THÜRINGER LANDTAG
2. Wahlperiode

Drucksache 2/2747
11.03.1998

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

durch den Präsidenten des Landtags

Zweiter Bericht über die Tätigkeit der Thüringer Landesbeauftragten für den Datenschutz

Der Thüringer Landesbeauftragte für den Datenschutz hat den obengenannten Bericht mit folgendem Schreiben vom 10. März 1998 zugeleitet:

"In der Anlage übersende ich gemäß § 40 Abs. 1 des Thüringer Datenschutzgesetzes den zweiten Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz für die Zeit vom 1. Januar 1996 bis 31. Dezember 1997.

Der Beirat hat den o.g. Bericht in seinen Sitzungen am 18.02.1998 und 10.03.1998 vorberaten."

Dr. Pietzsch
Präsident des Landtags

Hinweis der Landtagsverwaltung:
Der Bericht wird nach Auskunft der Landesbeauftragten im April 1998 als Broschüre herausgegeben und dann auch an die Mitglieder des Landtags verteilt.
Ein Exemplar des Berichts wurde vorab jeder Fraktion zur Verfügung gestellt. Der Bericht kann auch in der Landtagsbibliothek und im Landtagsinformationssystem unter obiger Drucksachennummer eingesehen werden.

Druck: Thüringer Landtag, 25. März 1998

TLfD

Der Thüringer Landesbeauftragte
für den Datenschutz

2. Tätigkeitsbericht

Berichtszeitraum
vom 1. Januar 1996 bis 31. Dezember 1997

Vorwort

Mit dem vorliegenden 2. Tätigkeitsbericht komme ich meiner Verpflichtung gemäß § 40 ThürDSG nach, dem Landtag und der Landesregierung mindestens alle 2 Jahre Bericht über meine Tätigkeit zu erstatten. Der Berichtszeitraum erstreckt sich vom 01.01.1996 bis 31.12.1997 und enthält wesentliche Feststellungen und Anregungen aus der Kontroll- und Beratungstätigkeit der öffentlichen Stellen des Freistaats Thüringen.
Ebenfalls wird auf wichtige rechtliche Regelungen auf dem Gebiet des Datenschutzes im Berichtszeitraum und auf Ergebnisse der stattgefundenen Konferenzen der Datenschutzbeauftragten des Bundes und der Länder eingegangen.
Der Bericht wurde gemäß § 40 Abs. 4 ThürDSG im Beirat vorberaten. Möge er einen Beitrag dazu leisten, das Recht auf informationelle Selbstbestimmung als festen Bestandteil unserer Rechtsordnung und als wertvolles Rechtsgut zu sehen, welches auch im Zeitalter der Informationsgesellschaft zu gewährleisten ist.

Erfurt, im Dezember 1997

Silvia Liebaug
Landesbeauftragte für den Datenschutz

2. Tätigkeitsbericht des TLfD
Berichtszeitraum vom 01.01.1996 bis 31.12.1997

Inhaltsverzeichnis
Abkürzungsverzeichnis

1. Einleitung
1.1 Die Dienststelle des TLfD
1.2 Das Datenschutzregister beim TLfD
1.3 Konferenzen und Arbeitskreise der Datenschutzbeauftragten des Bundes und der Länder

2. Europäischer und internationaler Datenschutz
2.1 Die Umsetzung der EG-Datenschutzrichtlinie - Novellierung der Datenschutzgesetze - Modernisierung des Datenschutzrechts
2.1.1 Die Datenschutzgruppe nach Artikel 29
2.1.2 Informationsveranstaltung zur EG-Datenschutzrichtlinie im Thüringer Landtag

3. Datenschutz im Parlament
3.1 Weitergabe von Sozialdaten an den Petitionsausschuß des Landtages
3.2 Informationsrecht der Abgeordneten und Datenschutz von Mitgliedern einer Tierschutzkommission
3.3 Mitteilungen über abschließende Entscheidungen in Strafverfahren gegen Mitglieder von gesetzgebenden Körperschaften

4. Neue Medien - Multimedia
4.1 Telekommunikationsgesetz (TKG) - Begleitgesetz zum TKG (BegleitG)
4.2 Telekommunikationsdiensteunternehmen-Datenschutzverordnung (TDSV)
4.3 Informations- und Kommunikationsdienste-Gesetz (IuKDG)
4.4 Mediendienste-Staatsvertrag
4.5 Thüringer Rundfunkgesetz (TRG)
4.6 Rundfunkänderungsstaatsvertrag
4.7 Rundfunkgebührenbefreiung aus sozialen Gründen
4.8 Veröffentlichung eines säumigen Beitragszahlers im Infokanal einer Antennengemeinschaft

5. Innenverwaltung - Kommunales - Sparkassen
5.1 Innenverwaltung
5.1.1 Einführung einer Asylcard
5.1.2 Vorschriften im Ausländerwesen
5.1.3 Übermittlung personenbezogener Daten bosnischer Bürgerkriegsflüchtlinge
5.1.4 Datenübermittlung aus Anlaß der Abschiebung von Vietnamesen
5.1.5 Ermittlungen im Rahmen von Scheineheverfahren gemäß § 92 Abs. 2 Nr. 2 Ausländergesetz (AuslG)
5.1.6 Veröffentlichung von Asylbewerberdaten
5.1.7 Verpflichtung zur Kostenübernahme nach § 84 AuslG
5.1.8 Kontrolle der LAST und ZAST

5.1.9 Kontrolle im Thüringer Landesverwaltungsamt
5.2 Kommunales
5.2.1 Gästemeldeschein zur Werbung der Kurverwaltung?
5.2.2 Online-Zugriff auf Meldedaten innerhalb von Gemeinden
5.2.3 Unterlagen und Verfahren zur Führung des Melderegisters
5.2.4 Melderegisterauskünfte an Adreßbuchverlage
5.2.5 Zusendung einer falschen Geburtsurkunde
5.2.6 Kontrolle in einem Sozialamt
5.2.7 Übermittlung von Sozialdaten an Polizei und Ausländerbehörde
5.2.8 Verarbeitung von Sozialhilfedaten bei Privatunternehmen?
5.2.9 Umgang mit Altdaten aus ehemaligen Polikliniken
5.2.10 Vorsorgeuntersuchung in Kindertagesstätten durch den Jugendgesundheitsdienst
5.2.11 Einladung zur amtsärztlichen Untersuchung mit Postkarte
5.2.12 Kontrolle eines Jugendamtes
5.2.13 Verwaltungsvereinfachung zu „einfach“
5.2.14 Festsetzung von Elterngebühren für die Benutzung von Kindertageseinrichtungen
5.2.15 Datenerhebung durch Jugendämter bei Kindertageseinrichtungen
5.2.16 Umgang mit Unterlagen nicht-öffentlicher Sitzungen
5.2.17 Veröffentlichung von Grundstücksdaten
5.2.18 Mangelnde Unterstützung des TLfD durch eine Stadtverwaltung
5.3 Sparkassen

6. Personalwesen

6.1 Personalaktenführungsrichtlinie
6.2 Personalaktenführung
6.3 Personalfragebogen für Bedienstete des Landes Thüringen
6.4 Personalverwaltung der Lehrer
6.5 Personalakten im Justizbereich
6.6 Einsichtnahme von Vorgesetzten in Personalakten
6.7 Verwaltungsvorschrift zur Thüringer Verordnung über Zuständigkeiten für die Feststellung, Berechnung und Anordnung der Zahlung der Bezüge von Bediensteten und Versorgungsempfängern (ThürZustVBezüge)
6.8 Veröffentlichung von Mitarbeiterdaten
6.9 Polizeiärztliche Untersuchungen im Rahmen von Bewerberauswahlverfahren für den polizeilichen Dienst
6.10 Einstellung in den Polizeidienst
6.11 Datenverarbeitung bei Personalkostenzuschüssen
6.12 Dienstvereinbarung über die elektronische Verarbeitung von Personaldaten
6.13 Führung von An- und Abwesenheitslisten der Mitarbeiter
6.14 Zulässigkeit behördlicher Organisations-/Arbeitsplatzuntersuchungen und von Mitarbeiter-/Bürgebefragungen
6.15 Personenbezogene Daten beim Personalrat
6.16 Abschottung der Beihilfestelle in einer Stadtverwaltung
6.17 Formular der Zentralen Beihilfestelle des Landesverwaltungsamtes
6.18 Datenschutz für private Eintragungen im „Schreibtischkalender“
6.19 Veröffentlichung der Ungültigkeitserklärung von Dienstausweisen
6.20 Anschriftenverzeichnis ehemaliger DDR-Arbeitgeber

7. Polizei

7.1 Bundeskriminalamtgesetz - BKAG
7.2 Polizeirechtsänderungsgesetz

7.3 Europol
7.4 Schengener Informationssystem - Schengener Durchführungsübereinkommen
7.5 Automatisiertes Fingerabdrucksystem (AFIS)
7.6 Datenschutzrechtliche Kontrollen im Polizeibereich
7.7 Speicherung personenbezogener Daten bei der Polizei
7.8 Personalien in einer polizeilichen Allgemeinverfügung
7.9 Vermerk des Aktenzeichens auf dem Briefkuvert
7.10 Erhebung und Verarbeitung von Daten im Rahmen der Verfolgung von Verkehrsordnungswidrigkeiten
7.11 Lichtbildernachweis in einem polizeilichen Auskunftssystem
7.12 Videoüberwachung

8. Verfassungsschutz
8.1 Kontrollbesuch beim Landesamt für Verfassungsschutz
8.2 Sicherheitsüberprüfung

9. Finanzen, Steuern, Rechnungsprüfung
9.1 Bereichsspezifische Regelungen in der Abgabenordnung (AO)
9.2 „Bescheidzustellung an Dritte“
9.3 Kontrolle im Thüringer Landesamt zur Regelung offener Vermögensfragen
9.4 Kontrollen in der Finanzverwaltung
9.5 Verfolgung von „Steuersündern“
9.6 Führung eines Fahrtenbuches durch Ärzte für steuerliche Zwecke
9.7 Datenschutz bei der Ausstellung und Versendung von Lohnsteuerkarten
9.8 Übermittlung von Fördermittelanträgen an Finanzamt
9.9 Einsichtsrecht des Rechnungshofs in Personalakten von Beamten

10. Justiz
10.1 Justizmitteilungsgesetz
10.2 Beratungen zum Strafverfahrensänderungsgesetz (StVÄG 1996)
10.3 Öffentliche Fahndung im Strafverfahren
10.4 DNA-Anlaye - „Genetischer Fingerabdruck“
10.5 Zentrales Staatsanwaltschaftliches Verfahrensregister
10.6 Entwurf eines Vierten Gesetzes zur Änderung des Bundeszentralregisters (4. BZRÄndG)
10.7 Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren/Videoaufzeichnungen von Zeugenvernehmungen
10.8 „Großer Lauschangriff“
10.9 Zentrale europäische Datenbanken, in denen gerichtliche Streitfälle gesammelt werden
10.10 Gesetz über das Versorgungswerk der Rechtsanwälte (ThürRAVG)
10.11 Einsatz automatisierter Verfahren im Justizbereich
10.11.1 MEGA
10.11.2 SIJUS-Straf-StA
10.11.3 Geschäftsstellenlösung der Justizvollzugsanstalten
10.12 Kontrollkompetenz des TLfD bei Gerichten
10.13 Telefonüberwachungsmaßnahmen
10.14 Täter-Opfer-Ausgleich und Datenschutz

10.15 Weitergabe personenbezogener Daten an gemeinnützige Einrichtungen
10.16 Übermittlung von Postsendungen von Staatsanwälten und Gerichten an kommunale Stellen
10.17 Datenschutz im Strafvollzug
10.18 Kontrolle einer Staatsanwaltschaft
10.19 Entsorgung „alter" Diktatkassetten einer Staatsanwaltschaft
10.20 Datenschutz im Notariat
10.21 Datenübermittlungen der Notare an die Gemeinden zur Ausübung des kommunalen Vorkaufsrechts

11. Gesundheits- und Sozialdatenschutz

11.1 Neues Transplantationsrecht
11.2 Sozialhilfedatenabgleichsverordnung (SozhiDAV)
11.3 Landesrechtliche Ausführungsvorschriften zum Pflegeversicherungsgesetz und deren Anwendung
11.4 Dritte Verordnung über die Pauschalförderung nach dem Krankenhausgesetz
11.5 Kontrolle eines Universitätsklinikums
11.6 Krankenhäuser als Wettbewerbsunternehmen nach § 26 ThürDSG
11.7 Bekenntnisfreiheit und Datenschutz im Krankenhaus
11.8 Datensicherungsmaßnahmen beim Versand von Gewebeproben
11.9 Archivierung von Krankenakten
11.10 Externe Archivierung von Krankenhausakten/Mikroverfilmung
11.11 Krankenakte im Krankenhaus verlegt
11.12 Einsichtsrecht des Patienten in Krankenhausakten
11.13 Chipkarten im Gesundheitswesen
11.14 Vorlage eines polizeilichen Führungszeugnisses für die Zulassung als Vertragsarzt
11.15 Umgang mit Kassenarztverzeichnis
11.16 Meldebögen der Landestierärztekammer Thüringen
11.17 Automatisierte Datenverarbeitung bei der AOK
11.18 Automatisierte Abrechnung durch die Krankenkassen
11.18.1 Datenträgeraustausch zwischen Krankenkassen und Zahnärzten
11.18.2 ICD-10-Code zur Abrechnung ungeeignet
11.18.3 Technisch-organisatorische Anforderungen an die Datenübermittlung
11.18.4 Löschung der Abrechnungsdaten
11.19 Falsch verstandene Auftragsdatenverarbeitung durch die AOK
11.20 Zweckfremde Nutzung von Sozialdaten?
11.21 Zu großer Verteiler beim Notarzteinsatzprotokoll
11.22 Prüfung einer Beratungsstelle des MDK
11.23 Einsicht des MDK in Krankenhausakten
11.24 Gemeinsame Nutzung von Daten durch Krankenkasse und Pflegekasse
11.25 Kontrolle eines Versorgungsamtes
11.26 Nachweis einer Schweigepflichtsentbindung durch die Versorgungsverwaltung
11.27 Zuverlässigkeitsprüfung von Heimträgern und Heimleitern
11.28 Antragsgestaltung für die Gewährung von Eingliederungshilfen
11.29 Gegenseitige Beauftragung der Träger der gesetzlichen Rentenversicherung mit der Versichertenbetreuung

12. Statistik

12.1 Einführung einer Strafverfolgungsstatistik im Freistaat Thüringen

12.2 Führung „Zentraler Register“

13. Bildung, Wissenschaft und Forschung

13.1 Datenerhebung im Rahmen der Schulgesundheitspflege

13.2 Schulpflichtüberwachung durch Schulamt?

13.3 Datenerhbungen der Kirchen zur Planung des Religionsunterrichts

13.4 Hochschuleinrichtung - öffentlich-rechtliches Wettbewerbsunternehmen?

13.5 Kontrolle einer Hochschule

13.6 Von Schimmelpilzen der Gattung Rhizopus, Mucor, Aspergillus fumigatus und flavus, Penicilium, Epicoccum sowie Modadium befallene Akten

13.7 Nutzung von Jugendgerichtshilfeakten zu Forschungszwekken

13.8 Staatsvertrag über ein gemeinsames Krebsregister der neuen Bundesländer und Berlins

13.9 Bestandsaufnahme der Asbestsituation in Thüringen

13.10 Anwendung des ThürDSG in Archiven

14. Wirtschaft, Verkehr, Wohnungswesen, Umwelt

14.1 Gesetz zur Änderung des Rechts der Architekten und Ingenieure

14.2 Thüringer Verordnung über den Gebrauchtwaren-, Edelmetall- und Altmetallhandel, über Auskunfteien, Detekteien, Reisebüros und die Vermittlung von Unterkünften

14.3 Verwaltungsvorschrift zu § 34a GewO und der Bewachungsverordnung

14.4 Bewerberliste der Bezirksschornsteinfeger

14.5 Veröffentlichungen von Handelsregisterdaten im Internet

14.6 Übermittlung von Gewerbeanzeigen an die AOK

14.7 Änderung straßenverkehrsrechtlicher Vorschriften

14.8 Kontrolle einer Führerscheinstelle

14.9 Kein „Wiederholungstäterregister“ von Parksündern

14.10 Der „Kuckuck“ mit der Schuldnerkralle

14.11 Fahrgastbefragung zur Ermittlung der Reiseweite im Ausbildungsverkehr

14.12 Datenübermittlung zwischen Wohnungsgesellschaft und Sozialamt

14.13 Aushang einer Hausordnung in einem Familienübergangshaus

14.14 Führung von Wohnungskarteikarten

14.15 Erarbeitung von Mietspiegeln

14.16 Datenübermittlung für Vermessungszwecke

14.17 Erhebungen von personenbezogenen Daten bei Zweckverbänden

14.18 Datenerhebung bei der Abfallentsorgung

14.19 Datenübermittlung aus dem Emissionskataster an eine Stadtverwaltung

14.20 Dorfbiotopkartierung in Thüringen

14.21 Kontrolle des ökologischen Landbaus durch private Stellen

15. Technischer und organisatorischer Datenschutz

15.1 Entwicklungen und Tendenzen der Informations- und Kommunikationstechnik

15.2 Corporate Network (CN) der Landesverwaltung

15.2.1 Einführung

15.2.2 Sprachkommunikation im CN

15.2.3 Datenkommunikation im CN

15.3 IT-Richtlinien in der Thüringer Landesverwaltung

15.4 Kontrolltätigkeit in öffentlichen Stellen

15.5 Einsatz von Zutrittskontrollsystemen

15.5.1 Begriffsbestimmung

15.5.2 Funktionsweise eines Zutrittskontrollsystems

15.5.3 Datenschutzrechtliche Anforderungen an Zutrittskontrollsysteme

15.6 Datenschutzfreundliche Technologien

15.7 Sicherheit mit -Kryptographischen Verfahren-

15.7.1 Einführung

15.7.2 Verschlüsselung

15.7.3 Symmetrische Verfahren

15.7.4 Asymmetrische Verfahren

15.7.5 Digitale Signatur

15.7.6 Kryptokontroverse

15.8 Das Signaturgesetz und die Signaturverordnung - ein wichtiger Schritt zum elektronischen Rechtsverkehr elektronischer Dokumente

15.9 Anforderungen zur informationstechnischen Sicherheit bei Chipkarten

15.10 Wartung von Informations- und Kommunikationstechnik

15.11 Virenschutz

15.12 Datenschutz beim Telefaxen

15.13 Datenspuren beim Zugriff auf Web-Server

Anlagen

Sachregister

Abkürzungsverzeichnis

Abkürz.	Bedeutung
AbfG	Abfallgesetz
Abs.	Absatz
AFIS	Automatisiertes Fingerabdruckidentifizierungssystem
AK	Arbeitskreis
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
ARoV	Amt zur Regelung offener Vermögensfragen
Art.	Artikel
AStBV (St)	Anweisung für das Straf- und Bußgeldverfahren (Steuer)
AuslG-VV	Allgemeine Verwaltungsvorschrift zum Ausländergesetz
AZR	Ausländerzentralregister
AZR-DV	Ausländerzentralregister-Durchführungsverordnung
AZRG	Ausländerzentralregistergesetz
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BauGB	Baugesetzbuch
bDSB	behördeninterner Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BegleitG	Begleitgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BImSchG	Bundes-Imissionsschutzgesetz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMF	Bundesfinanzministerium
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BSHG	Bundessozialhilfegesetz
BStatG	Bundesstatistikgesetz
BZR	Bundeszentralregister
BZRÄndG	Bundeszentralregister-Änderungsgesetz
BZRG	Bundeszentralregistergesetz
BZRGVwV	Verwaltungsvorschrift zum Bundeszentalregistergesetz
bzw.	beziehungsweise
CD-ROM	Compact Disk-Read Only Memory
CDLS	Chipkartenbasiertes Dienstleistungssystem
CN	Corporate Network
CPU	Central Processing Unit (Zentraleinheit)
DES	Data Encryption Standard (Symmetrischer Verschlüsselungsalgorithmus)
DF	Dedicated File
DNA-Analyse	Genetischer Fingerabdruck
DRF	Deutsche Rettungsflugwacht
DRK	Deutsches Rotes Kreuz
DSB	Datenschutzbeauftragter/ Datenschutzbeauftragte
DSRV	Datenstelle der Rentenversicherungsträger
DSS	Digital Signature Standard (Signieralgorithmus)
DT	Datenträger
DV	Datenverarbeitung
E-Mail	Elektronic-Mail (elektronische Post)
EDV	Elektronische Datenverarbeitung

EEPROM	Electrically Erasable Programmable Read Only Memory
EF	Elementary File
EG	Europäische Gemeinschaft
EPROM	Erasable Programmable Read Only Memory
ETB	elektronisches Telefonbuch
EU	Europäische Union
EUROPOL	Europäisches Polizeiamt
FAG	Fernmeldeanlagengesetz
FGG	Gesetz über die Angelegenheiten der Freiwilligen Gerichtsbarkeit
FKPG	Gesetz zur Umsetzung des Förderalen Konsolidierungsprogramms
GDD-ERFA-Kreis	Gesellschaft für Datenschutz und Datensicherheit-Erfahrungsaustausch-Kreis
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GKG	Gesetz über Kommunale Gemeinschaftsarbeit
GKR	Gemeinsames Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen
GSM-Netz	Global Standard for Mobile Kommunikation
GVBl	Gesetz- und Verordnungsblatt
HeilberfG	Heiberufsgesetz
HGB	Handelsgesetzbuch
HTML	Hypertext Markup Language
i. V. m.	in Verbindung mit
IABV	Integriertes Automatisches Besteuerungsverfahren
IBP	Informationssystem der Bayerischen Polizei
IDEA	International Data Encryption Algorithm (Blockchiffrieralgorithmus)
IEC	International Electrotechnical Commission
IGV-T	Integrationsverfahren Thüringen-Grundstufe
IHK	Industrie- und Handelskammer
IMA-IT	Interministerieller Ausschuß für Informationstechnik
IP	Internet Protokoll
ISDN	Integrated Services Digital Network (dienstintegrierendes Digitalnetz)
ISO	International Standard Organisation
ISTPOL	Informationssystem der Thüringer Polizei
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
IuKDG	Informations- und Kommunikationsdienste-Gesetz
JGG	Jugendgerichtsgesetz
JMBl	Justiz-Ministerialblatt
KAN	Kriminalaktennachweis
KB	Kilobyte
KfZ	Kraftfahrzeug
KHG	Krankenhausfinanzierungsgesetz
KitaG	Kindertageseinrichtungsgesetz
KRG	Krebsregistergesetz
KT	Kartenterminal
KV	Kassenärztliche Vereinigung
KVK	Krankenversicherungskarte
KZV	Kassenzahnärztliche Vereinigung
LAN	Local Area Network
LAST	Landesaufnahmestelle für Aussiedler
LfD	Landesbeauftragter für den Datenschutz

LHO	Landeshaushaltsordnung
LKA	Landeskriminalamt
LVA	Landesversicherungsanstalt
MAC	Message Authentication Code
MB	Megabyte
MDK	Medizinischer Dienst der Krankenkasse
MDR	Mitteldeutscher Rundfunk
MDS	Medizinischer Dienst der Spitzenverbände
MDStV	Mediendienste-Staatsvertrag
MEGA	Mehrländer-Gerichts-Anwendung
MF	Masterfile
MiStra	Mitteilungen in Strafsachen
MiZi	Mitteilungen in Zivilsachen
MPU	Medizinisch-Psychologische Untersuchung
NC	Netzcomputer
o. g.	oben genannt
OFD	Oberfinanzdirektion
PAG	Polizeiaufgabengesetz
PaßG	Paßgesetz
PBefAusglV	Personenbeförderungsausgleichsverordnung
PBefG	Personenbeförderungsgesetz
PC	Personal Computer
PD	Polizeidirektion
PDV	Ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit
PflegeVG	Pflegeversicherungsgesetz
PIN	Personen-Identifikations-Nummer
PKW	Personenkraftwagen
PRMD	Private Management Domains
PTRegG	Gesetz über die Regulierung der Telekommunikation und des Postwesens
PUK	Personal Unblocking Key
RAM	Random Access Memory
RiStBV	Richtlinie für das Straf- und Bußgeldverfahren
ROM	Read Only Memory (Nur-Lesespeicher)
RSA	assymetrisches Verschlüsselungsverfahren nach seinen Entwicklern benannt : Rivest, Shamir, Adlemann
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SHA	Secure Hash-Algorithmus
SigG	Signaturgesetz
SigV	Signaturverordnung
SIS	Schengener Informationssystem
StAnz	Staatsanzeiger der ehemaligen DDR
StGB	Strafgesetzbuch
StMBG	Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz
StPO	Strafprozeßordnung
StVÄG	Strafverfahrensänderungesetz
StVG	Straßenverkehrsgesetz
TB	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdiensteunternehmen-Datenschutzverordnung
TFM	Thüringer Finanzministerium
ThLARoV	Thüringer Landesamt zur Regelung offener Vermögensfragen
ThürAbfAG	Thüringer Abfallwirtschafts- und Altlastengesetz

ThürAGPflegeVG	Thüringer Ausführungsgesetz zum Pflegeversicherungsgesetz
ThürArchivG	Thüringer Archivgesetz
ThürBelRechtG	Thüringer Belegungsrechtegesetz
ThürBG	Thüringer Beamtengesetz
ThürBO	Thüringer Bauordnung
ThürDSG	Thüringer Datenschutzgesetz
ThürDSRegVO	Thüringer Datenschutzregisterverordnung
ThürHG	Thüringer Hochschulgesetz
ThürKAG	Thüringer Kommunalabgabengesetz
ThürKatG	Thüringer Katastergesetz
ThürKHG	Thüringer Krankenhausgesetz
ThürKO	Thüringer Kommunalordnung
ThürMeldeG	Thüringer Meldegesetz
ThürMScheinVO	Thüringer Meldescheinverordnung
ThürOBG	Thüringer Ordnungsbehördengesetz
ThürPersVG	Thüringer Personalvertretungsgesetz
ThürPolRÄG	Thüringer Polizeirechtsänderungsgesetz
ThürRAVG	Thüringer Rechtsanwaltsversorgungsgesetz
ThürSchulG	Thüringer Schulgesetz
ThürStatG	Thüringer Statistikgesetz
ThürVerf	Verfassung des Freistaats Thüringen
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
ThürVwZVG	Thüringer Verwaltungszustellungs- und Vollstrekkungsgesetz
ThürZustVBezüge	Verordnung über Zuständigkeiten für die Feststellung, Berechnung und Anordnung der Zahlung der Bezüge von Bediensteten
TIM	Thüringer Innenministerium
TK	Telekommunikationsanlage
TKG	Telekommunikationsgesetz
TKM	Thüringer Kultusministerium
TLfD	Thüringer Landesbeauftragter für den Datenschutz
TLfV	Thüringer Landesamt für Verfassungsschutz
TLL	Thüringer Landesanstalt für Landwirtschaft
TLRZ	Thüringer Landesrechenzentrum
TLS	Thüringer Landesamt für Statistik
TLVwA	Thüringer Landesverwaltungsamt
TMJE	Thüringer Ministerium für Justiz und Europaangelegenheiten
TMLNU	Thüringer Ministerium für Landwirtschaft, Naturschutz und Umwelt
TMSG	Thüringer Ministerium für Soziales und Gesundheit
TMWI	Thüringer Ministerium für Wirtschaft und Infrastruktur
TMWFK	Thüringer Ministerium für Wissenschaft, Forschung und Kultur
TOA	Täter-Opfer-Ausgleich
Tsk	Thüringer Staatskanzlei
TRG	Thüringer Rundfunkgesetz
v. H.	von Hundert
VerpflichtungsG	Verpflichtungsgesetz
VorlThürNatG	Vorläufiges Thüringer Naturschutzgesetz
VVThürDSG	Verwaltungsvorschriften zum Vollzug des Thüringer Datenschutzgesetzes
VwVfG	Verwaltungsverfahrensgesetz
VZR	Verkehrszentralregister
WAN	Wide Area Network
WWW	World Wide Web
z. B.	zum Beispiel

ZAST	Zentrale Anlaufstelle für Asylbewerber
ZG	Zentrale Gehaltsstelle Thüringen
ZSIS	Zentrales Schengener Informationssystem
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

1. Einleitung

In allen gesellschaftlichen Bereichen werden zunehmend Daten elektronisch erfaßt und gespeichert und digitalisiert mittels Computernetzen übertragen.
Personenbezogene Informationen können bei der Nutzung von Informations- und Kommunikationsdiensten in vielfältiger Weise anfallen, beliebig kombiniert, verändert oder ausgewertet werden.
Die Datenverarbeitung wird dadurch charakterisiert, daß sie nicht wie in den Anfangszeiten auf einer großen Datenverarbeitungsanlage stattfindet, sondern zunehmend im Netz mit einer Vielzahl von Beteiligten. Dabei sind die Kontrollmöglichkeiten des Nutzers in Anbetracht der zunehmenden Vernetzung erheblich eingeschränkt. Auch in der Informationsgesellschaft muß angesichts der rasanten technischen und technologischen Entwicklungen das „Recht auf informationelle Selbstbestimmung“ gesichert und vernünftiger Datenschutz praktiziert werden.
So müssen sowohl gesetzliche Rahmenbedingungen eine Antwort finden, als auch durch den Einsatz datenschutzfreundlicher Technologien, den Datenschutzrisiken wirksam begegnet werden. Dabei spielen Datensparsamkeit - Datenvermeidung - Anonymisierung und Pseudonymisierung eine Schlüsselrolle. Neue Technik bringt allerdings nicht nur Risiken sondern auch neue Chancen zum Schutz des „Rechts auf informationelle Selbstbestimmung“. Die Verschlüsselung von Daten, der Gebrauch digitaler Signaturen und der Einsatz vielfältiger Sicherheitsprodukte im Hard- und Softwarebereich bieten gute Ausgangspunkte für den Schutz der Privatsphäre der Bürger und den Schutz der personenbezogenen Daten.
Die vom Bundesverfassungsgericht im sogenannten „Volkszählungsurteil“ geprägten Grundprinzipien des Datenschutzes bleiben nach wie vor aktuell. Beschränkungen des „Rechts auf informationelle Selbstbestimmung“ sind nur zulässig im überwiegenden Allgemeininteresse, auf gesetzlicher Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entspricht und unter Beachtung des Grundsatzes der Verhältnismäßigkeit.
Große Herausforderungen gibt es auch für den Datenschutz. Die beratende Tätigkeit durch Datenschutzbeauftragte in den öffentlichen Stellen und deren rechtzeitige und effektive Einbindung in behördliche Organisationsabläufe im Zusammenhang mit der Verarbeitung personenbezogener Daten und beim Einsatz insbesondere von automatisierten Datenverarbeitungssystemen sind ein wichtiger Faktor bei der Einhaltung und Gewährleistung datenschutzrechtlicher Bestimmungen.
Datenverarbeitungssysteme müssen im Dienste der Menschen stehen und deren Privatsphäre achten. Die Transparenz der eingesetzten Datenverarbeitungssysteme für den Bürger ist ein weiterer wichtiger Punkt bei der Geltendmachung seiner Rechte in Bezug auf die Verarbeitung seiner personenbezogenen Daten durch die jeweilige datenverarbeitende Stelle.

