritte und damit an einem "geschäftsmäßigen Erbringen von Telekommunikationsleistungen". Dieses Ergebnis wird auch durch die amtliche Begründung zu den §§ 85 ff TKG belegt, wonach dem Fernmeldegeheimnis nur Nebenstellenanlagen in Betrieben und Behörden unterliegen, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind. Entsprechendes gilt für von § 2 Abs. 2 TDG vorausgesetzten Angebote von Teledienstleistungen an den Telearbeiter durch den Arbeitgeber/Dienstherr, da der Telearbeiter aus seinen arbeitsvertraglichen bzw. dienstrechtlichen Pflichten keine Auswahlmöglichkeiten zur Nutzung der Dienste hat, sondern ihm diese von seinem

Arbeitgeber/Dienstherrn zur Nutzung im Rahmen des Telearbeitsverhältnisses vorgegeben werden. Damit kommt eine Anwendung der bereichsspezifischen Datenschutzvorschriften des TKG und des TDDG allenfalls bzgl. einer privaten Nutzung der vom Arbeitgeber/Dienstherr zur Verfügung gestellten Technik in Frage. Da sich bei der Anwendung dieser Vorschriften keine Besonderheiten im Vergleich zur privaten Nutzung von Telekommunikationsanlagen im Betrieb bzw. in der Dienststelle ergeben, gehe ich im weiteren von einer ausschließlich dienstlichen Nutzungsmöglichkeit der Technik durch den Telearbeiter aus. Zudem wird der Arbeitgeber/Dienstherr im Regelfall aus Gründen der Sicherheit der Kommunikation die Nutzung der zur Erledigung der Telearbeit zur Verfügung gestellten Kommunikationsanlagen ausschließlich zur dienstlichen Verwendung gestatten.

Gesetzliche Regelungen, die den Einsatz von Telearbeit besonderen Voraussetzungen unterwerfen, existieren nicht. Daher gelten grundsätzlich dieselben Vorschriften wie für eine Datenverarbeitung im Betrieb bzw. in der Dienststelle, wobei unter Berücksichtigung der Sensibilität der verarbeiteten Daten besondere Vorkehrungen im Hinblick auf die Verarbeitung außerhalb der unmittelbaren Einwirkungsmöglichkeiten des Arbeitgebers/Dienstherrn zu treffen sind.

Die datenschutzrechtliche Verantwortlichkeit für die Telearbeit trägt gem. § 9 Satz 1 BDSG und § 9 Abs. 1 Satz 1 ThürDSG der Dienstherr/Arbeitgeber. Dazu haben die Stellen, die personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Vorschriften des Datenschutzes zu gewährleisten. Die gesetzlichen Anforderungen sind in der Anlage zu § 9 BDSG bzw. im § 9 Abs. 2 ThürDSG aufgeführt. Wie bei jeglicher Verarbeitung personenbezogener Daten, sind insbesondere die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Authentizität der Daten sowie die Ordnungsmäßigkeit, Revisionsfähigkeit und Transparenz der Datenverarbeitung sicherzustellen. Desweiteren sind dem Arbeitgeber bzw. Auftraggeber, dem behördlichen oder betrieblichen Datenschutzbeauftragten sowie für öffentliche Stellen den Landesbeauftragten für den Datenschutz bzw. für nicht-öffentliche Stellen den Aufsichtsbehörden die gesetzlich vorgegebenen Kontrollrechte vor Ort einzuräumen. Hierfür ist der Ar-

beitgeber bzw. Auftraggeber verantwortlich. Die Ausübung des Kontrollrechtes bedarf jedoch der ausdrücklichen Einwilligung des Telearbeiters. Die Einwilligung seitens des Telearbeiters zu einem Zutrittsrecht der datenschutzrechtlichen Kontrollinstanzen in seine private Wohnung ist deshalb unumgänglich, da durch Art. 13 GG die Unverletzlichkeit der Wohnung garantiert ist. Da die Möglichkeit der Kontrolle gesetzlich vorgegeben ist, kann Telearbeit nur dann ausgeführt werden, wenn dieses Kontrollrecht auch praktisch ausgeübt werden kann. D. h., wenn der Telearbeiter im Voraus keine Einwilligung zu einem solchen Kontrollrecht leistet, und dahingehend keine Vereinbarung zwischen Arbeitgeber/Dienstherr und dem Telearbeiter zustande kommt, wäre die Verarbeitung der personenbezogenen Daten beim Telearbeiter aus datenschutzrechtlicher Sicht aufgrund der eingeschränkten Kontrollmöglichkeiten unzulässig.

Generell ist zu bemerken, dass Telearbeitsplätze ohne entsprechende zusätzliche Schutzmaßnahmen größeren Gefahren im Hinblick auf die Vertraulichkeit, der Integrität und der Verfügbarkeit der Daten ausgesetzt sind, als die PC-Arbeitsplätze in der Daten verarbeitenden Stelle selbst. So ist der Kontroll- und Einflussbereich seitens des Arbeitgebers oder Dienstherrn aufgrund der räumlichen Trennung nicht unmittelbar gegeben. Besondere Gefährdungen ergeben sich insofern, dass der häusliche Arbeitsplatz zumindest gegenüber den Familienangehörigen bzw. Vertrauten des Telearbeiters keiner Zutrittskontrolle unterliegt, der Zugang auf den Rechner nicht ausreichend abgesichert ist und durch das einfache Einspielen privater Software Risiken für die Vertraulichkeit und Integrität der Daten bestehen. Ebenso kann die datenschutzgerechte Entsorgung von Datenträgern und Schriftgut unzureichend sein.

Gem. § 9 BDSG/ThürDSG ist der Arbeitgeber/Dienstherr verpflichtet, eine datenschutzgerechte Gestaltung der Telearbeitsplätze so vorzunehmen, dass die Betroffenen, um deren Daten es geht, angemessen d. h. ausreichend durch erforderliche technische und organisatorische Maßnahmen im Sinne von § 9 BDSG/ThürDSG geschützt werden. Die notwendigen Sicherheitsüberlegungen dürfen sich dabei nicht nur auf den Arbeitsplatz des Telearbeiters beschränken, sondern müssen die Übermittlung der Daten von und zur Daten verar-

beitenden Stelle und den Übergang in das behörden- bzw. firmeneigene Netz in die Betrachtungen einbeziehen.

Die für einen Telearbeitsplatz zu ergreifenden Sicherheitsmaßnahmen sollten im Ergebnis eine der Daten verarbeitenden Stelle äquivalentes Sicherheitsniveau ermöglichen. Auf keinen Fall ist die Verarbeitung personenbezogener Daten mittels Telearbeit zulässig, wenn im konkreten Fall die vorgesehenen Maßnahmen in ihrer Gesamtheit unzureichend sind, um einen Missbrauch von Daten zu verhindern. Nachfolgend sind grundlegende technische und organisatorische Maßnahmen aufgezeigt, die unabhängig von speziellen Gegebenheiten allgemein bei der Einrichtung von Telearbeitsplätzen zur Verarbeitung personenbezogener Daten zu beachten sind:

- Die zum Einsatz kommenden IT-Geräte, die erforderliche System-, Anwendungs- und Kommunikationssoftware sollten Eigentum der Daten verarbeitenden Stelle sein und nur für dienstliche Angelegenheiten benutzt werden.
- Der Einsatz von der Daten verarbeitenden Stelle nicht freigegebener Software oder die Nutzung nicht lizenzierter Software ist unzulässig.
- Das automatisierte Verfahren und der Telearbeitsrechner sind in das Anlagen- und Verfahrensverzeichnis gem. § 10 ThürDSG aufzunehmen.
- Der Telearbeiter muss umfassend über die Nutzung der bereitgestellten Hard- und Software unterrichtet sein.
- Das Einrichten, Aktualisieren sowie erforderliche Wartungsarbeiten sollte durch hierfür geschultes Personal der Daten verarbeitenden Stelle durchgeführt werden.
- Es wird empfohlen den Telearbeitsplatz in einem separaten Raum einzurichten. Dienstliche Unterlagen und Datenträger müssen vor unbefugtem Zugriff aufbewahrt werden. Hierfür sind entsprechende verschließbare Behältnisse erforderlich.
- Die datenschutzgerechte Entsorgung von dienstlichen Unterlagen und Datenträgern ist abzusichern. Soweit hierfür keine zentrale Entsorgung vorgesehen ist, sind Schriftgut mit Personenbezug zu schreddern und maschinenlesbare Datenträger, soweit sie noch funktionstüchtig sind, physikalisch zu löschen bzw. bei einem Defekt mechanisch zu vernichten.

- Notwendige Akten- und Datenträgertransporte zwischen dem Arbeitsplatz des Telearbeiters und der Daten verarbeitenden Stelle sollten in verschlossenen Behältnissen erfolgen. Entsprechend dem Schutzbedarf sind Festlegungen zu treffen, wer den Transport durchführen darf.
- Der Grundsatz der Datenvermeidung bzw. Datensparsamkeit ist insbesondere zu beachten.
- Soweit sensible personenbezogene Daten nicht in anonymisierter Form oder pseudonymisierter Form verarbeitet werden, sind sie in verschlüsselter Form zu speichern. Zu beachten ist, dass Daten, die einem besonderen Berufs- und Amtsgeheimnis unterliegen i. d. R. nur mit Zustimmung der Betroffenen für Telearbeit herangezogen werden dürfen.
- Vorgegebene Löschfristen von Daten sind einzuhalten. Ungeachtet dessen sind nicht mehr benötigte Daten unverzüglich zu löschen.
- Der Zugang auf den PC durch Unbefugte ist abzusichern. Die Zugriffsrechte sind gemäß der dienstlichen Aufgaben zu vergeben. Die im System involvierten Sicherheitsmechanismen (bspw. Boot- / Setup- / Login- Passwortschutz) sind zu aktivieren sowie gegebenenfalls zusätzliche Sicherheitsprodukte einzusetzen. Für die Passwortvergabe und -verwaltung sind die hinlänglich bekannten Regeln einzuhalten. Sicherer als die konventionelle Zugangskontrolle durch ein Passwort erweist sich jedoch der Einsatz einer Chipkarte oder sofern angemessen eines biometrischen Identifizierungsverfahrens, mit dem eine personenbezogene Authentifikation des Nutzers erreicht wird.
- Für Arbeitspausen ist eine Bildschirm- und wenn möglich eine Tastatursperre zu aktivieren.
- Das Diskettenlaufwerk darf nur dem Telearbeiter zugänglich sein.
- Benötigt der Telearbeiter aus dienstlichen Gründen einen Zugang zum Internet, so darf dieser nur im Rahmen der hierfür verbindlichen Sicherheitsrichtlinien der Daten verarbeitenden Stelle eingerichtet werden.
- Regelmäßig sind mit geeigneten Programmen Prüfungen auf Viren oder andere schadensstiftende Software vorzunehmen.
- Datensicherungen sind im erforderlichen Maße auf externe Datenträger oder auf den Server der Daten verarbeitenden

Stelle durchzuführen. Sicherungskopien sind unter Verschluss und nach Möglichkeit lokal getrennt vom Telearbeitsplatz aufzubewahren.

- Für die Nachvollziehbarkeit der automatisierten Verarbeitung personenbezogener Daten und von Sicherheitsverletzungen, sind relevante Ereignisse zu protokollieren. Die Auswertung und der Umgang mit den Protokollen hat sich an den diesbezüglichen Vorgaben der Daten verarbeitenden Stelle auszurichten. Auf die hierfür erforderliche Mitbestimmung des Personalrats gem. § 74 Abs. 3 Satz 1 Nr. 18 ThürPersVG sei hingewiesen.
- Eine sichere Übertragung von Nachrichten und Daten zwischen dem Telearbeitsplatz und der Daten verarbeitenden Stelle wird durch den Einsatz kryptographischer Verfahren erreicht. Durch Verschlüsselung der zu übertragenden Daten ist Vorsorge für die Vertraulichkeit und den Schutz der Daten vor einer bewussten Manipulation getroffen. Zur Prüfung der Integrität und der Authentizität der übermittelten Daten bzw. des Absenders bietet sich der Einsatz der digitalen Signatur an.
- Beim Aufbau einer Kommunikationsverbindung zwischen dem Telearbeitsplatz und der Daten verarbeitenden Stelle muss ein Verfahren zum Einsatz kommen, dass eine hinreichende Identifikation und Authentifikation zwischen sendender und empfangender Stelle sicherstellt.
- Auf Seiten der Daten verarbeitenden Stelle muss insbesondere auf einen besonders abgesicherten Netzzugang geachtet werden und darauf, dass die Zugangs- und Zugriffsrechte auf die in der Daten verarbeitenden Stelle vorgehaltenen Server entsprechend den Befugnissen vergeben sind.

Die Einrichtung von Telearbeitsplätzen sollte auf der Basis eines Datenschutz- und Datensicherheitskonzeptes ausgeführt werden, das auf die individuellen Gegebenheiten der Behörde abgestimmt ist. Ein solches Konzept sollte ausgehend von den datenschutzrechtlichen Aspekten der Telearbeit auch die für den konkreten Einsatzfall möglichen Risiken und zu deren Begegnung die erforderlichen Sicherheitsmaßnahmen ausweisen. Die technischen und organisatorischen Maßnahmen sollten in einer Dienstanweisung geregelt und für alle Telearbeiter verbindlich vorgegeben werden (z. B. durch Bezug-

nahme im Arbeitsvertrag oder besondere schriftliche Verpflichtung). Hier sind auch die Verfahrensweisen für eine eventuelle Beendigung der Telearbeit oder zur Vertretung von Telearbeitern festzulegen.

15.14 Identifikation und Authentifikation mittels biometrischer Verfahren

In zahlreichen Fällen fordern IT-Systeme und deren Anwendungen aus Sicherheitsgründen eine Identifikation und Authentifikation des Benutzers, um somit bspw. zu gewährleisten, dass nur Befugte im Rahmen ihrer Berechtigung den Zugang und Zugriff auf bestimmte Rechner und hier gespeicherte Datenbestände erhalten. Zur Feststellung der Identität einer Person bieten sich u. a. derzeit folgende unterschiedliche Methoden an:

- durch Wissen, bspw. Einsatz von Passwörtern oder Codewörtern,
- durch Besitz, bspw. Chipkarte, Ausweis, Schlüssel, Transponder,
- durch Einsatz kryptographischer Verfahren, bspw. digitale Signatur,
- durch biologische Merkmale, die personengebunden sind und die betreffende Person eindeutig spezifizieren.

Überwiegend erfolgt derzeit die Identifikation und Authentifikation von Personen durch eine Benutzer-Kennung und ein Geheimnis (Passwort), wobei letzteres nur die jeweilige berechtigte Person kennen sollte. Mit der Kennung, z. B. eines Namens, identifiziert sich die Person, mit dem Passwort authentisiert sie sich gegenüber dem System. Das heißt, sie weist mit der Preisgabe ihres "Geheimnisses" ihre vorgegebene Identität nach. Diese Verifizierung der Echtheit der angegebenen Identität wird als Authentifikation oder Authentisierung bezeichnet.

Eine solche Authentifikation erfolgt bspw. durch Eingabe einer PIN (Persönliche Identifikationsnummer) beim Abheben eines Geldbetrages mit EC-Karte am Geldautomaten oder durch die Eingabe eines Passwortes, um den Zugang auf einem PC und eventuell auch hiermit verbundene Zugriffsrechte auf Programme und Daten zu erhalten. Die Authentifikation mittels eines Passwortes gewährleistet, wie die Praxis zeigt, aufgrund möglicher menschlicher Schwächen bei der Passwortgestaltung und Aufbewahrung keine hinreichende Sicherheit. Die hiermit verbundene Authentifikation kann

jede Person vollziehen, die das Passwort kennt. Insofern ist diese Authentifikation auch nicht zwingend an die sie vollziehende Person gebunden. Deshalb werden zunehmend zur Identifizierung des Benutzers eine Kombination von Wissen und Besitz eingesetzt. So kann sich der Benutzer mit einer Chipkarte ausweisen, auf der u. a. seine Benutzerkennung als auch das geheime Passwort enthalten ist. Ein Vorteil dieser Methode zur Identifikation und Authentifikation aus sicherheitstechnischer Sicht ist, dass sie Besitz (Chipkarte) als auch Wissen (PIN) kombiniert. Um die Karte vor einer missbräuchlichen Verwendung bei Verlust zu sichern, muss der Benutzer sich jedoch wieder mit einer PIN gegenüber der Karte ausweisen.

Insbesondere der sich entwickelnde elektronische Handel (Electronic Commerce), der dadurch gekennzeichnet ist, dass Kunden und Anbieter von Waren nur noch über elektronische Medien statt persönlich (von Angesicht zu Angesicht) miteinander kommunizieren, benötigt zur Absicherung beider Vertragspartner Authentifikationsverfahren zur gegenseitigen und eindeutigen Feststellung der Identität. Für dieses Einsatzgebiet bieten sich zur Authentifikation vorwiegend digitale Signaturen an (2. TB 15.7.5). Auch bei diesem Verfahren ist es jedoch möglich, dass der Inhaber des Signaturzertifikats einer anderen Person ermöglicht stellvertretend in seinem Namen eine Authentifikation mit seinem privaten Schlüssel durchzuführen.

Die bisher erwähnten Methoden zur Feststellung der Identität weisen zwar einen Personenbezug auf, sind aber nicht personengebunden und können somit auch durch Personen mit Erfolg ausgeführt werden, denen der Befugte das Recht hierfür übertragen hat oder die sich dieses unberechtigt angeeignet haben. Für Anwendungen mit einem hohen Sicherheitsbedarf kann jedoch durch eine nicht zwingend an die Person gebundene Identitätsfeststellung eine ungewollte Schwachstelle vorliegen.

Anders verhält es sich bei biometrischen Verfahren, welche anhand bestimmter menschlicher Eigenschaften Personen identifizieren und daraus deren Authentizität ableiten. So verfügt jeder Mensch über einzigartige Körper- und Verhaltensmerkmale, mit denen sich feststellen lässt ob sich hinter der vorgegebenen Identität auch die betreffende Person verbirgt. Bei einem solchen Verfahren müssen sich

die betreffenden Personen keine Passwörter oder analoge Codewörter mehr merken. Sie greifen statt dessen nun auf etwas zurück, das ihnen sozusagen angeboren ist und das sie immer bei sich tragen, wie charakteristische Merkmale des Gesichtes, der Stimme, der Iris oder der Retina des Auges, des Fingerabdrucks, der Lippenbewegung beim Sprechen oder der Handschrift. Biometrische Verfahren ermöglichen somit eine personengebundene Authentifizierung.