1.1 Die Dienststelle des TLfD

Im Berichtszeitraum machten wiederum viele Bürger von ihrem Recht gemäß § 11 ThürDSG Gebrauch, sich direkt an den TLfD zu wenden, wenn sie sich bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten beeinträchtigt sahen. Dabei wurden die jeweiligen Anliegen nicht nur schriftlich, sondern mitunter auch telefonisch vorgebracht. Auch durch unmittelbares Vorsprechen in der Dienststelle haben Bürger direkt ihre Anfragen oder Beschwerden vorgetragen.

Die Kontrolltätigkeit des TLfD bei den öffentlichen Stellen des Landes bezüglich der Einhaltung der Vorschriften des ThürDSG und anderer Vorschriften über den Datenschutz und die Datensicherheit bildete weiter einen wichtigen Aufgabenschwerpunkt im Berichtszeitraum. Insgesamt kann gesagt werden, daß die Behörden bemüht sind, den datenschutzrechtlichen

Belangen hinreichend Rechnung zu tragen. Dort, wo ich aufgrund datenschutzrechtlicher Verstöße eine Beanstandung gemäß § 39 ThürDSG aussprechen mußte, verbunden mit einer gleichzeitigen Information der jeweiligen Aufsichtsbehörde, wurden regelmäßig die meinerseits geforderten Maßnahmen eingeleitet. In den Fällen, wo Fristversäumnisse der jeweiligen Stelle vorlagen oder eine mangelhafte Unterstützung dem TLfD entgegengebracht wurde, erfolgte durch Einschaltung und Information des jeweiligen Behördenleiters bzw. der Aufsichtsbehörde letztlich eine zufriedenstellende Beantwortung zu den erbetenen Auskünften.

Die beratende Tätigkeit durch den TLfD bei datenschutzrechtlichen Fragen in den Behörden wird zunehmend gewünscht. In diesem Zusammenhang möchte ich auch die immer besser stattfindende rechtzeitige Einbeziehung meiner Dienststelle durch die jeweilig zuständigen Fachressorts der Landesregierung in Vorbereitung von Entwürfen von Rechtsvorschriften erwähnen, die den Umgang mit personenbezogenen Daten berühren.

Im Rahmen der vorhandenen Möglichkeiten haben meine Mitarbeiter und ich zu Themen des Datenschutzes Vorträge gehalten.

Im Rahmen der Öffentlichkeitsarbeit wurden zu aktuellen Themen auf dem Gebiet des Datenschutzes Veröffentlichungen oder Rundschreiben von meiner Dienststelle herausgegeben. Zur Unterstützung der Tätigkeit der Datenschutzbeauftragten in den Behörden des Freistaats Thüringen habe ich eine Broschüre mit „Empfehlungen zu Aufgaben, Befugnissen und Zuständigkeiten vom behördeninternen Datenschutzbeauftragten“ herausgegeben. Sowohl 1996 als auch 1997 war der TLfD mit einem Stand anläßlich des „Tages der offenen Tür“ im Thüringer Landtag vertreten. Zahlreiche Besucher nutzten dies, Informationsmaterialien des TLfD zu erhalten und Anfragen an mich und meine Mitarbeiter zu richten.

Die Dienststelle des TLfD mit insgesamt 12 Mitarbeitern und Mitarbeiterinnen (Organigramm, Anlage 28) ist stets bemüht, alle Vorgänge möglichst kurzfristig zu bearbeiten, insbesondere, wenn es sich um Bürgeranliegen handelt. Um den wachsenden Beratungsbedarf in Datenschutz- und Datensicherheitsfragen so gut wie möglich erfüllen zu können, wird eine Personalaufstockung ins Auge zu fassen sein.
Ich werde meine diesbezüglichen Vorstellungen in absehbarer Zeit an die Abgeordneten des Thüringer Landtags herantragen.

Wie im 1. TB (2.2) ausgeführt, trägt die vereinbarte Übernahme routinemäßiger, üblicher Verwaltungstätigkeit für den TLfD durch die Landtagsverwaltung zur effektiven Verwaltungsführung bei und hat sich bewährt.

Der gemäß § 42 Abs. 1 ThürDSG vorgesehene Erfahrungsaustausch mit den Aufsichtsbehörden für die Datenverarbeitung nicht-öffentlicher Stellen wurde durchgeführt. Sowohl mit dem TLVwA als Aufsichtsbehörde für den nicht-öffentlichen Bereich als auch mit dem TIM als der obersten Aufsichtsbehörde fand eine unkomplizierte Zusammenarbeit und Meinungsaustausch statt.

1.2 Das Datenschutzregister beim TLfD

In meinem 1. TB (1.1.6, 2.1 und 2.3) habe ich bereits Ausführungen zum Datenschutzregister beim TLfD gemacht, welches ich, gemäß § 40 Abs. 7 i. V. m. § 12 ThürDSG, zu führen habe. Auch die in diesem Zusammenhang aufgetretenen Probleme fehlender und fehlerhafter Meldungen hatte ich bereits angesprochen.

Auch für den Berichtszeitraum 1996/97 muß eingeschätzt werden, daß eine Vielzahl mängelbehafteter Meldungen wiederum eingegangen sind, welche hätten vermieden werden können, wenn die rechtlichen Bestimmungen und Veröffentlichungen meinerseits in diesem Zusammenhang angemessen Berücksichtigung gefunden hätten. Häufig aufgetretene Fehler bei eingehenden Meldungen waren beispielsweise

auf dem Formblatt DSB 1:
- fehlende Dateikurzbezeichnung,
- fehlende Angabe des Datums der Meldung,
- kein Ankreuzen im jeweils vorgesehenen Kästchen, ob es sich um eine Erst-, Änderungs- oder Löschmeldung handelt,
- fehlende Beschreibung der Aufgabe, zu deren Erfüllung die Daten verarbeitet werden unter 2.d),
- fehlende oder unkonkrete Nennung der Rechtsgrundlage unter 2.e), aus der sich die Zulässigkeit der Verarbeitung der personenbezogenen Daten ergibt sowie
- fehlende Angabe der Regelfristen für die Löschung der Daten oder die Prüfung der Löschung unter 2.g) und

auf dem Formblatt DSB 2
- Stempel und Unterschrift der speichernden Stelle fehlen,
- bezüglich der Darstellung des Dateiinhalts mußten Hinweise gegeben werden, diese einzelnen Datenarten untereinander aufzuführen und mit fortlaufenden Nummern zu versehen. Freitextfelder sind in der Weise näher zu erläutern, indem aufgeführt wird, welche Bemerkungen hier gespeichert werden können.

Ich messe dem Datenschutzregister nicht nur deshalb eine große Bedeutung zu, weil dessen Führung gemäß § 40 Abs. 7 ThürDSG als meine gesetzliche Aufgabe beschrieben steht, sondern weil es der Transparenz der öffentlichen Verwaltung dient. Es enthält alle Angaben über die automatisierte Verarbeitung personenbezogener Daten in der öffentlichen Verwaltung, die der Bürger benötigt, um seine Schutzrechte sachgerecht geltend machen zu können. Auch für meine Tätigkeit, insbesondere im Zusammenhang mit der Vorbereitung von Kontrollen, sind die Angaben im Datenschutzregister eine wertvolle Grundlage. Anhand der Kenntnisnahme des Umfangs der automatisierten Verarbeitung personenbezogener Daten und der praktischen Durchführung können konkrete als auch allgemeingültige Schlußfolgerungen und Anregungen im Hinblick auf die Sicherstellung des Datenschutzes und der Datensicherheit gegeben werden.
Im Zuge eingehender Meldungen an mich war es auch oft so, daß Kopien von Datenschutzregistermeldungen eingingen. In das Datenschutzregister aufnahmefähig sind aber nur die Originale. Häufig war es auch der Fall, daß die Anlagen- und Verfahrensverzeichnisse gemäß § 10 ThürDSG an mich übersandt wurden, obwohl diese bei den öffentlichen Stellen zu führen sind, die Datenverarbeitungsanlagen und automatisierte Verfahren, mit denen personenbezogene Daten verarbeitet werden, einsetzen.

Im Zuge meiner Kontrolltätigkeit bei öffentlichen Stellen des Landes im Berichtszeitraum, die sich auf insgesamt 49 an der Zahl beliefen, mußte sowohl 1996 als auch 1997 bei mehreren öffentlichen Stellen festgestellt werden, daß eine automatisierte Verarbeitung personenbezogener Daten stattfand, obwohl keine entsprechende Datenschutzregistermeldung bei mir vorlag. Die ebenfalls in diesem Zusammenhang zumeist fehlende vorherige schriftliche Freigabe gemäß § 34 Abs. 2 ThürDSG wurde deshalb auch meinerseits förmlich beanstandet. Die jeweilige Freigabeentscheidung wurde meinerseits gefordert, da ansonsten die automatisierte Verarbeitung hätte eingestellt werden müssen. In der gesetzlich geforderten vorherigen schriftli-

chen Freigabe hinsichtlich der Datenarten und regelmäßigen Datenübermittlungen durch die Stelle, die den Datenschutz sicherzustellen hat, sehe ich nicht nur eine Formalität.
Hier geht es letztlich darum, vor dem erstmaligen Einsatz eines automatisierten Verfahrens rechtzeitig zu überprüfen, ob die vorgesehenen Datenspeicherungen und die vorgesehenen Datenübermittlungen datenschutzrechtlich zulässig sind. Die Notwendigkeit, dies so frühzeitig wie möglich durchzuführen, ergibt sich nicht zuletzt auch daraus, Fehlinvestitionen zu vermeiden, indem erforderliche Änderungen in der Regel vor der Programmierung bzw. vor dem Erwerb eines DV-Programms ausreichend berücksichtigt werden. Im Rahmen meiner Kontrolltätigkeit wurde beispielsweise auch festgestellt, daß automatisierte Verarbeitung von Personal-, Telefon- und Zeiterfassungsdaten der Mitarbeiter stattfand, ohne daß Freigabeentscheidungen vorlagen. Hier ist auch zu berücksichtigen, daß bei diesen DV-Projekten die Mitbestimmungs- und Mitwirkungsrechte des Personalrats beachtet werden. Gemäß § 74 Abs. 3 Thüringer Personalvertretungsgesetz (ThürPersVG) hat der Personalrat beispielsweise durch Abschluß von Dienstvereinbarungen mitzubestimmen über die Einführung, Anwendung, wesentliche Änderung oder Erweiterung automatisierter Datenverarbeitung personenbezogener Daten der Beschäftigten.

Für die form- und fristgerechte Abgabe der Datenschutzregistermeldung und die Beachtung der sonstigen rechtlichen Voraussetzungen einer automatisierten Verarbeitung personenbezogener Daten ist die jeweilige öffentliche Stelle verantwortlich.
Soweit von der jeweiligen obersten Landesbehörde nichts anderes zugelassen ist, ist die Meldung über die oberste Landesbehörde beim TLfD abzugeben. Gemäß § 3 Abs. 1 Thüringer Datenschutzregisterverordnung (ThürDSRegVO) leiten Landkreise und kreisfreie Städte die Meldungen ihrer speichernden Stellen unmittelbar, kreisangehörige Gemeinden und Städte über das Landratsamt an mich weiter. Zum Stand Dezember 1997 enthält das Datenschutzregister insgesamt 2.086 Meldungen.

Von einigen obersten Landesbehörden wie dem TIM, dem TMSG und dem TFM wurden Verwaltungsvorschriften zur Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten erlassen, die auch Festlegungen zur Datenschutzregistermeldung enthalten.

Als weitere Hilfestellung für die öffentlichen Stellen im Rahmen der Erstellung der jeweiligen Datenschutzregistermeldung habe ich vom TLRZ ein Programm erstellen lassen, welches die rechnergestützte Erfassung und den Druck der Formblätter ermöglicht. In dieses Erfassungssystem wurden von mir auch ausführliche Erläuterungen eingestellt, die praktische Fragen beim Ausfüllen der Meldungen beantworten helfen soll. Ich habe in einem Rundschreiben vom 12.12.1997 (Anlage 27) empfohlen, soweit die technischen Möglichkeiten in der Verwaltung vorhanden sind, das Programm für zukünftige Meldungen an mich einzusetzen. Ich gehe davon aus, daß damit die Fehlerquote bei den eingehenden Registermeldungen weiter zurückgeht.

1.3 Konferenzen und Arbeitskreise der Datenschutzbeauftragten des Bundes und der Länder

Wie im 1. TB (3.) berichtet, fanden auch wiederum im Berichtszeitraum Konferenzen der Datenschutzbeauftragten des Bundes und der Länder sowie vorbereitende Sitzungen der jeweilig zuständigen Facharbeitskreise statt. So führte 1996 für die 51. und 52. Konferenz der Hamburgische Datenschutzbeauftragte den Vorsitz. 1997 hatte den Vorsitz der Datenschutzkonferenz der Bayerische Landesdatenschutzbeauftragte inne. Es fanden 1997 neben der turnusmäßigen 53. und 54. Konferenz auch eine Sonderkonferenz zum The-

ma „Neue Herausforderungen für den Datenschutz“ in Bamberg statt. Die Entschließungen der Konferenzen, einschließlich der verabschiedeten Orientierungshilfen und Arbeitspapiere, denen ich zugestimmt habe, sind im 2. Tätigkeitsbericht in den Anlagen 1 bis 21 abgedruckt.

2. Europäischer und internationaler Datenschutz

Mit Interesse habe ich die Themen der Europäischen und Internationalen Datenschutzkonferenzen im Berichtszeitraum verfolgt. In den Anlagen 22 bis 26 habe ich zur Information gemeinsame Erklärungen und Stellungnahmen der Europäischen Datenschutzbeauftragten angefügt.

An der 18. Internationalen Datenschutzkonferenz am 18. und 19. September 1996 habe ich selbst auch teilgenommen. Im Mittelpunkt der Vorträge stand insbesondere die Zukunft des Datenschutzes und Auswirkungen der europäischen Datenschutzrichtlinie auf die Rechtsverordnungen in den Staaten außerhalb der Gemeinschaft, den sogenannten Drittstaaten. Ein weiterer Themenschwerpunkt waren Chancen datenschutzfreundlicher Technologien, das Erreichen einer Allianz von Technik und Datenschutz.

2.1 Die Umsetzung der EG-Datenschutzrichtlinie - Novellierung der Datenschutzgesetze - Modernisierung des Datenschutzrechts

In meinem 1. TB (4.1) hatte ich 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 berichtet. Die Mitgliedstaaten haben innerhalb einer dreijährigen Frist die Bestimmungen in nationales Recht umzusetzen. Diese Frist läuft im Oktober 1998 ab.
In einer Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 (Anlage 3) haben sie an die Gesetzgeber in Bund und Ländern appelliert, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann. Anläßlich der 54. Konferenz am 23./24. Oktober 1997 in Bamberg haben sich erneut die Datenschutzbeauftragten des Bundes und der Länder eingehend mit der Novellierung des Bundesdatenschutzgesetzes befaßt und eine Entschließung verabschiedet, die in Anlage 15 des vorliegenden 2. Tätigkeitsberichts abgedruckt ist. Angesichts der in weniger als einem Jahr ablaufenden Dreijahresfrist zur Umsetzung der Richtlinie appellieren die Datenschutzbeauftragten an die Bundesregierung, für eine fristgerechte Anpassung des Bundesdatenschutzgesetzes Sorge zu tragen. Sie mahnen die durch Verzögerungen des bisherigen Verfahrens höchst nachteilige Lage für die Entwicklung des Datenschutzes an, weil u. a. auch eine rechtliche Zersplitterung folgen könnte, weil in den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt. Im Dezember 1997 wurde der Entwurf eines Gesetzes zur Änderung des BDSG und anderer Gesetze vom BMI vorgelegt.
Auch von Seiten des TIM wurde mitgeteilt, daß die Ländergesetzgebung einer Anpassung um die Maßgaben der Richtlinie bedarf und das die Vorarbeiten zur Anpassung des ThürDSG bereits hausintern aufgenommen wurden.

2.1.1 Die Datenschutzgruppe nach Artikel 29

Im 1. TB (4.1) hatte ich über Zusammensetzung und Aufgaben der Datenschutzgruppe bereits berichtet, welche in den Artikeln 29 und 30 der EG-Datenschutzrichtlinie festgelegt sind. Ihre beratende Funktion trägt zur einheitlichen Anwendung der zur Umsetzung der Richtlinie erlassenen einzelstaatlichen Vorschriften bei. Im Rahmen der ständigen Zusammenarbeit der Kontrollstellen kann eine Weiterentwicklung des Datenschutzes auf Gemeinschaftsebene erreicht werden. Die Gruppe arbeitet auf der Grundlage einer gemeinsamen Geschäftsordnung. Unter Beachtung der förderalen Struktur der deutschen Datenschutzkontrolle nehmen an den Sitzungen der Gruppe auch ein Vertreter der Landesbeauftragten und der obersten Aufsichtsbehörden der Länder teil. Die Gruppe erstattet jährlich einen Bericht. Der erste Jahresbericht (Dok. XV/5025/97 - und DE-WP3) der Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten wurde zwischenzeitlich angenommen und veröffentlicht.

2.1.2 Informationsveranstaltung zur EG-Datenschutzrichtlinie im Thüringer Landtag

Am 10. September 1997 habe ich zu einer Informationsveranstaltung zur EG-Datenschutzrichtlinie eingeladen. Neben Datenschutzbeauftragten der obersten Landesbehörden, Landkreisen und kreisfreien Städten haben auch Mitglieder des GDD-ERFA-Kreises teilgenommen. Als Gäste waren von Seiten der Thüringer Aufsichtsbehörden für den nicht-öffentlichen Bereich Vertreter des TIM und des TLVwA anwesend. Vom Sächsischen Staatsministerium des Innern war ebenfalls ein Vertreter der Aufsichtsbehörde für den nicht-öffentlichen Bereich des Freistaats Sachsen anwesend. Der Sächsische Datenschutzbeauftragte, Dr. Giesen, hat interessante Ausführungen, insbesondere zur Rechtsstellung, Aufgaben und Befugnissen der Datenschutzkontrollstellen im Sinne des Artikel 28 der Richtlinie vorgetragen. Die EG-Datenschutzrichtlinie erweitert die Informationsrechte des Bürgers und verpflichtet die Mitgliedstaaten zur Einrichtung unabhängiger staatlicher Kontrollstellen, die die Einhaltung der in der Umsetzung der Richtlinie geschaffenen internationalen Vorschriften überwachen. Ziel der Richtlinie ist es, gleichwertigen Datenschutz in allen Mitgliedstaaten zu realisieren.

3. Datenschutz im Parlament

Die Thematik von Datenschutzregelungen für Parlamente und der Inhalt und Umfang einer rechtlichen Grundlage dafür wurden im Berichtszeitraum aktuell diskutiert. Von Seiten der Konferenz der Präsidentinnen und Präsidenten der deutschen Landesparlamente am 09. Mai 1995 in Konstanz liegen Thesen zu parlamentsspezifischen Datenschutzrecht vor. In diesem Zusammenhang wurde auch ein Musterentwurf einer entsprechenden Datenschutzordnung vorgelegt, wenn beispielsweise auf der Grundlage einer in die Landesdatenschutzgesetze aufzunehmenden Parlamentsklausel diese Datenschutzordnung verabschiedet wird.
Auch die Datenschutzbeauftragten des Bundes und der Länder beschäftigten sich mit dieser Problematik im Rahmen der 51. und der 52. Konferenz. Die eigens dafür einberufene Arbeitsgruppe arbeitete dazu die inhaltlichen und rechtlichen Fragen auf. Im Ergebnis der Diskussion bestand Einigkeit darüber, daß die Datenschutzbeauftragten ihre Beratung bei der Schaffung parlamentsspezifischer Datenschutzregelungen anbieten. Unter Berücksichtigung der Besonderheiten des jeweiligen Landesrechts spricht meines Erachtens einiges dafür, parlamentsspezifisches Datenschutzrecht durch ein formelles Gesetz umzusetzen. Dies habe ich dem Thüringer Landtag mitgeteilt.

3.1 Weitergabe von Sozialdaten an den Petitionsausschuß des Landtages

Unter den Datenschutzbeauftragten des Bundes und der Länder wurde die Frage diskutiert, unter welchen Voraussetzungen im Rahmen eines Petitionsverfahrens Sozialdaten an den Petitionsausschuß des Landtags übermittelt werden dürfen. Meine Nachfrage bei der Landtagsverwaltung hat ergeben, daß in der Praxis grundsätzlich keine Akten direkt dem Petitionsausschuß vorgelegt werden, obwohl dies in der Landesverfassung zugelassen ist. Im Petitionsverfahren wird die Landesregierung um eine Stellungnahme gebeten, die ihrerseits zu deren Erstellung die Akten im Rahmen ihrer Rechts- und Fachaufsicht bei den zuständigen Stellen anfordert. Sowohl die Vorlage von Akten als auch die Übermittlung sonstiger Sozialdaten im Rahmen der Stellungnahme der Landesregierung an den Petitionsausschuß ist in denjenigen Fällen unproblematisch, in denen sich diese Daten auf den Petenten selbst beziehen, da dieser das Petitionsverfahren angestoßen hat und in der Regel die Überprüfung seines konkreten Falles unter Verwendung seiner Sozialdaten wünscht. Anders stellt sich dies allerdings in denjenigen Fällen dar, in denen zur Beurteilung des Sachverhalts personenbezogene Daten Dritter erforderlich sind. Nach Art. 65 Abs. 2 i. V. m. Art. 64 Abs. 4 Satz 1 und 2 Verfassung des Freistaats Thüringen (ThürVerf) haben die Landesregierung und Behörden des Landes die Pflicht, angeforderte Akten vorzulegen und Auskünfte zu geben. Dadurch wird das Informationsrecht des Parlaments konkretisiert. Durch Art. 65 Abs. 2 i. V. m. Art. 67 Abs. 3 ThürVerf kann jedoch die Landesregierung die Beantwortung von Anfragen und Erteilung von Auskünften ablehnen, wenn dem Bekanntwerden des Inhalts gesetzliche Vorschriften, insbesondere des Datenschutzes entgegenstehen. Diesen Regelungen ist zu entnehmen, daß weder das Informationsrecht des Parlaments noch die Vorschriften zum Schutz des informationellen Selbstbestimmungsrechts von vornherein Vorrang haben. Es hat daher eine Abwägung beider verfassungsrechtlich verankerter Prinzipien im Einzelfall zu erfolgen, wobei beiden Grundsätzen soweit wie möglich zur Geltung zu verhelfen ist. Da die Ausschußsitzungen in nicht-öffentlicher Sitzung durchgeführt werden sowie größtenteils Sozialdaten des Betroffenen mit dessen Einwilligung dem Ausschuß bekanntgegeben werden, dürfte im Regelfall ein angemessener Ausgleich der widerstreitenden Interessen vorliegen. Beschwerden Betroffener habe ich bislang nicht erhalten.

3.2. Informationsrecht der Abgeordneten und Datenschutz von Mitgliedern einer Tierschutzkommission

Im Berichtszeitraum wurde ich um eine Stellungnahme im Zusammenhang mit einer Kleinen Anfrage gebeten, ob es aus datenschutzrechtlicher Sicht zulässig ist, daß die Landesregierung im Rahmen der Beantwortung einer Parlamentarischen Anfrage die Namen und Anschriften der Mitglieder der nach § 15 Abs. 1 Tierschutzgesetz berufenen Kommission mitteilt. Diese Kommission berät die zuständigen Behörden bei der Entscheidung über die Durchführung von Tierversuchen, hat jedoch keinerlei Entscheidungsbefugnisse und tagt auch nicht öffentlich. Die zuständigen Behörden sind nicht an die Äußerungen der Kommissionsmitglieder bei ihren Entscheidungen gebunden.

Auch in diesem Fall besteht ein Informationsrecht des Parlaments und des einzelnen Abgeordneten aufgrund von Art. 67 Abs. 1 ThürVerf i. V. m. den Vorschriften der Geschäftsordnung des Thüringer Landtags, dem ein Auskunftsverweigerungsrecht der Landesregierung nach Art. 67 Abs. 3 ThürVerf gegenübersteht, wenn dem Bekanntwerden des Inhalts der Antwort auf eine parlamentarische Anfrage datenschutzrechtlich geschützte Interessen Einzelner entgegenstehen. Hier sind ebenfalls die verfassungsrechtlichen Prinzipien

im Rahmen einer Abwägung einander so zuzuordnen, daß beide eine größtmögliche Wirkung entfalten. Weil die Beantwortung von parlamentarischen Anfragen entweder in der Öffentlichkeit erfolgt bzw. bei schriftlichen Anfragen die Antwort veröffentlicht wird, stellt die Bekanntgabe von Name und Adresse der Kommissionsmitglieder einen wesentlich stärkeren Eingriff in deren informationelles Selbstbestimmungsrecht dar, als eine Bekanntgabe ausschließlich gegenüber dem Abgeordneten. Im übrigen war wegen der nur beratenden und internen Funktion der Kommission keinerlei Erforderlichkeit für eine Veröffentlichung der Namen der Mitglieder der Kommission ersichtlich. Deswegen hielt ich in meiner Stellungnahme im vorliegenden Fall aus datenschutzrechtlicher Sicht die Bekanntgabe von Namen und Adressen der Kommissionsmitglieder in einem Landtagsausschuß für zulässig, da dies einen geringeren Eingriff in das Persönlichkeitsrecht der Kommissionsmitglieder darstellt, ohne daß hierbei der Informationsanspruch des Abgeordneten eingeschränkt würde.

3.3 Mitteilungen über abschließende Entscheidungen in Strafverfahren gegen Mitglieder von gesetzgebenden Körperschaften

Die Datenschutzbeauftragten haben sich mit der Frage befaßt, ob es aus datenschutzrechtlichen Gründen geboten sei, gemäß Nr. 192 Abs. 5 Richtlinie für das Straf- und Bußgeldverfahren (RiStBV) abschließende Entscheidungen im Strafverfahren an den Präsidenten der betreffenden „gesetzgebenden“ Körperschaft zu übermitteln. Die Information des Parlaments über die Notwendigkeit der Einleitung eines Strafverfahrens ist notwendige Voraussetzung dafür, daß das Parlament entscheiden kann, ob die Immunität aufgehoben werden soll. Da nach den Regelungen der Verfassung die Entscheidung darüber beim Parlament liegt, ist Strafverfolgung nur möglich, wenn notwendige Informationen an das Parlament gelangen. Regelungen darüber, wie zu verfahren ist, wenn das Verfahren seine Erledigung gefunden hat, gibt es nicht, so daß die Beurteilung davon abhängt, ob die Art der Erledigung für die weitere Tätigkeit des Abgeordneten bzw. des Parlaments von Bedeutung ist. Ich habe hierzu die Ansicht vertreten, daß in Fällen, in denen ein Landtagsabgeordneter aus dem Parlament ausgeschieden ist, eine derartige Notwendigkeit nicht besteht. Von der Landtagsverwaltung ist mir hierzu mitgeteilt worden, daß sie diese Auffassung teilt.

4. Neue Medien - Multimedia

4.1 Telekommunikationsgesetz (TKG) - Begleitgesetz zum TKG (BegleitG)

Die vorgesehene Liberalisierung im Telekommunikationsmarkt zum 01.01.1998 machte es erforderlich, hierfür auch den rechtlichen Rahmen zu schaffen. Das zum 01.08.1996 in Kraft getretene Telekommunikationsgesetz (TKG, BGBl I S. 1220f) hat hierfür geeignete Rahmenbedingungen geschaffen. Schon im Vorfeld hatten die Datenschutzbeauftragten (1. TB, Anlage 27) in ihrer Entschließung vom 09./10.11.1995 unter anderem die Forderung erhoben, einen wirksamen Datenschutz auch künftig als gleichberechtigtes Regulierungsziel zu gewährleisten, unabhängig davon, daß die Prinzipien der Datenvermeidung und der Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten Rechnung getragen werden sollte. Das TKG schreibt ausdrücklich für die privaten Betreiber von Fernmeldeanlagen die Wahrung des Fernmeldegeheimnisses vor. Sowohl der Inhalt der Telekommunikation als auch die näheren Umstände des Kommunikationsvorgangs unterliegen dem Fernmeldegeheimnis, so daß damit auch die Verbindungsdaten, wer, wann, mit wem, telefoniert hat, unter das Fernmeldegeheimnis fallen. Zur Einhaltung des Fernmeldegeheimnisses ist derjenige verpflichtet, der ge-

schäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. Damit unterliegen auch private Netze in Firmen (Corporate Networks), Nebenstellenanlagen in Krankenhäusern und Hotels dem Fernmeldegeheimnis, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind. Die Datenschutzbeauftragten hatten sich in der o. a. Entschließung dagegen ausgesprochen, die Datenschutzkontrolle auf die Regulierungsbehörde zu übertragen, da diese nicht über die hinreichende Unabhängigkeit verfügt. Nunmehr liegt die Zuständigkeit hierfür beim BfD. In der Praxis zeigte sich allerdings, daß in einigen Bereichen eine genaue Abgrenzung der Zuständigkeiten zwischen BfD, LfD und Aufsichtsbehörden für den nichtöffentlichen Bereich noch erforderlich sein wird. Im Kreise der Datenschutzbeauftragten wird dies derzeit erörtert. Erfreulich ist, daß nach § 89 Abs. 8 TKG die Rechte der Kunden im Telekommunikationsbereich bei der Eintragung in Telefonverzeichnisse eine Verstärkung erfahren haben. Nunmehr wird in das öffentliche Telefonbuch, unabhängig davon, ob es auf CD-ROM oder gedruckt abrufbar ist, nur noch derjenige aufgenommen, der dies beantragt hat. Zuvor erfolgte eine Registrierung lediglich dann nicht, wenn der Betroffene der Registrierung widersprochen hatte (1. TB, 5.2.4.7). Für Eintragungen, die vor Inkrafttreten des TKG in das Telefonbuch aber aufgenommen worden sind, bleibt es bei der Widerspruchslösung. Wer nicht will, daß außer der Telefonnummer weitere Angaben über ihn beauskunftet werden, muß ebenfalls Widerspruch erheben. Nach § 11 Abs. 3 TKG bestand die Verpflichtung, den Kunden über die Wahlmöglichkeit, ggf. auch über die Rufnummern hinausgehende Auskünfte zu erteilen, zu unterrichten.
Kritisch wird im Kreise der Datenschutzbeauftragten die Regelung des § 90 TKG betrachtet, die ein automatisiertes Abrufverfahren für die aktuellen Kundendaten aller Telekommunikationsdiensteanbieter u. a. an Gerichte, Staatsanwaltschaften, Polizei und Verfassungsschutzbehörden vorsieht. Hier wird kritisch zu beobachten sein, wie sich diese Vorschrift in der Praxis bewährt.
Im Nachgang zum Postneuordnungsgesetz von 1994 (Postreform II) und in Umsetzung des TKG bestand die Notwendigkeit, zahlreiche Rechtsvorschriften an die geänderte Rechtslage anzupassen. Dem hat der Bundesgesetzgeber mit dem Begleitgesetz zum Telekommunikationsgesetz vom 17.12.1997 (BGBl I S. 3108) Rechnung getragen. Während sich Artikel I mit der neu eingerichteten Regulierungsbehörde für Telekommunikation befaßt, enthält Artikel II zahlreiche Änderungen von Einzelvorschriften, zu denen auch das Streichen der Bezugnahme auf das Gesetz über Fernmeldeanlagen (FAG) im BDSG sowie Änderungen im Telekommunikationsgesetz selbst zählen. § 12 FAG, der zum 31.12.1997 außer Kraft treten sollte, sieht vor, daß unter bestimmten Voraussetzungen in strafgerichtlichen Untersuchungen Auskunft über die Telekommunikation verlangt werden kann. Hier war im BegleitG vorgesehen, einen neuen § 99 a Strafprozeßordnung (StPO) einzuführen. Danach sollte u. a. eine Auskunftserteilung nur bei Straftaten von nicht unerheblicher Bedeutung ermöglicht werden, wobei keine Unterrichtung des Betroffenen über diese Maßnahme vorgesehen war. Im weiteren Gesetzgebungsverfahren wurde diese Überlegung nicht weiter verfolgt. Die Geltung von § 12 FAG wurde dann noch einmal bis zum 31.12.1999 verlängert.

4.2 Telekommunikationsdiensteunternehmen-Datenschutzverordnung (TDSV)

Hinter dieser komplizierten Bezeichnung verbirgt sich die zum 1. Juli 1996 in Kraft getretene Verordnung (BGBl I S. 982) auf der Ermächtigungsgrundlage des § 10 Abs. 1 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG). Hier ist geregelt, wie Unternehmen, die Telekommunikationsdienstleistungen für die Öffentlichkeit erbringen oder daran mitwirken, unter anderem den Schutz personenbezogener

Daten der am Fernmeldeverkehr Beteiligten sicherzustellen haben. Die Verordnung enthält Vorschriften zum Umfang der Datenerhebung, -verarbeitung und -nutzung und enthält auch Fristen für die Löschung von Verbindungsdaten bei Abrechnungen und Bestandsdaten nach Beendigung des Vertragsverhältnisses. Die Verordnung erfaßt jedoch nur Unternehmen, die Telekommunikationsdienstleistungen für die Öffentlichkeit erbringen und daran mitwirken und nicht geschlossene Benutzergruppen, wie Corporate Networks. Um diese erfassen zu können, bedarf es einer neuen Rechtsverordnung, für die § 89 des zum 01.08.1996 in Kraft getretenen TKG die Rechtsgrundlage gibt. Daß eine neue Verordnung dringend erforderlich ist, ist allseits anerkannt. Ein entsprechender Entwurf liegt bisher noch nicht vor.

4.3 Informations- und Kommunikationsdienste-Gesetz (IuKDG)

Das zum 01.08.1997 in Kraft getretene als Artikelgesetz konzipierte IuKDG enthält neben den Änderungen verschiedener Rechtsvorschriften auch drei neue Gesetze, mit denen juristisches Neuland betreten wird. Dies gilt jedoch insbesondere für das Signaturgesetz (SigG), zu dem an anderer Stelle (15.8) nähere Ausführungen gemacht sind. Das Gesetz über die Nutzung von Telediensten (Teledienstegesetz - TDG) umfaßt u. a. Regelungen zur Zugangsfreiheit der Informations- und Kommunikationsdienste und zur Verantwortlichkeit für Diensteanbietern bei Telediensten. Entscheidend ist hierbei, daß als Teledienste die Kommunikationsdienste definiert werden, denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Das IuKDG regelt lediglich die Nutzung der mittels Telekommunikation übermittelten Inhalte, nicht die Telekommunikation selbst. In der Praxis bedeutet dies, daß der telekommunikationsrechtliche Datenschutz hier ebenfalls zu berücksichtigen ist. Als Teledienste sind nach § 2 Abs. 2 TDG unter anderem Telebanking, Datendienste zu Informationen wie Verkehr, Wetter und Umweltdaten sowie die Nutzung des Internets anzusehen. § 5 TDG stellt klar, daß Diensteanbieter, zu denen diejenigen zählen, die entweder eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln, nur für eigene Inhalte nach den allgemeinen Gesetzen verantwortlich sind und nicht für fremde Inhalte, zu denen sie lediglich den Zugang vermitteln. Wenn beispielsweise der Diensteanbieter keine Kenntnis davon hat, daß ein strafbarer Inhalt eingestellt worden ist und es ihm technisch nicht möglich und zumutbar ist, diese Nutzung zu unterbinden, kann er hierfür strafrechtlich nicht zur Verantwortung gezogen werden, was vor Inkrafttreten des Gesetzes zumindest umstritten war.
Im Teledienstedatenschutzgesetz (TDDSG), das bereichsspezifisch den Schutz personenbezogener Daten bei Telediensten im Sinne des TDG regelt, findet sich in § 3 Abs. 4 TDDSG erstmalig eine Regelung, die den Grundsatz der Datensparsamkeit und Datenvermeidung festlegt. Der Diensteanbieter darf nach § 3 Abs. 3 TDDSG die Erbringungen von Telediensten nicht von einer Einwilligung des Nutzers in die Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, wenn ein anderer Zugang zu diesen Telediensten nicht oder in nicht zumutbarer Weise möglich ist. Ich sehe dies als einen entscheidend positiven Gesichtspunkt dieses Gesetzes an, da damit für den Bürger die Teilnahme an der modernen Kommunikation auch ohne Preisgabe seiner Daten an Dritte ermöglicht wird. Auch dem aus datenschutzrechtlicher Sicht immer wieder geforderten Gesichtspunkt der Zulassung einer anonymen Nutzung wird Rechnung getragen, indem § 4 Abs. 1 TDDSG normiert, daß die Benutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonymen, soweit technisch möglich und zumutbar, ermöglicht werden soll. Die datenschutzrechtliche Diskussion wird seit Jahren davon bestimmt, daß verhindert werden soll, Nutzungsprofile zu erstellen, die zum „gläsernen Bürger“ führen. § 4 Abs. 4 TDDSG gestattet die Erstellung von Nutzungsprofilen nur dann, wenn hierzu Pseudonyme (vgl. zum Begriff 15.6) verwandt werden und verbietet es aus-

drücklich, daß dieses Pseudonym mit den Daten über den Träger des Pseudonyms zusammengeführt werden. Diese Regelung trägt sowohl dem Interesse des Nutzers an weitgehender Anonymität seines Konsumentenverhaltens als auch dem wirtschaftlichen Interesse des Diensteanbieters hinsichtlich der Auswertung der Inanspruchnahme der von ihm vermittelten Teledienste Rechnung.
Bei den sogenannten Bestandsdaten war ursprünglich vorgesehen, daß die Anbieter von Telediensten verpflichtet werden sollen, Polizei und Nachrichtendiensten Auskunft über Daten zur Begründung, inhaltlichen Ausgestaltung und Änderung der Vertragsverhältnisse ihrer Kunden zu erteilen. Hiergegen haben sich die Datenschutzbeauftragten mit ihrer Entschließung vom 17./18.04.1997 (Anlage 12) gewandt. Der Gesetzgeber hat bei der Beschlußfassung die kritisierte Übermittlungsregelung nicht übernommen. Wichtig ist auch die in § 6 TDDSG getroffene Regelung, wonach Nutzungsdaten nur erhoben und gespeichert werden können, soweit dies erforderlich ist, um dem Nutzer die Inanspruchnahme von Telediensten zu ermöglichen und die Verpflichtung, Nutzungsdaten spätestens unmittelbar nach Ende der jeweiligen Nutzung, soweit es sich nicht um Abrechnungsdaten handelt, zu löschen. Schließlich gibt § 7 TDDSG dem Benutzer das Recht, jederzeit die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten unentgeltlich beim Diensteanbieter einzusehen. Zur Datenschutzkontrolle verweist § 8 TDDSG auf § 38 BDSG, so daß die Kontrolle der Datenschutzvorschriften der Aufsichtsbehörde für den nicht-öffentlichen Bereich unterliegt. Erstmalig wird hier bereits in Anlehnung an die EG-Datenschutzrichtlinie vorgesehen, daß die Kontrolle durch die Aufsichtsbehörde nicht mehr an einen konkreten Anlaß gebunden sein muß. Eine neue Zuständigkeit erwächst hier für den BfD, der die Entwicklung des Datenschutzes bei Telediensten zu beobachten und hierzu in seinem Tätigkeitsbericht Stellung zu nehmen hat. Bei der Gesamtbetrachtung ist allerdings zu berücksichtigen, daß sich die Regelungen des IuKDG nur auf Diensteanbieter in der BRD beziehen.

4.4 Mediendienste-Staatsvertrag

Vor und im Laufe der Beratungen zum IuKDG (4.3) und des Mediendienste-Staatsvertrags (MDStV, GVBl S. 258), der am 01.08.1997 in Kraft trat, gab es intensive Beratungen zwischen Bund und Ländern zur Zuständigkeitsabgrenzung, da für Teilbereiche der neuen Medien sowohl der Bund als auch die Länder die Zuständigkeit für sich in Anspruch nahmen. Der Mediendienste-Staatsvertrag gilt nach der getroffenen Klärung gemäß § 2 für das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten. Hierzu zählen Verteildienste sowie Abrufdienste, bei denen Text, Ton und Bilddarbietungen aus elektronischen Speichern auf Anforderung zur Nutzung übermittelt werden. Die Abgrenzung zwischen Telediensten und Mediendiensten kann mitunter schwierig sein, da die Frage, ob die redaktionelle Gestaltung im Vordergrund steht, nicht einfach zu beantworten ist. Nach § 2 Abs. 4 Ziffer 3 TDG ist ein Verteil- und Abrufdienst, der dem Wortlaut nach unter das TDG fallen kann, in einem solchen Fall nämlich dem MDStV unterstellt. Ansonsten ist festzuhalten, daß die Regelungen des TDDSG und des MDStV, soweit bekannt, erstmalig in Form von Bundes- und Landesvorschriften weitestgehend aufeinander abgestimmt wurden. Eine Neuerung stellt das im TDDSG nicht enthaltene sogenannte Datenschutz-Audit dar, das den Anbietern von Mediendiensten die Möglichkeit eröffnet, zur Verbesserung von Datenschutz und Datensicherheit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen zu lassen. Zu den näheren Anforderungen bedarf es jedoch noch eines besonderen Gesetzes. Im Unterschied zum TDDSG sieht der MDStV auch vor, daß Verstöße gegen den Mediendienste-Staatsvertrag als Ordnungswidrigkeiten geahndet werden können.

4.5 Thüringer Rundfunkgesetz (TRG)

Im Berichtszeitraum wurde das Thüringer Rundfunkgesetz (TRG) neu gefaßt (GVBl S. 271), wobei ich vorgeschlagen habe, im Zusammenhang mit der Abrechnung von in Anspruch genommenen Programmangeboten eine Verpflichtung zur Unterrichtung von Mitbenutzern des Anschlusses aufzunehmen. Bei der Vorschrift zur Medienforschung habe ich angeregt, den Personenbezug zu löschen, sobald das nach dem Forschungsprojekt möglich ist. Meine Vorschläge wurden berücksichtigt.

4.6 Rundfunkänderungsstaatsvertrag

Im Berichtszeitraum trat zum 01.01.1996 der Zweite Rundfunkänderungsstaatsvertrag (GVBl S. 16) sowie am 01.01.1997 der Dritte Rundfunkänderungsstaatsvertrag (GVBl S. 87) in Kraft. Zum Datenschutz findet sich im letztgemeinten in § 47 die Übernahme einer wortgleichen Formulierung aus der bisherigen Regelung. Zwischenzeitlich gibt es nicht nur im Hinblick auf das digitale Fernsehen Überlegungen für einen Vierten Rundfunkänderungsstaatsvertrag, wobei auch an die Änderung des MDStV (4.4) gedacht wird. Von Datenschutzseite ist hier empfohlen worden, die bisherigen Regelungen zum Datenschutz an die Vorschriften des MDStV anzupassen, soweit nicht Änderungen im Hinblick auf die besonderen Bedingungen des Rundfunks geboten sind. Auch hier umfaßt der zur Zeit diskutierte Vorschlag die Einführung eines Datenschutz-Audit. Mit der Änderung des Staatsvertrags ist vorgesehen, auch andere Staatsverträge der Länder im Rundfunk/Medienbereich zu ergänzen. Die Abstimmungen auf Länderebene sind aber noch nicht abgeschlossen.

4.7 Rundfunkgebührenbefreiung aus sozialen Gründen

Auf die datenschutzwidrige Verfahrensweise bei der Befreiung von der Rundfunkgebührenpflicht aus sozialen Gründen habe ich bereits im 1. TB (11.9.1) aufmerksam gemacht. Im Berichtszeitraum wurde das Verfahren mit dem MDR und den für das Rundfunkrecht zuständigen Staatskanzleien weiter diskutiert. Ein Vorschlag der Datenschutzbeauftragten der MDR-Länder zur Änderung der Rundfunkgebührenbefreiungsverordnungen wurde bislang nicht aufgegriffen. Ziel einer möglichen Änderung der Verfahrensweise sollte es sein, sowohl die Antragsbearbeitung für den Bürger ortsnah zu gestalten als auch andererseits überflüssige Datenerhebungen und -verarbeitungen zu vermeiden. Obwohl sich im Berichtszeitraum in dieser Frage nichts getan hat, haben die Beteiligten weitere Gesprächsbereitschaft signalisiert. Das Ergebnis bleibt abzuwarten.

4.8 Veröffentlichung eines säumigen Beitragszahlers im Infokanal einer Antennengemeinschaft

Eine Antennengemeinschaft, die einen Infokanal betreibt, bat mich um Mitteilung, ob ein säumiger Beitragszahler im Infokanal mit Namen veröffentlicht werden könne. Nach § 59 Satz 2 Thüringer Rundfunkgesetz (TRG) besteht die Verpflichtung, personenbezogene Daten nicht über den in §§ 57 und 60 genannten Umfang hinaus zu verarbeiten und zu nutzen. Die Veröffentlichung personenbezogener Daten der Nichtzahler im Infokanal hätte eine Prangerwirkung, die das informationelle Selbstbestimmungsrecht der Betroffenen erheblich beeinträchtigen würde, zumal dies für die Abrechnung des Entgelts nicht erforderlich ist. Ich habe daher dem Petenten empfohlen, von diesen Überlegungen Abstand zu nehmen.

5. Innenverwaltung - Kommunales - Sparkassen

5.1 Innenverwaltung

5.1.1 Einführung einer Asylcard

In meinem 1. TB (5.3.2) hatte ich darauf hingewiesen, daß es Überlegungen gibt, eine sogenannte Asylcard einzuführen. Das TIM sieht ebenfalls auch die Vielzahl personenbezogener Daten, die auf der Karte gespeichert werden sollen, als einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen an. Es hat darauf verwiesen, daß es hierzu einer entsprechenden Rechtsgrundlage bedarf. Seitens des BMI ist eine Machbarkeitsstudie in Auftrag gegeben worden, deren Ergebnisse allerdings noch nicht vorliegen.

5.1.2 Vorschriften im Ausländerwesen

Allgemeine Verwaltungsvorschrift zum Ausländergesetz (AuslG-VV)

Zu dem mir zugeleiteten Referentenentwurf einer allgemeinen Verwaltungsvorschrift zum Ausländergesetz (AuslG-VV) habe ich Stellung genommen und zur Inanspruchnahme von Sozialleistungen empfohlen, eine datenschutzrechtlich präzise Formulierung vorzusehen und die Übermittlung von Daten nicht von der Ausübung des Ermessens abhängig zu machen. Bei Straf- und Bußgeldverfahren sieht § 76 Abs. 4 AuslG zur Übermittlung eine eindeutige Regelung vor, die in dem Entwurf der Verwaltungsvorschrift erweitert wurde. Soweit schon die Mitteilung der Einleitung eines strafrechtlichen Ermittlungsverfahrens vorgesehen wird, findet dies in § 76 Abs. 4 AuslG keine Rechtsgrundlage. Auch bei der Einstellung von Straf- oder Bußgeldverfahren nach § 170 Abs. 2 StPO oder der Ablehnung der Eröffnung des Hauptverfahren oder einem Freispruch besteht für die Übermittlung dieser Daten an die Ausländerbehörde keine Notwendigkeit. Das TIM hat sich meiner Auffassung angeschlossen. In Kraft getreten ist die Verwaltungsvorschrift noch nicht.

Allgemeine Verwaltungsvorschriften zum Ausländerzentralregister und zur Ausländerzentralregisterdurchführungsverordnung (AZR-DV)

Nachdem, wie im 1. TB (1.2.3) berichtet, die vorgetragenen Bedenken in der Verordnung zur Durchführung des Gesetzes für das Ausländerzentralregister nicht berücksichtigt worden waren, habe ich zum Entwurf einer allgemeinen Verwaltungsvorschrift zum AZRG und zur AZR-DV dem TIM empfohlen, auf Klarstellungen und Präzisierungen hinzuwirken. Die Vorschriften, die der Zustimmung des Bundesrats bedürfen, sind noch nicht in Kraft getreten.

Seit Dezember 1997 gibt es auch einen Entwurf zur Änderung des Gesetzes über das Ausländerzentralregister und zur Einrichtung einer Warndatei, der mir noch nicht vorliegt.

5.1.3 Übermittlung personenbezogener Daten bosnischer Bürgerkriegsflüchtlinge

Die Innenministerien der Länder wurden vom Bundesinnenministerium gebeten, die ihnen von den Ausländerbehörden übermittelten personenbezogenen Daten der bosnischen Bürgerkriegsflüchtlinge an eine beim Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) eingerichtete Projektgruppe zu übermitteln. Wie in einigen Ländern hatte auch das TIM zunächst im Hinblick auf die von mir geäußerten rechtlichen Bedenken von einer Übersendung personenbezogener Daten Abstand genommen. Im Zuge der

Diskussion wurde deutlich, daß Projekte für den Wiederaufbau nur genehmigt werden, wenn dem Antrag Listen beigefügt sind, in denen den wiederaufzubauenden Objekte sowohl Eigentümer als auch Wohnungsberechtigten zugeordnet waren. Da ohne die Angabe der genauen Herkunft der Flüchtlinge die finanzielle Förderung aus EU-Mitteln nicht möglich ist und die Zuständigkeit des Bundes für derartige Wiederaufbau- und Rückkehrprojekte unzweifelhaft gegeben ist, habe ich bezugnehmend auf § 21 Abs. 2 Satz 2 i. V. m. § 20 Abs. 2 Ziffer 6 ThürDSG meine ursprünglichen Bedenken für ausgeräumt angesehen.

5.1.4 Datenübermittlung aus Anlaß der Abschiebung von Vietnamesen

Der Ausländerbeauftragte der Landesregierung hatte mir gegenüber seine Besorgnis über die Übermittlung personenbezogener Daten im Rahmen des Vollzugs des Rückübernahmeabkommens für vietnamesische Staatsangehörige zum Ausdruck gebracht. Eine Prüfung des sogenannten Selbstangabe-Formulars (H.03) ergab, daß dies nicht eindeutig die Freiwilligkeit des Ausfüllens erkennen ließ. Bei den ausfüllenden Personen mußte auch der Eindruck entstehen, daß die Angaben in Deutschland verbleiben würden, was jedoch nicht der Fall war, da die Übermittlung der Daten an vietnamesische Behörden vorgesehen ist. Das TIM hat mir mitgeteilt, daß die Ausländerbehörden angewiesen wurden, den vietnamesischen Staatsangehörigen vor Abgabe der Selbstauskunft ebenfalls ein Merkblatt auszuhändigen, welches eindeutige Hinweise enthält Der in Rede stehende Vordruck H.03 steht auch in vietnamesischer Sprache zur Verfügung.

5.1.5 Ermittlungen im Rahmen von Scheineheverfahren gemäß § 92 Abs. 2 Nr. 2 AuslG

Nach § 17 Abs. 1 AuslG kann einem ausländischen Familienangehörigen eines deutschen Staatsangehörigen zum Zwecke des nach Artikel 6 GG gebotenen Schutzes von Ehe und Familie eine Aufenthaltserlaubnis für die Herstellung und Wahrung der familiären Lebensgemeinschaft mit dem Ausländer im Bundesgebiet erteilt und verlängert werden. Die Ausländerbehörden sehen sich hierbei dem Problem gegenüber, daß zum Zwecke der Aufenthaltserlaubnis mitunter eine „Scheinehe“ geschlossen wird, so daß nach § 75 Abs. 1 AuslG die Erhebung von Daten erforderlich wird. Der Umfang und die Art, wie die Ausländerbehörden hier zu Erkenntnissen kommen, die den Verdacht begründen, daß eine „Scheinehe“ vorliegt, birgt verschiedene datenschutzrechtliche Probleme. Mit Fragebögen versuchen die Ausländerbehörden zu ermitteln, ob der Verdacht einer „Scheinehe“ besteht, wobei die gestellten Fragen sehr weitgehend sind. Mein Hinweis an das TIM, daß ein in Thüringen verwandter Fragebogen hinsichtlich der meisten gestellten Fragen der Überarbeitung bedarf, wurde positiv aufgegriffen. Gemeinsam mit dem TIM wurde ein Fragebogen entwickelt, der auf nicht erforderliche Fragen verzichtet und die Ausländerbehörden in die Lage versetzen soll, die notwendigen Erkenntnisse zu gewinnen. Nachträglich wurde noch das Problem angesprochen, ob die Ausländerbehörden berechtigt sind, Befragungen (eventuell auch bei Nachbarn) vor Ort vorzunehmen, weil der Fragebogen allgemeine Fragen enthält, die hinsichtlich ihrer Grundangaben vorher zwischen den Eheleuten abgestimmt sein könnten. Ich habe hierzu die Auffassung vertreten, daß nach § 75 Abs. 2 AuslG ggf. auch Datenerhebungen bei Nachbarn erfolgen können, wobei bei derartigen Befragungen Zurückhaltung geboten ist. Der Umstand, daß bei Fragebögen Ehepartner deckungsgleiche Antworten geben, berechtigt allein nicht dazu, davon auszugehen, daß eine Nachbarbefragung angezeigt ist, da nicht automatisch aus deckungsgleichen Antworten die Schlußfolgerung zulässig ist, daß sich die Eheleute abgesprochen haben.