Für eine biometrische Erkennung ist zunächst die Erfassung und digitale Speicherung eines Referenzabdruckes der zu identifizierenden Person notwendig. Die eigentliche biometrische Erkennung erfolgt durch einen Vergleich der jeweils aktuell erfassten biometrischen Merkmale mit dem gespeicherten Referenzmuster (auch als Verifikation bezeichnet). Die Referenzabdrücke der zu erkennenden Personen können sowohl zentral auf einem Identifikationsserver oder dezentral in den Erfassungsgeräten bzw. auf Chipkarte vorgehalten werden. Die Speicherung von Referenzmustern auf Chipkarten (Smart-Cards), welche erhöhte Sicherheitsanforderungen (Zugriffsschutz, Verschlüsselung, Manipulations- und Ausleseschutz) realisieren und unter der Kontrolle der Benutzer stehen, können die Akzeptanz biometrischer Verfahren seitens der Nutzer positiv beeinflussen und diese Verfahren zukünftig zu einer breiteren Anwendung verhelfen.

Biometrische Merkmale selbst können von statischer oder dynamischer Art sein. So ändert sich beispielsweise der Fingerabdruck, Handgeometrie oder das Gesicht als ein typisches statisches Merkmal im Laufe des Lebens kaum. Anders verhält es sich bei der Stimme oder dem Tastatureingaberhythmus, die ein dynamisches Verhalten aufweisen. Insbesondere bei solchen verhaltensorientierten (dynamischen) Merkmalen kann es zu einer fehlerhaften Authentifikation kommen und zwar dann, wenn das mit einem Sensor gemessene biometrische Merkmal des Betroffenen mit dem von ihm gespeicherten Referenzmusters Abweichungen aufweist, die nicht mehr in einer vertretbaren Toleranzgrenze liegen. Somit könnte es in der Praxis vorkommen, dass die richtige Person fälschlicherweise zurückgewiesen wird oder eine falsche Person akzeptiert wird. Zwischen diesen beiden Fehlerarten besteht eine Korrelation insofern, dass das Abnehmen der einen Fehlerquelle die Wahrscheinlichkeit

des Eintretens der anderen Fehlerquelle verstärkt. Möchte ich also erreichen, dass mit hoher Sicherheit eine nicht berechnete Person abgewiesen wird, so ist andererseits die Wahrscheinlichkeit höher, dass eine berechnete Person nicht als solche erkannt wird. Die Festlegung der Fehlerraten, mit denen biometrische Systeme behaftet sind, müssen sich an dem konkreten Schutzziel orientieren.

Bisher wurden biometrische Verfahren schon vorwiegend eingesetzt, um den Zutritt zu Hochsicherheitsbereichen zu kontrollieren. In den letzten Jahren haben biometrische Identifikationssysteme deutliche Fortschritte gemacht. Unterschiedliche Lösungen werden bereits auf dem Markt angeboten, so auch Systeme die mehrere biometrische Merkmale zur Erkennung einsetzen. Für den praktischen Einsatz von biometrischen Systemen ergibt sich auch die Notwendigkeit, die unterschiedlichsten Verfahren direkt in die Anwendungen zur Benutzeridentifizierung einzubinden. Hierfür wird derzeit eine standardisierte Schnittstelle entwickelt, welche ohne großen Aufwand unterschiedliche biometrische Verfahren einbinden soll.

Die mit Verfahren der Biometrie erzielbare sichere Authentifikation von Personen hängt entscheidend davon ab, wie sicher vor einem unbefugten Zugriff die Referenzmuster gespeichert sind. Missbräuchliche Kopien dieser oder Manipulationen an diesen stellen eine nicht zu unterschätzende Gefahr für die Integrität dieser Systeme dar. Werden Referenzmuster in anderen Anwendungssystemen irregulär eingespeichert, ist zum einen die Sicherheit der hier gespeicherten Daten nicht mehr gewährleistet. Zum anderen ergibt sich insbesondere beim Einsatz statischer biometrischer Merkmale ein weiterer Nachteil. Im Gegensatz zu einem Passwort, das problemlos durch ein neues Passwort ausgewechselt werden kann, ist dies bei biometrischen Merkmalen nur beschränkt oder wie im Fall der Gesichtserkennung gar nicht möglich. Bei einem Fingerabdrucksystem sind maximal 10 unterschiedliche Referenzmuster möglich, wobei sich diese Anzahl bei Augenerkennungssystemen (Retina oder Iris) sogar nur auf zwei Möglichkeiten beschränken. Um diesen Nachteil zu vermeiden, werden bspw. Stimmerkennungssysteme angeboten, die nicht nur die persönliche Stimmfrequenz, sondern auch den gesprochenen Text in das Referenzmuster einbeziehen. Somit kann

durch Änderung des gesprochenen Textes auch eine Änderung des Referenzmusters erreicht werden.

Biometrische Systeme arbeiten mit persönlichen Daten, die zumindest längerfristig unabdingbar mit bestimmten Personen verbunden sind. Die Einzigartigkeit der Ausprägung biometrischer Merkmale kann zur Identifizierung des Inhabers führen. Naturgemäß eignen sich solche Verfahren bei einem missbräuchlichen Einsatz auch zur Überwachung von Personen. Enthalten diese Daten je nach Einsatzfall einen konkreten Personenbezug oder kann aus diesen Daten mit Hilfe zusätzlicher Daten oder Verfahren ein Personenbezug hergestellt werden, so handelt es sich gemäß den datenschutzrechtlichen Vorschriften (§ 3 Abs. 1 BDSG/ThürDSG) um personenbezogene Daten. Eine Erhebung und Verarbeitung solcher Daten ist nur aufgrund einer gesetzlichen Vorschrift zulässig bzw. muss mit Kenntnis der betreffenden Person und deren Zustimmung erfolgen. Eine Verknüpfung solcher persönlichen Daten mit weiteren Daten der Person ohne Beachtung vorgenannter Voraussetzungen wäre somit unzulässig. Infolgedessen muss grundsätzlich eine Zweckänderung der zur Authentisierung bzw. zur Verifikation von Personen zu verarbeitenden personenbezogenen Daten ausgeschlossen werden. In diesem Sinne sollten die gespeicherten Daten statt im Verfügungsbereich der Daten verarbeitenden Stelle unter der Kontrolle der jeweiligen Person stehen. Wie schon erwähnt bieten sich hierzu Chipkarten mit entsprechenden Sicherungsfunktionalitäten an. Ein wichtiges datenschutzrechtliches Kriterium bildet auch die Transparenz des eingesetzten Verfahrens, sie spielt auch für die Akzeptanz seitens der Benutzer eine mitentscheidende Rolle.

Auch bei der Entwicklung und bei der Auswahl einzusetzender biometrischer Systeme zur Identifikation ist der Grundsatz der Datensparsamkeit zu beachten, um einem Missbrauch der zum Teil sensiblen Daten vorzubeugen. Für eine Vielzahl von Einsatzfällen ist ein Personenbezug zur Identifizierung nicht erforderlich. Hier ist es ausreichend, wenn nur der gespeicherte Referenzdatensatz mit dem aktuell erfassten biometrischen Eingangsdatensatz der betreffenden Person verglichen wird. Durch die hier erfolgte Authentifizierung hat sich der Betroffene indirekt sicher identifiziert. Eine datenschutzfreundliche Technologie weisen insbesondere biometrische Verfah-

ren auf, die für eine sicheren Authentifikation keinen Abdruck der erhobenen biometrischen Daten speichern müssen. Im konkreten Einsatzfall sind Verfahren bevorzugt einzusetzen, die eine Identifikation der Betroffenen ermöglichen, ohne dass diese ihre Anonymität aufgeben müssen.

15.15 Neue Anforderungen an den technischen Datenschutz

Die rasche Entwicklung auf dem Gebiet der Informations- und Kommunikationstechnik erfordert auch eine Anpassung der technischen und organisatorischen Regelungen in den Datenschutzgesetzen. Die herkömmlichen Regelungen stellen vorwiegend auf eine zentralisierte Datenverarbeitung ab. Insbesondere die Dezentralisierung und Vernetzung der Daten verarbeitenden Systeme erfordern jedoch Sicherheitsstrategien, die mit den jetzigen technischen und organisatorischen Maßnahmen (§ 9 Abs. 2 ThürDSG, Anlage zu § 9 Satz 1 BDSG) allein nicht mehr im ausreichenden Maße abgesichert werden können. Im Zuge der erforderlichen Novellierung der Datenschutzgesetze infolge der Umsetzung der Vorgaben der EU-Datenschutzrichtlinie in nationales Recht, ist eine Anpassung der derzeitigen technischen und organisatorischen Regelungen zur Gewährleistung der Datensicherheit nicht nur geboten sondern dringend erforderlich. In diesem Sinne erarbeitete der AK-Technik der Bundes- und Landesbeauftragten für den Datenschutz auch unter Einbeziehung seiner praktischen Erfahrungen hierzu Lösungsvorschläge. Es werden u. a. Regelungsziele vorgeschlagen, die nicht mehr auf Technik orientierte Sicherheitsmaßnahmen sondern primär auf an Daten ausgerichtete Sicherheitsziele abstellen. Letztere sind technologieunabhängig und bilden einen allgemein gültigen Sicherheitsrahmen, der somit auch bei neuen Formen der Datenverarbeitung Bestand haben wird. Auf der Grundlage von Risikoanalysen wird dieser Sicherheitsrahmen mit konkreten, gemäß dem Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen aufgefüllt, welche die Ausführung der Vorschriften der Datenschutzgesetze sowie anderer Vorschriften über den Datenschutz sicherstellen. Sicherheitsziele sind insbesondere die Gewährleistung der Vertraulichkeit, der Integrität, der Verfügbarkeit und der Authentizität der zu verarbeitenden personenbezogenen Daten, wobei besonders auch die Notwendigkeit einer revisionsfähigen und

transparenten Datenverarbeitung herausgestellt wird. Letztere Forderungen resultieren aus der Kontrolltätigkeit, bei der oftmals festgestellt wurde, dass mangels ausreichender Protokollierung die nachträgliche Feststellbarkeit einzelner Datenverarbeitungsvorgänge unzureichend ist sowie aufgrund unzureichender Dokumentationen Verfahrensweisen nicht im ausreichenden Maße nachvollzogen werden können.

Für das Erreichen der o. g. Sicherheitsziele wurden besondere Maßnahmen beim Einsatz automatisierter Verfahren konkret benannt. Diese enthalten Regelungen zur Freigabe der Verfahren, zur Dokumentation der Datenprofile und Speicherorte sowie zur Dokumentation der Verfahren, zur Protokollierung und Nachvollziehbarkeit von Verarbeitungsschritten, zum Einsatz kryptographischer Verfahren, zum Test und zur Organisation der Datenverarbeitung, zur Systemadministration sowie zur Gestaltung automatisierter Verfahren aus datenschutzrechtlicher Sicht.

Um auch einen datenschutzgerechten Umgang mit neuen Verfahren und Systemen zu gewährleisten, werden auch spezifizierte Regelungen für mobile Datenverarbeitungssysteme (Laptop, Chipkarten), zur optisch-elektronischen Überwachung und Aufzeichnung (Video), zur Wartung sowie zu Fernmess- und Fernwirkdienste vorgeschlagen. Ausdrücklich wird der Grundsatz zur Datensparsamkeit hervorgehoben. Die Gestaltung von Verfahren und die Auswahl von informationstechnischen Produkten zum Einsatz in automatisierten Verfahren hat sich an diesem Grundsatz zu orientieren. Personenbezogene Daten sollen so weitgehend und früh wie möglich anonymisiert oder, falls dies nicht möglich ist, pseudonymisiert werden.

In dem Entwurf zur Novellierung des BDSG ist das Prinzip der Datenvermeidung und Datensparsamkeit (§ 3 a) einbezogen worden, um Gefahren für das informationelle Selbstbestimmungsrecht des Betroffenen von vornherein zu minimieren. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen. Einer Forderung der Datenschutzbeauftragten entspricht auch der im Entwurf neu eingefügte § 9 a BDSG, welcher ein Datenschutzaudit zur Verbesserung des Datenschutzes und der Datensicherheit vorsieht. Das Datenschutzaudit soll das Ziel verfolgen datenschutzfreundliche Produkte auf dem Markt zu fördern, in dem deren Datenschutzkonzept evaluiert wird. Der Entwurf enthält

weiterhin Regelungen zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (§ 6 b) sowie für mobile personenbezogene Speicher- und Verarbeitungsmedien (§ 6 c).

Die Anlage zu § 9 Satz 1 des BDSG-Entwurfs, welche technische und organisatorische Maßnahmen benennt, die insbesondere je nach Art der zu schützenden personenbezogenen Daten zu treffen sind, lässt erkennen, dass hier Ergänzungen und Änderungen im Hinblick auf die heutigen Gegebenheiten der IuK erfolgten. Nach meiner Auffassung sollten allerdings auch die vom AK-Technik (s. o.) vorgeschlagenen Regelungsziele bei der Novellierung der Datenschutzgesetze Beachtung finden, um die hier an den Daten ausgerichteten technikunabhängigen Sicherheitsziele bzw. -funktionen ausdrücklich zu verdeutlichen.

Anlage 1

Entschließung

der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 19./20. März 1998 in Wiesbaden

Datenschutz beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, dass bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, dass erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, dass auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen („Free TV“ und „Pay TV“) muss die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, dass die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muss sich an dem Ziel ausrichten, dass so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden.;
- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;
- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;
- wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d. h. Veranstalter können ihr Datenschutzkonzept

und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten könnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zählleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Schutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

Anlage 2

Entschließung

der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 19./20. März 1999 in Wiesbaden

Datenschutzprobleme der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen „Schattenkonten“ der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese „Schattenkonten“ noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluss der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, dass ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, dass auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

Anlage 3

Entschließung

der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 05./06. Oktober 1998 in Wiesbaden

Prüfungscompetenz der Datenschutzbeauftragten bei den Gerichten

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, dass in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlass von Unsicherheiten ist. Sie weisen daher darauf hin, dass die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u. a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, dass Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

Anlage 4

Entschließung

der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 05./06. Oktober 1998 in Wiesbaden

Fehlende bereichsspezifische Regelungen bei der Justiz

Derzeit werden in allen Bereichen der Justiz - bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern - im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, dass sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, dass die Rechtsprechung des Bundesverfassungsgerichts zum so genannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluss an ihren Beschluss der 48. Konferenz vom 26./27.09.1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

- weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien

namentlich die

- Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;
- Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;
- Datenübermittlung zu wissenschaftlichen Zwecken;
- Datenverarbeitung in der Zwangsvollstreckung;
- Datenverarbeitung im Jugendstrafvollzug;
- Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeit geleistet worden sind, aufgreifen. Dabei ist nicht jeweils geübte Praxis zu legalisieren, sondern es muss vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, wel-

che Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein „StVÄG 1996“ erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück. Zu kritisieren sind vor allem:

- Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung
- Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte
- Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltschaftlichen Dateien und Informationssystemen

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

Anlage 5

Entschließung

der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 05./06. Oktober 1998 in Wiesbaden

Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlass an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlass an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

Anlage 6

EntschlieÙung

der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 05./06. Oktober 1998 in Wiesbaden

Weitergabe von Meldedaten an Adressbuchverlage und Parteien

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, dass sie persönlich adressierte Wahlwerbung der Parteien bekommen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen - erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

Anlage 7

Entschließung

der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 05./06. Oktober 1998 in Wiesbaden

Entwicklungen im Sicherheitsbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z. B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, dass die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

Anlage 8

EntschlieÙung

der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 05./06. Oktober 1998 in Wiesbaden

Dringlichkeit der Datenschutzmodernisierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüÙt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefassten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

- Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.
- Die anlassfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muss in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.
- Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.
- Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweck-

bindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.

- Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

Anlage 9

Entschließung

der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 25./26. März 1999 in Schwerin

zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation

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

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

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

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

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

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

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

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

Anlage 10

EntschlieÙung

der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 25./26. März 1999 in Schwerin

**Entwurf einer RatsentschlieÙung zur Überwachung der Telekommunikation
(ENFOPOL '98)**

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

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

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

Anlage 11

Entschließung

der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 25./26. März 1999 in Schwerin

Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben

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

Die Konferenz begrüßt, dass jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung

darüber aus, dass diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

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

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

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

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

Anlage 12

Entschließung

der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 25./26. März 1999 in Schwerin

Transparente Hard- und Software

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

Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PCs auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number - PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, dass die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.

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

Werden Daten der Nutzerinnen oder Nutzer übermittelt, ohne dass sie dies bemerken, kann deren missbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann aus-

reichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.

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

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

Anlage 13

Entschlieung

der Datenschutzbeauftragten des Bundes und der Lnder
vom 17. Juni 1999

**Parlamentarische Kontrolle von
Lauschangriffen in den Bundeslndern**

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

Im Gegensatz dazu vertritt die Konferenz der Datenschutzbeauftragten des Bundes und der Lnder die Auffassung, dass die Verfassung eine effektive parlamentarische Kontrolle von Lauschangriffen auf Landesebene vorschreibt, die der Kontrolle auf Bundesebene gleichwertig sein muss. Bei Manahmen zur Strafverfolgung durch Landesbehrden besteht die parlamentarische Verantwortlichkeit gegenber den Landesparlamenten. Die Landtage mssen die Mglichkeit haben, die ihnen in anonymisierter Form bermittelten Berichte der Landesregierungen ffentlich zu errtern. Die Landesparlamente sollten deshalb durch Gesetz eine regelmige Berichtspflicht der Landesregierung fr prventiv-polizeiliche und repressive Lauschangriffe vorsehen. Nur auf diese Weise ist eine wirksame parlamentarische Kontrolle der Ausbung dieser einschneidenden berwachungsbefugnisse gewhrleistet.

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

Anlage 14

Entschlieung

der Datenschutzbeauftragten des Bundes und der Lnder
vom 16. August 1999

**Angemessener Datenschutz auch fr
Untersuchungsgefangene**

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

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

Der Gesetzentwurf der Bundesregierung trgt diesem Anliegen durch differenzierende Vorschriften teilweise Rechnung, lsst allerdings noch Raum fr datenschutzrechtliche Verbesserungen. Die Stellungnahme des Bundesrates betont demgegenber einseitig das staatliche Vollzugsinteresse und entfernt sich damit deutlich vom Ziel einer sorgfltigen Gterabwgung.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Lnder muss die gesetzliche Regelung insbesondere folgenden Anforderungen gengen:

- Entgegen dem Vorschlag des Bundesrates, von einer inhaltlichen berwachung nur ausnahmsweise nach dem Ermessen des Gerichts abzusehen, sollte im weiteren Gesetzgebungsverfahren an der Konzeption der Bundesregierung festgehalten werden. Der Gesetzentwurf der Bundesregierung differenziert bei der ber-

wachung der Unterhaltung mit Besucherinnen und Besuchern sowie bei der Kontrolle des Textes von Schriftstücken sachgerecht nach Haftgründen. Nur im Falle der Untersuchungshaft wegen Verdunklungsgefahr sollten diese Maßnahmen unmittelbar und generell durch Gesetz vorgeschrieben werden, während sie bei Vorliegen anderer Haftgründe (z. B. Fluchtgefahr) nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen.

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

- Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigten muss auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot wirksamer Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen, wie vom Bundesrat befürwortet.
- Bei Datenübermittlungen an öffentliche Stellen außerhalb der Vollzugsanstalt (z. B. Sozialleistungsträger, Ausländerbehörden) und an Forschungseinrichtungen müssen die schutzwürdigen Interessen der Betroffenen nur im Rahmen einer Abwägung berücksichtigt werden. Auch die Erteilung von Auskünften an die Verletzten der Straftat sollte der Gesetzgeber unter Beachtung der Unschuldsvermutung regeln.
- Die vom Bundesrat vorgeschlagene erhebliche Einschränkung des Auskunfts- und Akteneinsichtsrechts von Gefangenen im Hinblick auf den Zweck der Untersuchungshaft würde wesentliche Datenschutzrechte in einem besonders sensiblen Bereich weitgehend entwerten und ist daher abzulehnen.

Anlage 15

EntschlieÙung

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

„Gesundheitsreform 2000“

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

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

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

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

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

Insbesondere klärungsbedürftig sind folgende Punkte:

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

Der Wortlaut des Entwurfes beschreibt diese Aufgabe allerdings nur vage. Er lässt nicht erkennen, was auf die Patientinnen und Patienten zukommt. Weder ist klar geregelt, wie weit die Beratung reichen darf, noch mit welchen Rechtsfolgen die oder der Einzelne rechnen muss. Es ist zu befürchten, dass diese Beratung dazu dienen wird, die Patientinnen und Patienten, Ärztinnen und Ärzte und die sonstigen Leistungserbringer zu kontrollieren und zu beeinflussen und dass hierdurch das Arzt-Patienten-Vertrauensverhältnis belastet wird.

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

Der Entwurf sieht im Gegensatz zum bisherigen System vor, dass Abrechnungsdaten und Diagnosen aus der ambulanten ärztlichen Behandlung generell patientenbezogen an die Krankenkassen übermittelt werden. Dadurch entstehen bei den Kassen umfangreiche sensible Datenbestände, aus denen sich für jede einzelne

Patientin und jeden einzelnen Patienten ein vollständiges Gesundheitsprofil erstellen lässt. Wegen der Verpflichtung, die Diagnosen nach dem international gültigen ICD-10-Schlüssel zu codieren, sind diese medizinischen Informationen z. B. im Bereich der Psychotherapie auch hochdifferenziert.

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

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

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

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

gemeinschaften. Abzulehnen ist auch die völlig mangelhafte Zweckbindung der Daten bei den Krankenkassen.

Anlage 16

EntschlieÙung

der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 07./08. Oktober 1999 in Rostock

Patientenschutz durch Pseudonymisierung

Im Gesundheitsausschuss des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, dass die Krankenkassen künftig von den Leistungserbringern (z. B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten“ verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, dass in den Ausschussberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

Anlage 17

Entschließung

der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 07./08. Oktober 1999 in Rostock

**Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten
in der Telekommunikation**

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weit reichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten lässt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch perso-

nenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31.12.1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozessordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100 a StPO neu geregelt werden.

Anlage 18

EntschlieÙung

der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 07./08. Oktober 1999 in Rostock

zum

Beschluss des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

Der Europäische Rat hat anlässlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluss heißt es: „Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern“.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeits-

recht (Art. 2 Abs. 1 i.V. m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Anlage 19

Entschließung

der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 07./08. Oktober 1999 in Rostock

Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, sodass zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z. B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre lässt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang musste befürchtet werden, dass auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger“ besonders hervorgehoben.

Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,

- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,
- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offen gelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muss Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Anlage 20

Entschließung

der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 07./08. Oktober 1999 in Rostock

„Täter-Opfer-Ausgleich und Datenschutz“

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28.05.1999) sieht in § 155 a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des „Täter-Opfer-Ausgleichs“ nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei“ könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei her-

kömmlichen Verfahren sichergestellt werden, wenn durch die „fachlich geleitete Auseinandersetzung“ der „am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden“.

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z. B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, dass an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, dass die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am „Täter-Opfer-Ausgleich“ Beteiligten muss gesetzlich geschützt werden.

Anlage 21

EntschlieÙung

der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 07./08. Oktober 1999 in Rostock

Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer EntschlieÙung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 09./10.03.1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Straftakten nach rechtskräftigem Abschluss eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluss vom 16.08.1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluss von 17.09.1998 darauf hingewiesen, dass die Aufbewahrung von Straftakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

Anlage 22

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates

vom 24. Oktober 1995

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Das Europäische Parlament und der Rat der Europäischen Union -

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 100a,

auf Vorschlag der Kommission ⁽¹⁾,

nach Stellungnahme des Wirtschafts- und Sozialausschusses ⁽²⁾,

gemäß dem Verfahren des Artikels 189b des Vertrags ⁽³⁾,

in Erwägung nachstehender Gründe:

- (1) Die Ziele der Gemeinschaft, wie sie in dem durch den Vertrag über die Europäische Union geänderten Vertrag festgelegt sind, bestehen darin, einen immer engeren Zusammenschluss der europäischen Völker zu schaffen, engere Beziehungen zwischen den in der Gemeinschaft zusammengeschlossenen Staaten herzustellen, durch gemeinsames Handeln den wirtschaftlichen und sozialen Fortschritt zu sichern, indem die Europa trennenden Schranken beseitigt werden, die ständige Besserung der Lebensbedingungen ihrer Völker zu fördern, Frieden

¹ ABl. Nr. C 277 vom 05.11.1990, S. 3, und ABl. Nr. C 311 vom 27.11.1992, S. 30

² ABl. Nr. C 159 vom 17.06.1991, S. 38

³ Stellungnahme des Europäischen Parlaments vom 11. März 1992 (ABl. Nr. C 94 vom 13.04.1992, S. 198), bestätigt am 02. Dezember 1993 (ABl. Nr. C 342 vom 20.12.1993, S. 30). Gemeinsamer Standpunkt des Rates vom 20. Februar 1995 (ABl. Nr. C 93 vom 13.04.1995, S. 1) und Beschluss des Europäischen Parlaments vom 15. Juni 1995 (ABl. Nr. C 166 vom 03.07.1995)

und Freiheit zu wahren und zu festigen und für die Demokratie einzutreten und sich dabei auf die in den Verfassungen und Gesetzen der Mitgliedstaaten sowie in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten anerkannten Grundrechte zu stützen.

- (2) Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen.
- (3) Für die Errichtung und das Funktionieren des Binnenmarktes, der gem. Artikel 7a des Vertrags den freien Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleisten soll, ist es nicht nur erforderlich, dass personenbezogene Daten von einem Mitgliedstaat in einen anderen Mitgliedstaat übermittelt werden können, sondern auch, dass die Grundrechte der Personen gewahrt werden.
- (4) Immer häufiger werden personenbezogene Daten in der Gemeinschaft in den verschiedenen Bereichen wirtschaftlicher und sozialer Tätigkeiten verarbeitet. Die Fortschritte der Informationstechnik erleichtern die Verarbeitung und den Austausch dieser Daten beträchtlich.
- (5) Die wirtschaftliche und soziale Integration, die sich aus der Errichtung und dem Funktionieren des Binnenmarktes im Sinne von Artikel 7a des Vertrags ergibt, wird notwendigerweise zu einer spürbaren Zunahme der grenzüberschreitenden Ströme personenbezogener Daten zwischen allen am wirtschaftlichen und sozialen Leben der Mitgliedstaaten Beteiligten im öffentlichen wie im privaten Bereich führen. Der Austausch personenbezogener Daten zwischen in verschiedenen Mitgliedstaaten niedergelassenen Unternehmen wird zunehmen. Die Verwaltungen der Mitgliedstaaten sind aufgrund des Gemeinschafts-

rechts gehalten, zusammenzuarbeiten und untereinander personenbezogene Daten auszutauschen, um im Rahmen des Raums ohne Grenzen, wie er durch den Binnenmarkt hergestellt wird, ihren Auftrag erfüllen oder Aufgaben anstelle der Behörden eines anderen Mitgliedstaats durchführen zu können.

- (6) Die verstärkte wissenschaftliche und technische Zusammenarbeit sowie die koordinierte Einführung neuer Kommunikationsnetze in der Gemeinschaft erfordern und erleichtern den grenzüberschreitenden Verkehr personenbezogener Daten.
- (7) Das unterschiedliche Niveau des Schutzes der Rechte und Freiheiten von Personen, insbesondere der Privatsphäre, bei der Verarbeitung personenbezogener Daten in den Mitgliedstaaten kann die Übermittlung dieser Daten aus dem Gebiet eines Mitgliedstaats in das Gebiet eines anderen Mitgliedstaats verhindern. Dieses unterschiedliche Schutzniveau kann somit ein Hemmnis für die Ausübung einer Reihe von Wirtschaftstätigkeiten auf Gemeinschaftsebene darstellen, den Wettbewerb verfälschen und die Erfüllung des Auftrags der im Anwendungsbereich des Gemeinschaftsrechts tätigen Behörden verhindern. Dieses unterschiedliche Schutzniveau ergibt sich aus der Verschiedenartigkeit der einzelstaatlichen Rechts- und Verwaltungsvorschriften.
- (8) Zur Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten ist ein gleichwertiges Schutzniveau hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten unerlässlich. Insbesondere unter Berücksichtigung der großen Unterschiede, die gegenwärtig zwischen den einschlägigen einzelstaatlichen Rechtsvorschriften bestehen, und der Notwendigkeit, die Rechtsvorschriften der Mitgliedstaaten zu koordinieren, damit der grenzüberschreitende Fluss personenbezogener Daten kohärent und in Übereinstimmung mit dem Ziel des Binnenmarktes im Sinne des Artikels 7a des Vertrags geregelt wird, lässt sich dieses für den Binnenmarkt grundlegende Ziel nicht allein durch das Vorgehen der Mitgliedstaaten verwirklichen.

Deshalb ist eine Maßnahme der Gemeinschaft zur Angleichung der Rechtsvorschriften erforderlich.

- (9) Die Mitgliedstaaten dürfen aufgrund des gleichwertigen Schutzes, der sich aus der Angleichung der einzelstaatlichen Rechtsvorschriften ergibt, den freien Verkehr personenbezogener Daten zwischen ihnen nicht mehr aus Gründen behindern, die den Schutz der Rechte und Freiheiten natürlicher Personen und insbesondere das Recht auf die Privatsphäre betreffen. Die Mitgliedstaaten besitzen einen Spielraum, der im Rahmen der Durchführung der Richtlinie von den Wirtschafts- und Sozialpartnern genutzt werden kann. Sie können somit in ihrem einzelstaatlichen Recht allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung festlegen. Hierbei streben sie eine Verbesserung des gegenwärtig durch ihre Rechtsvorschriften gewährten Schutzes an. Innerhalb dieses Spielraums können unter Beachtung des Gemeinschaftsrechts Unterschiede bei der Durchführung der Richtlinie auftreten, was Auswirkungen für den Datenverkehr sowohl innerhalb eines Mitgliedstaats als auch in der Gemeinschaft haben kann.
- (10) Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und -freiheiten, insbesondere des auch in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern muss im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.
- (11) Die in dieser Richtlinie enthaltenen Grundsätze zum Schutz der Rechte und Freiheiten der Personen, insbesondere der Achtung der Privatsphäre, konkretisieren und erweitern die in dem Übereinkommen des Europarats vom 28. Januar 1981 zum

Schutze der Personen bei der automatischen Verarbeitung personenbezogener Daten enthaltenen Grundsätze.

- (12) Die Schutzprinzipien müssen für alle Verarbeitungen personenbezogener Daten gelten, sobald die Tätigkeiten des für die Verarbeitung Verantwortlichen in den Anwendungsbereich des Gemeinschaftsrechts fallen. Auszunehmen ist die Datenverarbeitung, die von einer natürlichen Person in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten - wie zum Beispiel Schriftverkehr oder Führung von Anschriftenverzeichnissen - vorgenommen wird.
- (13) Die in den Titeln V und VI des Vertrags über die Europäische Union genannten Tätigkeiten, die die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates oder die Tätigkeiten des Staates im Bereich des Strafrechts betreffen, fallen unbeschadet der Verpflichtungen der Mitgliedstaaten gem. Artikel 56 Absatz 2 sowie gem. den Artikeln 57 und 100a des Vertrags zur Gründung der Europäischen Gemeinschaft nicht in den Anwendungsbereich des Gemeinschaftsrechts. Die Verarbeitung personenbezogener Daten, die zum Schutz des wirtschaftlichen Wohls des Staates erforderlich ist, fällt nicht unter diese Richtlinie, wenn sie mit Fragen der Sicherheit des Staates zusammenhängt.
- (14) In Anbetracht der Bedeutung der gegenwärtigen Entwicklung im Zusammenhang mit der Informationsgesellschaft bezüglich Techniken der Erfassung, Übermittlung, Veränderung, Speicherung, Aufbewahrung oder Weitergabe von personenbezogenen Ton- und Bilddaten muss diese Richtlinie auch auf die Verarbeitung dieser Daten Anwendung finden.
- (15) Die Verarbeitung solcher Daten wird von dieser Richtlinie nur erfasst, wenn sie automatisiert erfolgt oder wenn die Daten, auf die sich die Verarbeitung bezieht, in Dateien enthalten oder für solche bestimmt sind, die nach bestimmten personenbezogenen Kriterien strukturiert sind, um einen leichten Zugriff auf die Daten zu ermöglichen.

- (16) Die Verarbeitung von Ton- und Bilddaten, wie bei der Videoüberwachung, fällt nicht unter diese Richtlinie, wenn sie für Zwecke der öffentlichen Sicherheit, der Landesverteidigung, der Sicherheit des Staates oder der Tätigkeiten des Staates im Bereich des Strafrechts oder anderen Tätigkeiten erfolgt, die nicht unter das Gemeinschaftsrecht fallen.
- (17) Bezüglich der Verarbeitung von Ton- und Bilddaten für journalistische, literarische oder künstlerische Zwecke, insbesondere im audiovisuellen Bereich, finden die Grundsätze dieser Richtlinie gem. Artikel 9 eingeschränkt Anwendung.
- (18) Um zu vermeiden, dass einer Person der gemäß dieser Richtlinie gewährleistete Schutz vorenthalten wird, müssen auf jede in der Gemeinschaft erfolgte Verarbeitung personenbezogener Daten die Rechtsvorschriften eines Mitgliedstaats angewandt werden. Es ist angebracht, auf die Verarbeitung, die von einer Person, die dem in dem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen unterstellt ist, vorgenommen werden, die Rechtsvorschriften dieses Staates anzuwenden.
- (19) Eine Niederlassung im Hoheitsgebiet eines Mitgliedstaats setzt die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus. Die Rechtsform einer solchen Niederlassung, die eine Agentur oder eine Zweigstelle sein kann, ist in dieser Hinsicht nicht maßgeblich. Wenn der Verantwortliche im Hoheitsgebiet mehrerer Mitgliedstaaten niedergelassen ist, insbesondere mit einer Filiale, muss er vor allem zur Vermeidung von Umgehungen sicherstellen, dass jede dieser Niederlassungen die Verpflichtungen einhält, die im jeweiligen einzelstaatlichen Recht vorgesehen sind, das auf ihre jeweiligen Tätigkeiten anwendbar ist.
- (20) Die Niederlassung des für die Verarbeitung Verantwortlichen in einem Drittland darf dem Schutz der Personen gemäß dieser Richtlinie nicht entgegenstehen. In diesem Fall sind die Verarbeitungen dem Recht des Mitgliedstaats zu unterwerfen, in

dem sich die für die betreffenden Verarbeitungen verwendeten Mittel befinden, und Vorkehrungen zu treffen, um sicherzustellen, dass die in dieser Richtlinie vorgesehenen Rechte und Pflichten tatsächlich eingehalten werden.

- (21) Diese Richtlinie berührt nicht die im Strafrecht geltenden Territorialitätsregeln.
- (22) Die Mitgliedstaaten können in ihren Rechtsvorschriften oder bei der Durchführung der Vorschriften zur Umsetzung dieser Richtlinie die allgemeinen Bedingungen präzisieren, unter denen die Verarbeitungen rechtmäßig sind. Insbesondere nach Artikel 5 in Verbindung mit den Artikeln 7 und 8 können die Mitgliedstaaten neben den allgemeinen Regeln besondere Bedingungen für die Datenverarbeitung in spezifischen Bereichen und für die verschiedenen Datenkategorien gem. Artikel 8 vorsehen.
- (23) Die Mitgliedstaaten können den Schutz von Personen sowohl durch ein allgemeines Gesetz zum Schutz von Personen bei der Verarbeitung personenbezogener Daten als auch durch gesetzliche Regelungen für bestimmte Bereiche, wie zum Beispiel die statistischen Ämter, sicherstellen.
- (24) Diese Richtlinie berührt nicht die Rechtsvorschriften zum Schutz juristischer Personen bei der Verarbeitung von Daten, die sich auf sie beziehen.
- (25) Die Schutzprinzipien finden zum einen ihren Niederschlag in den Pflichten, die den Personen, Behörden, Unternehmen, Geschäftsstellen oder anderen für die Verarbeitung verantwortlichen Stellen obliegen; diese Pflichten betreffen insbesondere die Datenqualität, die technische Sicherheit, die Meldung bei der Kontrollstelle und die Voraussetzungen, unter denen eine Verarbeitung vorgenommen werden kann. Zum anderen kommen sie zum Ausdruck in den Rechten der Personen, deren Daten Gegenstand von Verarbeitungen sind, über diese informiert zu werden, Zugang zu den Daten zu erhalten, ihre Be-

ichtigung verlangen bzw. unter gewissen Voraussetzungen Widerspruch gegen die Verarbeitung einlegen zu können.