5.1.6 Veröffentlichung von Asylbewerberdaten

Im Rahmen einer Petition wurde mir vorgetragen, daß durch ein Verwaltungsgericht den bevollmächtigten Rechtsanwälten eines Asylbewerbers eine sogenannte Abgangsliste der Erstaufnahmeeinrichtung Tambach-Dietharz mit einer Vielzahl von Namen, Vornamen und Geburtsdaten von Asylbewerbern übermittelt worden war, obwohl die Bevollmächtigten nur einen der aufgeführten Asylbewerber im anhängigen Asylverfahren vertraten. Ich habe mich daraufhin mit dem zuständigen Verwaltungsgericht in Verbindung gesetzt und gebeten, mir mitzuteilen, weshalb diese Datenübermittlung erfolgt ist. Nach § 37 Abs. 4 ThürDSG beschränkt sich meine Zuständigkeit bei Gerichten nur auf Verwaltungsangelegenheiten, was hier zweifelhaft sein konnte, da unter Angabe eines verwaltungsgerichtlichen Aktenzeichens von einem Richter unterzeichnet die Liste übersandt worden ist, so daß ich das Verwaltungsgericht auch insoweit um Stellungnahme gebeten habe. Das Verwaltungsgericht hat es zwar als äußerst bedenklich im Hinblick auf § 37 Abs. 4 ThürDSG angesehen, ob die von Richtern verfügte Versendung der Listen im Rahmen einer Betreibensaufforderung nach § 81 AsylVfG meiner Kontrolle unterliegt, hat gleichwohl aber meinem Anliegen dadurch Rechnung getragen, daß künftig von einer Versendung der Listen abgesehen oder die Namen der nicht am Verfahren beteiligten Asylbewerber geschwärzt werden. Die Übersendung der Liste an das Verwaltungsgericht wurde vom Landratsamt veranlaßt, wobei man mir auf meine Anfrage mitteilte, daß versehentlich die Liste komplett ohne die Schwärzung nicht verfahrensbeteiligter Asylbewerber übermittelt wurde. Nachdem man mir versichert hatte, daß die Mitarbeiter der Ausländerbehörde noch einmal darüber belehrt wurden, den Datenschutz diesbezüglich genauestens einzuhalten, habe ich die Angelegenheit als abgeschlossen angesehen und den Petenten entsprechend informiert.

5.1.7 Verpflichtung zur Kostenübernahme nach § 84 Ausländergesetz (AuslG)

Die Ausländerbehörden machen eine Visumerteilung von der Vorlage einer Verpflichtungserklärung nach § 84 Abs. 1 AuslG abhängig. Bei der Abgabe der Verpflichtungserklärung wird ein Nachweis verlangt, daß der Gastgeber in der Lage ist, für die Kosten aufzukommen. Es werden vom Gastgeber Angaben zu seinen Wohnungs-, Einkommens- und Vermögensverhältnissen abverlangt. So muß er mitteilen, ob er Mieter oder Eigentümer der von ihm bewohnten Wohnung ist. Auch muß der Name des Arbeitgebers angegeben werden. § 84 AuslG stellt für derartige Datenerhebungen keine Rechtsgrundlage dar, sondern normiert nur die Verpflichtung, daß der Gastgeber die Kosten für den Lebensunterhalt des Ausländers zu tragen und ggf. verauslagte öffentliche Mittel zu erstatten hat. Das TIM hat sich meinen Bedenken angeschlossen und verlangt künftig nur noch die Vorlage einer Meldebescheinigung, einer Bankbürgschaft oder die Hinterlegung eines Sparbuchs.

5.1.8 Kontrolle der LAST und ZAST

Sowohl die Landesaufnahmestelle für Aussiedler (LAST) in Eisenberg als auch die Zentrale Anlaufstelle für Asylbewerber (ZAST) in Tambach-Dietharz, die zum TLVwA gehören, wurden von mir einer datenschutzrechtlichen Kontrolle unterzogen.

In der LAST stellte ich fest, daß alle Aussiedler in einer Registraturliste mit Namen, Vornamen, Herkunftsland, Geburtsdatum, Beruf und Konfession erfaßt werden, die in kopierter Form u. a. an die Diakonie, die Arbeiterwohlfahrt, den Sozialdienst, den Krankenbereich des DRK und das Arbeitsamt weitergegeben wurden. Es ist jedoch nicht einzusehen, daß von einem Be-

troffenen, der nicht krank ist, alle Daten an den Krankenbereich gemeldet werden oder an die betreffende Mitarbeiterin, die für die Bearbeitung von Anträgen auf Gewährung pauschaler Wiedereingliederungshilfe zuständig ist, gemeldet werden, obwohl nicht alle einen derartigen Antrag stellen. Mir wurde zugesichert, daß die Weitergabe der Liste künftig nur noch an die notwendigen Stellen erfolgt. Über die Verteilung der Betroffenen in Übergangswohnheime wird ebenfalls eine Liste erstellt, aus der sich ergibt, welche Person zu welchen Familienverbänden gehören, die an das jeweilige Übergangswohnheim weitergeleitet wird. Zur Praxis, täglich eine Kopie einer Liste über alle abreisenden Personen an die unterschiedlichsten Bereiche im Hause weiterzuleiten, erklärte sich schon während der Kontrolle die LAST bereit, auch hier das Verfahren zu ändern und gegenüber den Bereichen, in denen es nicht auf die Namen ankommt, auf deren Nennung zu verzichten. Eingestellt wurde auch das Verfahren, Arbeitsunfähigkeitsbescheinigungen der Mitarbeiter vor der Übersendung an die hierfür zuständige OFD - Zentrale Gehaltsstelle - im Original zu kopieren und über einen Zeitraum von bis zu einem Jahr aufzubewahren, da hierfür keine Notwendigkeit besteht. Bei der ZAST konnte ich feststellen, daß seit Ende 1995 ein Besucherbuch geführt wurde, in welchem Name, Vorname, Nationalität, Wohnanschrift des Besuchers sowie der Name des Besuchten, Zimmernummer und Beginn und Ende des Besuchs notiert wurden. Auf den Hinweis, daß eine so lange Aufbewahrung der Besucherdaten nicht erforderlich erscheint, wurde zugesichert, das Besucherbuch nur noch für den Zeitraum eines halben Jahres aufzubewahren. Ähnlich wird künftig auch mit den Ausgangskarten verfahren, die Asylbewerber erhalten, wenn sie die Einrichtung verlassen. Das bisherige Verfahren, diese Karten jeweils zu den Akten zu nehmen, wird eingestellt, da man eingesehen hat, daß dies auch nicht erforderlich ist. Die bisherige Praxis, die Leistungsakten von Asylbewerbern zu kopieren und eine Kopie an die aufnehmende Einrichtung zu übersenden, wenn Asylbewerber die Einrichtung verlassen, wird aufgegeben, da sich eine Erforderlichkeit für die Aufbewahrung und etwaige Auskunftserteilung nur auf den Zeitraum erstrecken kann, in dem sich ein Asylbewerber in der Zentralen Aufnahmestelle befand. Die ZAST hat auch meine Anregung aufgegriffen, die Vielzahl von Unterlagen, für die eine Aufbewahrungsnotwendigkeit über einen längeren Zeitraum nicht erkennbar ist, auf das notwendige Maß zu reduzieren.

5.1.9 Kontrolle im Thüringer Landesverwaltungsamt

Das Thüringer Landesverwaltungsamt (TLVwA) wurde im Berichtszeitraum auf Einhaltung technischer und organisatorischer Maßnahmen nach § 9 ThürDSG kontrolliert. Bei der Kontrolle wurden neben einigen organisatorischen Unzulänglichkeiten auf dem Gebiet des Datenschutzes insbesondere technische und organisatorische Mängel bei der Anwendung der automatisierten Datenverarbeitung festgestellt. Zum Zeitpunkt der Kontrolle stand von Seiten des TLVwA kein bDSB als Ansprechpartner zur Verfügung. Das gemäß § 10 ThürDSG zu führende Verfahrensverzeichnis, welches alle eingesetzten automatisierten Verfahren beinhalten muß, mit denen personenbezogene Daten verarbeitet werden, entsprach zum Zeitpunkt der Kontrolle nicht dem aktuellen Stand und den gesetzlichen Anforderungen gemäß § 10 Abs. 2 ThürDSG. Für eine erhebliche Anzahl eingesetzter automatisierte Verfahren konnten keine datenschutzrechtlichen Freigaben gemäß § 34 ThürDSG vom TLVwA vorgelegt werden, was ich beanstandet habe. Im TLVwA werden eine Vielzahl von Verfahren, mit denen personenbezogene Daten verarbeitet werden, eingesetzt. Die stichprobenhafte Kontrolle in einer Abteilung zeigte, daß den erforderlichen technischen und organisatorischen Maßnahmen gemäß § 9 ThürDSG hier nicht im ausreichenden Maß entsprochen wurde. Dies habe ich beanstandet. Es war festzustellen, daß in den kontrollierten Bereichen zumeist Sicherheitsmaßnahmen für diese Verfahren

ohne konzeptionellen Zusammenhang, zumeist sporadisch und im eigenen Ermessen der jeweiligen Mitarbeiter festgelegt wurden. Insbesondere fehlten verbindliche Regelungen und Vorgaben sowohl für ein sicheres Betreiben der vor Ort kontrollierten Verfahren, als auch bereichsübergreifende Richtlinien in Form eines IT-Sicherheitskonzeptes. In Einzelfällen waren so z. B. Sicherheitsmaßnahmen bezüglich der Zugriffe auf den Server nicht aktiviert, die Boot-/Setup- Paßwörter an den PC nicht eingerichtet, kein Schutz für Diskettenlaufwerke vorgesehen sowie Zugriffsrechte im Ermessen des Administrators eingerichtet. Desweiteren wurde festgestellt, daß an einen vernetzten PC mittels Modem ein Anschluß an das öffentliche Netz eingerichtet war, um den T-Online Dienst zu nutzen. Mit der Nutzung des T-Online Dienstes und dem damit verbundenen Zugang zum Internet wurde das lokale Netz des Referates ohne notwendige Schutzmaßnahmen den hiermit verbundenen Sicherheitsrisiken ausgesetzt (1. TB, 15.13). Das Modem war nicht in dem entsprechenden Geräteverzeichnis aufgeführt. Desweiteren wurde bei einer Stichprobe eines Verfahrens festgestellt, daß Daten-Felder, die zur Aufgabenerfüllung nicht erforderlich sind, nicht gesperrt waren, eine Auswertung der Protokollierung nicht durchgeführt wurde und erforderliche Regelungen (z. B. für Sicherheitsmaßnahmen und zur Paßwortgestaltung) nicht vorlagen. Für den Einsatz der TK-Anlage fehlten Festlegungen zu den eingerichteten Leistungsmerkmalen.
Zwischenzeitlich sind die festgestellten Mängel behoben worden. Nach Angaben des TLVwA sollte ein IT-Sicherheitskonzept bis Ende 1997 vorliegen. Eine Mitteilung, ob dies geschehen ist, liegt noch nicht vor.

5.2 Kommunales

5.2.1 Gästemeldeschein zur Werbung der Kurverwaltung?

Gemäß § 9 des Kommunalabgabengesetzes können Gemeinden, die ganz oder teilweise als Kurort oder Erholungsort staatlich anerkannt sind, von Personen, die sich zu Heil-, Kur- oder Erholungszwecken in diesem Gebiet aufhalten, ohne daß sie dort ihre Hauptwohnung im Sinne des Melderechts haben, einen Kurbeitrag erheben. Nach § 25 Abs. 3 ThürMeldeG können für die Zwecke der Erhebung des Kurbeitrages sowie für Zwecke der Fremdenverkehrs- und Beherbergungsstatistik die erforderlichen Daten mittels Durchschriften der von den Einrichtungen, die gewerbs- oder geschäftsmäßig fremde Personen beherbergen, gemäß § 24 ThürMeldeG zu führende Meldescheine erhoben werden. Da eine Übermittlung der erhobenen Daten an die Kurverwaltung jedoch nur im erforderlichen Umfang zulässig ist, dürfen die personenidentifizierenden Daten in der Durchschrift nicht enthalten sein. Zur Vereinfachung und um Mißverständnisse zu vermeiden wurde in die Thüringer Meldescheinverordnung das Muster eines für Beherbergungseinrichtungen verbindlichen Meldescheines aufgenommen, der diese Vorgaben erfüllt. Dieser für Beherbergungsstätten gemäß § 2 ThürMScheinVO vorgegebene Meldeschein war in einem Kurort auch gleichzeitig für die Erhebung und Nachweisführung des Kurbeitrages genutzt worden. Entgegen der Beschriftung des Meldescheines hatte jedoch die Kurverwaltung mit Anschreiben an die Beherbergungsstätten verfügt, daß ihr nicht der letzte, anonymisierte Durchschlag der Anmeldung zu übergeben ist, sondern die für den Betroffenen als Nachweis vorgesehene Belegdurchschrift, die noch den Namen und Heimatanschrift des Betroffenen enthält. Die Kurverwaltung wollte sich dadurch die Möglichkeit eröffnen, die Gäste auch nach ihrer Abreise über interessante Kurangebote zu unterrichten. Wegen der Zweckbindung der Meldedaten und der fehlenden Rechtsgrundlage für diese Datenübermittlung habe ich die Gemeinde darüber informiert, daß eine Übermittlung der Anschriften der Gäste an die Kurverwaltung zum Zwecke der Werbung nur auf Grundlage der Einwilligung der Betroffenen zulässig ist. Aufgrund meiner Hinweise wurde von der Kurverwaltung die Verfahrensweise sofort den

gesetzlichen Vorgaben entsprechend verändert und die Beherbergungsstätten davon unterrichtet. Um auch künftig für Werbezwecke die Anschriften ihrer Gäste zu erhalten, wurde die Kur- und Gästekarte umgestaltet. Sie enthält nunmehr einen Hinweis, daß diese nach Beendigung des Aufenthaltes bei der Kurverwaltung abgegeben werden kann, mit dem Ziel, die Anschriften für eigene Werbung der Kurverwaltung weiter nutzen zu können.

5.2.2 Online-Zugriff auf Meldedaten innerhalb von Gemeinden

Wie bereits in meinem 1. TB (5.2.3) festgestellt, werden im Rahmen der Einführung lokaler Netze innerhalb von Gemeindeverwaltungen häufig auch Online-Zugriffe auf Meldedaten durch die verschiedensten Ämter eingerichtet. Dies ist auch gemäß § 29 Abs. 7 ThürMeldeG innerhalb einer Gemeinde oder einer Verwaltungsgemeinschaft zulässig. Zu beachten ist dabei aber, daß zunächst von der jeweiligen Meldebehörde in Zusammenarbeit mit der anfordernden Stelle die Erforderlichkeit des Online-Zugriffs, insbesondere hinsichtlich der Datenarten und des zugriffsberechtigten Personenkreises, zu prüfen und kontrollfähig festzulegen ist. In der Praxis zeigt sich mitunter bei Kontrollen, daß aufgrund programmtechnischer Probleme und unter Berücksichtigung der Einsparung von Kosten ein für den Online-Zugriff einmal bestimmter Datensatz mehreren Bereichen oder Ämtern undifferenziert zur Verfügung gestellt wird, obwohl diese Stellen zur Aufgabenerfüllung nur einen Teil der Daten benötigen. Dies ist aus datenschutzrechtlichen Gründen unzulässig. Bei entsprechenden Feststellungen habe ich deshalb die Behörden aufgefordert, soweit eine Beschränkung des Datenzugriffs nicht auf das erforderliche Maß möglich ist, von der Einrichtung oder Nutzung eines Online-Zugriffs künftig abzusehen. Da diese Probleme nicht nur im Meldewesen, sondern regelmäßig bei der Einrichtung von Online-Verfahren auftreten können, empfiehlt es sich, daß alle beteiligten Stellen unter Einbeziehung des bDSB vor Erwerb bzw. der Entwicklung von automatisierten Verfahren die Möglichkeit und die Zulässigkeit der Einrichtung von Online-Zugriffen prüfen. Maßgeblich aus datenschutzrechtlicher Sicht ist dabei insbesondere neben der Beurteilung durch den bDSB die des Fachbereiches, der entsprechend seiner Aufgabenstellung für die Erhebung, Verarbeitung und Nutzung der Daten zuständig ist. Dort ist die Entscheidung über die Notwendigkeit der Datenverarbeitung, zur Vergabe von Zugriffsrechten sowie vorgesehenen Datenübermittlungen zu treffen. In Wahrnehmung dieser Verantwortung hat er darauf Einfluß zu nehmen, daß durch entsprechende Protokollierungen eine Kontrolle dieser Zugriffe und Übermittlungen jederzeit möglich ist. Der EDV-technische Bereich kann dabei nur die für die technische Umsetzung vermittelnde Stelle sein und nicht, wie mitunter auch bei Prüfungen der Eindruck entsteht, als „Herr der Daten“ und somit Entscheidungsbefugter zum Umgang mit den Daten in Erscheinung treten. In jedem Fall ist durch organisatorische Regelungen zu gewährleisten, daß Entscheidungen zur Einführung und Nutzung automatisierter Verfahren oder Abrufverfahren mit personenbezogenen Daten nicht nur aus wirtschaftlichen oder technologischen Gründen getroffen werden, ohne daß vorher die Erforderlichkeit und die Zulässigkeit der Datenflüsse geprüft wurde.

5.2.3 Unterlagen und Verfahren zur Führung des Melderegisters

Bereits in meinem 1. TB (5.2.2) habe ich dargelegt, daß in den Meldeämtern Thüringens die verschiedensten automatisierten Verfahren zur Führung der Melderegister genutzt werden. Bei Kontrollen war immer wieder festzustellen, daß die landesspezifischen Regelungen im Meldegesetz, insbesondere zum Datenumfang und zur Einrichtung von Auskunftssperren, nicht ausreichend realisiert werden. In diesen Fällen habe ich die Meldebehörden aufgefordert, geeignete Maßnahmen (z. B. Programmänderungen) zu ergreifen. Datenschutzrechtliche Prüfungen im Berichtszeitraum zeigten, daß mitunter

noch immer alte unbereinigte Meldekarteien der ehemaligen DDR genutzt werden. Soweit sich die Unterlagen nicht bereits in den kommunalen Archiven befanden und damit die entsprechenden archivrechtlichen Vorschriften greifen, habe ich diese Meldebehörden beanstandet und aufgefordert, unverzüglich die nach § 43 ThürMeldeG geforderte Löschung unzulässig gespeicherter Meldedaten vorzunehmen, was in allen Fällen auch erfolgt ist. Da in nächster Zeit mit einer ersten Änderung des Thüringer Meldegesetzes sowie einer Meldedatenübermittlungsverordnung zu rechnen ist, wird gerade auch die technische Umsetzung der Rechtsvorschriften eine wichtige Aufgabe der Meldeämter sein.

5.2.4 Melderegisterauskünfte an Adreßbuchverlage

Wie auch in den anderen Bundesländern und bereits in meinem 1. TB (5.2.4.7) erörtert, ist die Übermittlung von Meldedaten an Adreßbuchverlage ein Dauerthema. Immer wieder gibt es Anfragen aus der Bevölkerung, meist bei der Ankündigung oder nach Erscheinen von Adreßbüchern. Im Berichtszeitraum wurde wegen der Mißachtung der Bestimmungen des Thüringer Meldegesetzes im Ergebnis meiner Beanstandung die gesamte Auflage eines Adreßbuches eingezogen. Ursache dafür war insbesondere die unzulässige Datenübermittlung und Aufnahme von Personen unter 18 Jahren im Adreßbuch.
In einer Gemeinde kam es aufgrund von Mißverständnissen zur Veröffentlichung von Meldedaten. Die Betroffenen hatten beim Meldeamt bei der Ankündigung der Herausgabe des vorhergehenden Adreßbuches eine Widerspruchserklärung abgegeben. Sie hatten dazu einen Vordruck verwendet, der einen Hinweis enthielt, daß sich der Widerspruch nur auf die nächste Ausgabe des Adreßbuchs bezieht. Dieses übersehend, waren die Betroffenen davon ausgegangen, daß sie ihren Widerspruch gegen eine Datenübermittlung bis auf Widerruf gegenüber dem Meldeamt zum Ausdruck gebracht hätten. Da aber im Meldeamt kein erneuter Widerspruch eingelegt worden war, waren die Sperrvermerke im Melderegister automatisch gelöscht worden, mit der Folge, daß auch die Adressen derjenigen an den Adreßbuchverlag übermittelt wurden, die bei der ersten Ausgabe widersprochen haben.

Das Problem der Herausgabe von Meldedaten an Adreßbuchverlage hat insbesondere auch durch die technische Entwicklung eine neue Dimension erhalten. Es bestehen zunehmend auch Bestrebungen, Meldedaten zur Herstellung elektronischer Verzeichnisse zu nutzen. Darüber hinaus sollen Adreßverzeichnisse auch im Internet weltweit veröffentlicht werden. Gleichgültig, ob der Gesetzgeber wie in einigen Bundesländern durch gesetzliche Regelungen zu verhindern sucht, daß Meldedaten in elektronischer Form veröffentlicht werden, kann letztlich doch jedermann die gedruckten Verzeichnisse durch Einscannen in ein elektronisches Verzeichnis umwandeln und diese problemlos mit anderen Datenbeständen zusammenführen und nach beliebigen Kriterien auswerten. Ab dem Zeitpunkt der Veröffentlichung von Adreßbüchern sind die Daten öffentlich. Hier gibt es kaum rechtliche Möglichkeiten, zu verhindern, daß sich Dritte dieser Datenfülle uneingeschränkt bedienen. Dieser Entwicklung kann man sich schlecht entziehen. Es bedeutet aber, daß der einzelne Betroffene das Risiko einer Nutzung seiner Daten entgegen seinen Interessen immer schwerer abschätzen kann. Allein die Möglichkeit, daß durch die Nutzung von Daten aus Adreßbüchern gegen den Willen der Betroffenen diese belästigt werden können, sollten dem Gesetzgeber Anlaß geben, hinsichtlich der Datenübermittlung, die Erforderlichkeit zu überprüfen. Die bisher angewandte Widerspruchslösung zeigt, daß dieses Verfahren zur Gewährleistung des informationellen Selbstbestimmungsrechts der Bürger unter den geschilderten technischen Rahmenbedingungen nicht immer ausreicht, weil beispielsweise ein Teil der Einwohner die gesetzlich geforderten allgemeinen Bekanntmachungen darüber aus den

vielfältigsten Gründen nicht zur Kenntnis nehmen bzw. die Bedeutung ihres Widerspruchsrechts nicht kennen.

Gegenwärtig wird ein erstes Änderungsgesetz zum Thüringer Meldegesetz vorbereitet. Darin ist nach meiner Kenntnis vorgesehen, daß eine Datenübermittlung an Adreßbuchverlage nur für die Herausgabe von gedruckten Adreßbüchern zulässig sein soll. Darüber hinaus sollen im Rahmen des allgemeinen Widerspruchsrechts die Betroffenen die Möglichkeit erhalten, auch einer Veröffentlichung in einzelnen Teilen des Adreßbuchs (alphabetischer Teil/Straßenübersichten) zu widersprechen. Diese neuen Vorgaben können jedoch nach meiner Auffassung letztlich nicht das Grundproblem der unkontrollierten Nutzung von Meldedaten lösen. Aus datenschutzrechtlicher Sicht sollte auch deshalb, wie mittlerweile im letzten Jahr bereits in zwei Bundesländern beschlossen, die Einwilligung der Betroffenen als Grundlage einer Datenübermittlung an Adreßbuchverlage vorgesehen werden.

5.2.5 Zusendung einer falschen Geburtsurkunde

In der Eingabe eines Bürgers hatte dieser mir mitgeteilt, daß die Urkundenstelle der Standesämter anstelle der gewünschten eigenen Geburtsurkunde dem Bürger daraufhin die Geburtsurkunde einer ihm völlig fremden Person zugesandt hatte.
Auf meine Anfrage hin teilte mir das Landratsamt zu dem Vorfall mit, daß der datenschutzrechtliche Verstoß im Rahmen eines Disziplinarverfahrens gegen den hierfür verantwortlichen Standesbeamten ausgewertet wurde. Ich habe abschließend das betroffene Landratsamt aufgefordert, zukünftig dafür Sorge zu tragen, daß die erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, die die Wiederholung eines solchen Vorfalls ausschließen.

5.2.6 Kontrolle in einem Sozialamt

Bei einer Kontrolle in einem Sozialamt konnte ich Hinweise zu Maßnahmen aus technischer und organisatorischer Sicht vorschlagen, um die Rahmenbedingungen, unter denen Sozialdaten verarbeitet werden, zu verbessern. Obwohl bereits im 1. TB (12.4) als unzulässig dargestellt, wurden in diesem Sozialamt zu den Sozialhilfeformularen nach wie vor noch Zusatzbögen verwandt, mit denen Angaben zur letzten Schul- und Berufsausbildung erhoben wurden. Auch hier wurde als Erforderlichkeit die Durchführung der Bundesstatistik nach den §§ 127 ff. BSHG angeführt. Da es sich jedoch um eine sogenannte Sekundärstatistik handelt, bei der nur solche Daten zu statistischen Zwecken genutzt werden dürfen, die ohnehin im Rahmen der Verwaltungsaufgabe gebraucht werden, durfte eine eigens für diese Statistik erhobene Abfrage des höchsten Bildungsabschlusses und weiterer Angaben nicht erfolgen. Lediglich in den Fällen, in denen es zur Bearbeitung des Sozialhilfeantrages auf die Schulbildung ankommt (z. B. Hilfsmaßnahmen bezüglich einer Schul- oder Berufsausbildung), dürfen die Daten hierfür erhoben und anschließend im Rahmen der Sozialhilfestatistik weitergeleitet werden. Das Sozialamt hat daraufhin die Benutzung des Zusatzbogens eingestellt und wird Daten zur Schul- und Berufsausbildung nur noch dann erfragen und an das TLS weiterleiten, wenn dies für die Antragsbearbeitung im Sozialamt erforderlich ist. Dem Sozialhilfeantrag war ein vom Antragsteller auszufüllender Vordruck mit der Überschrift „Vermögenserklärung zur Vorlage beim Sozialamt“ beizufügen, worin Angaben zum Kontoinhaber, Kontonummer, Kontostand und Kontostand vor drei Monaten (auch von in Haushaltsgemeinschaften mit dem Antragsteller lebenden Familienmitgliedern) durch die Bank als richtig und vollständig bzw. nicht richtig bestätigt werden sollte. Auf der Rückseite sollten Angaben weiterer Vermögenswerte (Bausparverträge, Wertpapiere, Kapitalversicherung etc.) des Antragstellers

sowie von Familienmitgliedern gemacht werden. Diese „Vermögenserklärung“ wurde standardisiert bei jedem Sozialhilfeantrag abverlangt. Ein regelmäßiges Anfordern der Vorlage einer Bankbestätigung ohne Vorliegen konkreter Anhaltspunkte, daß die vom Hilfesuchenden abgegebene Erklärung zu den Vermögensverhältnissen unrichtig ist, stellt eine nach § 60 Abs. 1 Nr. 1 SGB I überflüssige und damit nicht erforderliche Ermittlungstätigkeit dar. Diese Praxis hatte das Sozialamt auf mein Bestreben hin eingestellt und wird zukünftig eine solche Bankbestätigung nur bei bestimmten Verdachtsmomenten verlangen. Dadurch, daß die Bankbestätigung als „Vermögenserklärung zur Vorlage beim Sozialamt“ überschrieben ist, wird der Betroffene dazu veranlaßt, seine Antragstellung auf Sozialhilfe gegenüber seiner Bank zu offenbaren. Darüber hinaus werden auch Daten seiner Familienangehörigen übermittelt. Ich habe das Sozialamt aufgefordert, daß zukünftig, soweit erforderlich, neutrale Vordrucke verwendet werden sollen, die gegenüber der Bank den Zweck der weiteren Verwendung nicht erkennen lassen sowie daß für jedes einzelne in der Haushaltsgemeinschaft lebende Familienmitglied ein gesonderter Vordruck zum Einsatz kommt. Im übrigen hat das Sozialamt bei der Entscheidung, ob eine Bankauskunft angefordert wird, zu prüfen, ob ein geringerer Eingriff in das Persönlichkeitsrecht dadurch möglich ist, daß die angegebenen Vermögenswerte des Antragstellers durch Vorlage von Sparbücher, Versicherungsscheinen oder Kontoauszügen oder anderer Unterlagen belegt werden können.

Das in der betreffenden Kommunalverwaltung praktizierte Verfahren zur Aufzeichnung und Abrechnung von Telefongebührendaten des Personals sah in einer mit dem Personalrat abgeschlossenen Dienstvereinbarung vor, daß eine detaillierte Aufstellung der von dem Bediensteten geführten Privatgespräche auf dessen Antrag nur gegen eine Gebühr von 20,00 DM erstellt wird. Dieser Betrag sollte darüber hinaus nur bei einem berechtigtem Widerspruch zurückerstattet werden. Diese Regelung konnte im Hinblick auf § 13 Abs. 1 Satz 1 Nr. 2 und Abs. 2 ThürDSG, nach dem der Betroffene Anspruch auf kostenlose Auskunft über die zu seiner Person gespeicherten Daten hat, nicht aufrechterhalten bleiben. Eine entsprechende Änderung der Dienstvereinbarung, die als Voraussetzung für den detaillierten Ausdruck von Privatgesprächen lediglich einen schriftlichen Antrag begründet, wurde zwischenzeitlich in Kraft gesetzt.

5.2.7 Übermittlung von Sozialdaten an Polizei und Ausländerbehörde

Häufig wird die Frage diskutiert, unter welchen Voraussetzungen die Sozialämter und Ausländerbehörden personenbezogene Daten von Betroffenen an Polizei und Strafverfolgungsbehörden übermitteln dürfen oder gar müssen. Im Berichtszeitraum erreichte mich ausgelöst durch Presseveröffentlichungen die Anfrage einer Sozialverwaltung, ob es datenschutzrechtlich zulässig sei, daß Mitarbeiter des Sozialamtes die Polizei verständigen, wenn sie einen im Sozialamt vorsprechenden Sozialhilfeempfänger als einen zur Fahndung ausgeschriebenen Straftäter erkannt haben. Dem anfragenden Sozialamt habe ich mitgeteilt, daß ich dies nach § 68 Abs. 1 SGB X für zulässig ansehe. Danach dürfen der Polizei Name, Geburtsdatum und -ort, die derzeitige Anschrift des Betroffenen sowie Namen und Anschriften seiner derzeitigen Arbeitgeber übermittelt werden. Unter den Begriff der derzeitigen Anschrift ist auch der momentane Aufenthalt des Betroffenen im Sozialamt zu fassen. Daher wäre auch eine Bestätigung durch Mitarbeiter des Sozialamts gegenüber der Polizei auf die telefonische Anfrage, ob der Betroffene sich derzeit im Sozialamt aufhält, zulässig. Das Sozialamt teilte meine Auffassung. Wie dieser Fall zeigt, gibt es zahlreiche Instrumente für die Strafverfolgungsbehörden zur Verbrechensbekämpfung. So haben in diesem Bereich Polizei und Staatsanwaltschaft bei der Durchführung von Strafverfahren wegen Verbrechen oder sonstiger Straftaten von erheblicher Bedeutung nach § 73

SGB X die Möglichkeit, aufgrund einer richterlichen Anordnung sich weitere Sozialdaten übermitteln zu lassen. Handelt es sich um ein gerichtliches Verfahren in Angelegenheiten des Sozialamtes, z. B. ein Strafverfahren wegen Subventionsbetrug, so darf das Sozialamt Daten des Betroffenen nach § 69 Abs. 1 Nr. 2 SGB X an Polizei und Staatsanwaltschaft übermitteln. Ohne eine richterliche Anordnung ist jedoch die Mitteilung des nächsten Vorsprachetermins oder gar die Führung regelrechter Fahndungslisten im Sozialamt nach geltendem Recht nicht möglich. Andernfalls würde dies dazu führen, daß die Sozialämter regelmäßig Aufgaben der Strafverfolgung übernehmen müßten, die ihnen jedoch nach dem Gesetz nicht zugewiesen sind.

Im Bereich der Ausländerverwaltung ist nach § 71 Abs. 2 SGB X i. V. m. § 76 Abs. 2 Ausländergesetz das Sozialamt nicht nur berechtigt, sondern verpflichtet, die Ausländerbehörde unverzüglich zu unterrichten, wenn es Kenntnis über einen Ausländer erlangt, der keine gültige Aufenthaltsgenehmigung oder Duldung besitzt. Daher darf außer dem momentanen Aufenthalt des Betroffenen im Sozialamt auch ein zukünftig vereinbarter Termin der Ausländerbehörde mitgeteilt werden. Im Rahmen der Verhältnismäßigkeit kommt aber zunächst nur die Mitteilung des gewöhnlichen Aufenthaltsorts in Frage, soweit ein solcher vom Betroffenen angegeben wurde.

5.2.8 Verarbeitung von Sozialhilfedaten bei Privatunternehmen?

Ein Landratsamt fragte an, ob eine Verarbeitung der Sozialhilfedaten des Landratsamtes durch ein Privatunternehmen im Auftrag des Sozialamtes zulässig wäre. Dabei war beabsichtigt, dem Auftragnehmer auf dessen Rechner den gesamten Sozialhilfedatenbestand des Sozialamtes zu übergeben. Eine klare Antwort auf diese Frage gibt § 80 Abs. 5 SGB X, wonach eine Auftragsdatenverarbeitung durch nicht-öffentliche Stellen nur dann zulässig ist, wenn die übertragenen Arbeiten vom Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfaßt. Der überwiegende Teil der Speicherung des Gesamtdatenbestandes muß dabei beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist, verbleiben. Zielrichtung dieser Vorschrift ist, daß im Regelfall sensible Sozialdaten im Einflußbereich der Sozialleistungsträger oder zumindest bei öffentlichen Stellen bleiben sollen. Selbst wenn die Datenverarbeitung beim Auftragnehmer erheblich kostengünstiger besorgt werden könnte, lag hier die Voraussetzung nicht vor, den gesamten Datenbestand an einen privaten Auftragnehmer weiterleiten zu können. Das Landratsamt hat daraufhin ein Rechenzentrum beauftragt, das in öffentlicher Trägerschaft betrieben wird. Gegen eine solche Auftragsdatenverarbeitung bestanden keine Bedenken, sofern die sonstigen Voraussetzungen nach § 80 SGB X eingehalten werden.

5.2.9 Umgang mit Altdaten aus ehemaligen Polikliniken

Nach langwierigen Abstimmungen wurden am 03.06.1996 „Gemeinsame Hinweise und Empfehlungen des Thüringer Ministeriums für Soziales und Gesundheit und des Thüringer Innenministeriums zur Aufbewahrung und Nutzung von Patientenunterlagen aus Gesundheitseinrichtungen der ehemaligen DDR“ (ThürStAnz. 1996, S. 1287) veröffentlicht. Auf das Fehlen solcher Regelungen war von mir im 1. TB (11.3.1) hingewiesen worden. Adressaten der Hinweise sind Gemeinde, Städte und Landkreise des Freistaats Thüringen, die die uneingeschränkte Verantwortung für die Aufbewahrung dieser Unterlagen unter Wahrung des Arztgeheimnisses und der Gewährleistung weitergehender datenschutzrechtlicher Anforderungen zu tragen haben. In diesen Hinweisen wird die bereits bisher praktizierte Verfahrensweise befürwortet, die Patientenunterlagen dem örtlich zuständigen Gesundheitsamt zur Verwahrung zu übergeben. Von diesem ist durch geeignete techni-

sche und organisatorische Maßnahmen sicherzustellen, daß ein unbefugter Zugriff bzw. eine unbefugte Nutzung ausgeschlossen ist. Die Unterlagen sind entsprechend den gesetzlichen Fristen aufzubewahren, wobei den Patienten ein Auskunfts- bzw. Einsichtsrecht zusteht. Im Berichtszeitraum wurde ich mehrfach mit Fragen der Umsetzung dieser gemeinsamen Hinweise und Empfehlungen befaßt. Dabei habe ich das TMSG gebeten, sich in den Kreisen und kreisfreien Städten einen Überblick darüber zu verschaffen, in welchem Umfang Poliklinikakten von Betriebspolikliniken bei den Gesundheitsämtern aufbewahrt werden. Eine vom TMSG durchgeführte Umfrage ergab, daß der überwiegende Teil der Akten der Betriebspolikliniken in den Gesundheitsämtern der Landkreise und kreisfreien Städte archiviert ist. Darüber hinaus wurde ein Teil der Patientenakten von den ehemaligen behandelnden und nunmehr frei praktizierenden Ärzten übernommen, was nach den o. g. Hinweisen unter der Nr. 4 dann als zulässig angesehen wird, wenn der Patient eingewilligt hat. Eine Einwilligung kann auch darin gesehen werden, daß der Patient sich weiter in der Behandlung des betreffenden Arztes befindet. Vereinzelt werden auch von Nachfolgebetrieben Betriebspoliklinikunterlagen dem zuständigen Gesundheitsamt zur Archivierung übergeben. Soweit es sich um Akten aus Betriebspolikliniken der Wismut handelt, so werden diese mit Wirkung vom 01.10.1996 durch die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin verwaltet.

Daß allein rechtliche Regelungen nicht ausreichen, den Patientenakten aus staatlichen Einrichtungen des Gesundheitswesens der ehemaligen DDR den notwendigen Schutz vor unbefugter Einsichtnahme zu gewährleisten, sondern deren praktische Umsetzung maßgeblich ist, wurde bei einer Kontrolle in einem Gesundheitsamt deutlich. Hier waren die Unterlagen in Kellerräumen eines Privatgebäudes gelagert, deren Türen und Fenster nahezu gewaltfrei durch Unbefugte geöffnet werden konnten. Unmittelbar am Wochenende vor meiner Prüfung hatten Unbekannte den Nachweis dafür erbracht. Erst durch den Einbruch in Kellerräume des Amtes und in Auswertung meiner Prüfung war man sich bewußt geworden, daß die bisherigen technischen und organisatorischen Maßnahmen völlig unzureichend waren, um Unbefugten den Zugang zu den besonders schützenswerten personenbezogenen Daten zu verwehren. Aufgrund meiner Beanstandung wurden von den Verantwortlichen sofort alle notwendigen Maßnahmen für eine künftig sichere Verwahrung der Akten eingeleitet.

Ein Gesundheitsamt beabsichtigte, die Archivierung der Patientenunterlagen einem Privatunternehmen zu übertragen, das sich auf die Archivierung von Akten spezialisiert hatte. Da es sich hierbei um einen Fall von grundsätzlicher Bedeutung handelte, habe ich mich zur Bewertung, unter welchen Voraussetzungen eine solche externe Archivierung als zulässig anzusehen ist, mit dem TIM, dem TMSG sowie dem TMJE im Verbindung gesetzt. In Übereinstimmung mit allen drei Ministerien gehe ich davon aus, daß eine Archivierung der Poliklinikakten außerhalb der Räume des Gesundheitsamtes außer mit Einwilligung des jeweils Betroffenen nur zulässig ist, wenn ausgeschlossen ist, daß die Mitarbeiter des Archivierungsunternehmens die Möglichkeit erhalten, unbemerkt Zugriff sowohl auf den Namen desjenigen, über den eine Patientenakte angelegt worden ist wie auch auf den Inhalt der Akte nehmen zu können. Dies kann beispielsweise dadurch geschehen, daß die Akten in verschlossenen Behältnissen aufbewahrt werden, auf deren Inhalt die Mitarbeiter des Archivierungsunternehmens keinen Zugriff haben (sogenannte „Container-Lösung“). Durch das TMJE wurden meine zunächst geäußerten Zweifel, ob auch hinsichtlich der außerhalb des Gesundheitsamtes gelagerten Behältnisse der Beschlagnahmeschutz des § 97 StPO greift, entkräftet, indem die Auffassung vertreten wird, daß auch die dem Gesundheitsamt übergebenen Unterlagen als Fälle des abgeleiteten Gewahrsams dem Schutzbereich des § 203 StGB unterliegen. Für die Beschlagnahmefrei-

heit nach § 97 Abs. 2 Satz 1 StPO wird vorausgesetzt, daß sich die Unterlagen im Gewahrsam eines zeugnisverweigerungsberechtigten Arztes befinden. Dabei genüge Mitgewahrsam. Sofern die tatsächliche Zugriffsmöglichkeit der Mitarbeiter des Archivunternehmens auf die Unterlagen in den verschlossenen Behältnissen nicht gegeben sei, steht den Mitarbeitern des Archivierungsunternehmens neben dem Gesundheitsamt lediglich ein Mitgewahrsam zu, so daß diese Unterlagen nicht der Beschlagnahme unterliegen. Zwischenzeitlich hat das TMSG die Gesundheitsämter über diese einvernehmliche Rechtsauffassung zur Zulässigkeit der externen Archivierung von Patientenunterlagen informiert (vgl. auch 11.11 zur externen Archivierung von Krankenhausakten).

5.2.10 Vorsorgeuntersuchung in Kindertagesstätten durch den Jugendgesundheitsdienst

Aufgrund einer Anfrage hatte ich mich mit dem Problem der Datenerhebung und -verarbeitung bei Vorsorgeuntersuchungen durch den jugendärztlichen Dienst in Tageseinrichtungen beschäftigt. Dabei war ich im konkreten Fall gebeten worden, daß von einem Gesundheitsamt den Eltern übergebene Informationsschreiben mit beigefügten Fragebogen einer datenschutzrechtlichen Prüfung zu unterziehen. Gemäß § 15 KitaG führt der öffentliche Gesundheitsdienst jährlich in den Tageseinrichtungen eine ärztliche und zahnärztliche Vorsorgeuntersuchung der Kinder durch. Voraussetzung dafür ist die Zustimmung der Erziehungsberechtigten. Aus dem im vorliegenden Fall den Eltern übergebenen Fragebogen zur Erstuntersuchung konnte dies nicht entnommen werden, da ausschließlich ein Hinweis zur Freiwilligkeit der Ausfüllung des Vordrucks nicht aber zur Untersuchung selbst enthalten war. Aufgrund der Tatsache, daß im Rahmen der freiwilligen Vorsorgeuntersuchung durch den Arzt Daten der Kinder erhoben werden, bedarf es gemäß § 4 ThürDSG einer entsprechenden Unterrichtung der betroffenen Eltern und deren schriftlicher Einwilligung. Darüber hinaus bedarf es gleichfalls einer Einwilligung der Eltern, wenn die Untersuchungsdaten der Vorsorgeuntersuchungen in den Kindertagesstätten in die Unterlagen der schulärztlichen Untersuchungen übernommen werden sollen. Eine Kopplung der Vorsorgeuntersuchungen im Kindergarten, die freiwillig sind, mit denen der Pflichtuntersuchungen in den Schulen ist mangels einer entsprechenden Rechtsnorm nur mit Einwilligung möglich. Aufgrund meiner Empfehlungen wurden die Fragebögen überarbeitet unter zusätzlicher Aufnahme einer Erklärung, daß bei den Untersuchungen die jeweiligen Erzieherinnen anwesend sein dürfen.

5.2.11 Einladung zur amtsärztlichen Untersuchung mit Postkarte

In der Eingabe eines Bürgers hatte sich dieser darüber beschwert, daß sein Sohn mittels einer Postkarte von einem Gesundheitsamt dazu aufgefordert wurde, sich zu einer amtsärztlichen Untersuchung einzufinden. Darüber hinaus war dieser Karte zu entnehmen, daß die Untersuchung „auf Antrag des Sozialamts“ erfolgt und der „Befund vom Hausarzt“ mitzubringen ist. Ich hatte daraufhin dem Gesundheitsamt mitgeteilt, daß durch die Verwendung einer Postkarte mit personenbezogenem Inhalt, unbefugte Dritte Rückschlüsse auf die Beziehung des Betroffenen zu einem Sozialleistungsträger ziehen können. Der Bürger hat ein berechtigtes, schutzwürdiges Interesse an der Geheimhaltung der auf der Postkarte aufgeführten persönlichen und sachlichen Verhältnisse. Eine unbefugte Offenbarung dieser Verhältnisse kann bei einer offenen Versandart, wie dies bei einer Postkarte gegeben ist, aber nicht ausgeschlossen werden. Die öffentliche Stelle hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, personenbezogene Daten der Bürger zu schützen. Nach § 9 Abs. 3 ThürDSG zählt hierzu auch, daß beim Transport ein unbefugter Zugriff der Daten durch

Dritte zu verhindern ist. Das Gesundheitsamt bedauerte diesen Vorfall außerordentlich. Die Mitarbeiter wurden schriftlich darüber belehrt, künftig alle Vorladungen und Untersuchungsaufforderungen nur noch in verschlossenen Umschlägen zu versenden.

5.2.12 Kontrolle eines Jugendamtes

In einem Jugendamt habe ich im Berichtszeitraum eine datenschutzrechtliche Kontrolle durchgeführt, bei der u. a. die technischen und organisatorischen Maßnahmen zur Datensicherheit überprüft wurden. Dabei wurde festgestellt, daß die schriftlichen Freigaben der in der Behörde eingesetzten Verfahren zur automatisierten Verarbeitung personenbezogener Daten nicht vorlagen. Entsprechende Freigaben wurden im Ergebnis meiner Beanstandung nachgeholt. Es wurden weiter Hinweise gegeben, um das Datenschutzniveau zu verbessern. So wurden auf meine Anregung hin z. B. Regelungen für einen Zugriff auf die Unterlagen im Bedarfsfall auch durch den Vertreter bzw. den Vorgesetzten getroffen, Sicherungskopien der Datenverarbeitung in einem feuersicheren Schrank untergebracht sowie die Mitarbeiter zum regelmäßigen Paßwortwechsel verpflichtet. Im Zuge der Kontrolle wurde ein vom Jugendamt selbst entwickeltes Formular vorgelegt, das im Zusammenhang mit der Bearbeitung von Unterhaltsangelegenheiten von unter der Vormundschaft des Jugendamtes stehenden Mündeln Verwendung findet. Darin wurden vom Unterhaltspflichtigen neben Name, Wohnanschrift, Beruf und Arbeitgeber u. a. auch der Name und die Anschrift der Krankenkasse erfragt. Außerdem sollte der Unterhaltspflichtige in einer kleingedruckten Erklärung versichern, daß die Angaben nach bestem Wissen und Gewissen abgegeben wurden, sowie, daß Arbeitsdienstbescheinigungen beim jeweiligen Arbeitgeber angefordert und beim Finanzamt Auskünfte über Einkommens- und Vermögensverhältnisse erfragt werden können. Auf meine Anregung hin wurde die sehr pauschal gehaltene Einwilligungserklärung, die im übrigen auch nicht gesondert von der Versicherung der wahrheitsgemäßen Angaben getrennt unterschrieben werden sollte, aus dem Vordruck entfernt. Ferner wurde ein klarer Hinweis auf die Zwecke und die Rechtsgrundlagen für die Erhebung der benötigten Daten auf dem Vordruck aufgenommen. Inhaltlich wurde von mir die regelmäßige Abfrage von Name und genauer Anschrift der Krankenkasse kritisiert, da hierfür keinerlei Erforderlichkeit ersichtlich war. Nach Auffassung des Jugendamts sei die Angabe der Krankenkasse notwendig, damit möglicherweise von der Krankenkasse an den Unterhaltspflichtigen zu zahlendes Krankengeld gepfändet werden kann, falls dieser seine Zahlungen auf freiwilliger Basis einstellen sollte. Nach § 55 SGB VIII wird eine Amtspflegschaft bzw. Amtsvormundschaft durch einzelne Beamte des Jugendamtes ausgeübt, die nach § 56 Abs. 1 SGB VIII die Vorschriften des BGB zu beachten haben. Soweit es sich um einen Auskunftsanspruch des Kindes gegenüber dem Unterhaltspflichtigen handelt, ist hier § 1605 BGB einschlägig. Aufgrund von § 68 Abs. 1 SGB VIII darf der Amtsvormund aber Sozialdaten nur erheben, soweit sie für seine Aufgabenerfüllung erforderlich sind. Hierzu zählt zwar auch die Pfändung von Krankengeld, sofern der Verpflichtete seinen Unterhaltspflichten nicht (mehr) nachkommt und einen Anspruch auf Krankengeld gegenüber seiner Krankenkasse hat. Dies rechtfertigt jedoch nur dann die Erhebung und Speicherung der Adresse der Krankenkasse des Verpflichteten, wenn dieser tatsächlich seinen Verpflichtungen im Einzelfall nicht nachkommt. Eine regelmäßige Erhebung von Daten über die jeweilige Krankenkasse im Zusammenhang mit der Ermittlung der Höhe der Unterhaltsforderung stellt daher eine unzulässige Datenvorratshaltung dar. Das Jugendamt habe ich über meine Beurteilung unterrichtet und aufgefordert, die regelmäßige Erhebung dieses Datums zukünftig zu unterlassen. Gleichzeitig habe ich das TMSG gebeten, die Jugendämter im Zuständigkeitsbereich über meine Einschätzung zu informieren. Sowohl das Jugendamt als auch das TMSG haben sich meiner Beurteilung angeschlos-

sen. Das Jugendamt hat den entsprechenden Bogen überarbeitet, der zukünftig keine Angaben über die Krankenkasse des Unterhaltspflichtigen mehr enthält.

5.2.13 Verwaltungsvereinfachung zu „einfach“

Zur Beurteilung eines Unterhaltsanspruches und ggf. zur Festsetzung des Unterhalts im Wege einer außergerichtlichen Einigung hatte ein Sorgeberechtigter das zuständige Jugendamt bevollmächtigt, Auskünfte beim unterhaltspflichtigen Elternteil einzuholen. Mit Übersendung der angeforderten Unterlagen hatte der Unterhaltspflichtige das Jugendamt gleichzeitig um die Beantwortung einiger Fragen hinsichtlich der Möglichkeit der Berücksichtigung bzw. Vernachlässigung von Einkommensbestandteilen bzw. sonstigen Ausgaben bei der Berechnung des Unterhaltsanspruchs gebeten. Im Antwortschreiben des Jugendamtes waren dem Betroffenen zunächst seine gestellten Fragen beantwortet und im weiteren der berechnete Unterhaltsbetrag mitgeteilt worden. Der geschiedene Ehepartner erhielt „zur Vereinfachung der Verwaltung“ eine Kopie dieses Schreibens. Diese Verfahrensweise entspricht nicht den datenschutzrechtlichen Bestimmungen, da sich der Inhalt des ersten Teils des Schreibens ausschließlich auf die Beantwortung von Fragen richtete, die vom Betreffenden an das Jugendamt im Hinblick auf dessen beratender Funktion gerichtet waren. Die Übermittlung dieser Sachverhalte an den geschiedenen Ehepartner war weder zur Erfüllung der Aufgaben des Jugendamtes erforderlich bzw. noch lag ein berechtigtes Interesse des geschiedenen Ehepartners an der Kenntnis dieser Daten vor. Der geschiedene Ehepartner hat zwar gegenüber dem Betroffenen ein Recht auf Informationen zur Feststellung der unterhaltsrechtlichen Leistungsfähigkeit, gleichwohl ist es dem Jugendamt nicht gestattet, diese Informationen unaufgefordert zu übermitteln, insbesondere wenn sie Tatsachen enthalten, die bei der Beurteilung des Leistungsvermögen unberücksichtigt bleiben können. Ich habe dem Jugendamt meine Rechtsauffassung mitgeteilt und gebeten, dies künftig zu beachten.

5.2.14 Festsetzung von Elterngebühren für die Benutzung von Kindertageseinrichtungen

In Thüringen wird im Kindertageseinrichtungsgesetz (KitaG) bestimmt, daß zur Finanzierung der Betreuung in Kindertagesstätten teilweise Beiträge von den Erziehungsberechtigten zu erheben sind. Die örtlichen Träger haben dabei eine soziale Staffelung der Beiträge vorzunehmen. Das TMSG gibt den Trägern hierfür Empfehlungen. In der Praxis bestimmen die Kommunen selbst das anzuwendende Verfahren. Grundsätzlich wird ein Durchschnittssatz bestimmt, der von allen Eltern zu zahlen ist. Da nicht alle Erziehungsberechtigte finanziell in der Lage sind, diesen zu tragen, bestimmen die Kommunen durch Satzung die Höhe und Staffelung der Gebühren. Die Satzung besitzt Rechtsnormcharakter und ist damit für die entsprechenden kommunalen Einrichtungen verbindlich. Eine Stadtverwaltung hatte die Eltern von Kindern, die eine Kindertagesstätte besuchen, über die neue Gebührensatzung und die daraus sich ergebenden Datenerhebungen sowie die Zweckbestimmung der Daten ordnungsgemäß unterrichtet. Gleichzeitig hatte sie den Eltern zur Neufestsetzung der Elterngebühren für die Benutzung von Kindertageseinrichtungen einen Vordruck als Bescheinigung über den Arbeitsverdienst übergeben, auf dem die Arbeitgeber der Eltern für jeden einzelnen Monat detailliert die Bruttobezüge sowie die von ihm verrechneten gesetzlichen und sonstigen Abzüge eintragen und unterzeichnen sollten. Darüber hinaus sollten die Betroffenen weitere Angaben über die wirtschaftlichen Verhältnisse des Haushaltes (Einkünfte und Ausgaben) machen und diese durch geeignete Unterlagen nachweisen. Die Bewertung ergab, daß der Umfang der Datenerhebung, insbesondere im Vordruck zur Bescheinigung über

den Arbeitsverdienst, nicht erforderlich war. Nach der geltenden Gebührensatzung waren die betroffenen Eltern nur verpflichtet, Auskünfte über ihr monatliches Einkommen zu erteilen und entsprechend nachzuweisen. Detaillierte Angaben über die Einkommensbestandteile oder gar gesetzliche Pflichtabzüge waren nach der Satzung nicht vorgesehen. Darüber hinaus fehlte im Vordruck ein Hinweis, daß bei der Vorlage geeigneter Unterlagen Daten gelöscht bzw. geschwärzt werden konnten, die für die Festsetzung der Gebühren nicht erforderlich sind. Auf Rückfrage beim zuständigen Jugendamt wurde mir mitgeteilt, daß die übergebenen Vordrucke nur als Unterstützung den Eltern übergeben worden waren und keinesfalls als verbindlich betrachten werden sollten. Um Mißverständnisse zu vermeiden erhielten deshalb die betroffenen Eltern in den Kindereinrichtungen dazu eine ergänzende Information mit dem Hinweis, daß auch andere geeignete Einkommensnachweise vorgelegt werden können. Künftig wird auf jeglichen Einkommensnachweis verzichtet, wenn aufgrund der Höhe des monatlichen Einkommens (nach der geltenden Satzung von über 6.000,- DM) ohnehin der Höchstbeitrag gezahlt werden muß.

5.2.15 Datenerhebung durch Jugendämter bei Kindertageseinrichtungen

Ein freier Träger einer Kindertageseinrichtung hatte sich bei mir erkundigt, ob es datenschutzrechtlich zulässig wäre, auf Aufforderung der Stadt, eine Namensliste mit Geburtsdatum und Anschrift aller für einen Platz angemeldeten Kinder zu übermitteln. Ich habe mich deshalb an die Stadt gewandt und dort darauf hingewiesen, daß die Erhebung von Sozialdaten bei Kindertageseinrichtungen datenschutzrechtlich unzulässig ist, weil weder § 62 SGB VIII noch eine spezialgesetzliche Rechtsvorschrift dies erlaubt. Begründet wurde die Anforderung der Listen von der Stadtverwaltung insbesondere mit dem Nachfrageverhalten der Eltern, die teilweise ihre Kinder in mehreren Kindertageseinrichtungen anmelden und nach Zusage bezüglich der übrigen Plätze keine fristgerechte Absage erteilen würden. Außerdem würden aus verschiedenen Gründen einige Tageseinrichtungen bevorzugt, während sich für andere nur wenige Eltern entscheiden würden. Die Erhebung der Daten durch das Jugendamt sei erforderlich für die Aufstellung eines genauen Bedarfplanes für die einzelnen Wohngebiete. Aufgrund meines Hinweises hat die Stadt mir daraufhin mitgeteilt, daß sie ihren Anmeldemodus geändert hat. Die freien Träger müssen künftig nur noch die Anzahl der Anmeldungen, das Alter der Kinder und das Wohngebiet bzw. die Straße melden.

Zusätzlich habe ich gegenüber dem TMSG die Problematik geschildert und darauf hingewiesen, daß eine solche Übermittlung von namentlichen Listen nur zulässig wäre, wenn der Landesgesetzgeber das KitaG um einen entsprechenden Passus ergänzen würde. Das TMSG hat daraufhin erklärt, daß die listenmäßige Übermittlung von Name, Anschrift und Alter der in den Tageseinrichtungen angemeldeten Kinder für die Bedarfsplanung nicht erforderlich sei und ein Änderungsbedarf im KitaG daher nicht bestehe.