- (26) Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen. Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. Die Verhaltensregeln im Sinne des Artikels 27 können ein nützliches Instrument sein, mit dem angegeben wird, wie sich die Daten in einer Form anonymisieren und aufbewahren lassen, die die Identifizierung der betroffenen Person unmöglich macht.
- (27) Datenschutz muss sowohl für automatisierte als auch für nicht automatisierte Verarbeitungen gelten. In der Tat darf der Schutz nicht von den verwendeten Techniken abhängen, da andernfalls ernsthafte Risiken der Umgehung entstehen würden. Bei manuellen Verarbeitungen erfasst diese Richtlinie lediglich Dateien, nicht jedoch unstrukturierte Akten. Insbesondere muss der Inhalt einer Datei nach bestimmten personenbezogenen Kriterien strukturiert sein, die einen leichten Zugriff auf die Daten ermöglichen. Nach der Definition in Artikel 2 Buchstabe c) können die Mitgliedstaaten die Kriterien zur Bestimmung der Elemente einer strukturierten Sammlung personenbezogener Daten sowie die verschiedenen Kriterien zur Regelung des Zugriffs zu einer solchen Sammlung festlegen. Akten und Aktsammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind, fallen unter keinen Umständen in den Anwendungsbereich dieser Richtlinie.
- (28) Die Verarbeitung personenbezogener Daten muss gegenüber den betroffenen Personen nach Treu und Glauben erfolgen. Sie hat den angestrebten Zweck zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen. Die Zwecke müssen

eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Zweckbestimmungen der Weiterverarbeitungen nach der Erhebung dürfen nicht mit den ursprünglich festgelegten Zwecken unvereinbar sein.

- (29) Die Weiterverarbeitung personenbezogener Daten für historische, statistische oder wissenschaftliche Zwecke ist im Allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, wenn der Mitgliedstaat geeignete Garantien vorsieht. Diese Garantien müssen insbesondere ausschließen, dass die Daten für Maßnahmen oder Entscheidungen gegenüber einzelnen Betroffenen verwendet werden.
- (30) Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn sie auf der Einwilligung der betroffenen Person beruht oder notwendig ist im Hinblick auf den Abschluss oder die Erfüllung einer gesetzlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse, in Ausübung hoheitlicher Gewalt oder wenn sie im Interesse einer anderen Person erforderlich ist, vorausgesetzt, dass die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen. Um den Ausgleich der in Frage stehenden Interessen unter Gewährleistung eines effektiven Wettbewerbs sicherzustellen, können die Mitgliedstaaten insbesondere die Bedingungen näher bestimmen, unter denen personenbezogene Daten bei rechtmäßigen Tätigkeiten im Rahmen laufender Geschäfte von Unternehmen und anderen Einrichtungen an Dritte weitergegeben werden können. Ebenso können sie die Bedingungen festlegen, unter denen personenbezogene Daten an Dritte zum Zweck der kommerziellen Werbung oder der Werbung von Wohltätigkeitsverbänden oder anderen Vereinigungen oder Stiftungen, z. B. mit politischer Ausrichtung, weitergegeben werden können, und zwar unter Berücksichtigung der Bestimmungen dieser Richtlinie, nach denen betroffene Personen ohne Angabe von Gründen und ohne Kosten Widerspruch gegen die Verarbeitung von Daten, die sie betreffen, ergehen können.

- (31) Die Verarbeitung personenbezogener Daten ist ebenfalls als rechtmäßig anzusehen, wenn sie erfolgt, um ein für das Leben der betroffenen Person wesentliches Interesse zu schützen.
- (32) Es ist nach einzelstaatlichen Recht festzulegen, ob es sich bei dem für die Verarbeitung Verantwortlichen, der mit der Wahrnehmung einer Aufgabe betraut wurde, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht oder das Privatrecht fallende Person, wie beispielsweise eine Berufsvereinigung, handeln soll.
- (33) Daten, die aufgrund ihrer Art geeignet sind, die Grundfreiheiten oder die Privatsphäre zu beeinträchtigen, dürfen nicht ohne ausdrückliche Einwilligung der betroffenen Person verarbeitet werden. Ausnahmen von diesem Verbot müssen ausdrücklich vorgesehen werden bei spezifischen Notwendigkeiten, insbesondere wenn die Verarbeitung dieser Daten für gewisse auf das Gesundheitswesen bezogene Zwecke von Personen vorgenommen wird, die nach dem einzelstaatlichen Recht dem Berufsgeheimnis unterliegen, oder wenn die Verarbeitung für berechnete Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, deren Ziel es ist, die Ausübung von Grundfreiheiten zu ermöglichen.
- (34) Die Mitgliedstaaten können, wenn dies durch ein wichtiges öffentliches Interesse gerechtfertigt ist, Ausnahmen vom Verbot der Verarbeitung sensibler Datenkategorien vorsehen in Bereichen wie dem öffentlichen Gesundheitswesen und der sozialen Sicherheit - insbesondere hinsichtlich der Sicherung von Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen -, der wissenschaftlichen Forschung und der öffentlichen Statistik. Die Mitgliedstaaten müssen jedoch geeignete besondere Garantien zum Schutz der Grundrechte und der Privatsphäre von Personen vorsehen.

- (35) Die Verarbeitung personenbezogener Daten durch staatliche Stellen für verfassungsrechtlich oder im Völkerrecht niedergelegte Zwecke von staatlich anerkannten Religionsgesellschaften erfolgt ebenfalls im Hinblick auf ein wichtiges öffentliches Interesse.
- (36) Wenn es in bestimmten Mitgliedstaaten zum Funktionieren des demokratischen Systems gehört, dass die politischen Parteien im Zusammenhang mit Wahlen Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen eines wichtigen öffentlichen Interesses zugelassen werden, sofern angemessene Garantien vorgesehen werden.
- (37) Für die Verarbeitung personenbezogener Daten zu journalistischen, literarischen oder künstlerischen Zwecken, insbesondere im audiovisuellen Bereich, sind Ausnahmen von bestimmten Vorschriften dieser Richtlinie vorzusehen, soweit sie erforderlich sind, um die Grundrechte der Person mit der Freiheit der Meinungsäußerung und insbesondere der Freiheit, Informationen zu erhalten oder weiterzugeben, die insbesondere in Artikel 10 der Europäischen Konvention zum Schutze der Menschenrechte und der Grundfreiheiten garantiert ist, in Einklang zu bringen. Es obliegt deshalb den Mitgliedstaaten, unter Abwägung der Grundrechte Ausnahmen und Einschränkungen festzulegen, die bei den allgemeinen Maßnahmen zur Rechtmäßigkeit der Verarbeitung von Daten, bei den Maßnahmen zur Übermittlung der Daten in Drittländer sowie hinsichtlich der Zuständigkeiten der Kontrollstellen erforderlich sind, ohne dass jedoch Ausnahmen bei den Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung vorzusehen sind. Ferner sollte mindestens die in diesem Bereich zuständige Kontrollstelle bestimmte nachträgliche Zuständigkeiten erhalten, beispielsweise zur regelmäßigen Veröffentlichung eines Berichts oder zur Befassung der Justizbehörden.
- (38) Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein

einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden.

- (39) Bestimmte Verarbeitungen betreffen Daten, die der Verantwortliche nicht unmittelbar bei der betroffenen Person erhoben hat. Desweiteren können Daten rechtmäßig an Dritte weitergegeben werden, auch wenn die Weitergabe bei der Erhebung der Daten bei der betroffenen Person nicht vorgesehen war. In diesen Fällen muss die betroffene Person zum Zeitpunkt der Speicherung der Daten oder spätestens bei der erstmaligen Weitergabe der Daten an Dritte unterrichtet werden.
- (40) Diese Verpflichtung erübrigt sich jedoch, wenn die betroffene Person bereits unterrichtet ist. Sie besteht auch nicht, wenn die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist oder wenn die Unterrichtung der betroffenen Person unmöglich ist oder unverhältnismäßigen Aufwand erfordert, was bei Verarbeitungen für historische, statistische oder wissenschaftliche Zwecke der Fall sein kann. Diesbezüglich können die Zahl der betroffenen Personen, das Alter der Daten und etwaige Ausgleichsmaßnahmen in Betracht gezogen werden.
- (41) Jede Person muss ein Auskunftsrecht hinsichtlich der sie betreffenden Daten, die Gegenstand einer Verarbeitung sind, haben, damit sie sich insbesondere von der Richtigkeit dieser Daten und der Zulässigkeit ihrer Verarbeitung überzeugen kann. Aus denselben Gründen muss jede Person außerdem das Recht auf Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne des Artikels 15 Absatz 1, besitzen. Dieses Recht darf weder das Geschäftsgeheimnis noch das Recht an geistigem Eigentum, insbesondere das Urheberrecht zum Schutz von Software, berühren. Dies darf allerdings nicht zu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.

- (42) Die Mitgliedstaaten können die Auskunfts- und Informationsrechte im Interesse der betroffenen Person oder zum Schutz der Rechte und Freiheiten Dritter einschränken. Zum Beispiel können sie vorsehen, dass Auskunft über medizinische Daten nur über ärztlicher Personal erhalten werden kann.
- (43) Die Mitgliedstaaten können Beschränkungen des Auskunfts- und Informationsrechts sowie bestimmter Pflichten des für die Verarbeitung Verantwortlichen vorsehen, soweit dies beispielsweise für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, für zwingende wirtschaftliche oder finanzielle Interessen eines Mitgliedstaats oder der Union oder für die Ermittlung und Verfolgung von Straftaten oder von Verstößen gegen Standesregeln bei reglementierten Berufen erforderlich ist. Als Ausnahmen und Beschränkungen sind Kontroll-, Überwachungs- und Ordnungsfunktionen zu nennen, die in den drei letztgenannten Bereichen in Bezug auf öffentliche Sicherheit, wirtschaftliches oder finanzielles Interesse und Strafverfolgung erforderlich sind. Die Erwähnung der Aufgaben in diesen drei Bereichen lässt die Zulässigkeit von Ausnahmen und Einschränkungen aus Gründen der Sicherheit des Staates und der Landesverteidigung unberührt.
- (44) Die Mitgliedstaaten können aufgrund gemeinschaftlicher Vorschriften gehalten sein, von den das Auskunftsrecht, die Information der Personen und die Qualität der Daten betreffenden Bestimmungen dieser Richtlinie abzuweichen, um bestimmte der oben genannten Zweckbestimmungen zu schützen.
- (45) Auch wenn die Daten Gegenstand einer rechtmäßigen Verarbeitung aufgrund eines öffentlichen Interesses, der Ausübung hoheitlicher Gewalt oder der Interessen eines Einzelnen sein können, sollte doch jede betroffene Person das Recht besitzen, aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen Widerspruch dagegen einzulegen, dass die sie betreffenden Daten verarbeitet werden. Die Mitgliedstaaten können allerdings innerstaatliche Bestimmungen vorsehen, die dem entgegenstehen.

- (46) Für den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, und zwar sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Verarbeitung, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern. Die Mitgliedstaaten haben dafür Sorge zu tragen, dass der für die Verarbeitung Verantwortliche diese Maßnahmen einhält. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.
- (47) Wird eine Nachricht, die personenbezogene Daten enthält, über Telekommunikationsdienste oder durch elektronische Post übermittelt, deren einziger Zweck darin besteht, Nachrichten dieser Art zu übermitteln, so gilt in der Regel die Person, von der die Nachricht stammt, und nicht die Person, die den Übermittlungsdienst anbietet, als Verantwortlicher für die Verarbeitung der in der Nachricht enthaltenen personenbezogenen Daten. Jedoch gelten die Personen, die diese Dienste anbieten, in der Regel als Verantwortliche für die Verarbeitung der personenbezogenen Daten, die zusätzlich für den Betrieb des Dienstes erforderlich sind.
- (48) Die Meldeverfahren dienen der Offenlegung der Zweckbestimmungen der Verarbeitungen sowie ihrer wichtigsten Merkmale mit dem Zweck der Überprüfung ihrer Vereinbarkeit mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.
- (49) Um angemessene Verwaltungsformalitäten zu vermeiden, können die Mitgliedstaaten bei Verarbeitungen, bei denen eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen nicht zu erwarten ist, von der Meldepflicht absehen oder sie

vereinfachen, vorausgesetzt, dass diese Verarbeitungen den Bestimmungen entsprechen, mit denen der Mitgliedstaat die Grenzen solcher Verarbeitungen festgelegt hat. Eine Befreiung oder eine Vereinfachung kann ebenso vorgesehen werden, wenn ein vom für die Verarbeitung Verantwortlichen benannter Datenschutzbeauftragter sicherstellt, dass eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen durch die Verarbeitung nicht zu erwarten ist. Ein solcher Beauftragter, ob Angestellter des für die Verarbeitung Verantwortlichen oder externer Beauftragter, muss seine Aufgaben in vollständiger Unabhängigkeit ausüben können.

- (50) Die Befreiung oder Vereinfachung kann vorgesehen werden für Verarbeitungen, deren einziger Zweck das Führen eines Registers ist, das gemäß einzelstaatlichem Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht.
- (51) Die Vereinfachung oder Befreiung von der Meldepflicht entbindet jedoch den für die Verarbeitung Verantwortlichen von keiner der anderen sich aus dieser Richtlinie ergebenden Verpflichtungen.
- (52) In diesem Zusammenhang ist die nachträgliche Kontrolle durch die zuständigen Stellen im Allgemeinen als ausreichende Maßnahme anzusehen.
- (53) Bestimmte Verarbeitungen können jedoch aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung - wie beispielsweise derjenigen, betroffene Personen von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrags auszuschließen - oder aufgrund der besonderen Verwendung einer neuen Technologie besondere Risiken im Hinblick auf die Rechte und Freiheiten der betroffenen Personen aufweisen. Es obliegt den Mitgliedstaaten, derartige Risiken in ihren Rechtsvorschriften aufzuführen, wenn sie dies wünschen.

- (54) Bei allen in der Gesellschaft durchgeführten Verarbeitungen sollte die Zahl der Verarbeitungen mit solchen besonderen Risiken sehr beschränkt sein. Die Mitgliedstaaten müssen für diese Verarbeitungen vorsehen, dass vor ihrer Durchführung eine Vorabprüfung durch die Kontrollstelle oder in Zusammenarbeit mit ihr durch den Datenschutzbeauftragten vorgenommen wird. Als Ergebnis dieser Vorabprüfung kann die Kontrollstelle gemäß einzelstaatlichem Recht eine Stellungnahme abgeben oder die Verarbeitung genehmigen. Diese Prüfung kann auch bei der Ausarbeitung einer gesetzgeberischen Maßnahme des nationalen Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme erfolgen, die die Art der Verarbeitung und geeignete Garantien festlegt.
- (55) Für den Fall der Missachtung der Rechte der betroffenen Personen durch den für die Verarbeitung Verantwortlichen ist im nationalen Recht eine gerichtliche Überprüfungsmöglichkeit vorzusehen. Mögliche Schäden, die den Personen aufgrund einer unzulässigen Verarbeitung entstehen, sind von dem für die Verarbeitung Verantwortlichen zu ersetzen, der von seiner Haftung befreit werden kann, wenn er nachweist, dass der Schaden ihm nicht angelastet werden kann, insbesondere weil ein Fehlverhalten der betroffenen Person oder ein Fall höherer Gewalt vorliegt. Unabhängig davon, ob es sich um eine Person des Privatrechts oder des öffentlichen Rechts handelt, müssen Sanktionen jede Person treffen, die die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht einhält.
- (56) Grenzüberschreitender Verkehr von personenbezogenen Daten ist für die Entwicklung des internationalen Handels notwendig. Der in der Gemeinschaft durch diese Richtlinie gewährte Schutz von Personen steht der Übermittlung personenbezogener Daten in Drittländer, die ein angemessenes Schutzniveau aufweisen, nicht entgegen. Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, ist unter Berücksichtigung aller Umstände im Hinblick auf eine Übermittlung oder eine Kategorie von Übermittlungen zu beurteilen.

- (57) Bietet hingegen ein Drittland kein angemessenes Schutzniveau, so ist die Übermittlung personenbezogener Daten in dieses Land zu untersagen.
- (58) Ausnahmen von diesem Verbot sind unter bestimmten Voraussetzungen vorzusehen, wenn die betroffene Person ihre Einwilligung erteilt hat oder die Übermittlung im Rahmen eines Vertrags oder Gerichtsverfahrens oder zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist, wie zum Beispiel bei internationalem Datenaustausch zwischen Steuer- oder Zollverwaltungen oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind. Ebenso kann eine Übermittlung aus einem gesetzlich vorgesehenen Register erfolgen, das der öffentlichen Einsichtnahme oder der Einsichtnahme durch Personen mit berechtigtem Interesse dient. In diesem Fall sollte eine solche Übermittlung nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten umfassen. Ist ein Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, so sollte die Übermittlung nur auf Antrag dieser Person oder nur dann erfolgen, wenn diese Person die Adressaten der Übermittlung sind.
- (59) Besondere Maßnahmen können getroffen werden, um das unzureichende Schutzniveau in einem Drittland auszugleichen, wenn der für die Verarbeitung Verantwortliche geeignete Sicherheiten nachweist. Außerdem sind Verfahren für die Verhandlungen zwischen der Gemeinschaft und den betreffenden Drittländern vorzusehen.
- (60) Übermittlungen in Drittstaaten dürfen auf jeden Fall nur unter voller Einhaltung der Rechtsvorschriften erfolgen, die die Mitgliedstaaten gemäß dieser Richtlinie, insbesondere gem. Artikel 8, erlassen haben.
- (61) Die Mitgliedstaaten und die Kommissionen müssen in ihren jeweiligen Zuständigkeitsbereichen die betroffenen Wirtschaftskreise ermutigen, Verhaltensregeln auszuarbeiten, um unter Berücksichtigung der Besonderheiten der Verarbeitung

in bestimmten Bereichen die Durchführung dieser Richtlinie im Einklang mit den hierfür vorgesehenen einzelstaatlichen Bestimmungen zu fördern.