5.2.16 Umgang mit Unterlagen nicht-öffentlicher Sitzungen

Einem Pressebericht zufolge waren in einer Stadt Unterlagen aus einer nicht-öffentlichen Sitzung des Stadtrates bei der Räumung einer Privatwohnung gefunden worden. Dies gab mir Anlaß, vor Ort den Umgang mit Unterlagen aus nicht-öffentlichen Sitzungen des Stadtrates zu überprüfen.
Bei der Kontrolle in der Stadtverwaltung habe ich festgestellt, daß die bisherige Verfahrensweise und die Regelungen zum Umgang mit den Unterlagen nicht-öffentlicher Sitzungen nicht ausreichend den datenschutzrechtlichen Anforderungen genügten. Insbesondere die Praxis, regelmäßig alle Vorlagen und Protokolle nicht-öffentlicher Sitzungen auf Dauer den Stadtratsmitgliedern sowie den Amtsleitern zu überlassen, eröffnete vielfältige Möglichkei-

ten für Unbefugte, in diese Unterlagen einsehen zu können. Im weiteren gab es auch keine besonderen technischen oder organisatorischen Vorkehrungen zum Schutz geheimhaltungsbedürftiger Unterlagen. Inwieweit dies jedoch ursächlich im Zusammenhang mit dem festgestellten Verstoß gegen geltendes Datenschutzrecht stand, konnte dabei nicht geklärt werden. Im Ergebnis des Vorfalls und der Überprüfung wurde die Dienstanweisung zur Vorbereitung und Ausführung der Beschlüsse des Stadtrates in der Stadtverwaltung dahingehend geändert, daß künftig Vorlagen für nicht-öffentliche Sitzungen mit dem Aufdruck „Nicht-öffentlicher Teil“ und mit einer persönlichen lfd. Nummer des jeweiligen Empfängers (Stadtrat) gekennzeichnet werden. Schriftliche Begründungen zu den Vorlagen werden so abgefaßt, daß ggf. auf einzelne Angaben oder Ausführungen aufgrund schutzwürdiger Interessen einzelner oder des Allgemeinwohls verzichtet wird. Bei Bedarf können dann im Sitzungsverlauf ergänzende Angaben gemacht werden. Im Beschlußtext wird künftig aufgenommen, ob und wann eine Geheimhaltung aufgehoben wird. In Umsetzung der Bestimmungen des § 42 ThürKO, wonach Ratsmitgliedern jederzeit Einsicht in Niederschriften zu geben ist und darüber hinaus Abschriften der in öffentlichen Sitzungen gefaßten Beschlüsse zu erteilen sind, werden die Beschlüsse künftig nur noch den jeweils zuständigen Ämtern übergeben, während das Sitzungsprotokoll nur in einem Exemplar angefertigt und für eine mögliche Einsichtnahme beim Sitzungsdienst unter Verschluß verwahrt wird. Eine Versendung erfolgt nicht mehr. Die Einsichtnahmen werden protokolliert. Nach der abschließenden Beratung werden Unterlagen nicht-öffentlicher Sitzungen dem Sitzungsdienst zurückgegeben.

Sowohl vom Bürgermeister wie auch den Stadtratsmitgliedern sind die Belange des Datenschutzes auch zu beachten. Gemäß § 12 Abs. 3 ThürKO sind Ratsmitglieder verpflichtet, über die ihnen bei der Ausübung des Ehrenamtes bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren, soweit nicht diese Tatsachen offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Die Pflicht zur Verschwiegenheit besteht, wie in den einschlägigen Kommentierungen zur ThürKO vermerkt ist, auch gegenüber Parteien, Wählergruppen und Wählern und natürlich auch gegenüber der Presse. Die Verschwiegenheit bezieht sich dabei auf alle Angelegenheiten, deren Geheimhaltung ihrer Natur nach erforderlich ist oder die besonders vorgeschrieben ist. Jede Übermittlung von personenbezogenen Daten an einen Unbefugten ist damit ein Verstoß gegen datenschutzrechtliche Bestimmungen. Aufgrund des Charakters nicht-öffentlicher Sitzungen ist es selbstverständlich, daß die dort bekanntgewordenen Tatsachen der Geheimhaltung unterliegen und die Daten nur für die Zwecke genutzt werden dürfen, zu denen sie erhoben wurden. Für Kreistagsmitglieder gilt nach § 94 ThürKO entsprechendes.

Im Hinblick auf mögliche Verstöße gegen datenschutzrechtliche Bestimmungen durch einzelne Gemeinderats- oder Kreistagsmitglieder besteht im übrigen mit dem TIM dahingehend Einvernehmen, daß gegebenenfalls die Adressaten für erforderliche Beanstandungen durch den TLfD gemäß § 39 ThürDSG die jeweilige Gemeindeverwaltung oder das Landratsamt sind. Begründet wird dies damit, daß Gemeinderats-/Kreistagsmitglieder Teil des Organs Gemeinderat/Kreistag sind, die wiederum im weiteren Sinn Teil der Verwaltung der Gemeinde bzw. des Landkreises sind, und ihnen die Daten bei Ausübung des Ehrenamts bekanntgegeben werden. Die Beanstandung gegenüber der Gemeindeverwaltung bzw. dem Landratsamt gibt dem Gemeinderat/Kreistag zudem die Möglichkeit, die Sachlage zugleich im Hinblick auf einen Verstoß gegen die Verschwiegenheitspflicht nach § 12 Abs. 3 ThürKO zu überprüfen.

5.2.17 Veröffentlichung von Grundstücksdaten

Ein Stadtrat hatte beschlossen, der Öffentlichkeit jeweils den Vollzug der Veräußerung eines kommunalen Grundstücks, unter Angabe der Grundstücksdaten und des Käufers, bekanntzugeben. Man wollte dadurch Transparenz schaffen und dem Vorwurf begegnen, daß einzelne Personen bevorzugt würden. Gemäß § 40 Abs. 1 ThürKO sind Sitzungen des Gemeinderats öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder das berechtigte Interesse einzelner entgegenstehen. Ausnahmen, die den Ausschluß der Öffentlichkeit notwendig machen, sind regelmäßig Beratungen bei Grundstücksangelegenheiten, da insbesondere Verkaufs- oder Kaufabsichten der Gemeinde häufig Anlaß zu Grundstücksspekulationen geben, die die Entwicklung der Gemeinde mitunter nachteilig beeinflussen können. Darüber hinaus sind auch berechtigte Interessen der Käufer oder Verkäufer zu berücksichtigen, die einer Veröffentlichung von personenbezogenen Daten entgegenstehen können. Um dennoch für die Bürger die in nichtöffentlicher Sitzung beschlossenen Grundstücksangelegenheiten nachvollziehbar zu machen, besteht gemäß § 40 Abs. 2 ThürKO die Möglichkeit, die in nicht-öffentlicher Sitzung gefaßten Beschlüsse zu veröffentlichen, sobald die Gründe für die Geheimhaltung weggefallen sind. Die Entscheidung hierüber trifft der Gemeinderat. Nach Beschlußfassung des Verkaufs eines kommunalen Grundstücks kann regelmäßig davon ausgegangen werden, daß ein weiterer Ausschluß der Öffentlichkeit aufgrund möglicher Nachteile für die Stadt gegenstandslos geworden ist. Dennoch besteht durchaus ein schutzwürdiges Interesse des Betroffenen gegen eine Veröffentlichung. Die Veröffentlichung personenbezogener Daten ist eine Übermittlung an eine nicht-öffentliche Stelle gemäß § 22 ThürDSG und stellt die weitreichendste Form einer Offenbarung dar. Da mit der Veröffentlichung keine weitere Zweckbindung der Daten verbunden ist, werden die Daten jeglicher weiteren Kontrolle hinsichtlich ihrer Nutzung entzogen. Gemäß § 22 ThürDSG ist eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereiches zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgabe erforderlich ist, was im vorliegenden Fall nicht vorlag. Nach dem Beschluß war jedoch nicht nur die Veröffentlichung von Grundstücksdaten, sondern auch der Name des Käufers vorgesehen. Die Erforderlichkeit dafür ist nicht erkennbar. Soweit dies im Einzelfall für erforderlich gehalten wird, bedarf es dazu nach Abwägung der Interessen aller Beteiligten einer konkreten Beschlußfassung. Zur Beurteilung der Schutzwürdigkeit der Interessen des Käufers sind nicht nur das Bekanntwerden seiner persönlichen Verhältnisse, sondern auch hieraus möglicherweise entstehende Folgen des Käufers zu betrachten. Da auch seitens der Rechtsaufsichtsbehörde meine Auffassung geteilt wurde, sah sich die Gemeindevertretung veranlaßt, ihren Beschluß dahingehend zu ändern, daß künftig beim Verkauf kommunaler Grundstücke regelmäßig nur Angaben zum Grundstück, jedoch nicht zum Käufer veröffentlicht werden.

In einem weiteren Fall hatte eine Gemeinde ihre neu beschlossene Satzung über die Erhebung wiederkehrender Beiträge für die öffentlichen Verkehrsanlagen im Amtsblatt bekannt gemacht. In der Anlage hatte sie ein Verzeichnis der einbezogenen Grundstücke beigefügt, in dem neben der Größe und Lage der Grundstücke auch die Namen der jeweiligen Eigentümer und deren Anschriften veröffentlicht worden waren. Hierfür gab es keine spezialgesetzliche Grundlage. Nach § 22 Abs. 1 ThürDSG wäre die Übermittlung bzw. im konkreten die Veröffentlichung personenbezogener Daten durch öffentliche Stellen nur zulässig, wenn dies zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgabe erforderlich wäre und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden oder der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein

schutzwürdiges Interesse am Ausschluß der Übermittlung hat. Die Rückfrage in der Gemeinde ergab, daß die Veröffentlichung nicht das Ergebnis einer falschen Interessenabwägung war, sondern es sich nur um ein bedauerliches Mißverständnis handelte. Zu keiner Zeit war vorgesehen, die Übersicht über die Grundstücksdaten und deren Eigentümer zu veröffentlichen. Im Ergebnis führte der Vorfall dazu, die bisherigen arbeitsorganisatorischer Abläufe zu verändern, um künftig gleichartige Vorfälle auszuschließen. Darüber hinaus erfolgte eine öffentliche Entschuldigung und Klarstellung gegenüber den Betroffenen durch die Gemeindeverwaltung.

5.2.18 Mangelnde Unterstützung des TLfD durch eine Stadtverwaltung

Eine Stadtverwaltung war im Zusammenhang mit der Bearbeitung von zwei Vorgängen aufgefordert worden, entsprechende Informationen bzw. Stellungnahmen zukommen lassen. In einem Fall handelte es sich um eine Bürgereingabe, bei der trotz mehrmaliger Erinnerung die konkret gestellten Fragen nach fast einem halben Jahr nicht beantwortet wurden. Beim zweiten Vorgang wurden von Mitarbeitern der Stadtverwaltung z. T. widersprüchliche Aussagen zu den gestellten Fragen gemacht, wobei der Eindruck entstehen mußte, als ob kein Interesse bestand, umfassende Auskünfte zu geben. Die öffentlichen Stellen sind nach § 38 ThürDSG verpflichtet, den TLfD und seine Beauftragten in der Erfüllung ihrer Aufgaben zu unterstützen. Dazu zählt auch die Erteilung von Auskünften in angemessener Frist. Nachdem ich gegenüber der Stadtverwaltung die mangelnde Unterstützung beanstandet habe, wurden schließlich die entsprechenden Auskünfte erteilt, die mich in die Lage versetzten, die beiden Vorgänge zu bewerten.

5.3 Sparkassen

Aufzeichnung von Kundentelefongesprächen bei der Abwicklung von Handelsgeschäften (Interbankenhandel)

Im Berichtszeitraum hatte ich gemeinsam mit dem Hessischen Datenschutzbeauftragten einen Informationsbesuch zur Aufzeichnung von Kundentelefongesprächen bei der Abwicklung von Handelsgeschäften (Interbankenhandel) in der Landesbank Hessen-Thüringen durchgeführt. Wie ich mich überzeugen konnte, werden dort alle Telefongespräche, die auf einer der zahlreichen Telefonkanäle in der Handelsplatzabteilung geführt werden, von einer Aufzeichnungsanlage vollständig mitgeschnitten. Über die Handelsplätze werden ausschließlich Kundengeschäfte abgewickelt, bei denen es zumeist um sehr hohe Beträge geht. Die Gründe für die Installation dieser Aufzeichnungsanlage liegen deshalb nach Angaben der Helaba in erster Linie in der Beweissicherung. Der Zugang zur Aufzeichnungsanlage erfolgt nach dem „Vier-Augen-Prinzip“, d. h. es haben nur zwei berechtigte Mitarbeiter gleichzeitig Zugang zu den aufgezeichneten Gesprächen. Für die Aufzeichnungsanlage sind von der Helaba die erforderlichen technischen und organisatorischen Maßnahmen getroffen worden, um einen Mißbrauch der aufgezeichneten Gespräche zu verhindern. Außerdem steht jedem Handelsplatzmitarbeiter ein Telefonapparat zur Verfügung, der für private Telefonate genutzt werden kann und bei dem keine Aufzeichnungen erfolgen.

Ich bin mit meinem Hessischen Kollegen zu der Auffassung gelangt, daß die Nutzung der Aufzeichnungsanlage im gegenwärtigen Verfahren den Vorschriften der anzuwendenden Datenschutzgesetze (ThürDSG, BDSG und HDSG) nicht entgegen steht. Da die Helaba als öffentliche Stelle am Wettbewerb teilnimmt und gleichzeitig die aufgezeichneten Kundentelefongespräche im Interbankenhandel - obwohl digitalisiert aufgenommen - keinen Dateibezug haben, sind die Vorschriften des ThürDSG sowie des BDSG hier nicht anwendbar. Hingegen findet die bereichsspezifische Norm des § 34

HDSG zum Datenschutz bei Dienst- und Arbeitsverhältnissen nach dem Staatsvertrag zur Bildung einer gemeinsamen Sparkassenorganisation auch auf öffentlich-rechtliche Wettbewerbsunternehmen Anwendung, ohne daß es dabei auf die Verarbeitung personenbezogener Daten in oder aus Dateien ankommt. Die Verarbeitung von Personaldaten ist nach § 34 Abs. 1 HDSG u. a. zulässig, wenn dies zur Durchführung innerdienstlicher organisatorischer, sozialer und personeller Maßnahmen erforderlich ist. Man kann deshalb davon ausgehen, daß die Aufzeichnung der am Telefon geführten Handelsgespräche eine geeignete und zweckmäßige Maßnahme zur Beweissicherung darstellt, die aufgrund der hohen Handelsbeträge der am Telefon abgewickelten Geschäfte auch verhältnismäßig ist.
Das Verfahren bewegt sich auch im Rahmen der Vorschrift des § 201 Abs. 1 Nr. 1 Strafgesetzbuch (StGB). Danach wird bestraft, wer unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt. Während die Zulässigkeit des Mitschnitts eines Telefongesprächs für die bei der Helaba beschäftigten Personen eine rechtliche Grundlage in § 34 Abs. 1 HDSG hat (s. o.), ist bei den Geschäftspartnern die Befugnis zur Aufzeichnung in einer konkludenten Einwilligung zu sehen, die daraus abzuleiten ist, daß die Geschäftspartner bei der ersten Kontaktaufnahme auf die Tatsache der Aufzeichnung hingewiesen werden. Solche Hinweise bei der ersten Geschäftsanbahnung werden solange erforderlich sein, bis sich aus dem Verfahren ein Handelsbrauch entwickelt hat und dann allgemein davon ausgegangen werden kann, daß allen Handelspartnern die Durchführung der Telefonaufzeichnungen bekannt sein muß. Durch die Bereitstellung einer aufzeichnungsfreien Telefonleitung an jedem Handelsplatz für die Erledigung von privaten Telefongesprächen ist zudem sichergestellt, daß keine privaten Telefonate aufgezeichnet werden, wofür es keine Rechtsgrundlage gäbe.

6. Personalwesen

6.1 Personalaktenführungsrichtlinie

Schon in meinem 1. TB (6.1.1) hatte ich auf die Notwendigkeit verwiesen, klare Regelungen zur Personalaktenführung zu treffen. Eine derartige Richtlinie liegt bisher nur in einem Entwurf vor, zu dem ich ausführlich Stellung genommen habe. Nach der Ressortanhörung wurde mir der Entwurf noch einmal zugeleitet.
Meine Hinweise und Empfehlungen fanden größtenteils Berücksichtigung.

6.2 Personalaktenführung

Ein Mitarbeiter einer Verwaltungsbehörde setzte mich von einer Dienstaufsichtsbeschwerde zur Personalaktenführung im Hinblick auf seine Personalakte in Kenntnis. Ich habe daraufhin eine Kontrolle vorgenommen, bei der sich herausstellte, daß zwischenzeitlich die unterbliebene Durchnumerierung der Personalakte nachgeholt wurde. Soweit der Beschwerdeführer darauf verwiesen hatte, daß Nebenaktennotizen noch nicht zur Personalakte genommen worden waren, standen hierzu noch erforderliche Klärungen aus, so daß zum Prüfungszeitpunkt noch keine Veranlassung bestand, die Vorgänge in die Personalakte aufzunehmen. Soweit man dem Beschwerdeführer verweigert hatte, in die dort geführte Nebenakte Einblick zu nehmen, war dies unzulässig, da es jedem Beschäftigten zusteht, in seine Personalakte einschließlich der Teil- und Nebenakten Einsicht zu nehmen. Diese Auffassung hatte ich auch bei meiner Kontrolle zum Ausdruck gebracht. Die öffentliche Stelle war zunächst der Auffassung, bis zum Inkrafttreten einer Personalaktenführungsrichtlinie keine Festlegungen für seinen Zuständigkeitsbereich einschließlich des nachgeordneten Bereichs treffen zu müssen. Es wurde dann aber die Führung von Nebenakten einer Regelung zugeführt, die nach

einer nochmaligen Modifizierung die datenschutzrechtlichen Bedenken ausräumen.

6.3 Personalfragebogen für Bedienstete des Landes Thüringen

In meinem 1. TB (6.1.2) hatte ich ausgeführt, daß die Auslegung der Regelungen des § 97 ThürBG hinsichtlich des erforderlichen Umfangs von Personalaktendaten in Personalfragebogen Schwierigkeiten bereitet. Das TKM hatte eingeräumt, daß der Personalfragebogen in Abstimmung mit dem TIM und dem TFM überarbeitet werden müsse, um den Erfordernissen des Datenschutzes zu genügen.
Seitens des TKM wurde ein überarbeiteter Entwurf eines Personalfragebogens vorgelegt, bei dem die datenschutzrechtlich bedenklich erscheinenden Punkte ausgeräumt wurden.

6.4 Personalverwaltung der Lehrer

In meinem 1. TB (6.1.10) hatte ich auf die Probleme der Personalverwaltung der Lehrer im Hinblick auf die festgestellte „doppelte Aktenführung“ in den Schulämtern sowie die ungeklärten Fragen bei der Zuordnung und Aufbewahrung von Personalakten der vor dem 03.10.1990 aus dem Schuldienst ausgeschiedener Lehrer und Erzieher hingewiesen. Soweit ich dies im Berichtszeitraum bei meinen Kontrollen bestätigt fand, habe ich das gegenüber dem Landesverwaltungsamt, den jeweiligen Schulämtern und auch gegenüber einem Landratsamt beanstandet.
Seit Mitte 1997 liegt ein novelliertes Schulaufsichtsgesetz vor, wonach künftig den Schulämtern als untere Schulaufsichtsbehörden die Dienstaufsicht über die Schulleiter, Lehrer, sonderpädagogischen Fachkräfte und Erzieher obliegt. Zur Umsetzung der Neuregelung wurde zwischenzeitlich auch eine vorläufige Zuständigkeits- und Verfahrensregelung für die Personalverwaltung und Personalaktenführung im Geschäftsbereich des Thüringer Kultusministeriums wirksam. Danach sind die Schulämter im Rahmen der Personalverwaltung insbesondere auch für die Führung der Personalakten der Lehrer und Erzieher ihres Zuständigkeitsbereiches verantwortlich. Mit der Übernahme der laufenden Personalunterlagen vom Landesverwaltungsamt werden nunmehr auch die von mir beanstandeten unzulässig in den Schulämtern geführten Personalnebenakten aufgelöst bzw. zur Vervollständigung der Personalakten genutzt. Doppelte Unterlagen werden dabei vernichtet, soweit es sich nicht um beglaubigte Urkunden handelt, die den Betroffenen zurückzugeben sind.
Darüber hinaus wurden die Schulämter verpflichtet, die bei den Landratsämtern aufbewahrten Personalakten aller vor dem 03.10.1990 aus dem Schuldienst ausgeschiedenen Lehrer und Erzieher zu übernehmen. Trotz entsprechender Terminvorgaben durch die Aufsichtsbehörden wurde die Übergabe der Altakten noch immer nicht in allen Kreisen abgeschlossen.

6.5 Personalakten im Justizbereich

Im 1. TB (6.1.12) hatte ich zur Führung der Personalakten der Strafvollzugsbediensteten berichtet. Im Berichtszeitraum wurden im Justizbereich anläßlich durchgeführter Kontrollen in drei weiteren Stellen (eine Justizvollzugsanstalt, eine Staatsanwaltschaft und ein Amtsgericht) die Personalaktenführung überprüft. Dies führte zu jeweils weiteren Beanstandungen gemäß § 39 ThürDSG. Die Beanstandungen waren letztendlich auch deswegen auszusprechen, da die Personalakten in den kontrollierten Bereichen nach der Verwaltungsvorschrift des Thüringer Justizministeriums vom 01.10.1992 zur Führung von Personalakten geführt wurden. Diese Verwaltungsvorschrift sieht insbesondere unter Ziffer 2 vor, daß Personalakten von Bediensteten je nach Laufbahn und entsprechend im Angestelltenverhältnis bei mehreren

Stellen geführt werden. In der Praxis bedeutet dies, daß Richter, Staatsanwälte, Beamte im gehobenen Dienst bei ihrer Dienststelle, bei der nächsthöheren Dienststelle bzw. den höheren Dienststellen und auch im Ministerium jeweils eine vollständige Personalakte haben. Im Gegensatz hierzu sieht § 97 Abs. 2 Satz 1 des Thüringer Beamtengesetzes (ThürBG) vom 10.06.1994 vor, daß über jeden Beamten nur eine Personalakte zu führen ist. In Folge der Kontrollen wurde gefordert, die Verwaltungsvorschrift auf die Vereinbarkeit mit dem ThürBG und dem Erforderlichkeitsgrundsatz zu überprüfen und anzupassen. Da die Problematik der Verwaltungsvorschrift dem TMJE seit Ende 1995 bekannt war, konnte jedoch nicht weiter hingenommen werden, daß diese eindeutig gegen gesetzliche Regelungen verstoßende Vorschrift weiterhin für die öffentlichen Stellen im Geschäftsbereich des TMJE als verbindlich aufrecht erhalten wird, so daß ich mich veranlaßt sah, die Verwaltungsvorschrift gemäß § 39 ThürDSG zu beanstanden. Seitens des TMJE wurde daraufhin zugesagt, schnellstmöglich eine novellierte Fassung der Verwaltungsvorschrift im Einklang mit den gesetzlichen Bestimmungen zu erarbeiten. Zwar wird die Überarbeitung der Verwaltungsvorschrift unabhängig von der landeseinheitlichen Richtlinie zur Anlage und Führung von Personalakten überarbeitet, die endgültige Fassung der novellierten Verwaltungsvorschrift wird jedoch erst nach Inkrafttreten einer allgemeinverbindlichen Personalaktenführungsrichtlinie in Geltung gesetzt werden. Ich habe dies akzeptiert, um eine doppelte Überarbeitung zu vermeiden. Unabhängig davon haben mir die kontrollierten Stellen berichtet, daß dort anhand meiner gegebenen Anregungen begonnen wurde, die vorhandenen Personalakten zu überarbeiten.

6.6 Einsichtnahme von Vorgesetzten in Personalakten

Im Berichtszeitraum wurde die Anfrage an mich herangetragen, ob der Abteilungsleiter das Recht habe, in die Personalakte Einsicht zu nehmen. Ich teilte mit, daß nach § 97 Abs. 3 ThürBG nur Beschäftigte, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, Zugang zur Personalakten haben und nur, soweit dies zu Zwecken der Personalverwaltung und der Personalwirtschaft erforderlich ist. Damit ist eindeutig geregelt, daß nicht mit der Personalverwaltung befaßte Bedienstete keinen Zugang zur Personalakte haben dürfen. Der vorgesetzte Fachabteilungsleiter zählt grundsätzlich nicht zu denjenigen, die mit der Bearbeitung von Personalangelegenheiten betraut sind. Wenn die Personalverwaltung den Fachvorgesetzten bei einem Vorstellungsgespräch hinzuzieht, erhält dieser nur Kenntnis von den personenbezogenen Daten, die Gegenstand des Vorstellungsgesprächs sind und die sich ggf. aus den Bewerbungsunterlagen ergeben. Dies begegnet auch keinen Bedenken. Mit der Einstellung gehen derartige Unterlagen aber in die Personalakte ein und sind danach für den fachvorgesetzten Abteilungsleiter nicht mehr zugänglich, es sei denn, was im vorliegenden Fall nicht der Fall war, daß er ausdrücklich nach § 100 Abs. 2 ThürBG hierzu ermächtigt ist. Die betreffende Stelle hat mitgeteilt, daß der Abteilungsleiter kein Einsichtsrecht in die Personalakte hat.

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

Seitens einer Dienststelle des Landes wurde die Frage an mich gerichtet, ob es zulässig ist, daß der Zentralen Gehaltsstelle (ZG) zur Berechnung des Ruhegehaltes die komplette Personalakte übersandt wird. Die Bedenken richteten sich dagegen, daß in der Personalakte auch Dienstzeugnisse und persönliche Wertungen enthalten sind, die zur Bestimmung des Ruhegehaltes

nicht erforderlich sind. In meiner Antwort habe ich darauf hingewiesen, daß in der vorbezeichneten Angelegenheit § 101 Abs. 1 Satz 2 ThürBG, wonach ohne Einwilligung des Beamten die Personalakte der Pensionsbehörde vorgelegt werden kann, einschlägig ist. § 101 Abs. 1 Satz 2 ThürBG begegnet aus meiner Sicht keinen datenschutzrechtlichen Bedenken, da im Regelfall nur die komplette Durchsicht der Personalakte, die auch Angaben zu Vorbeschäftigungsverhältnissen enthält, die Pensionsbehörde in die Lage versetzt, festzustellen, welche Tätigkeit im einzelnen für die Festsetzung der ruhegehaltsfähigen Dienstbezüge in Ansatz zu bringen sind. Zwar ist zuzugeben, daß für die Festsetzungen von ruhegehaltsfähigen Dienstbezügen vom Grundsatz her nicht die Kenntnis der gesamten Personalakte zwingend erforderlich ist. Hier im einzelnen aber praktikable Lösungen zu finden, welche Vorgänge zu entnehmen sind, erscheint mir problematisch zu sein, da nicht jeder Beschäftigte, der mit der Personalverwaltung zu tun hat, die Kenntnisse haben wird, zu differenzieren, auf welche Unterlagen es für die Ruhegehaltsfestsetzung ankommt. Von einer Übersendung der Personalakte an die ZG zur Berechnung des Ruhegehaltes geht auch der Entwurf für die Verwaltungsvorschrift zur ThürZustVBezüge aus. Das TFM hat mich an der Erarbeitung des Entwurfs dieser Verwaltungsvorschrift beteiligt.
Diese Verwaltungsvorschrift ist immer noch nicht in Kraft getreten, was bedauerlich ist, da auf die Notwendigkeit klarer Regelungen in diesem Zusammenhang schon in meinem 1. TB (6.3.1) hingewiesen worden war.

6.8 Veröffentlichung von Mitarbeiterdaten

In vielfältiger Form werden von öffentlichen Stellen die Namen ihrer Mitarbeiter und deren Funktionen veröffentlicht. Dies erfolgt z. B. durch das Anbringen von Türschildern, die Verpflichtung zum Tragen von Namensschilder, die Aufstellung von Wegweisern in den Behörden, durch die Veröffentlichung von Behörden- und Telefonverzeichnissen oder auch von Vorlesungsverzeichnissen. In jedem Fall stellt sich für den Betroffenen die Frage nach der datenschutzrechtlichen Zulässigkeit für die Veröffentlichung seiner Daten. Beschäftigte im öffentlichen Dienst können sich gegenüber dem Staat nur auf ihr informationelles Selbstbestimmungsrecht berufen, soweit sie nicht als Amtsträger für den Staat handeln, dem diese Tätigkeit zugerechnet wird. Insoweit muß es der Bedienstete auch hinnehmen, daß sein Name in den von ihm bearbeiteten Vorgängen oder auch dienstlichen Verzeichnissen bekannt wird. Darüber hinaus kann es notwendig und zweckmäßig sein, im Zusammenhang mit seinen dienstlichen Aufgaben den Namen des Mitarbeiters an Tür- oder auf Namensschildern Dritten gegenüber bekanntzumachen. Dies ist insbesondere notwendig, um die Ansprechbarkeit zu ermöglichen und einen angemessenen Umgangston pflegen zu können. Gleichzeitig wird der Amtsträger insoweit aus der Anonymität herausgeführt, daß er mit seinem Namen für die Richtigkeit seiner Amtshandlung einstehen muß. Es bestehen deshalb keine datenschutzrechtlichen Bedenken, wenn es darum geht, den Bürger in allgemeiner Form darüber zu informieren, wo er sich mit welchem Anliegen hinwenden kann bzw. wer der Bearbeiter seines Anliegens ist. Dennoch trägt auch bei der Offenbarung von Mitarbeiterdaten die öffentliche Stelle eine Verantwortung, zu prüfen, ob im überwiegenden Allgemeininteresse die Bekanntgabe der Namen erforderlich ist. Um dem Bürger die konkrete Ansprechbarkeit eines Leiters oder Mitarbeiters zu ermöglichen bzw. den Bediensteten innerhalb der Stelle näher bestimmen zu können, reicht im Regelfall die Bekanntgabe seiner Funktion, des Nachnamens, ggf. seines Titels und ergänzend dazu die Anrede Herr bzw. Frau aus. Eine Nennung des Vornamens dürfte regelmäßig über das erforderliche Maß hinausgehen, da der Mitarbeiter aufgrund seines Aufgabengebietes und des Nachnamens bereits hinreichend konkretisiert werden kann. Da jedoch die Kenntnis von Vor- und Nachnamen unter Nutzung weiterer Datenbeständen, wie Adreßbüchern, Telefonverzeichnissen u. a. durchaus geeignet ist, den betref-

fenden Mitarbeiter auch außerhalb der Behörde und damit als Privatperson zu identifizieren und dort im Einzelfall nicht ausgeschlossen werden kann, daß dies zum Nachteil der Betroffenen (z. B. durch Belästigungen) genutzt wird, sollte grundsätzlich auf die Nennung des Vornamens verzichtet werden, soweit nicht die Einwilligung des Betroffenen vorliegt.

Im Rahmen Ihrer Öffentlichkeitsarbeit erstellen z. B. viele Behörden zur Gestaltung einer bürgernahen und effizienten Verwaltung sogenannte Behördenverzeichnisse oder Wegweiser. Üblich und zweckmäßig ist es dabei, die jeweiligen Leiter insbesondere der publikumsintensiven Fachbereiche und Sachgebiete namentlich zu benennen. Aufgrund einer Anfrage hatte ich mich diesbezüglich mit einem Behördenwegweiser zu beschäftigen, in dem jeweils auch die Vornamen der Mitarbeiter genannt wurden. Eine Begründung zur Erforderlichkeit konnte von der Behörde nicht gefunden werden, so daß künftig darauf verzichtet wird.

Entsprechendes gilt selbstverständlich auch bei der Erstellung und Verteilung von Telefonverzeichnissen in öffentlichen Stellen. Auch wenn es sich um ein dienstliches Verzeichnis handelt, gibt es regelmäßig keinen Grund die Vornamen aufzunehmen, insbesondere aber dann nicht, wenn das Verzeichnis auch über die Behörde hinaus verteilt wird. Gegenwärtig wird in Thüringen auf der Basis eines Corporate Network auf Landesebene ein Telefonverzeichnis aller Landesbehörden erstellt. Ich habe in diesem Zusammenhang gebeten, den Inhalt des Verzeichnisses hinsichtlich seiner Erforderlichkeit zu überprüfen. Da es sich um ein dienstliches Verzeichnis handelt, ist es selbstverständlich, daß für diese Zwecke alle telefonisch erreichbaren Mitarbeiter in das Verzeichnis aufgenommen werden. Wichtig ist außerdem, daß bei den einzelnen Mitarbeitern die jeweilige Arbeitsaufgabe und die Funktion konkret benannt wird. Demgegenüber dürfte regelmäßig der Vorname des Mitarbeiters unerheblich sein, wenn statt dessen die jeweilige Anrede in das Verzeichnis aufgenommen wird. Ich habe diesbezüglich um Berücksichtigung gebeten.

Besondere Probleme treten zusätzlich dann auf, wenn zunächst interne Verzeichnisse veröffentlicht werden sollen. Aufgrund eines Hinweises hatte ich erfahren, daß ein Fernsprechverzeichnis einer Behörde aus Kostengründen mit Werbeinseraten versehen von einer privaten Druckerei hergestellt wurde. Gleichzeitig hat man die Möglichkeit eingeräumt, daß jedermann beim Verlag das Telefonverzeichnis gegen entsprechendes Entgelt beziehen konnte. Ein berechtigtes Interesse an der Kenntnis der in einem behördlichen Telefonverzeichnis aufgeführter personenbezogener Daten aller Mitarbeiter in der Öffentlichkeit ist nicht erkennbar. Nur soweit Mitarbeiter dienstlich in Erscheinung treten, ist ein Nutzen für die Öffentlichkeit aus der Kenntnis der konkreten personellen Zusammensetzung bzw. Zuordnung anzuerkennen, wie das in sogenannten Behördenverzeichnissen bzw. Wegweisern gängige Praxis ist. Ansonsten steht der Persönlichkeitsschutz der Bediensteten generell einer Übermittlung entgegen. Behördliche Telefonverzeichnisse sind für den dienstlichen Gebrauch bestimmt und gelten somit nicht als allgemein zugängliche Quelle im Sinne des Datenschutzgesetzes. Ein Verkauf oder eine Veröffentlichung eines vollständigen behördlichen Fernsprechverzeichnisses scheidet deshalb aus. Aufgrund meiner Empfehlung wurde der weitere Verkauf eingestellt.

Selbstverständlich kann im Einzelfall auch entschieden werden, daß statt des Nachnamens nur der Vornamen bekanntgegeben wird. Die Entscheidung, ob z. B. das Pflegepersonal in Krankenhäusern traditionsgemäß nur Namensschilder mit dem Vornamen und der Funktionsbezeichnung oder die Anrede und den Nachnamen tragen, bleibt der jeweiligen Einrichtung ggf. unter Beteiligung der Personalvertretung überlassen. Eine Verpflichtung der Be-

schäftigten zum Tragen von Namensschildern mit Vor- und Zunamen dürfte demgegenüber regelmäßig nicht erforderlich sein.

Wie mir bekannt ist, bestehen auch von Seiten der Hoch- und Fachhochschulen Bestrebungen, personenbezogene Daten von Hochschulangehörigen und Studenten im Internet zu veröffentlichen. Für Veröffentlichungen von personenbezogenen Daten im Internet durch eine öffentliche Stelle sind zunächst die Zulässigkeitsvoraussetzungen gemäß § 22 Abs. 1 ThürDSG zu überprüfen. Danach ist eine Übermittlung von personenbezogenen Daten an nicht-öffentliche Stellen nur dann zulässig, wenn sie im konkreten Fall zur Erfüllung der in der Zuständigkeit der Hochschule liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen würden oder der Empfänger ein berechtigtes Interesse an der Kenntnis der Daten darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. Einer Zurverfügungstellung bzw. Übermittlung der Daten in Verzeichnisse, deren Empfänger nicht näher bestimmt werden können, wie das besonders im Internet der Fall ist, stehen regelmäßig schutzwürdige Interessen der Betroffenen entgegen. Dies wäre daher nur mit Einwilligung der betroffenen Beschäftigten zulässig (vgl. § 22 Abs. 1 Nr. 2 ThürDSG). Diese Einwilligung bedarf gemäß § 4 Abs. 2 ThürDSG regelmäßig der Schriftform. Das trifft in gleichem Maß auf ausführliche Vorlesungsverzeichnisse mit Adreßteil der Bediensteten zu. Während jedoch die Fernsprechverzeichnisse ausschließlich für den Dienstgebrauch vorgesehen sind und ein entsprechender Zugriff auf die Daten durch Unbefugte auszuschließen ist, bestehen grundsätzlich bei der Veröffentlichung von Vorlesungsverzeichnissen gegen die Nennung der Professoren und Dozenten, einschließlich der jeweiligen dienstlichen Anschrift sowie soweit zweckmäßig auch der dienstlichen Telefonnummer sowohl in Papierform als auch im Internet keine datenschutzrechtlichen Bedenken, da Vorlesungsverzeichnisse ihrem Zweck nach öffentliche Quellen und die Dozenten in amtlicher Funktion tätig sind.
Die Aufnahme „privater“ Adressen in vorgenannte Verzeichnissen ist selbstverständlich auszuschließen oder bedarf der Zustimmung der Betroffenen.
Für die Nutzung von personenbezogenen Daten Studierender gelten aufgrund der Zweckbestimmung der an Hochschulen erhobenen Daten der Studenten die gleichen datenschutzrechtlichen Anforderungen.

6.9 Polizeiärztliche Untersuchungen im Rahmen von Bewerberauswahlverfahren für den polizeilichen Dienst

Von einem anderen Datenschutzbeauftragten wurde mir mitgeteilt, daß bei polizeiärztlichen Untersuchungen im Rahmen von Bewerberauswahlverfahren für den polizeilichen Dienst nach der Polizeidienstvorschrift „Ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit“ (PDV 300) verfahren wird, die unter anderem vorsieht, daß Lebenslauf und Zeugnisse von den für die Polizeiauswahlentscheidung zuständigen Stellen an die mit der Auswahl und Untersuchung beauftragten Polizeiärzte mitgeteilt werden, was problematisch ist, weil diese Unterlagen für die bei der ärztlichen Untersuchung zu treffenden Feststellungen nicht erforderlich sind. Nach der Dienstvorschrift ist vorgesehen, daß Tätowierungen zu beschreiben und ggf. zu dokumentieren sind, wobei die Beurteilung dann nicht durch den Arzt sondern im Rahmen des Auswahl- und Einstellungsverfahrens erfolgen soll. Hier stellt sich die Frage, ob Bewerbern für den Polizeidienst deutlich wird, daß die vom Arzt im Rahmen der Einstellungsuntersuchung durchgeführte Dokumentation seiner Tätowierungen an die für die Personalauswahlentscheidung zuständige Stelle weitergegeben wird. Dieses Verfahren begegnet erheblichen rechtlichen Bedenken, so daß hier eine den Persönlichkeitsrechten der Bewerbern angemessene Verfahrensweise gefunden werden sollte. Ziffer 11.1 der PDV sieht vor, daß Bewerber auch nach Familiena-

namnesen, überstandenen Gemüts- und Geisteskrankheiten, Suizidversuchen, Bettnässen und häufigem Wechsel des Berufs, von Freunden und Vorgesetzten befragt werden. Derartige Fragestellungen gehen in die Intimsphäre von Bewerbern und deren Familienangehörigen hinein, so daß sie nicht zu rechtfertigen sind. Ob Bettnässen in der Kindheit bei erwachsenen Bewerbern für den Polizeidienst noch relevant ist, erscheint zumindest fraglich. Ein häufiger Vorgesetztenwechsel muß keineswegs dem zu Untersuchenden anzulasten sein. Auch wenn man zuerkennen muß, daß im Vergleich zu anderen Bewerbern für den öffentlichen Dienst bei Bewerbern für den Polizeidienst höhere Anforderungen an die physische und psychische Belastbarkeit gestellt werden müssen, sind derartige Fragestellungen bedenklich. In einem Gespräch mit dem Ärztlichen Dienst der Thüringer Polizei wurde festgestellt, daß diese von der Einsichtnahme in Personalakten Abstand nimmt und keine Fragen zur Persönlichkeitsbeurteilung stellt. Der Ärztliche Dienst der Thüringer Polizei zeigte sich gegenüber den datenschutzrechtlichen Belangen sehr aufgeschlossen. Die Überarbeitung der PDV 300 steht noch aus; es bleibt abzuwarten, ob allen vorgetragenen Bedenken gegen die derzeitige Fassung darin Rechnung getragen wird.

6.10 Einstellung in den Polizeidienst

Ein Bewerber für den Polizeidienst in einem anderen Bundesland zeigte sich darüber verwundert, daß eine nach § 60 Abs. 1 Nr. 7 Bundeszentralregistergesetz (BZRG) im Erziehungsregister vermerkte Entscheidung von der zuständigen Polizeidienststelle in Thüringen weitergegeben worden war, die nach § 61 BZRG nicht zur Weiterleitung vorgesehen war. Er hatte hierbei übersehen, daß er bei der für die Einstellung zuständigen Dienststelle sein Einverständnis dazu erklärt hatte, daß polizeiliche Auskünfte bei der für ihn zuständigen Polizeidienststelle eingeholt werden konnten. Da er damit sein Einverständnis mit der Weitergabe der Daten erklärt hatte, begegnete die Auskunftserteilung keinen Bedenken.

6.11 Datenverarbeitung bei Personalkostenzuschüssen

Durch einige Anfragen wurde ich mit der Fragestellung befaßt, in welchem Umfang personenbezogene Daten der Mitarbeiter Freier Träger der Jugendhilfe im Zusammenhang mit der Beantragung und Bewilligung von Fördermitteln des Landes von den zuständigen Stellen erhoben werden dürfen. Unsicherheiten gab es bei den bei mir anfragenden Freien Trägern der Jugendhilfe insbesondere bzgl. der angeforderten detaillierten Angaben zur Gehaltszusammensetzung, der Pflicht zur Vorlage der Arbeitsverträge sowie der Lebensläufe der Mitarbeiter. Ich habe mich daraufhin mit dem für die Bearbeitung der Förderanträge zuständigen Landesjugendamt in Verbindung gesetzt und um die Vorlage der im Bereich der Kinder- und Jugendhilfe verwendeten Antragsvordrucke gebeten. Danach gibt es zwei unterschiedliche Modelle der Förderung von Personalkosten bei Beratungsstellen im Bereich der Kinder- und Jugendhilfe. In einigen Bereichen werden je eingesetzter Fachkraft entsprechend ihrer Qualifikation monatliche Festbeträge bezahlt. Bei den anderen Förderprogrammen werden Personalkostenzuschüsse in Höhe eines bestimmten Prozentsatzes der tatsächlich angefallenen Personalkosten gewährt. Bei beiden Modellen setzen die Förderrichtlinien voraus, daß zum zweckentsprechenden Einsatz der Fördermittel ausreichend qualifiziertes Personal eingesetzt wird, was im Rahmen der Antragstellung und der Rechnungsprüfung nachzuweisen ist. Auch über den Umfang der Tätigkeit (Vollzeit- oder Teilzeitbeschäftigung) sind entsprechende Angaben zur Mittelbewilligung vorzulegen.

Die direkte Anforderung der Mitarbeiterdaten durch das Landesjugendamt bei den Freien Trägern stellt eine Datenerhebung bei Dritten dar. Rechts-

grundlage hierfür ist § 62 Abs. 4 SGB VIII. Dieser setzt voraus, daß der Betroffene nicht zugleich Leistungsberechtigter oder sonst an der Leistung beteiligt ist und die Kenntnis der Daten für die Gewährung von Leistungen nach dem SGB VIII erforderlich sind. Bei der Gewährung von Personalkostenzuschüssen an Freie Träger der Jugendhilfe handelt es sich um Leistungen nach §§ 12 und 74 SGB VIII in Verbindung mit den jeweiligen Förderrichtlinien. Leistungsberechtigte in diesen Fällen sind ausschließlich die jeweiligen Freien Träger, nicht jedoch deren Mitarbeiter. Letztere profitieren lediglich indirekt von der Leistungsgewährung. Unter der Voraussetzung, daß die personenbezogenen Angaben zu Lohn- und Gehaltsbestandteilen, zur Qualifikation sowie zum Umfang der Beschäftigung für die Gewährung der Zuwendungen, d. h. einer Leistung nach dem SGB VIII notwendig sind, dürfen diese Angaben auch bei Leistungsberechtigten (Dritten), d. h. bei den jeweiligen Freien Trägern erhoben werden. In entsprechender Anwendung von § 62 Abs. 2 Satz 2 SGB VIII sollten jedoch die Mitarbeiter der Freien Träger über diese Datenerhebung informiert werden. Ich habe daher dem TMSG vorgeschlagen, auf dem jeweils letzten Blatt des Antragsformulars die Versicherung des Antragstellers aufzunehmen, daß die mit Landesmitteln zu fördernden Mitarbeiterinnen und Mitarbeiter darüber informiert wurden, daß für das Zuwendungsverfahren notwendige personenbezogene Daten (z. B. Name, Anschrift, Geburtsdatum, Familienstand, Vergütungsgruppe, Anzahl und Alter der Kinder, Qualifikation, Funktion, Arbeitszeitumfang, Arbeitsplatzbeschreibung) gemäß § 62 Abs. 4 SGB VIII dem Zuwendungsgeber übermittelt werden dürfen. Darüber hinaus habe ich dem TMSG mitgeteilt, daß ich in den Fällen, in denen die Förderung von Personalkosten in Form von Festbeträgen erfolgt, lediglich Name des Mitarbeiters, Angaben zu Qualifikation und Funktion sowie zum Umfang der Arbeitszeit zur Überprüfung einer möglicherweise unzulässigen Doppelförderung für erforderlich halte, weil es auf die konkrete Gehaltszusammensetzung in diesen Fällen nicht ankommt. Das TMSG hat zwischenzeitlich die Antragsformulare in diesem Sinn überarbeitet und zusätzlich den Hinweis bei der Anforderung von Arbeitsverträgen angebracht, daß auf Kopien Angaben, die über Name, Adresse, Beginn und Ende der Beschäftigung, Beschäftigungsumfang und Vergütungsgruppe hinausgehen, geschwärzt werden können. Im übrigen bestand Einvernehmen auch dahingehend, daß eine dauerhafte Speicherung von Arbeitsverträgen und Qualifikationsnachweisen beim Landesjugendamt nicht erforderlich ist, sondern diese Unterlagen nach abschließender Prüfung und Berücksichtigung des Prüfergebnisses im Antragsprüfvermerk zusammen mit dem Bewilligungsbescheid an den Antragsteller zurückgesandt werden können und dieser verpflichtet wird, für eine eventuelle Rechnungsprüfung die Unterlagen bereitzuhalten. Grundsätzlich gilt bei der Aufbewahrung dieser Unterlagen, daß diese von den übrigen den Freien Träger betreffenden Unterlagen getrennt aufbewahrt werden, da es sich um Unterlagen handelt, die mit Personaldaten vergleichbar sind und daher einer besonderen Zweckbindung unterworfen werden sollten.

6.12 Dienstvereinbarung über die elektronische Verarbeitung von Personaldaten

Im 1. TB (15.5.3) hatte ich berichtet, daß die Thüringer Landesverwaltung die Einführung des Personalverwaltungssystems PERSOSTH, das von mir datenschutzrechtlich begleitet worden ist, zur Einführung vorgesehen hat. Mittlerweile haben verschiedene Dienststellen mit der Einführung begonnen, entsprechende Meldungen zum Datenschutzregister liegen vor. In diesem Zusammenhang habe ich Empfehlungen gegeben, die sich u. a. auf die Paßwortgestaltung, die Begrenzung der Anzahl der Anmeldefehlversuche, Zugriffsrechte und Protokollierung bezogen.

6.13 Führung von An- und Abwesenheitslisten von Mitarbeitern

Hinweise aus der Presse und Anfragen von Mitarbeitern, daß in einer Verwaltungsbehörde neben einem elektronischen Zeiterfassungssystem täglich An- bzw. Abwesenheitslisten für alle Mitarbeiter unter Angabe der Gründe ihrer Abwesenheit zentral erstellt und der Behördenleitung sowie allen Abteilungen zur Information zur Verfügung gestellt werden, gaben mir Anlaß, die Führung von An- und Abwesenheitslisten bei den Landesbehörden zu hinterfragen. Darüber hinaus erfolgten in zwei Ministerien Kontrollen, bei denen sich obiger Sachverhalt bestätigte. Gleichzeitig wurde in einem Ministerium festgestellt, daß täglich Auszüge aus dem automatisierten Verfahren gewonnen wurden, ohne eine entsprechende Vereinbarung mit dem Personalrat. Zu den Aufgaben der Personalverwaltung gehört die Führung von Übersichten über die An- und Abwesenheit der einzelnen Mitarbeiter, insbesondere bei Gewährung von Freistellungen aus den verschiedensten Gründen, wie Krankheit und Urlaub, als Bestandteil der Personalunterlagen (§ 97 ThürBG). Darüber hinaus obliegt dem jeweiligen Dienstvorgesetzten die Kontrolle der Einhaltung der täglichen Arbeitszeit. Da überwiegend für die Mitarbeiter in der Landesverwaltung Gleitzeitregelungen bestehen, sind die betreffenden Mitarbeiter verpflichtet, Zeiterfassungsblätter zu führen, die jeweils dem unmittelbaren Dienstvorgesetzten am Monatsende vorzulegen sind. In vielen Behörden werden stattdessen bereits automatisierte Verfahren (Zeiterfassungssysteme) genutzt. Zu beachten ist dabei, daß die Einführung, Anwendung, wesentliche Änderung oder Erweiterung automatisierter Verarbeitung personenbezogener Daten, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen oder zu erfassen, durch den jeweiligen Personalrat gemäß § 74 Abs. 3 Ziff. 18 ThürPersVG mitbestimmungspflichtig sind. In den abzuschließenden Dienstvereinbarungen sind insbesondere der Umfang und die Dauer der Erhebung und Verarbeitung von Beschäftigtendaten sowie die Möglichkeiten ihrer Auswertung festzulegen.
Ungeachtet der Form zur Arbeitszeiterfassung ist es unstrittig, daß der jeweilige Vorgesetzte im Rahmen seiner Dienstaufsicht aus arbeitsorganisatorischen Gründen An- und Abwesenheitslisten über seine Mitarbeiter führen kann. Soweit es die Behördenleitung wünscht, jederzeit über den anwesenden Mitarbeiterbestand informiert zu sein, gibt es nur insoweit Einwände, als dort im allgemeinen auf die konkrete Nennung des Abwesenheitsgrundes verzichten werden sollte. Wird es darüber hinaus für erforderlich gehalten, weiteren Leitern oder Mitarbeitern in den verschiedensten Organisationseinheiten der Behörde Übersichten zu übergeben, aus denen hervorgeht, welche Mitarbeiter zu welchem Zeitpunkt abwesend sind, ist dies nur unter Beachtung des Erforderlichkeitsgrundsatz zulässig. Nicht nachvollziehbar ist aber, wenn wie bei der Stelle praktiziert, uneingeschränkt allen Abteilungsleitern und Mitarbeitern des technischen Bereiches, wie der Pforte regelmäßig bekannt sein muß, welche Mitarbeiter der gesamten Behörde in welchem Zeitraum nicht anwesend sind. Eine Erforderlichkeit für die Kenntnis der Personaldaten aller Beschäftigten zur Aufgabenerfüllung dieser Bediensteten kann man sicher verneinen. Wenn es darüber hinaus im Einzelfall zweckmäßig und erforderlich sein sollte, einem begrenzten Personenkreis regelmäßig listenmäßig über die „voraussichtliche“ oder „planmäßige“ Abwesenheit von Mitarbeiter zu informieren, so sind die Mitarbeiter von dieser Verfahrensweise in Kenntnis zu setzen. In jedem Fall sollte aber die Führung von Abwesenheitslisten schriftlich insbesondere hinsichtlich der Datenerhebung, des Verwendungszweckes, der Verteilung und der Löschung von Listen geregelt werden, um zu verhindern, daß, wie auch die Kontrollen zeigten, Übersichten über längere Zeit aufbewahrt und teilweise über das erforderliche Maß hinaus gestreut werden. Soweit zur Erstellung von täglichen An- und Abwesenheitslisten auch Daten aus dem jeweiligen automatisierten Zeiterfassungssystem genutzt werden sollen, ist dies nur zulässig, wenn dazu in der Dienstvereinbarung mit dem Personalrat Regelungen getroffen sind. In Auswertung

der durchgeführten Prüfungen haben zwischenzeitlich die kontrollierten Behörden ihre bisherigen Verfahrensweise zur Führung von Abwesenheitslisten den datenschutzrechtlichen Anforderungen entsprechend verändert.

6.14 Zulässigkeit behördlicher Organisations-/Arbeitsplatzuntersuchungen und von Mitarbeiter-/Bürgerbefragungen

In Zeiten knapper werdender Haushaltsmittel gehen Behörden zunehmend dazu über, Organisationsuntersuchungen in den Dienststellen durchzuführen, in deren Mittelpunkt die Prüfung der Aufbau- und Ablauforganisation der betreffenden Verwaltungseinheit steht. Dies macht mitunter auch Arbeitsplatzuntersuchungen erforderlich, bei denen Befragungen von Stelleninhabern durchgeführt werden. Ob derartige Datenerhebungen zulässig sind, wurde auch im Kreise der Datenschutzbeauftragten erörtert. Nach § 19 Abs. 1 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Die Erforderlichkeit zur Durchführung von Organisationsuntersuchungen wird man nicht verneinen können; auch wird man den Beschäftigten aus der Pflicht, seinen Vorgesetzten zu beraten und zu unterstützen, für verpflichtet ansehen müssen, Anordnungen auszuführen und damit auch Fragen im Rahmen von Organisationsuntersuchungen zu beantworten. Handelt es sich jedoch um eine reine Mitarbeiterbefragung, bei der es nur um die subjektive Bewertung des Arbeitsumfelds geht, ohne daß diese in eine Organisationsuntersuchung einbezogen ist, geht dies nur auf freiwilliger Basis. Eine Stadtverwaltung hatte einen Fragebogen entwickelt, um Bürger und Bürgerinnen zur Beurteilung der Qualität der Mitarbeiter der Stadtverwaltung aufzufordern. Die Beurteilung der Arbeit von Mitarbeitern in einer Stadtverwaltung hängt nicht zuletzt davon ab, wie man mit einer getroffenen Entscheidung zufrieden ist. Beim Verlassen des Ordnungs- und Sozialamtes ist dies sicherlich anders zu betrachten als bei einer Eheschließung im Standesamt. Die Repräsentativität einer derartigen Befragung zu einer personenbezogenen Datenerhebung muß in Zweifel gezogen werden, da hier auch Manipulationen für oder gegen einzelne Mitarbeiter denkbar erscheinen. Soweit daher das Ergebnis der Befragung zur Beurteilung von Mitarbeitern und damit zu Personalentscheidungen herangezogen werden sollte, habe ich die beabsichtigte Form und den Inhalt der Datenerhebung unter Berücksichtigung des überwiegenden schutzwürdigen Interesses der betroffenen Mitarbeiter für datenschutzrechtlich unzulässig gehalten. Ich habe daher empfohlen, auf die Erhebung personenbezogener Daten zu verzichten. Die Stadtverwaltung ist diesem Vorschlag gefolgt.

6.15 Personenbezogene Daten beim Personalrat

Die Personalvertretung ist zur Durchführung ihrer Aufgaben rechtzeitig und umfassend unter Vorlage der Unterlagen, die die Dienststelle zur Vorbereitung der von ihr beabsichtigten Maßnahmen beigezogen hat, zu unterrichten (§ 68 Abs. 2 ThürPersVG). Die Unterrichtungspflicht umfaßt damit auch personenbezogene Daten, deren Speicherung beim Personalrat nach Abschluß des Beteiligungsverfahrens grundsätzlich nicht mehr erforderlich ist. Die Dauer der Speicherung von personenbezogenen Daten ist an die Erforderlichkeit zur Aufgabenerfüllung geknüpft. Aufgrund einer Anfrage bin ich der Frage nachgegangen, ob der Personalrat als Teil der Dienststelle, ihm zugeleitete Unterlagen wie Beurteilungen u. ä. fotokopieren und damit speichern darf. Diese Verfahrensweise würde nämlich dazu führen, daß beim Personalrat eine Personaldatenvorratshaltung entstehen kann, die der Bildung von Personalnebenakten gleichkommt, für die eine Rechtsgrundlage nicht besteht. Es stellte sich heraus, daß die Dienststelle dem Personalrat üblicherweise Schreiben, in denen umfänglich personenbezogene Daten enthalten waren, zum Zweck der Beteiligung zugeleitet hatte. Diese wurden urschrift-

lich der Dienststelle zurückgegeben. Der Personalrat sah sich veranlaßt, generell hiervon Kopien zu ziehen, um zu dokumentieren, daß eine Beteiligung stattgefunden hatte und auf welcher Beratungsgrundlage eine Entscheidung getroffen worden war. Dies betraf z. B. Unterlagen im Bewerbungsverfahren oder auch die Angabe der Gesamtbewertung einer Beurteilung bei Beförderungen. Selbstverständlich dürfen Anschreiben der Dienststelle, aufgrund derer der Personalrat tätig wird, vom Personalrat zu Sachakten genommen werden, da sie der Dokumentation der Tätigkeit dienen. Hierbei ist jedoch darauf zu achten, daß in diesen Anschreiben nur erforderliche personenbezogene Daten enthalten sind. Alle über die Bezeichnung des Beratungsgegenstands hinausgehenden Daten wären nicht erforderlich. Die betroffene Dienststelle hat mir zugesagt, daß in Abstimmung mit der Personalvertretung die Anfragen gemäß § 69 Abs. 2 Satz 4 ThürPersVG auf das unbedingt Notwendige beschränkt werden. Zukünftig enthalten diese nur den Namen des Betroffenen, die beabsichtigte Maßnahme und den vorgesehenen Zeitpunkt. Weitere personenbezogene Daten werden bei Bedarf, soweit notwendig, im Rahmen des Verfahrens gemäß § 69 ThürPersVG mündlich erörtert. Dagegen ist aus datenschutzrechtlicher Sicht nichts einzuwenden.