- (62) Die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten ist ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten.
- (63) Diese Stellen sind mit den notwendigen Mitteln für die Erfüllung dieser Aufgabe auszustatten, d. h. Untersuchungs- und Einwirkungsbefugnissen, insbesondere bei Beschwerden, sowie Klagerecht. Die Kontrollstellen haben zur Transparenz der Verarbeitungen in dem Mitgliedstaat beizutragen, dem sie unterstehen.
- (64) Die Behörden der verschiedenen Mitgliedstaaten werden einander bei der Wahrnehmung ihrer Aufgaben unterstützen müssen, um sicherzustellen, dass die Schutzregeln in der ganzen Europäischen Union beachtet werden.
- (65) Auf Gemeinschaftsebene ist eine Arbeitsgruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten einzusetzen, die ihre Aufgaben in völliger Unabhängigkeit wahrzunehmen hat. Unter Berücksichtigung dieses besonderen Charakters hat sie die Kommission zu beraten und insbesondere zur einheitlichen Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften beizutragen.
- (66) Für die Übermittlung von Daten in Drittländern ist es zur Anwendung dieser Richtlinie erforderlich, der Kommission Durchführungsbefugnisse zu übertragen und ein Verfahren gemäß den Bestimmungen des Beschlusses 87/373/EWG des Rates ⁽⁴⁾ festzulegen.

⁴ ABl. Nr. B 197 vom 18.07.1987, S. 33

- (67) Am 20. Dezember 1994 wurde zwischen dem Europäischen Parlament, dem Rat und der Kommission ein Modus vivendi betreffend die Maßnahmen zur Durchführung der nach dem Verfahren des Artikels 189b des EG-Vertrags erlassenen Rechtsakte vereinbart.
- (68) Die in dieser Richtlinie enthaltenen Grundsätze des Schutzes der Rechte und Freiheiten der Personen und insbesondere der Achtung der Privatsphäre bei der Verarbeitung personenbezogener Daten können - besonders für bestimmte Bereiche - durch spezifische Regeln ergänzt oder präzisiert werden, die mit diesen Grundsätzen in Einklang stehen.
- (69) Den Mitgliedstaaten sollte eine Frist von längstens drei Jahren ab Inkrafttreten ihrer Vorschriften zur Umsetzung dieser Richtlinie eingeräumt werden, damit sie die neuen einzelstaatlichen Vorschriften fortschreitend auf alle bereits laufenden Verarbeitungen anwenden können. Um eine kosteneffiziente Durchführung dieser Vorschriften zu erleichtern, wird den Mitgliedstaaten eine weitere Frist von zwölf Jahren nach Annahme dieser Richtlinie eingeräumt, um die Anpassung bestehender manueller Dateien an bestimmte Vorschriften dieser Richtlinie sicherzustellen. Werden in solchen Dateien enthaltene Daten während dieser erweiterten Umsetzungsfrist manuell verarbeitet, so sollten die Dateien zum Zeitpunkt der Verarbeitung mit diesen Vorschriften in Einklang gebracht werden.
- (70) Die betroffene Person braucht nicht erneut ihre Einwilligung zu geben, damit der Verantwortliche nach Inkrafttreten der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie eine Verarbeitung sensibler Daten fortführen kann, die für die Erfüllung eines in freier Willenserklärung geschlossenen Vertrags erforderlich ist und vor Inkrafttreten der genannten Vorschriften mitgeteilt wurde.
- (71) Diese Richtlinie steht den gesetzlichen Regelungen eines Mitgliedstaats im Bereich der geschäftsmäßigen Werbung gegenüber in seinem Hoheitsgebiet ansässigen Verbrauchern nicht

entgegen, sofern sich diese gesetzlichen Regelungen nicht auf den Schutz der Person bei der Verarbeitung personenbezogener Daten beziehen.

- (72) Diese Richtlinie erlaubt bei der Umsetzung der mit ihr festgelegten Grundsätze die Berücksichtigung des Grundsatzes des öffentlichen Zugangs zu amtlichen Dokumenten -

haben folgende Richtlinie erlassen:

Kapitel I

Allgemeine Bestimmungen

Artikel 1

Gegenstand der Richtlinie

(1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.

(2) Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gem. Absatz 1 gewährleisteten Schutzes.

Artikel 2

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

- a) „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren

spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

- b) „Verarbeitung personenbezogener Daten“ („Verarbeitung“) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;
- c) „Datei mit personenbezogenen Daten“ („Datei“) jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, gleichgültig ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird;
- d) „für die Verarbeitung Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden;
- e) „Auftragsverarbeiter“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;
- f) „Dritter“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person,

dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;

- g) „Empfänger“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die Daten erhält, gleichgültig, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines einzelnen Untersuchungsauftrags möglicherweise Daten erhalten, gelten jedoch nicht als Empfänger;
- h) „Einwilligung der betroffenen Person“ jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.

Artikel 3

Anwendungsbereich

(1) Diese Richtlinie gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

(2) Diese Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten,

- die für die Ausübung der Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich;

- die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird.

Artikel 4

Anwendbares einzelstaatliches Recht

(1) Jeder Mitgliedstaat wendet die Vorschriften, die er zur Umsetzung dieser Richtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten an,

- a) die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält;
- b) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht in seinem Hoheitsgebiet, aber an einem Ort niedergelassen ist, an dem das einzelstaatliche Recht dieses Mitgliedstaats gemäß dem internationalen öffentlichen Recht Anwendung findet;
- c) die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.

(2) In dem in Absatz 1 Buchstabe c) genannten Fall hat der für die Verarbeitung Verantwortliche einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter zu benennen, unbeschadet der

Möglichkeit eines Vorgehens gegen den für die Verarbeitung Verantwortlichen selbst.

Kapitel II

Allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten

Artikel 5

Die Mitgliedstaaten bestimmen nach Maßgabe dieses Kapitels die Voraussetzungen näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

Abschnitt I

Grundsätze in Bezug auf die Qualität der Daten

Artikel 6

(1) Die Mitgliedstaaten sehen vor, dass personenbezogene Daten

- a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;
- b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im Allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;
- c) den Zwecken entsprechen, für die sie erhoben und/ oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;

- d) sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden;
 - e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Person ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.
- (2) Der für die Verarbeitung Verantwortliche hat für die Einhaltung des Absatzes 1 zu sorgen.

Abschnitt II

Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten

Artikel 7

Die Mitgliedstaaten sehen vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

- a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;
- b) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;

- c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;
- e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen werden;
- f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gem. Artikel 1 Absatz 1 geschützt sind, überwiegen.

Abschnitt III

Besondere Kategorien der Verarbeitung

Artikel 8

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.

(2) Absatz 1 findet in folgenden Fällen keine Anwendung:

- a) Die betroffene Person hat ausdrücklich in die Verarbeitung der genannten Daten eingewilligt, es sei denn, nach den Rechtsvor-

schriften des Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen nicht aufgehoben werden;

oder

- b) die Verarbeitung ist erforderlich, um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist;

oder

- c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich, sofern die Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;

oder

- d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt, im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen an Dritte weitergegeben werden;

oder

- e) die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich.

(3) Absatz 1 gilt nicht, wenn die Verarbeitung der Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal erfolgt, das nach dem einzelstaatlichen Recht, einschließlich der von den zuständigen einzelstaatlichen Stellen erlassenen Regelungen, dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen.

(4) Die Mitgliedstaaten können vorbehaltlich angemessener Garantien aus Gründen eines wichtigen öffentlichen Interesses entweder im Wege einer nationalen Rechtsvorschrift oder im Wege einer Entscheidung der Kontrollstelle andere als die in Absatz 2 genannten Ausnahmen vorsehen.

(5) Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen betreffen, darf nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen, wobei ein Mitgliedstaat jedoch Ausnahmen aufgrund innerstaatlicher Rechtsvorschriften, die geeignete besondere Garantien vorsehen, festlegen kann. Ein vollständiges Register der strafrechtlichen Verurteilungen darf allerdings nur unter behördlicher Aufsicht geführt werden.

Die Mitgliedstaaten können vorsehen, dass Daten, die administrative Strafen oder zivilrechtliche Urteile betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen.

(6) Die in den Absätzen 4 und 5 vorgesehenen Abweichungen von Absatz 1 sind der Kommission mitzuteilen.

(7) Die Mitgliedstaaten bestimmen, unter welchen Bedingungen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen.

Artikel 9

Verarbeitung personenbezogener Daten und Meinungsfreiheit

Die Mitgliedstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von diesem Kapitel sowie von den Kapiteln IV und VI nur insofern vor, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen.

Abschnitt IV

Information der betroffenen Person

Artikel 10

Information bei der Erhebung personenbezogener Daten bei der betroffenen Person

Die Mitgliedstaaten sehen vor, dass die Person, bei der die sie betreffenden Daten erhoben werden, vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhält, sofern diese ihr noch nicht vorliegen:

- a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters,
- b) Zweckbestimmungen der Verarbeitung, für die die Daten bestimmt sind,
- c) weitere Informationen, beispielsweise betreffend
 - die Empfänger oder Kategorien der Empfänger der Daten,

- die Frage, ob die Beantwortung der Fragen obligatorisch oder freiwillig ist, sowie mögliche Folgen einer unterlassenen Beantwortung,
- das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten,

sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Artikel 11

Informationen für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden

(1) Für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden, sehen die Mitgliedstaaten vor, dass die betroffene Person bei Beginn der Speicherung der Daten bzw. im Fall einer beabsichtigten Weitergabe der Daten an Dritte spätestens bei der ersten Übermittlung vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen erhält, sofern diese ihr noch nicht vorliegen:

- a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters,
- b) Zweckbestimmungen der Verarbeitung,
- c) weitere Informationen, beispielsweise betreffend
 - die Datenkategorien, die verarbeitet werden,
 - die Empfänger oder Kategorien der Empfänger der Daten,
 - das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten,

sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

(2) Absatz 1 findet - insbesondere bei Verarbeitungen für Zwecke der Statistik oder der historischen oder wissenschaftlichen Forschung - keine Anwendung, wenn die Information der betroffenen Person unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist. In diesen Fällen sehen die Mitgliedstaaten geeignete Garantien vor.

Abschnitt V

Auskunftsrecht der betroffenen Person

Artikel 12

Auskunftsrecht

Die Mitgliedstaaten garantieren jeder betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen Folgendes zu erhalten:

- a) frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten
 - die Bestätigung, dass es Verarbeitungen sie betreffender Daten gibt oder nicht gibt, sowie zumindest Informationen über die Zweckbestimmungen dieser Verarbeitungen, die Kategorien der Daten, die Gegenstand der Verarbeitung sind, und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden;
 - eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie die verfügbaren Informationen über die Herkunft der Daten;

- Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne von Artikel 15 Absatz 1;
- b) je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieser Richtlinie entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind;
- c) die Gewähr, dass jede Berichtigung, Löschung oder Sperrung, die entsprechend Buchstabe b) durchgeführt wurde, den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist.

Abschnitt VI

Ausnahmen und Einschränkungen

Artikel 13

Ausnahmen und Einschränkungen

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Pflichten und Rechte gem. Artikel 6 Absatz 1, Artikel 10, Artikel 11 Absatz 1, Artikel 12 und Artikel 21 beschränken, sofern eine solche Beschränkung notwendig ist für

- a) die Sicherheit des Staates;
- b) die Landesverteidigung;
- c) die öffentliche Sicherheit;

- d) die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen;
- e) ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten;
- f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind;
- g) den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.

(2) Vorbehaltlich angemessener rechtlicher Garantien, mit denen insbesondere ausgeschlossen wird, dass die Daten für Maßnahmen oder Entscheidungen gegenüber bestimmten Personen verwendet werden, können die Mitgliedstaaten in Fällen, in denen offensichtlich keine Gefahr eines Eingriffs in die Privatsphäre der betroffenen Person besteht, die in Artikel 12 vorgesehenen Rechte gesetzlich einschränken, wenn die Daten ausschließlich für Zwecke der wissenschaftlichen Forschung verarbeitet werden oder personenbezogen nicht länger als erforderlich lediglich zur Herstellung von Statistiken aufbewahrt werden.

Abschnitt VII

Widerspruchsrecht der betroffenen Person

Artikel 14

Widerspruchsrecht der betroffenen Person

Die Mitgliedstaaten erkennen das Recht der betroffenen Person an,

- a) zumindest in den Fällen von Artikel 7 Buchstaben e) und f) jederzeit aus überwiegenden, schutzwürdigen, sich aus ihrer besonderen Situation ergebenden Gründen dagegen Widerspruch einlegen zu können, dass sie betreffende Daten verarbeitet werden; dies gilt nicht bei einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung. Im Fall eines berechtigten Widerspruchs kann sich die vom für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung nicht mehr auf diese Daten beziehen;
- b) auf Antrag kostenfrei gegen eine vom für die Verarbeitung Verantwortlichen beabsichtigte Verarbeitung sie betreffender Daten für Zwecke der Direktwerbung Widerspruch einzulegen oder vor der ersten Weitergabe personenbezogener Daten an Dritte oder vor deren erstmaliger Nutzung im Auftrag Dritter zu Zwecken der Direktwerbung informiert zu werden, kostenfrei gegen eine solche Weitergabe oder Nutzung Widerspruch einlegen zu können.

Die Mitgliedstaaten ergreifen die erforderlichen Maßnahmen, um sicherzustellen, dass die betroffenen Personen vom Bestehen des unter Buchstabe b) Unterabsatz 1 vorgesehenen Rechts Kenntnis haben.

Artikel 15

Automatisierte Einzeleinscheidungen

(1) Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens.

(2) Die Mitgliedstaaten sehen unbeschadet der sonstigen Bestimmungen dieser Richtlinie vor, dass eine Person einer Entscheidung nach Absatz 1 unterworfen werden kann, sofern diese

- a) im Rahmen des Abschlusses oder Erfüllung eines Vertrags ergeht und dem Ersuchen der betroffenen Person auf Abschluss oder Erfüllung des Vertrags stattgegeben wurde oder die Wahrung ihrer berechtigten Interessen durch geeignete Maßnahmen - beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen - garantiert wird oder
- b) durch ein Gesetz zugelassen ist, das Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.

Abschnitt VIII

Vertraulichkeit und Sicherheit der Verarbeitung

Artikel 16

Vertraulichkeit der Verarbeitung

Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, es bestehen gesetzliche Verpflichtungen.

Artikel 17

Sicherheit der Verarbeitung

(1) Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unbe-

rechtigten Zugang - insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden - und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

(2) Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen.

(3) Die Durchführung einer Verarbeitung im Auftrag erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere Folgendes vorgesehen ist:

- Der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen;
- die in Absatz 1 genannten Verpflichtungen gelten auch für den Auftragsverarbeiter, und zwar nach Maßgabe der Rechtsvorschriften des Mitgliedstaats, in dem er seinen Sitz hat.

(4) Zum Zwecke der Beweissicherung sind die datenschutzrelevanten Elemente des Vertrags oder Rechtsakts und die Anforderungen in Bezug auf Maßnahmen nach Absatz 1 schriftlich oder in einer anderen Form zu dokumentieren.

Abschnitt IX

Meldung

Artikel 18

Pflicht zur Meldung bei der Kontrollstelle

(1) Die Mitgliedstaaten sehen eine Meldung durch den für die Verarbeitung Verantwortlichen oder gegebenenfalls seinen Vertreter bei der in Artikel 28 genannten Kontrollstelle vor, bevor eine vollständig oder teilweise automatisierte Verarbeitung oder eine Mehrzahl von Verarbeitungen zur Realisierung einer oder mehrerer verbundener Zweckbestimmungen durchgeführt wird.

(2) Die Mitgliedstaaten können eine Vereinfachung der Meldung oder eine Ausnahme von der Meldepflicht nur in den folgenden Fällen und unter folgenden Bedingungen vorsehen:

- Sie legen für Verarbeitungskategorien, bei denen unter Berücksichtigung der zu verarbeitenden Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist, die Zweckbestimmungen der Verarbeitung, die Daten oder Kategorien der verarbeiteten Daten, die Kategorie(n) der betroffenen Personen, die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden, und die Dauer der Aufbewahrung fest und/oder
- der für die Verarbeitung Verantwortliche bestellt entsprechend dem einzelstaatlichen Recht, dem er unterliegt, einen Datenschutzbeauftragten, dem insbesondere Folgendes obliegt:
 - die unabhängige Überwachung der Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Bestimmungen,

- die Führung eines Verzeichnisses mit den in Artikel 21 Absatz 2 vorgesehenen Informationen über die durch den für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung,

um auf diese Weise sicherzustellen, dass die Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung nicht beeinträchtigt werden.

(3) Die Mitgliedstaaten können vorsehen, dass Absatz 1 keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen eines Registers ist, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht.

(4) Die Mitgliedstaaten können die in Artikel 8 Absatz 2 Buchstabe d) genannten Verarbeitungen von der Meldepflicht ausnehmen oder die Meldung vereinfachen.

(5) Die Mitgliedstaaten können die Meldepflicht für nicht automatisierte Verarbeitungen von personenbezogenen Daten generell oder in Einzelfällen vorsehen oder sie einer vereinfachten Meldung unterwerfen.

Artikel 19

Inhalt der Meldung

(1) Die Mitgliedstaaten legen fest, welche Angaben die Meldung zu enthalten hat. Hierzu gehört zumindest Folgendes:

- a) Name und Anschrift des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters;
- b) die Zweckbestimmung(en) der Verarbeitung;
- c) eine Beschreibung der Kategorie(n) der betroffenen Personen und der diesbezüglichen Daten oder Datenkategorien;

- d) die Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können;
- e) eine geplante Datenübermittlung in Drittländer;
- f) eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach Artikel 17 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

(2) Die Mitgliedstaaten legen die Verfahren fest, nach denen Änderungen der in Absatz 1 genannten Angaben der Kontrollstelle zu melden sind.

Artikel 20

Vorabkontrolle

(1) Die Mitgliedstaaten legen fest, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, und tragen dafür Sorge, dass diese Verarbeitungen vor ihrem Beginn geprüft werden.

(2) Solche Vorabprüfungen nimmt die Kontrollstelle nach Empfang der Meldung des für die Verarbeitung Verantwortlichen vor, oder sie erfolgen durch den Datenschutzbeauftragten, der im Zweifelsfall die Kontrollstelle konsultieren muss.

(3) Die Mitgliedstaaten können eine solche Prüfung auch im Zuge der Ausarbeitung einer Maßnahme ihres Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme durchführen, die die Art der Verarbeitung festlegt und geeignete Garantien vorsieht.

Artikel 21

Öffentlichkeit der Verarbeitungen

(1) Die Mitgliedstaaten erlassen Maßnahmen, mit denen die Öffentlichkeit der Verarbeitungen sichergestellt wird.

(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstelle ein Register der gem. Artikel 18 gemeldeten Verarbeitungen führt.

Das Register enthält mindestens die Angaben nach Artikel 19 Absatz 1 Buchstaben a) bis e).

Das Register kann von jedermann eingesehen werden.

(3) Die Mitgliedstaaten sehen vor, dass für Verarbeitungen, die von der Meldung ausgenommen sind, der für die Verarbeitung Verantwortliche oder eine andere von den Mitgliedstaaten benannte Stelle zumindest die in Artikel 19 Absatz 1 Buchstabe a) bis e) vorgesehenen Angaben auf Antrag jedermann in geeigneter Weise verfügbar macht.

Die Mitgliedstaaten können vorsehen, dass diese Bestimmungen keine Anwendung auf Verarbeitungen findet, deren einziger Zweck das Führen von Registern ist, die gemäß den Rechts- und Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt sind und die entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen stehen.

Kapitel III

Rechtsbehelfe, Haftung und Sanktionen

Artikel 22

Rechtsbehelfe

Unbeschadet des verwaltungsrechtlichen Beschwerdeverfahrens, das vor Beschreiten des Rechtsweges insbesondere bei der in Artikel 28 genannten Kontrollstelle eingeleitet werden kann, sehen die Mitgliedstaaten vor, dass jede Person bei der Verletzung der Rechte, die ihr durch die für die betreffende Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, bei Gericht einen Rechtsbehelf einlegen kann.

Artikel 23

Haftung

(1) Die Mitgliedstaaten sehen vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht zu vereinbarenden Handlung ein Schaden entsteht, das Recht hat, von dem für die Verarbeitung Verantwortlichen Schadenersatz zu verlangen.

(2) Der für die Verarbeitung Verantwortliche kann teilweise oder vollständig von seiner Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann.

Artikel 24

Sanktionen

Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um die volle Anwendung der Bestimmungen dieser Richtlinie sicherzustellen, und legen insbesondere die Sanktionen fest, die bei Verstößen gegen

die zur Umsetzung dieser Richtlinie erlassenen Vorschriften anzuwenden sind.

Kapitel IV

Übermittlung personenbezogener Daten in Drittländer

Artikel 25

Grundsätze

(1) Die Mitgliedstaaten sehen vor, dass die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.

(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Bestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt.

(3) Die Mitgliedstaaten und die Kommission unterrichten einander über die Fälle, in denen ihres Erachtens ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

(4) Stellt die Kommission nach dem Verfahren des Artikel 31 Absatz 2 fest, dass ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels aufweist, so treffen die Mitgliedstaaten die erforderlichen Maßnahmen, damit keine gleichartige Datenübermittlung in das Drittland erfolgt.

(5) Zum geeigneten Zeitpunkt leitet die Kommission Verhandlungen ein, um Abhilfe für die gem. Absatz 4 festgestellte Lage zu schaffen.

(6) Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen, die es insbesondere infolge der Verhandlungen gem. Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 3 gewährleistet.

Die Mitgliedstaaten treffen die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.

Artikel 26

Ausnahmen

(1) Abweichend von Artikel 25 sehen die Mitgliedstaaten vorbehaltlich entgegenstehender Regelungen für bestimmte Fälle im innerstaatlichen Recht vor, dass eine Übermittlung oder eine Kategorie von Datenübermittlungen personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, vorgenommen werden kann, sofern

- a) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat oder
- b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist oder
- c) die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll, oder

- d) die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist oder
- e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist oder
- f) die Übermittlung aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

(2) Unbeschadet des Absatzes 1 kann ein Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland genehmigen, das kein angemessenes Schutzniveau im Sinne des Artikel 25 Absatz 2 gewährleistet, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben.

(3) Der Mitgliedstaat unterrichtet die Kommission und die anderen Mitgliedstaaten über die von ihm nach Absatz 2 erteilten Genehmigungen.

Legt ein anderer Mitgliedstaat oder die Kommission einen in Bezug auf den Schutz der Privatsphäre, der Grundrechte und der Person hinreichend begründeten Widerspruch ein, so erlässt die Kommission die geeigneten Maßnahmen nach dem Verfahren des Artikel 31 Absatz 2.

Die Mitgliedstaaten treffen die aufgrund des Beschlusses der Kommission gebotenen Maßnahmen.

(4) Befindet die Kommission nach dem Verfahren des Artikels 31 Absatz 2, dass bestimmte Standardvertragsklauseln ausreichende Garantien gem. Absatz 2 bieten, so treffen die Mitgliedstaaten die aufgrund der Feststellung der Kommission gebotenen Maßnahmen.

Kapitel V

Verhaltensregeln

Artikel 27

(1) Die Mitgliedstaaten und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen, die die Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassen.

(2) Die Mitgliedstaaten sehen vor, dass die Berufsverbände und andere Vereinigungen, die andere Kategorien von für die Verarbeitung Verantwortlichen vertreten, ihre Entwürfe für einzelstaatliche Verhaltensregeln oder ihre Vorschläge zur Änderung oder Verlängerung bestehender einzelstaatlicher Verhaltensregeln der zuständigen einzelstaatlichen Stelle unterbreiten können.

Die Mitgliedstaaten sehen vor, dass sich diese Stellen insbesondere davon überzeugt, dass die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Sie holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint.

(3) Die Entwürfe für gemeinschaftliche Verhaltensregeln sowie Änderungen oder Verlängerungen bestehender gemeinschaftlicher Verhaltensregeln können der in Artikel 29 genannten Gruppe unterbreitet werden. Die Gruppe nimmt insbesondere dazu Stellung, ob die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richt-

linie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Sie holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint. Die Kommission kann dafür Sorge tragen, dass die Verhaltensregeln, zu denen die Gruppe eine positive Stellungnahme abgegeben hat, in geeigneter Weise veröffentlicht werden.

Kapitel VI

Kontrollstelle und Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten

Artikel 28

Kontrollstelle

(1) Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen.

Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.

(3) Jede Kontrollstelle verfügt insbesondere über:

- Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;
- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der

Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;

- das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.

Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.

(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.

Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gem. Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, dass eine Überprüfung stattgefunden hat.

(5) Jede Kontrollstelle legt regelmäßig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.

(6) Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gem. Absatz 3 übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden.

Die Kontrollstellen sorgen für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen.

(7) Die Mitgliedstaaten sehen vor, dass die Mitglieder und Bediensteten der Kontrollstellen hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach Ausscheiden aus dem Dienst, unterliegen.

Artikel 29

Datenschutzgruppe

(1) Es wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt (nachstehend „Gruppe“ genannt).

Die Gruppe ist unabhängig und hat beratende Funktion.

(2) Die Gruppe besteht aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen und einem Vertreter der Stelle bzw. der Stellen, die für die Institutionen und Organe der Gemeinschaft eingerichtet sind, sowie einem Vertreter der Kommission.

Jedes Mitglied der Gruppe wird von der Institution, der Stelle oder den Stellen, die es vertritt, benannt. Hat ein Mitgliedstaat mehrere Kontrollstellen bestimmt, so ernennen diese einen gemeinsamen Vertreter. Gleiches gilt für die Stellen, die für die Institutionen und die Organe der Gemeinschaft eingerichtet sind.

(3) Die Gruppe beschließt mit der einfachen Mehrheit der Vertreter der Kontrollstellen.

(4) Die Gruppe wählt ihren Vorsitzenden. Die Dauer der Amtszeit des Vorsitzenden beträgt zwei Jahre. Wiederwahl ist möglich.

(5) Die Sekretariatsgeschäfte der Gruppe werden von der Kommission wahrgenommen.

(6) Die Gruppe gibt sich eine Geschäftsordnung.

(7) Die Gruppe prüft die Fragen, die der Vorsitzende von sich aus oder auf Antrag eines Vertreters der Kontrollstellen oder auf Antrag der Kommission auf die Tagesordnung gesetzt hat.

Artikel 30

(1) Die Gruppe hat die Aufgabe,

- a) alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen;
- b) zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen;
- c) die Kommission bei jeder Vorlage zur Änderung dieser Richtlinie, zu allen Entwürfen zusätzlicher oder spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zu allen anderen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken;
- d) Stellungnahmen zu den auf Gemeinschaftsebene erarbeiteten Verhaltensregeln abzugeben.

(2) Stellt die Gruppe fest, dass sich im Bereich des Schutzes von Personen bei der Verarbeitung personenbezogener Daten zwischen den Rechtsvorschriften oder der Praxis der Mitgliedstaaten Unterschiede ergeben, die die Gleichwertigkeit des Schutzes in der Gemeinschaft beeinträchtigen können, so teilt sie dies der Kommission mit.

(3) Die Gruppe kann von sich aus Empfehlungen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen.

(4) Die Stellungnahmen und Empfehlungen der Gruppe werden der Kommission und dem in Artikel 31 genannten Ausschuss übermittelt.

(5) Die Kommission teilt der Gruppe mit, welche Konsequenzen sie aus den Stellungnahmen und Empfehlungen gezogen hat. Sie erstellt hierzu einen Bericht, der auch dem Europäischen Parlament und dem Rat übermittelt wird. Dieser Bericht wird veröffentlicht.

(6) Die Gruppe erstellt jährlich einen Bericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und in Drittländern, den sie der Kommission, dem Europäischen Parlament und dem Rat übermittelt. Dieser Bericht wird veröffentlicht.

Kapitel VII

Gemeinschaftliche Durchführungsmaßnahmen

Artikel 31

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und in dem der Vertreter der Kommission den Vorsitz führt.

(2) Der Vertreter der Kommission unterbreitet dem Ausschuss einen Entwurf der zu treffenden Maßnahmen. Der Ausschuss gibt seine Stellungnahme zu diesem Entwurf innerhalb einer Frist ab, die der Vorsitzende unter Berücksichtigung der Dringlichkeit der betreffenden Frage festsetzen kann.

Die Stellungnahme wird mit der Mehrheit abgegeben, die in Artikel 148 Absatz 2 des Vertrags vorgesehen ist. Bei der Abstimmung im Ausschuss werden die Stimmen der Vertreter der Mitgliedstaaten gemäß dem vorgenannten Artikel gewogen. Der Vorsitzende nimmt an der Abstimmung nicht teil.

Die Kommission erlässt Maßnahmen, die unmittelbar gelten. Stimmt sie jedoch mit der Stellungnahme des Ausschusses nicht überein, werden sie von der Kommission unverzüglich dem Rat mitgeteilt. In diesem Fall gilt Folgendes:

- Die Kommission verschiebt die Durchführung der von ihr beschlossenen Maßnahmen um drei Monate vom Zeitpunkt der Mitteilung an;
- der Rat kann innerhalb des im ersten Gedankenstrich genannten Zeitraums mit qualifizierter Mehrheit einen anders lautenden Beschluss fassen.

Schlussbestimmungen

Artikel 32

(1) Die Mitgliedstaaten erlassen die erforderlichen Rechts- und Verwaltungsvorschriften, um dieser Richtlinie binnen drei Jahren nach ihrer Annahme nachzukommen.

Wenn die Mitgliedstaaten derartige Vorschriften erlassen, nehmen sie in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten der Bezugnahme.

(2) Die Mitgliedstaaten tragen dafür Sorge, dass Verarbeitungen, die zum Zeitpunkt des Inkrafttretens der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie bereits begonnen wurden, binnen drei Jahren nach diesem Zeitpunkt mit diesen Bestimmungen in Einklang gebracht werden.

Abweichend von Unterabsatz 1 können die Mitgliedstaaten vorsehen, dass die Verarbeitungen von Daten, die zum Zeitpunkt des Inkrafttretens der einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie bereits in manuellen Dateien enthalten sind, binnen zwölf Jahren nach Annahme dieser Richtlinie mit den Artikeln 6, 7 und 8 in Einklang zu bringen sind. Die Mitgliedstaaten gestatten jedoch, dass die betroffene Person auf Antrag und insbesondere bei Ausübung des Zugangsrechts die Berichtigung, Löschung oder Sperrung von Daten erreichen kann, die unvollständig, unzutreffend oder auf eine Art und Weise aufbewahrt sind, die mit den vom für die Verarbeitung Verantwortlichen verfolgten rechtmäßigen Zwecken unvereinbar ist.

(3) Abweichend von Absatz 2 können die Mitgliedstaaten vorbehaltlich geeigneter Garantien vorsehen, dass Daten, die ausschließlich zum Zwecke der historischen Forschung aufbewahrt werden, nicht mit den Artikeln 6, 7 und 8 in Einklang gebracht werden müssen.

(4) Die Mitgliedstaaten teilen der Kommission den Wortlaut der innerstaatlichen Vorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 33

Die Kommission legt dem Europäischen Parlament und dem Rat regelmäßig, und zwar erstmals drei Jahre nach dem in Artikel 32 Absatz 1 genannten Zeitpunkt, einen Bericht über die Durchführung dieser Richtlinie vor und fügt ihm gegebenenfalls geeignete Änderungsvorschläge bei. Dieser Bericht wird veröffentlicht.

Die Kommission prüft insbesondere die Anwendung dieser Richtlinie auf die Verarbeitung personenbezogener Bild- und Tondaten und unterbreitet geeignete Vorschläge, die sich unter Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen könnten.

Artikel 34

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Luxemburg am 24. Oktober 1995.

Im Namen des Europäischen
Parlaments

Der Präsident

K. Hänsch

Im Namen des Rates

Der Präsident

L. Atienza Serna

Anlage 23

Hinweise zum Umgang mit personenbezogenen Daten im Rahmen von Behördenumzügen

Umzugsrichtlinien

Bei einem Umzug ist der Transport von personenbezogenen Daten (Akten als auch maschinelle Datenträger) sicherheitstechnisch als kritisch zu bewerten und stellt eine erhebliche Gefährdung der Daten hinsichtlich ihrer Verfügbarkeit, Vertraulichkeit und Integrität dar. Die Daten verlassen bis zum Eintreffen am Zielort nicht nur für eine gewisse Zeit ihren Sicherheitsbereich, sondern befinden sich während des Transports auch in einem für gewöhnlich sehr schwach gesicherten Zustand. Obendrein wird das Umzugsgut für den Transport mitunter auch Personal übergeben, das im Rahmen der normalen Verarbeitung keinerlei Zugriffsrechte hätte. Aus den genannten Gründen sollte das gesamte Umzugsverfahren einer Behörde besonderen Restriktionen unterworfen werden, mit dem Ziel, dass während des Umzugs keine unbefugte Kenntnisnahme von personenbezogenen Daten erfolgen kann und der Transport selbst so abläuft, dass eine Beeinträchtigung der Datenträger und ein Datenverlust verhindert wird.

Geeignete Maßnahmen und Verfahrensschritte für einen erfolgreichen störungsfreien und nachvollziehbaren Transport sind unter anderem:

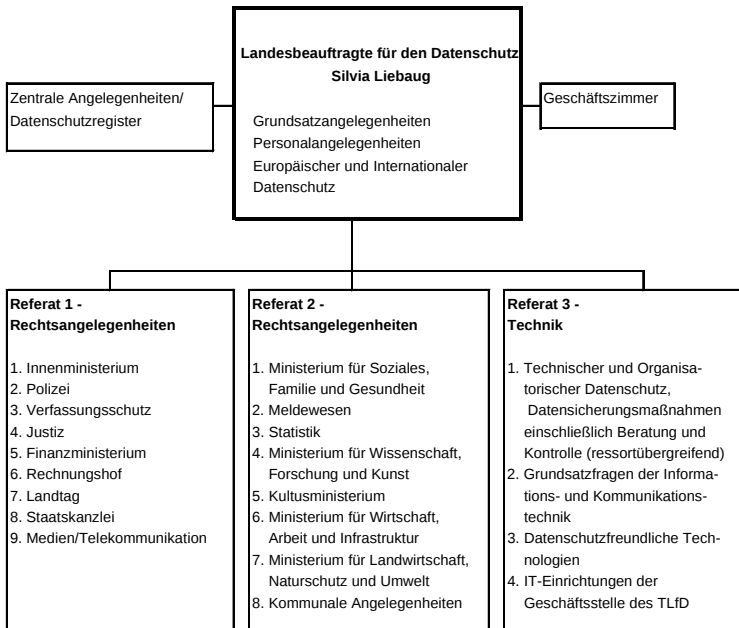
- Ausgehend von konkreten Festlegungen wer, was, wann, wie und wohin umzieht, sollten weitere konkrete Zuständigkeiten und Verantwortlichkeiten sowie Kontrollzuständigkeiten, einschließlich Berichtspflichten an die Behördenleitung, sichergestellt sein. Bereits in die Umzugsvorbereitung sollten beispielsweise auch der behördliche Datenschutzbeauftragte und der Geheimschutzbeauftragte mit einbezogen werden.
- Entsprechend der Sensibilität der personenbezogenen Daten oder des zu beachtenden Geheimhaltungsgrades der zu transportierenden Daten sind die konkreten Transportbedingungen und der Einsatz der zu verwendenden Transportbehältnisse festzulegen.

- Transportpapiere bzw. Transportbegleitscheine sollten ausgegeben werden, wo beispielsweise Datum, Uhrzeit des Verlassens des Datenmaterials im ehemaligen Behördenstandort, Bezeichnung und Umfang des Datenmaterials, des Transportverantwortlichen, einschließlich eines Kenntnisvermerkes des Vorgesetzten oder Umzugsverantwortlichen aufgenommen werden sollten.
- Nach erfolgtem Transport sollte zum Zwecke der Vollständigkeitsprüfung ebenfalls wieder Datum, Uhrzeit und Name des Mitarbeiters quittiert werden, der die Entgegennahme vornimmt.
- Das Transportgut, die Transportbehältnisse, PC-Technik etc. sollten speziell in Vorbereitung und Durchführung des Transports eindeutig gekennzeichnet sein. Die Kennzeichnung muss dabei so erfolgen, dass sie nicht beliebig entfernt, wiedergebracht, vertauscht oder vernichtet werden kann.
- Auch während eines Umzugs sollten die behördlichen Dienstweisungen und sonstigen Festlegungen im Zusammenhang mit Datensicherungsmaßnahmen durchgängig Gültigkeit haben bzw., entsprechend der besonderen Bedingungen (Zutrittsmöglichkeit Transportpersonal etc.), noch entsprechend vorübergehend ergänzt bzw. angepasst werden. Das betrifft z. B. die bestehende Haus- und Schlüsselordnung der Behörde, Wachdienstverstärkung und andere zusätzliche Kontrollmaßnahmen während des gesamten Umzugsverfahrens.
- Die erforderlichen Datensicherungsmaßnahmen haben sich sowohl an der Schutzwürdigkeit der Daten als auch an den konkreten Umständen der Art und Weise des vorzunehmenden Transports abzuleiten (z. B. Transport durch eigenes Personal oder Transportfirma). Bezüglich der vorzunehmenden Datensicherungsmaßnahmen sollten Mindestanforderungen vorgegeben werden, um nicht ausschließlich dem Mitarbeiter dies selbst zu überlassen.
- Grundsätzlich sollte vor dem Transport von den Daten der Rechner-Festplatte eine aktuelle Sicherungskopie vorliegen, um die Verfügbarkeit der Daten zu gewährleisten.
- Vor dem beabsichtigten Transport sind eventuelle Löschverpflichtungen zu realisieren. Dabei sind die Datenträger auch auf Restinformationen und eine verdeckte Datenspeicherung zu überprüfen.

- Der Transport von besonders schützenswerten Daten auf maschinellen Datenträgern sollte nur in verschlüsselter Form oder/und unter zuverlässiger Transportbegleitung erfolgen. Ist ein Einsatz von Verschlüsselungssoftware nicht möglich, sollten nach Erstellen der Sicherungskopie diese schutzwürdigen Daten auf dem Rechner vor dessen Transport physisch gelöscht werden.

Anlage 24

Thüringer Landesbeauftragter für den Datenschutz (TLfD)



Anschrift	Postanschrift
Johann-Sebastian-Bach-Str. 1 99096 Erfurt	PF 941 99019 Erfurt
Tel. 0361/ 3771900 Fax 0361/ 3771904 E-Mail: poststelle@datenschutz.thueringen.de	

Sachregister

Abgabenordnung	1/9.1.8; 2/9.1, 9.8; 3/5.2.6, 9.1, 9.3, 9.7, 9.11, 9.14
Abgeordneter	2/3.3; 3/3.1, 5.1.10, 5.2.7, 5.2.8, 9.15
Abgleich von Fingerabdrücken	2/7.6
Abrufdienst	2/4.4; 3/9.4
Abrufverfahren	1/5.2.3, 5.3.1, 10.5, 11.1.1; 2/4.1, 5.2.2, 11.29; 3/9.7
Adressbücher	1/5.2.4.7, 15.3; 2/5.2.4; 3/4.1, 5.2.1
Adressdaten	2/11.19; 3/5.1.9, 5.2.6, 5.2.11, 5.3.2, 13.4, 14.8
Adressenfeststellungsverfahren	2/9.5
Adressmittlungsverfahren	3/13.4
Akteneinsicht	1/8.1,10.4; 2/9.2; 3/5.1.7, 10.1, 10.18, 11.6
Akustische Wohnraumüberwachung	2/10.8; 3/10.4
Altdateien	1/2.3, 5.2.2, 6.1.6, 6.1.9, 6.1.10, 7.2, 10.2, 10.3, 10.11.1, 11.3.1, 11.3.2; 2/5.2.3, 5.2.9, 14.14; 3/11.12
Amtsarzt	1/11.3.3; 2/5.2.11; 3/11.12
Analyse	2/7.3; 3/2.3
Anhörungsbogen	1/7.5.1; 2/7.10, 14.9; 3/5.2.5, 7.17, 14.13
Anlagen- und Verfahrensverzeichnis	2/15.4; 3/6.3, 11.8, 11.14, 11.15, 14.5, 14.13, 15.13
Anonymisierung	1/7.3, 11.3.5, 11.5, 11.6, 12.3, 12.5, 13.1.2, 13.1.7, 13.3.1, 15.15.1; 2/11.4, 13.9, 15.6; 3/4.1, 11.14, 11.16, 13.8, 15.8, 15.11, 15.13, 15.15
Antragsformular	1/11.9.3, 14.1.2, 14.3.2, 14.3.5; 2/5.2.6; 3/5.2.9, 5.2.10, 11.16, 12.2, 14.3, 14.4, 14.5
Antragsverfahren	2/11.28

Anweisung für das Straf- und Bußgeldverfahren (Steuer)	2/9.5
Arbeitsdatei	2/7.3
Architektenliste	2/14.1
Archivierung	1/7.2, 10.11.1, 13.4, 13.4.2, 13.4.3; 2/5.2.9, 11.9, 11.10, 13.6, 13.10; 3/5.1.10
Asylbewerber	2/5.1.6; 3/11.3
Asylcard	1/5.3.2; 2/5.1.1; 3/5.1.3, 15.14
Asylverfahrensgesetz	3/11.3
Asymmetrische Verschlüsselung	2/15.7; 3/15.6.4
Aufbewahrung	1/6.1.9, 11.3.1, 11.3.2; 2/5.1.8, 5.2.9, 10.17, 11.9; 3/5.1.10, 6.2, 7.3, 10.11, 10.18, 10.20, 11.12
Aufenthaltserlaubnis	2/5.1.5
Aufnahmeformular	2/11.5
Auftragsdatenverarbeitung	1/ 2.5, 5.2.3, 6.1.10, 9.2.7, 14.4.2, 15.9, 15.4.5; 2/5.2.8, 11.10, 11.17, 11.19, 11.29; 3/5.1.5, 6.4, 7.5, 7.13, 9.11, 11.12, 11.15, 11.17, 11.22, 15.4, 15.6.4, 15.8, 15.13
Ausbildungsverkehr	2/14.11
Auskunftserteilung	1/1.1.6, 6.3.2, 9.1.6, 9.2.3; 2/5.1.8; 3/5.1.7, 5.2.4, 5.2.12, 9.6, 10.21, 11.20, 14.12
Auskunftspflicht	2/11.3; 3/8.2, 12.4
Auskunftssperre	3/5.2.4
Ausländer	2/5.1.2; 3/5.1.4, 5.1.5, 5.1.6, 5.1.7, 5.11
Ausländerbehörde	1/5.3.1; 2/5.1.6, 5.2.7; 3/5.1.4, 5.1.5, 5.1.7
Ausländergesetz	2/5.1.2, 5.1.7; 3/5.1.1
Ausländerzentralregister	1/1.2.3, 5.3.1; 2/5.1.2, 7.6; 3/5.1.5
Authentifikation/Authentizität	3/5.1.8, 9.2, 11.7, 14.7, 15.6, 15.13, 15.14, 15.15

automatisierte Verfahren	2/9.4, 10.11, 10.11.3, 10.12; 3/5.1.5, 10.7, 10.16, 10.17, 10.22, 15.4, 15.6, 15.8
Beanstandung	1/1.1.3, 2.1, 2.3, 2.4, 5.1.2, 5.1.3.1, 5.2.2, 5.2.4.5, 6.1.10, 6.1.11; 2/1., 1.1, 1.2, 5.1.9, 5.2.3, 5.2.4, 5.2.9, 5.2.12, 5.2.16, 5.2.18, 6.4, 6.5, 7.6, 7.8, 8.1, 9.3, 9.4 9.5, 10.12, 10.18, 10.19, 11.19, 14.11, 15.4; 3/1.1, 5.2.2, 5.2.6, 5.2.7, 5.2.9, 6.3, 7.10, 7.12, 7.14, 7.15, 10.13, 11.11, 11.12, 11.14, 11.15, 12.3, 14.5, 14.13, 15.6.3, 15.6.4
Bedrohungs- und Risikoanalyse	2/10.5; 3/15.3, 15.4, 15.5
behördeninterner Datenschutzbeauf- tragter	2/5.1.9; 3/11.8, 11.22
Beihilfearbeitung	3/6.4
Beirat beim TLfD	3/1.2
Bekennnisfreiheit	1/11.3.4; 2/11.7
belegungsgebundener Wohnraum	2/14.14
Berufsrecht der Rechtsanwälte	3/2.6
Beschlagnahmeschutz	2/5.2.9; 3/2.6, 11.7, 11.12
Besucherdaten	2/10.17; 3/10.19
Betretungsverbot	2/7.8
Bewerbungen	3/6.1, 6.2, 6.8
Bild-Ton-Aufzeichnung	2/7.12, 10.7; 3/5.2.8
Biometrische Verfahren	3/15.13, 15.14
Biotopkartierung	2/14.20
Bodenbewertungsverfahren	2/9.4
Briefzustellung	3/9.8
Browser	2/15.13
Bundesgrenzschutzgesetz	3/7.1
Bundeskriminalamt, -Gesetz	1/1.2.3, 7.6; 2/7.3, 7.5; 3/7.5

Bundeszentralregister	1/5.2.6.2, 10.5, 10.8, 10.9, 13.2.2, 14.1.5, 14.2.3; 2/10.6, 11.14, 11.27; 3/10.13, 11.5,
CD-ROM	1/5.2.4.7, 15.11, 15.14.5; 2/4.1
Chipkarte	1/5.3.2, 11.10, 15.1, 15.10; 2/11.13, 14.18, 15.9; 3/13.5, 15.14
Container-Lösung	2/5.2.9, 11.10
Cookies	2/15.13
Corporate Network	1/15.5.1; 2/4.1, 4.2, 15.2; 3/4.4, 15.3, 15.4, 15.5, 15.12
Datenaustausch	2/11.2, 15.4; 3/5.1.5, 9.2, 11.23, 11.24, 14.5, 15.6.4
Datenerhebung	1/6.1.2, 11.5, 11.9.3, 12.5, 12.6; 2/8.2; 3/5.2.3, 5.2.5, 5.2.9, 5.2.10, 6.5, 7.3, 7.4, 7.6, 7.9, 7.16, 9.10, 12.4, 13.1, 13.3, 14.3, 14.10, 14.11
Datennetze	2/11.13; 3/11.1, 11.7
Datenschutz-Audit	2/4.4, 4.5; 3/4.1, 15.15
Datenschutzfreundliche Technologien	2/15.6; 3/15.1, 15.10, 15.14
Datenschutzklausel	2/11.25
Datenschutzregistrierung	1/1.1.6, 2.1, 2.3, 10.16, 15.2; 2/1.2, 9.3, 9.4, 13.10; 3/5.1.5, 5.1.8, 6.3, 7.15, 15.6.2, 15.8
Datensicherheit	1/7.7, 10.5, 15.2, 15.3; 2/4.4; 3/6.3, 7.14, 10.7, 10.16, 11.22, 14.7, 15.5, 15.13, 15.15
Datensparsamkeit	2/4.3, 15.6; 3/4.1, 13.8, 15.10, 15.13, 15.14, 15.15
Datenspeicher Wohnungspolitik	2/14.14
Datenträgerentsorgung	2/15.4; 3/12.3, 15.13
Datenträgervereinbarung	2/11.18

Datenübermittlung	1/4.3, 5.2.3, 5.2.4.2, 5.3.3, 6.1.15, 7.4, 8.3, 9.1.3, 9.2.1, 9.2.2, 10.1, 10.7, 13.2.1, 14.3.6; 2/5.1.3, 5.1.4, 9.5, 10.9, 10.10, 10.14, 10.15, 10.16, 10.20, 10.21, 14.16; 3/3.1, 4.6, 5.2.6, 5.2.7, 5.3.3, 6.3, 6.4, 7.2, 9.9, 9.10, 10.9, 10.12, 10.21, 10.22, 11.2, 11.3, 11.14, 14.1, 14.6, 14.8, 14.9, 14.10, 15.7, 15.8, 15.9, 15.13
Diensteanbieter	2/4.3
Digitale Signatur	2/15.7, 15.8, 15.12; 3/2.7, 9.3, 11.7, 15.3, 15.5, 15.9, 15.13, 15.14
DNA-Analyse	2/10.4; 3/10.8
EG-Datenschutzrichtlinie	1/4.1; 2/2.; 3/2.1, 9.1, 15.15
EG-Führerscheinrichtlinie	1/14.2.1; 2/14.7; 3/14.4
EG-Telekommunikationsdatenschutz-richtlinie	3/2.4
Ehescheidungsverbundurteile	1/10.12; 2/10.11
Eingliederungshilfe	2/11.28
Einkommensnachweis	2/5.2.14; 3/11.8
Einmessungsverfahren	2/14.16
Einreisesperre	3/5.1.4
Einsichtsrecht	1/1., 6.1.4, 8.4, 9.1.6, 10.11.1, 13.2.2, 14.1.3; 2/9.9, 10.17, 10.18, 11.12; 3/11.10

Einwilligung	1/6.1.5, 6.1.7, 10.11.3, 11.2.6, 11.10, 13.3, 13.3.1, 14.1.2, 14.1.4, 14.3.5, 14.3.6; 2/5.1.4, 5.2.4, 5.2.12, 10.9, 10.14, 10.15, 11.15, 11.16, 11.26; 3/3.2, 4.1, 4.6, 5.1.3, 5.2.1, 5.2.2, 5.3.2, 5.3.3, 9.9, 10.8, 10.9, 10.12, 11.1, 11.6, 11.7, 11.13, 11.21, 15.13
Einzelangaben	2/12.2; 3/13.8
elektronische Geldbörse	3/15.11
elektronischer Fingerabdruck	2/7.5; 3/5.1.3, 15.14
E-Mail	3/4.4, 15.7
Emissionskataster	2/14.19
ENFOPOL	3/2.5
Erhebungsbogen	2/5.2.12, 13.3, 14.17; 3/12.2, 14.3
Errichtungsanordnung	1/1.2.5, 7.1, 7.4, 7.6, 10.5; 2/7.6, 10.5; 3/5.5, 7.5, 7.6
Europäische Datenbank über gerichtliche Verfahren	2/10.9
Europäischer Datenschutz	2/2.; 3/2.2, 2.6, 9.1
Europol	1/7.9; 2/7.3; 3/2.3
Fahndung	1/4.3; 2/7.6, 10.3; 3/7.7
Fahrerfoto	2/7.10; 3/7.16
Fahrtenbuch	2/9.6; 3/9.14
Fangschaltung	3/4.3
Fax-PC	2/15.12
Fehlbelegung in Krankenhäusern	2/11.23
Fernmeldegeheimnis	2/4.1; 3/2.5, 10.5
Fernwartung	2/15.10; 3/15.6.4
Finddateien	2/13.10; 3/11.12
FISCUS	3/9.2, 9.5
Forschung	1/1.1.5, 5.2.4.8, 13.1.2, 13.3.1, 13.3.3; 2/11.9, 13.4, 13.7, 13.8, 13.9

Freigabe automatisierter Verfahren	1/6.1.11, 7.7, 15.7.3; 2/1.2, 9.3, 9.4, 10.18; 3/5.1.5, 6.3, 7.15, 11.14, 11.15, 14.13, 15.6, 15.6.4, 15.8, 15.13, 15.15
Führerschein	1/14.2.4; 2/14.8, 14.9; 3/7.2, 14.4, 14.5
Führungszeugnis	2/11.14; 3/11.5, 14.5
Fußfessel	3/10.10
Gebäuderegister	2/12.2
Gebrauchtwarenhandel	2/14.2
Geburtsurkunde	2/5.2.5
Gefahrenabwehr	2/7.1, 7.12
Gefahrstoffdatenbank	2/13.9
Gehaltspfändungen	3/6.6
Geldauflagen	2/10.15; 3/10.12
Gemeinderat	2/5.2.16, 5.2.17; 3/5.1.10, 5.2.7, 5.2.8
Gemeinsame Kontrollinstanz	2/7.4; 3/2.3, 5.1.4
Generierung	2/15.10
Genetischer Fingerabdruck	2/10.4; 3/10.8
Gerichte	3/10.7, 10.8, 10.16
Geschäftsordnung, Landtag	3/3.3
Gesundheitsamt	2/5.2.11; 3/11.3, 11.12
Gesundheitsreform	3/11.1
Gewerbeanzeige	2/14.6; 3/5.2.6
Gewerbebehörde	2/14.3; 3/5.2.6, 5.2.12
Großer Lauschangriff	2/10.8; 3/10.4
Grundbuchamt	1/10.13; 2/10.12
Grundstücksdaten	2/5.2.17; 3/5.1.8, 14.10, 14.11
GSM-Netze	2/15.1; 3/15.1
Gutachten	2/11.22; 3/11.13
Handelsregisterdaten	2/14.1, 14.2, 14.5
Handwerkskammer	3/14.1, 14.2
Hausordnungen	2/14.13
Health Professional Card	2/11.13

Hochschule	2/7.12, 13.4, 13.5, 13.6; 3/13.5, 13.6
ICD-10-Code	2/11.18; 3/11.19
Identifikation	3/15.6, 15.10, 15.14
Identitätsfeststellung	3/7.1, 10.8, 10.19, 11.20, 15.14
Immunität	2/3.3
Industrie- und Handelskammer	1/14.1.2, 14.1.3, 14.1.4; 2/14.5; 3/14.1, 14.2
Informationsanspruch des Abgeordneten	2/3.2; 3/3.2
Informations- und Kommunikationsdienste-Gesetz	2/4.3, 15.8; 3/2.7, 15.8, 15.13
INPOL	2/7.6, 7.7; 3/7.5, 10.13
Insolvenzverfahren	3/10.3
Integriertes Automatisches Besteuerungsverfahren	2/9.4; 3/9.5, 9.7, 15.6.4
International Data Encryption Algorithm	2/15.7
Internationaler Datenschutz	2/2.
Internet	1/15.1, 15.13; 2/14.5; 3/4.4, 4.6, 7.7, 9.3, 13.6, 14.7, 15.1, 15.3, 15.5, 15.8, 15.10, 15.13
Intranet	2/15.2; 3/15.3, 15.5, 15.13
IT-Maßnahmenregelung	2/15.3; 3/15.6.3
IT-Ressortplan	1/15.4; 2/15.3
IT-Richtlinien	2/15.3
Jahr 2000-Problem	3/15.12
Jugendamt	2/5.2.12, 5.2.13; 3/7.8
Jugendgerichtshilfe	2/13.7
Jugendgesundheitsdienst	2/5.2.10
jugendschutz.net	3/4.2
Justizmitteilungsgesetz	1/10.1; 2/10.1; 3/3.1, 10.2, 10.11
Justizvollzugsanstalt	1/6.1.12, 10.11, 11.3.2; 2/10.11.3, 10.17; 3/10.19

Kartierung	2/14.20
Kassenärztliche Bundesvereinigung	2/11.18
Kassenärztliche Vereinigung	2/11.14, 11.15; 3/11.14
Kassenarztverzeichnis	2/11.15
Katasteramt	2/14.16; 3/5.1.8
Kettenbriefe	3/5.1.9
Kindertageseinrichtungen	1/5.1.3.3, 5.2.4.2, 11.9.3; 2/5.2.15
Kindertagesstättenbeitrag	2/5.2.14
Kommunalstatistik	2/12.2; 3/12.4
Kontrollkompetenz	1/5.1.2, 5.4.1, 7.9, 9.3, 11.1.1; 2/10.12; 3/10.7, 11.17
Kontrolltätigkeit	2/14.21; 3/5.1.5, 5.1.8, 5.2.12, 6.3, 6.8, 6.9, 7.1, 7.10, 7.12, 7.14, 7.15, 7.16, 7.17, 8.1, 9.7, 9.9, 9.13, 10.4, 10.13, 11.8, 11.10, 11.11, 11.12, 11.14, 11.15, 11.22, 12.2, 12.3; 14.5, 14.11, 14.13, 15.6.1, 15.6.2, 15.6.3, 15.6.4, 15.6.5
Kostenübernahme	2/5.1.7
Krankenakte	2/11.10, 11.11, 11.12; 3/11.10, 11.11
Krankenhaus	1/1.1.5, 11.2.5, 11.3.4, 13.3.1; 2/11.5, 11.6, 11.7, 11.9, 11.22, 11.23; 3/5.2.10, 11.13
Krankenkasse	1/11.2, 11.2.4, 11.2.5; 2/5.2.12, 11.17, 11.20, 11.22, 11.24, 14.6; 3/11.14, 11.18
Krankenversichertenkarte	3/11.18
Krebsregistergesetz	1/1.2.2, 13.3.2; 2/13.8
Kriminalaktennachweis	2/7.6; 3/10.8
Kriminalpolizeiliche Angelegenheiten	2/7.1
Kriminalstatistik	2/7.6
Kryptographie	2/15.7, 15.8; 3/15.9
Kurbeitrag	2/5.2.1

LaDiVA	3/5.1.5
Landesärztekammer	3/11.8
Landesaufnahmestelle für Aussiedler (LAST)	2/5.1.8
Landesbank Hessen-Thüringen	1/5.4.1; 2/5.3; 3/5.3.1
Landeshaushaltsordnung	2/9.9
Landestierärztekammer	2/11.16
Landwirtschaft	2/14.21; 3/14.12
Lebenslauf	2/13.5
Leistungsmissbrauch	2/11.2; 3/11.23
Lichtbilddatei	2/7.11
Liegenschaftskataster	2/14.17; 3/14.10
Lohnsteuerkarte	1/9.1.1, 9.1.2; 2/9.7; 3/9.11
Löschung	1/14.2.3, 15.2, 15.9, 15.11, 15.14.2; 2/7.7, 11.18; 3/2.3, 5.1.4, 5.1.10, 5.2.8, 6.10, 10.1, 10.13, 10.18, 15.8, 15.12, 15.13
Lügendetektor	3/10.6
Machbarkeitsstudie	2/5.1.1; 3/5.1.3
Mediendienste	2/4.4, 4.6; 3/4.2
Medienforschung	2/4.5
Medizinischer Dienst	1/11.2.4, 11.2.6; 2/11.22, 11.23; 3/11.13, 11.21
Mehrländer-Gerichts-Anwendung (MEGA)	2/10.11
Meldebehörden	1/1.1.1, 1.2.1, 5.2, 9.1.2, 9.1.4; 2/5.2.3
Meldebogen	2/11.16
Meldedaten	1/5.2; 2/5.2.1, 5.2.2, 5.2.4, 14.18; 3/4.1, 4.5, 5.2.1, 5.2.2, 5.2.4, 5.2.5, 7.16, 10.13, 14.10, 14.11, 14.13
Meldekarteien	1/5.2.2; 2/5.2.3
Melderegisterauskünfte	1/5.2.3, 5.2.4; 2/5.2.4; 3/4.1, 5.2.1; 5.2.2, 5.2.4, 14.10, 14.11

Mietschuldner	2/14.12
Mietspiegel	2/14.15
Mikroverfilmung	2/11.10; 3/11.12
Mitgliederwerbung	1/11.2.1; 2/11.20; 3/11.18
Mitgliedstaat	2/7.3
Mitnutzer	2/4.5
Mitteilungen:	
- in Strafsachen	2/10.1, 10.16; 3/10.2, 10.14
- in Zivilsachen	2/10.1; 3/10.2
- zum Wählerverzeichnis	2/10.16
Mitteilungsverordnung	2/9.8
Modellversuch	3/5.1.3, 10.10, 11.14
MPU-Gutachten	1/14.2.5; 2/14.9; 3/14.4, 14.5
Müllgebühren	2/14.18; 3/14.11
Namenslisten	2/5.2.15; 3/14.9
Namensschilder an Haftraumtüren	2/10.17
Naturschutz	2/14.20
Netzcomputer	2/15.1
nicht-öffentliche Sitzung	2/3.1, 5.2.16, 5.2.17; 3/5.2.7, 5.2.8
Notare	3/10.20
Notarielle Urkunde	2/10.20
Notarzteinsatzprotokoll	1/11.7; 2/11.21
Novellierung Datenschutzgesetze	3/15.15
Nutzungsprofil	2/4.3; 3/15.1, 15.8, 15.10, 15.11
Öffentliche Sitzung	3/14.8
Öffentlichkeitsarbeit	2/1.1
Online-Zugriff	2/5.2.2; 3/5.1.5, 11.22, 15.10
Ordnungswidrigkeiten	1/7.5, 14.2.2; 2/14.9; 3/7.2, 7.4
Organisierte Kriminalität	2/10.8
Orientierungshilfen	2/1.3; 3/15.6.3
Outsourcing	3/11.17
Parlament	2/3., 3.1, 3.3; 3/3.2

Passeinträge	3/5.1.1
Passwort	1/15.14; 2/9.4, 10.18; 3/11.22, 15.4, 15.6, 15.6.2, 15.6.3, 15.6.4, 15.13, 15.14
Patienten	1/1.1.5, 11.2.4, 11.2.5, 11.3, 11.10; 2/9.6, 11.8, 11.11, 11.12
Patientenverwaltungssystem	2/11.5
Pauschalförderung von Krankenhäusern	2/11.4
Personalakten	1/6.1.1, 6.1.10, 6.1.11, 6.1.12, 8.4; 2/9.3, 9.9, 10.12, 10.18; 3/6.2, 6.3, 6.7, 6.8, 6.9
Personalaktenführungsrichtlinie	3/6.1, 6.2
Personalnebenakten	1/6.1.10, 6.1.11, 6.1.12, 6.1.16, 9.1.7; 2/9.4; 3/6.7
Personenbeförderung	2/14.11
Petitionsausschuss	2/3.1
Pfändung	2/14.10
Pflegedienst	2/11.3; 3/11.21
Pflegekassen	2/11.24; 3/11.21
Pflegeplanung	2/11.3
Pflegeversicherung	1/11.2.6; 2/11.3, 11.24
Pflichtuntersuchungen	1/13.1.3; 2/5.2.10; 3/10.8, 11.3, 13.1
Pisa-Studie	3/13.7
Planungsaufgaben	2/14.19; 3/12.4
Poliklinikakten	1/11.3.1; 2/5.2.9; 3/6.9, 11.12
Polizeiärztlicher Dienst	3/6.9
Polizeidirektion	1/7.7; 2/7.6
polizeiliche automatisierte Verfahren	2/7.6
Polizeiliches Auskunftssystem	2/7.11
Polizeiliches Informationssystem	2/7.1
Polizeipräsidium Thüringen	1/6.1.11; 2/7.6
Protokollierung	3/15.1, 15.3, 15.6, 15.7, 15.8, 15.13, 15.15
Prozessor	2/15.9; 3/15.1, 15.10
Pseudonym	2/4.3; 3/11.1, 15.8, 15.13, 15.15

Pseudonymität	2/15.6
Psychotherapeut	3/11.16
Public-Key-Verfahren	2/15.7; 3/15.3, 15.5, 15.9, 15.13, 15.14
Rechenzentrum	2/11.17; 3/15.4, 15.6.4
Rechnungshof	1/6.1.4, 9.3; 2/9.9; 3/9.15
Rechnungsprüfung	2/11.3; 3/9.15, 10.3
Referenzperson	2/8.1
Regulierungsbehörde	2/15.8
Religionsunterricht	2/13.3; 3/13.3
Rentenversicherungsträger	2/11.29; 3/11.22
Rettungsdienst	1/1.1.4, 11.7; 2/11.21
Risikoanalyse	1/15.3; 2/15.3; 3/15.3, 15.4, 15.15
RSA	2/15.7, 15.12
ruhender Verkehr	1/14.2.2; 2/14.9; 3/14.6
Rundfunkgebühren	1/11.9.1; 2/4.7; 3/4.1
Scheinehe	2/5.1.5; 3/5.1.7
Schengener Durchführungsüberein- kommen	2/7.4; 3/5.1.4
Schengener Informationssystem	1/4.3; 2/7.4; 3/5.1.4
SCHUFA	3/5.3.3, 10.21
Schulärztliche Untersuchung	1/13.1.3; 2/13.1; 3/13.1
Schuldnerkralle	2/14.10
Schuldnerverzeichnis	3/10.22
Schuldunfähigkeit	2/10.6
Schule	3/4.6, 13.2, 13.3, 13.4
Schülervergleich	3/13.7
Schulgesundheitspflege	1/13.1.3; 2/5.2.10, 13.1; 3/13.1
Schulpflichtüberwachung	2/13.2
Schwarze Liste	3/14.1

Schweigepflicht, ärztliche	1/11.3, 11.10.2, 13.3.3; 2/11.12, 11.21, 11.24, 11.25, 11.26; 3/9.14, 11.5, 11.6, 11.7, 11.9, 11.14, 11.16, 12.1
Sekundärstatistik	1/12.4, 13.1.1; 2/12.1
Sicherheitskonzept	1/15.3; 2/5.1.9, 7.6, 9.4, 15.3, 15.4; 3/6.3, 15.3, 15.4, 15.5, 15.6.5, 15.13
Sicherheitsüberprüfung	1/6.3.2, 8.1, 8.2, 8.4; 2/8.1, 8.2; 3/8.2
Signaturgesetz	2/4.3, 15.8
Signatur Schlüssel, elektronischer	2/15.8; 3/15.3, 15.5, 15.9, 15.13, 15.14
Signaturverordnung	2/15.8
SIJUS-Straf	2/10.11.2; 3/10.17
Smart-Card	3/5.1.3, 15.14
Sozialamt	1/9.2.2, 11.9.1, 12.4, 14.3.6; 2/4.7, 5.2.6, 5.2.7; 3/5.2.9, 5.2.10, 11.2, 11.23
Sozialdaten	1/11.; 2/3.1, 5.2.7, 5.2.8, 14.13; 3/5.2.11, 11.2, 11.20
Sozialhilfe	1/14.3.6; 2/11.2, 11.28; 3/5.2.9, 11.24
- datenabgleich	2/11.2; 3/11.23
- empfänger	2/14.13
- statistik	1/12.4; 2/5.2.6
- träger	2/11.2
Sparkassen	3/5.3.3, 9.9
Sparkassenorganisation Hessen- Thüringen	3/5.3.1
Staatsanwaltschaft	2/10.11, 10.14, 10.18; 3/10.15, 10.21
Staatsanwaltschaftliche Register	2/10.11
Staatskasse	3/9.7
Standesamt	1/5.1.6, 5.1.7; 2/5.2.5; 3/9.10
Stasi-Überprüfungsunterlagen	3/5.1.10

Statistik	1/4.2, 11.3.5, 12., 13.1.1, 2/5.2.6, 12.1, 14.15; 3/12.1, 12.2, 12.4
- geheimnis	1/4.2, 12.5, 14.1.1; 2/13.3; 3/12.2
Steganographie	2/15.7
Steuerdaten-Abruf	3/9.4, 9.7
Steuererhebung	2/9.4; 3/9.3, 9.13
Steuergeheimnis	1/9.1.3, 9.1.8; 2/9.1; 3/9.5, 9.7, 9.11, 14.2
Steuerverwaltung	3/6.5, 9.2, 9.3, 9.4, 9.5, 9.10, 9.13, 14.2, 15.4, 15.6.4,
Stichtagserhebungen	2/11.23
Strafprozessordnung	2/5.1.2
Strafverfahrensänderungsgesetz (StVÄG)	1/10.4; 2/10.2, 10.4, 10.14; 3/10.1
Strafverfolgung	2/7.1; 3/10.21
Strafverfolgungsstatistik	2/12.1
Strafvollzugsänderungsgesetz	1/10.1, 10.11; 2/10.17
Strafvollzugsgesetz	3/10.18
Straßenverkehrsgesetz	1/14.2.1, 14.2.4; 2/14.7; 3/14.4
Symmetrische Verschlüsselung	2/15.7
Täter-Opfer-Ausgleich	2/10.14; 3/10.9
technisch-organisatorische Mängel	2/10.18; 3/15.3, 15.6
technisch-organisatorische Maßnahmen	1/6.3.1, 14.4.2, 15.2; 2/7.6, 9.4, 10.5, 10.12, 10.19, 11.8, 11.18, 11.29, 14.8; 3/9.15, 11.22, 15.
Telearbeit	3/11.22, 15.13
Teledienste	2/4.3, 4.4; 3/4.6
- gesetz	3/15.8, 15.13
- datenschutzgesetz	3/15.8, 15.13
Telefax	2/15.12

Telefon	
- aufzeichnung	3/7.10
- gebührenabrechnung	2/11.25
- gespräch	1/15.7; 2/5.3; 3/11.20, 15.3, 15.5, 15.6.4
- gesprächsdaten	3/6.10
- gesprächslisten	2/10.18
- überwachung	2/10.13; 3/10.5, 10.18
- verzeichnis	2/4.1
Telekommunikation	1/15.7, 15.14.4, 2/4.1, 4.2, 4.3; 3/2.4, 2.5, 4.3, 4.4
Telekommunikations-Datenschutz- Verordnung	3/4.3
Telekommunikationsüberwachung	3/10.5
Telemedizin	3/11.7
TESTA	3/15.5
Tierschutzkommission	2/3.2
Tilgungsfristen	1/10.8, 2/10.6
Transplantation	2/11.1
Übergangsbonus	1/10.1; 2/12.1; 3/10.1
Unterhaltsfestsetzung	1/9.1.6, 2/5.2.13
Unterstützungspflicht	2/5.2.18
Untersuchungshaftvollzugsgesetz	3/10.18
Untersuchungshaftvermeidung	2/13.7
Urkundenstelle	2/5.2.5
Verbrechensbekämpfung	1/ 1.2.3, 1.2.5, 10.5; 2/10.13
Verkehrsbetrieb	1/ 14.2.8; 2/14.11
Verkehrsordnungswidrigkeiten	1/7.5, 2/7.10; 3/7.4, 7.16, 7.17, 14.5
Verkehrsüberwachung	2/7.12
Vermögensfragen	2/9.2
Verpflichtung, förmliche	1/13.3.1; 2/14.21
Verschlüsselung	1/15.6, 15.10; 2/15.7, 15.8, 15.12; 3/9.3, 11.7, 13.6, 15.3, 15.4, 15.5, 15.6.4, 15.9, 15.13

Verschlusssache	3/5.1.2, 15.6.3
Versorgungsamt	2/11.25, 11.26, 11.27
Video	2/7.12, 10.7, 13.5; 3/2.1
Viren	2/15.11; 3/15.1, 15.13
Volkszählung	3/12.1
Vollstreckung	2/14.10; 3/9.8
Vorkaufsrecht der Gemeinde	2/10.21
Vorlage von Grundstückskaufverträgen	2/10.21
Vorsorgeuntersuchungen	2/5.2.10
Wahlausschlussgründe	1/5.2.6.2; 2/10.16
Wahlen	3/5.2.2, 5.2.3, 5.2.4
Warndatei	2/5.1.2
Wartung	2/15.10; 3/15.6.4, 15.13, 15.15
Wasser-/Abwasserzweckverbände	1/14.4.2; 2/14.17; 3/14.10
Werbung	2/5.2.1; 3/5.3.2
Wettbewerbsunternehmen	2/11.6; 3/14.9
Widerspruch	1/1.2.1, 5.2.4.5, 5.2.4.6, 5.2.4.7, 8.4, 9.2.5, 13.1.6, 13.2.1, 13.3.3, 14.1.2, 14.1.6, 14.3.6; 2/5.2.4, 8.1; 3/5.2.1, 5.2.2, 5.3.2, 13.2
Wohnungsdateien	1/14.3.1, 2/14.14
Wohnungsgesellschaft	1/14.3.3, 14.3.6; 2/14.12, 14.15; 3/14.9
X.400	1/15.5.2, 15.14.2; 2/15.2; 3/15.3, 15.5, 15.7
Zensus 2001	3/12.1
Zentrale Abschiebestelle im TIM (ZAS)	3/5.1.5
Zentrale Anlaufstelle für Asylbewerber (ZAST)	2/5.1.8
Zentrale Bußgeldstelle	3/7.17
Zentrale Informationsstelle für Steuerfahndungsdienst	3/9.2

Zentrales Fahrerlaubnisregister	1/14.2.1; 2/14.7; 3/14.4, 14.5
Zentrales Staatsanwaltschaftliches Ver- fahrensregister	1/1.2.5, 10.5; 2/10.5
Zentrum für Informationsverarbeitung der Thür. Landesverwaltung (ZIV)	3/15.4
Zertifizierungsstellen	2/15.8; 3/15.5
Zeugenschutz	2/10.7
Zeugenvernehmung	2/10.7
Zeugnisverweigerungsrecht	2/4.1, 10.8; 3/2.6, 10.4, 11.7
Zugangskontrolle	2/15.4, 15.5; 3/15.1, 15.4, 15.6.3, 15.6.4, 15.7, 15.13, 15.14
Zugriffe	1/15.14; 2/9.4, 10.11.3, 11.5, 11.22, 11.29, 15.4, 15.5; 3/6.3, 10.5, 11.22, 15.1, 15.4, 15.5, 15.6, 15.7, 15.8, 15.13, 15.14
Zulassungsausschuss für Vertragsärzte	1/11.11.2, 2/11.14
Zutrittskontrolle	2/5.1.9, 15.5; 3/15.13
Zutrittskontrollsystem	2/15.4, 15.5; 3/15.4, 15.6.4, 15.7, 15.14
zweckfremde Nutzung	2/11.20