6.16 Abschottung der Beihilfestelle in einer Stadtverwaltung

Wie bereits im 1. TB (6.2.3) dargestellt, bedarf es bei der Abwicklung der Beihilfe nach § 98 ThürBG einer strikten Abschottung der Gesundheitsdaten von der übrigen Personalverwaltung. Dadurch, daß Beihilfeberechtigte einen Teil ihrer Arztkosten vom Dienstherrn erstattet bekommen, dürfen sie nicht gegenüber Mitarbeitern benachteiligt werden, die nicht beihilfeberechtigt sind und deren Gesundheitsdaten selbstverständlich nicht von der Krankenversicherung dem Personalamt zugänglich gemacht werden dürfen. In einer größeren Stadt habe ich daher die Einhaltung dieser Abschottungsvorschriften überprüft. Obwohl die Beihilfestelle dort im Personalamt angesiedelt war, konnten die organisatorischen Vorkehrungen (z. B. getrennte räumliche Unterbringung, getrennter Postlauf direkt zur Beihilfestelle etc.), die sicherstellen sollen, daß Personalsachbearbeiter keinen Zugriff auf die Beihilfedaten haben, als ausreichend angesehen werden. Lediglich bei der Gestaltung von Beihilfevordrucken gab ich einige Hinweise, um zu vermeiden, daß unnötigerweise immer wieder dieselben Daten vom Betroffenen und seinen Familienangehörigen erhoben werden, obwohl keine Änderungen vorlagen und diese bereits bei der Beihilfestelle vorlagen. Mit Neufassung der Formulare wurde diesen Forderungen entsprochen.
Als dennoch problematisch erwies sich die Eingliederung der Beihilfestelle in das Personalamt deswegen, weil im Rahmen von Beschwerden, Widersprüchen und Eingaben nicht ausgeschlossen war, daß die entsprechenden Unterlagen dem Vorgesetzten bzw. auch dem Behördenleiter vorgelegt werden können. Zwar war die Bearbeitung von Widersprüchen durch eine mündliche Weisung des Personalamtsleiters der Leiterin der Personalabrechnung zugewiesen, die im Gegensatz zum Amtsleiter bzw. Behördenleiter keine Aufgaben und Befugnisse bei Personalentscheidungen hat. Aufgrund der Weisungsgebundenheit war es den Vorgesetzten aber jederzeit möglich, sich im Einzelfall derartige Fälle vorlegen zu lassen. In zwei Fällen konnte ich feststellen, daß Widerspruchsbescheide in Beihilfesachen vom Leiter des Personalamtes gezeichnet worden waren. Mit dem Abschottungsgebot des § 98 ThürBG soll aber gerade vermieden werden, daß solchen Stellen, die Personalentscheidungen zu fällen haben, Unterlagen über gesundheitliche Verhältnisse des Betroffenen zur Kenntnis gelangen. Ich habe daher die Stadt aufgefordert, entweder die Beihilfestelle in eine andere, nicht mit Personalangelegenheiten befaßte Stelle einzugliedern oder aber durch eine schriftliche Anweisung konkret bezeichneten Mitarbeitern die ausschließliche Befugnis zur Bearbeitung und Entscheidung aller mit Beihilfeangelegenheiten zusammenhängenden Vorgänge abschließend zu übertragen. Die Stadt hat

sich für die letztere Möglichkeit entschieden und die Leiterin der Personalabrechnungsstelle mit der abschließenden Bearbeitung von Beihilfeangelegenheiten beauftragt. Wie bereits im 1. TB (6.2.3) dargestellt, halte ich gleichwohl eine Ansiedlung der Beihilfestelle außerhalb des Personalamts bzw. außerhalb der Gemeindeverwaltung für die vorzugswürdige Lösung, um von vornherein Konfliktsituationen auszuschließen. Die Landesregierung hat sich in ihrer Stellungnahme zu meinem 1. TB dieser Auffassung angeschlossen. Durch das Landesverwaltungsamt wurden die Landkreise und kreisfreien Städte in einem Rundschreiben auf die Möglichkeit zur Bildung einer zentralen Beihilfestelle in Form eines Zweckverbandes aufgrund der §§ 16 ff Gesetz über die kommunale Gemeinschaftsarbeit (GKG) hingewiesen.

6.17 Formular der Zentralen Beihilfestelle des Landesverwaltungsamtes

Verschiedene Beihilfeberechtigte haben mich gebeten, mich des Beihilfeformulars der Zentralen Beihilfestelle anzunehmen. Insbesondere richtete sich die Kritik dagegen, daß jeweils erneut Daten erhoben werden, obwohl sich keine Änderung gegenüber dem Vorantrag ergeben haben. Das LVwA, dem die Beihilfestelle angegliedert ist, hat dies eingeräumt, allerdings darauf verwiesen, daß mit der Einführung des Beihilfeabrechnungsprogramms ABBA die Erarbeitung eines neuen Beihilfeformulars erforderlich wird, das dem Formblatt des BMI entspricht. Danach obliegt es dem Antragsteller lediglich durch Ankreuzen zu kennzeichnen, daß sich keine Änderung bei den persönlichen Verhältnissen ergeben hat. Angesichts der angekündigten Einführung des Beihilfeabrechnungsprogramms ABBA habe ich die Angelegenheit auf sich bewenden lassen, da künftig meinen Bedenken Rechnung getragen zu werden schien. Bisher ist das Beihilfeabrechnungsprogramm ABBA aber noch nicht eingeführt worden.

6.18 Datenschutz für private Eintragungen im „Schreibtischkalender“

Zur datenschutzrechtlichen Bewertung wurde folgender Sachverhalt an mich herangetragen:
Ein Amtsleiter hatte Schreibtischkalender von Bediensteten für dienstliche Zwecke angefordert. Diese enthielten aber zum Teil private Eintragungen der Bediensteten. Die Prüfung der Rechtslage ergab, daß es sich bei einem Schreibtischkalender, der vom Dienstherrn zur Verfügung gestellt und von den Bediensteten geführt wird, um eine dienstliche Unterlage handelt, die grundsätzlich entsprechend § 63 Abs. 3 ThürBG auf Verlangen des Dienstvorgesetzten herauszugeben ist. Wenn einem Bediensteten also ein Schreibtischkalender nicht ausschließlich nur zu eigenen Zwecken zur Verfügung gestellt wird, muß er damit rechnen, daß seitens des Dienstherrn auch Einsicht begehrt wird. Gegen eine Heranziehung der Schreibtischkalender mit den darin enthaltenen Strichlisten war daher grundsätzlich nichts einzuwenden, wobei zur weiteren Beurteilung auch die Umstände des Einzelfalls hinsichtlich der Erforderlichkeit und Verhältnismäßigkeit gesehen werden müssen. Problematisch stellt sich die Angelegenheit jedoch im Hinblick auf die privaten Eintragungen dar. Daher sollten die Bediensteten darauf hingewiesen werden, daß die Schreibtischkalender unter Umständen für die Überprüfung von Angaben herangezogen werden können, so daß sie sich gegebenenfalls noch einen rein persönlichen Kalender anlegen können. Vor Einzug der Schreibtischkalender sollte, sofern die Einsichtsmöglichkeit durch den Dienstvorgesetzten nicht bekannt war, die Möglichkeit gegeben werden, rein private Eintragungen zu entfernen. Damit wäre sichergestellt, daß der Dienstvorgesetzte nicht unbeabsichtigterweise rein private Termine zur Kenntnis nimmt, wozu auch keinerlei Erforderlichkeit besteht.

6.19 Veröffentlichung der Ungültigkeitserklärung von Dienstausweisen

Wiederholt war im Thüringer Staatsanzeiger sinngemäß zu lesen, daß „Der Dienstausweis mit der Nummer (...) des ... (Dienstbezeichnung, Name, Vorname) verloren gegangen ist und für ungültig erklärt wird."
Ich habe mich mit dieser Angelegenheit an das TIM zur Klärung der Rechtsgrundlage und der Erforderlichkeit dieser Veröffentlichungen gewandt. Aus datenschutzrechtlicher Sicht begegnet die namentliche Bekanntgabe wegen der Prangerwirkung für die Betroffenen erheblichen datenschutzrechtlichen Bedenken. Zur Warnung Dritter davor, daß der einen in Verlust geratenen Dienstausweis Vorlegende nicht der Berechtigte sein kann, bedarf es einer Veröffentlichung des Namens nicht. Hier reicht die Angabe der Ausstellungsbehörde, des Ausstellungsdatums sowie der Dienstausweisnummer aus. Ich habe weiter angeregt, daß das TIM im Rahmen der Zuständigkeit als oberste Kommunalaufsichtsbehörde über das Landesverwaltungsamt und die Kreise und kreisfreien Städte entsprechende rechtliche Hinweise gibt.
Das TIM hat mir in dieser Sache geantwortet, daß Einvernehmen zwischen den Ressorts der Thüringer Landesregierung bestehe, die bisherige Veröffentlichungspraxis einzustellen. Die obersten Landesbehörden und das Landesverwaltungsamt wurden von Seiten des TIM darüber informiert, daß sich Mitteilungen der nachgeordneten Behörden sowie eine entsprechende Vorlage an die Redaktion des Thüringer Staatsanzeigers erübrigen.

6.20 Anschriftenverzeichnis ehemaliger DDR-Arbeitgeber

Immer wieder stellt sich die Frage nach der Zuständigkeit und dem Verbleib von Altakten. Im Berichtszeitraum erhielt ich Kenntnis davon, daß der Bundesversicherungsanstalt für Angestellte zur Klärung rentenrechtlicher Ansprüche ein Arbeitgeber- Verzeichnis vorliegt. Durch Gegenüberstellung der ehemaligen Betriebe und Einrichtungen der früheren DDR mit den jetzigen Rechtsnachfolgern wird in diesem Verzeichnis ein Überblick über den Verbleib der Lohn- und Gehaltsunterlagen dieser früheren Institutionen gegeben.

7. Polizei

7.1 Bundeskriminalamtgesetz - BKAG

Mit dem am 01.08.1997 in Kraft getretenen neuen Bundeskriminalamtgesetz (BGBl I S. 1650) hat der Bundesgesetzgeber bereichsspezifische Regelungen zur Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten und für die Wahrnehmung der Aufgaben des BKA auf den Gebieten der Gefahrenabwehr und Strafverfolgung geschaffen. Nach § 7 Abs. 6 BKAG bedarf es einer Rechtsverordnung über die Art der Daten, die nach den §§ 8 bis 9 BKAG als Daten der Zentralstelle und sonstige Dateien gespeichert werden dürfen. Diese Rechtsverordnung steht noch aus. Zu begrüßen ist, daß ausdrücklich normiert ist, daß die von den Ländern in das polizeiliche Informationssystem eingegebenen Datensätze von den jeweiligen Landesbeauftragten im Zusammenhang mit der Wahrnehmung ihrer Prüfungsaufgaben in den Ländern kontrolliert werden können, soweit die Länder nach § 12 Abs. 2, 3 BKAG verantwortlich sind.

7.2 Polizeirechtsänderungsgesetz

Seitens des TIM wurde ich im Vorfeld zum Thüringer Gesetz zur Änderung polizeirechtlicher Vorschriften (Thüringer Polizeirechtsänderungsgesetz vom 27.11.1997 - ThürPolRÄG, GVBl S. 422) beteiligt. Zur vorgesehenen Änderung von § 14 Abs. 1 Nr. 5 PAG, die die Einführung von verdachts- und ereignisunabhängigen Kontrollmöglichkeiten für allgemeine Personen- und

Fahrzeugkontrollen auf Bundesstraßen vorsieht, habe ich Bedenken im Hinblick auf die Einhaltung des Grundsatzes der Verhältnismäßigkeit geäußert. Nach dem bisherigen § 19 Abs. 1 Nr. 2 PAG war eine Ingewahrsamnahme nur bei Straftaten von erheblicher Bedeutung möglich. Der Gesetzentwurf hierzu sah vor, daß diese Beschränkung gestrichen wird, so daß nunmehr auch in Fällen leichter Kriminalität eine Ingewahrsamnahme möglich sein soll. Den damit möglichen Eingriff in das informationelle Selbstbestimmungsrecht sehe ich als unverhältnismäßig an. Meine diesbezüglichen Hinweise sind nicht aufgegriffen worden.

7.3 Europol

Gegen Ende des Berichtszeitraums verabschiedete der Bundestag am 10.10.1997 das Gesetz zu dem Übereinkommen vom 26.07.1995 auf Grundlage von Artikel K.3 des Vertrages über die Europäische Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL-Gesetz), zu dem auch der Bundesrat seine Zustimmung gegeben hat. Damit ist die Europol-Konvention ratifiziert und kann, wenn auch die anderen Staaten das Gesetz ratifiziert haben, in Kraft treten. Daß in einem zusammenwachsenden Europa grenzüberschreitende Verbrechensbekämpfung angezeigt ist, ist allgemein anerkannt.

Europol soll personenbezogene Daten aus den Mitgliedstaaten zentral speichern und auswerten, wobei die Berechtigung zur Abfrage und Einspeicherung das BKA und die LKA haben. Die Zuständigkeit für Europol ist u. a. gegeben für die Bereiche Terrorismus, illegaler Drogenhandel und sonstige schwerwiegende Formen internationaler Kriminalität, zu denen unter anderem Waffenhandel und Menschenhandel zählen. Zu Europol hat die europäische Datenschutzkonferenz in Manchester am 24./25.04.1996 (Anlage 23) festgestellt, daß die Konvention dem Datenschutz erhebliche Bedeutung beimißt. Europol hat keine eigene Ermittlungszuständigkeit, sondern verfolgt das Ziel, durch die Sammlung von Informationen und deren Übermittlung an die Mitgliedsstaaten, die Leistungsfähigkeit der dort zuständigen Behörden und ihre Zusammenarbeit zu verbessern. Dies soll dadurch erreicht werden, daß die nationalen Stellen - in Deutschland das BKA - Europol aus eigener Initiative Informationen liefern. Im Informationssystem von Europol dürfen nur die für die Erfüllung der Aufgaben von Europol erforderlichen Daten über Personen, die nach Maßgabe des nationalen Rechts einer Straftat, für die Europol zuständig ist, verdächtigt werden oder wegen einer solchen Straftat verurteilt worden sind oder bei denen bestimmte schwerwiegende Tatsachen nach Maßgabe des nationalen Rechts die Annahme rechtfertigen, daß sie Straftaten im Zuständigkeitsbereich von Europol begehen werden, gespeichert werden. Um welche Daten es sich handelt, ist in der Konvention ebenfalls näher bestimmt. Die Datenschutzbeauftragten haben in ihrer Konferenz vom 17./18.04.1997 zu Europol die Forderung des Europäischen Parlaments unterstützt, daß u. a. alle Informationen persönlichen Charakters von der Erfassung in Europol auszuschließen seien (Anlage 13). Detailliert ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu den Arbeitsdateien zu Anlaysezwecken geregelt, wobei auch ausdrücklich normiert ist, daß Daten nur übermittelt werden dürfen, soweit diese nach dem jeweiligen nationalen Recht zu Zwecken der Verhütung, Bekämpfung und Analyse von Straftaten verarbeitet werden dürfen. Für bedeutsam sehe ich an, daß es bei den Durchführungsbestimmungen, die vom Verwaltungsrat zu den Dateien ausgearbeitet werden, sowie bei den Bestimmungen über die Sicherheit der Daten und die interne Kontrolle ihrer Verwendung der Einstimmigkeit des Rates bedarf. Dabei werden auch Prüffristen und die Speicherungsdauer festgesetzt. Ebenfalls ist festzulegen, an wen die Daten übermittelt werden dürfen. Eine Verwendung der Daten für andere Zwecke oder durch andere Behörden ist nur zulässig, wenn der Mitgliedsstaat, der die Daten übermittelt

hat, hierzu seine Zustimmung gegeben hat und dies nach nationalem Recht des Mitgliedstaats zulässig ist. Eine Datenübermittlung an Drittstaaten oder Drittstellen kommt nur in Betracht, wenn dort ein angemessener Datenschutzstandard gewährleistet ist. Jeder kann einen Antrag stellen, um Auskunft über die von bei Europol über ihn gespeicherten Daten zu erhalten. Zur Kontrolle gibt es eine Gemeinsame Kontrollinstanz, in der neben einem auf Vorschlag des BfD zu ernennenden Vertreter auch ein vom Bundesrat zu wählender Ländervertreter teilnimmt. Nach § 5 Abs. 2 des Gesetzes über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union wird die Stellungnahme des Ländervertreters hierbei maßgeblich zu berücksichtigen sein. Europol kann aufgrund der Konvention erst dann in Aktion treten, wenn auch das Gesetz zu dem Protokoll vom 19.06.1997 aufgrund des Artikel K.3 des Vertrags über die Europäische Union und von Artikel 41 Abs. 3 des Europol-Übereinkommens über die Vorrechte und Immunität für Europol, die Mitglieder der Organe, die stellvertretenden Direktoren und die Bediensteten von Europol (Europol-Immunitätenprotokollgesetz) in Kraft getreten ist. Dies steht derzeit im Bundestag zur Beratung an.

7.4 Schengener Informationssystem - Schengener Durchführungsübereinkommen

Wie im 1. TB (4.3) berichtet, ist das Schengener Durchführungsübereinkommen (SDÜ), das zum Wegfall der gemeinsamen Binnengrenzen geführt hat, am 26.03.1995 in Kraft getreten.
Die für die datenschutzrechtliche Kontrolle des in Betrieb genommenen Schengener Informationssystems (SIS) eingesetzte gemeinsame Kontrollinstanz nach Artikel 115 SDÜ, in der die deutsche Delegation durch den BfD und den Hessischen Datenschutzbeauftragten vertreten ist, hat zwischenzeitlich einen Tätigkeitsbericht über den Zeitraum März 1995 bis März 1997 vorgelegt (Bundesratsdrucksache 423/97 vom 16.05.1997). Darin sind Ausführungen zu den Rechtsvorschriften, zum Schutz personenbezogener Daten und zu der Kontrollinstanz und deren Aufgaben sowie das Ergebnis einer Kontrolle der gemeinsamen Kontrollinstanz des ZSIS, des Zentralen Schengener Informationssystems mit Sitz in Straßburg, dargestellt.

Im Zusammenhang mit dem SDÜ ist weiterhin auch die Koordinierung der unterschiedlichen europäischen Datenverarbeitungssysteme (Schengener Informationssystem, Zollinformationssystem, Europol, Europäisches Informationssystem) sowie die Entwicklung der polizeilichen und justitiellen Zusammenarbeit zu diskutieren.

7.5 Automatisiertes Fingerabdrucksystem (AFIS)

Im 1. TB (7.6) hatte ich ausgeführt, daß AFIS ohne Errichtungsanordnung geführt wird. Im Hinblick auf das neue BKAG wird auf diesen Vorgaben die Errichtungsanordnung neu erarbeitet. Das TIM hat mir signalisiert, daß es meine Vorschläge in die erneute Abstimmung auf Länderebene einfließen lassen wird.

7.6 Datenschutzrechtliche Kontrollen im Polizeibereich

Bei den im Berichtszeitraum durchgeführten datenschutzrechtlichen Kontrollen im Polizeibereich wurde auch die Führung von polizeilichen automatisierten Verfahren einbezogen.
Bei einer Polizeidirektion (PD) habe ich mich über die Möglichkeiten von Abfragen aus den zentralen polizeilichen Dateien, unter anderem aus dem Ausländerzentralregister (AZR) und INPOL, auf die über das Landessystem „Informationssystem der Thüringer Polizei“ (ISTPOL), das mit dem Landes-

kriminalamt (LKA) verbunden ist, Zugriff genommen werden kann, informiert. Bei Anfragen von Bediensteten im Streifendienst werden Auskünfte über Personen, die in diesen Dateien erfaßt sind, erteilt. Bezüglich der Zugangs- und Zugriffsberechtigungen erfolgt halbjährlich eine Prüfung durch das LKA anhand einer Zugriffsprotokollierung. Zu den technischen und organisatorischen Maßnahmen ergaben sich in diesem Zusammenhang keine weiteren Fragen.
In der PD wird auch das „Integrationsverfahren Thüringen - Grundstufe“ (IGV-T) mit verschiedenen Programmteilen, u. a. auch Thüringer Zentraldateien genutzt. Im Rahmen dieses Verfahrens steht den PD auch die Möglichkeit offen, eigene Dateien anzulegen. Hierzu sind ebenfalls jeweils gesonderte Errichtungsanordnungen gemäß § 46 PAG, die einer datenschutzrechtlichen Freigabe nach § 34 Abs. 2 ThürDSG entsprechen, sowie Meldungen zum Datenschutzregister erforderlich. Da diese nicht vorlagen, erfolgte eine Beanstandung.
Bei der Kriminalinspektion der PD wird der Kriminalaktennachweis (KAN) als automatisierte Datei geführt. Die erstmalige Aufnahme von Daten führt zum Anlegen einer Grundakte, alle weiteren relevanten Ereignisse auch im Bereich anderer Dienststellen werden der aktenführenden Dienststelle zur Eintragung in diese Datei mitgeteilt. Für die PD sind alle Daten dieser Datei, die von Thüringer Polizeidienststellen angegeben werden, abrufbar. Die Überwachung der Löschfristen erfolgt durch das LKA.

Im Rahmen einer Kontrolle eines Informationssystems beim Polizeipräsidium Thüringen habe ich Empfehlungen zur Login-Protokollierung gegeben. Bei der Protokollierung wird festgehalten, welcher Nutzer an welchem Tag und um welche Uhrzeit sein Terminal aus- und einschaltet. Eine Änderung von Daten kann sodann in Verbindung mit der Berechtigungsdatei und kriminalistischer Mittel nachvollzogen werden. Eine meinerseits geforderte erweiterte Protokollierung des Zugriffs auf bestimmte Dateien und im Abrufverfahren als technisch-organisatorische Maßnahmen gemäß § 9 Abs. 2 Nr. 5 ThürDSG erschien den Verantwortlichen zunächst aus Verhältnismäßigkeitsgründen nicht realisierbar. Im Rahmen der Weiterentwicklung von IBP sollen neue Sicherheitsmechanismen nach Auskunft des LKA eingearbeitet werden.
Das Fehlen von datenschutzrechtlichen Freigaben von automatisierten Verfahren im Bereich der Personalverwaltung habe ich beanstandet.

Der Einsatz eines Zutrittskontrollsystems im LKA wurde mangels Freigabe und unzureichender Sicherungsmaßnahmen beanstandet. Die Beanstandung wurde zwischenzeitlich behoben.
Beim LKA, das nach § 8 Abs. 2 des Polizeiorganisationsgesetzes Zentralstelle für die polizeiliche Datenverarbeitung und Datenübermittlung ist, ließen sich die Mitarbeiter des TLfD unter anderem das Verfahren der Personenfahndung, des Abgleichs von Fingerabdrücken sowie die Führung der Kriminalstatistik darstellen.
Das Verfahren der Personenfahndung wird auf Veranlassung der Staatsanwaltschaft von den Polizeidirektionen, soweit nicht eine eigene Zuständigkeit des LKA begründet ist, in Gang gesetzt. Die Daten der Fahndungsausschreibungen werden über das LKA an das BKA übermittelt. Da die Fahndungsausschreibungen regelmäßig befristet sind, erfolgt vor Ablauf der Fahndungsfrist vom BKA die Übersendung von Fristenüberwachungslisten, die zur weiteren Veranlassung vom LKA an die PDs weitergegeben werden, da diese die Löschung oder die Fristverlängerung zu veranlassen haben.
Neben einer alphabetischen Sammlung der Fingerabdruckblätter werden die Fingerabdrücke auch automatisiert über AFIS erfaßt, um einen bundesweiten Abgleich zu ermöglichen.

Zur Führung der Kriminalstatistik ergaben sich keine Bedenken. Anonymisierung der Daten ist gewährleistet, eine Reanonymisierung erscheint ausgeschlossen.
Im Rahmen der zentralen Aufgabe im technischen Bereich für die Polizeidienststellen des Landes werden beim LKA auf dem zentralen Rechner auch Speicherkapazitäten für Dateien der Polizeidienststellen zur Verfügung gestellt. Das LKA ist hierbei lediglich im technischen Sinne verantwortlich. Die Verantwortung für die Dateiinhalte dieser sogenannten SPUDOK-Dateien verbleibt bei der zuständigen Polizeidienststelle.
Den datenschutzrechtlichen Forderungen und Empfehlungen im Ergebnis der Kontrolle ist weitestgehend nachgekommen worden. Zu einigen Punkten befinde ich mich noch in der Diskussion. Dazu gehört insbesondere die notwendige Erstellung eines umfassenden IT-Sicherheitskonzeptes.

7.7 Speicherung personenbezogener Daten bei der Polizei

Eine Petentin machte geltend, daß sie nach ihren Feststellungen im INPOL gespeichert war, obwohl hierfür keine Veranlassung bestand. Bei der Überprüfung des Vorgangs stellte sich heraus, daß gegen die Petentin ermittelt und das Verfahren nach § 170 Abs. 2 StPO eingestellt worden war. Von der Einstellung des Verfahrens im Jahre 1992 durch die Staatsanwaltschaft war jedoch die Polizei durch die Staatsanwaltschaft nicht informiert worden. Dies geschah erst nach Einschaltung des TLfD, so daß erst 1996 die personenbezogenen Daten im INPOL/ISTPOL gelöscht und das BKA darüber informiert wurde. Darüber habe ich den BfD, über den die Petition an mich herangetragen worden war, informiert.

7.8 Personalien in einer polizeilichen Allgemeinverfügung

Anläßlich einer verbotenen Versammlung in Saalfeld wurde von der dortigen Polizeidirektion im Oktober 1997 ein Betretungsverbot auf der Grundlage des § 18 Abs. 1 PAG verfügt. Mit der Verfügung, die in Saalfeld verteilt wurde, wurden die Personen, denen sie ausgehändigt wurde, aufgefordert, die darin aufgeführten Straßen bzw. Straßenzüge im Stadtgebiet Saalfeld bis zu einem genannten Termin, nicht zu betreten.

In der Begründung der schriftlichen Verfügung wurde der Name, Geburtsdatum und Wohnanschrift eines Bürgers angegeben, welcher im Stadtgebiet Saalfeld einen Demonstrationszug angemeldet hatte. Die Bekanntgabe der Personalien im Betretungsverbot war meiner Meinung nach nicht erforderlich und die Datenübermittlung demzufolge unzulässig. Gegenüber der PD Saalfeld habe ich deshalb gemäß § 39 ThürDSG eine Beanstandung ausgesprochen und das Polizeipräsidium Thüringen sowie das TIM als deren Aufsichtsbehörde gleichzeitig davon informiert.
Im Zusammenhang mit der ausgesprochenen Beanstandung forderte ich eine Stellungnahme und Mitteilung bezüglich der eingeleiteten Maßnahmen, um derartige Datenschutzverstöße zukünftig zu vermeiden. Das TIM teilte daraufhin mit, daß es unter Beachtung von § 22 ThürDSG nicht geboten war, Wohnsitzangabe und Geburtsdatum eines Bürgers im Betretungsverbot aufzunehmen. Es erfolgte an die Dienststellen der Thüringer Landespolizei die Anweisung, daß künftig bei der Erstellung von Handzetteln in Vorbereitung auf polizeiliche Einsätze die Aufnahme von personenbezogenen Daten unterlassen wird. Ich habe daraufhin die Beanstandung als behoben angesehen und weiter mitgeteilt, daß, auch wenn die Wohnanschrift eines Bürgers im Adreßbuch einer Stadt veröffentlicht und damit offenkundig ist, dies nicht die Bekanntgabe in einer polizeilichen Verfügung rechtfertigt.

7.9 Vermerk des Aktenzeichens auf dem Briefkuvert

Von einem Thüringer Bürger wurde mir mitgeteilt, daß auf der Außenseite des Briefumschlages des von einer Thüringer Polizeiinspektion an ihn gerichteten Schreibens ein Teil des Aktenzeichens dieses Schreibens handschriftlich vermerkt war.
Die betreffende Polizeiinspektion habe ich daraufhin um Stellungnahme zur Problematik gebeten, insbesondere um Information darüber, ob aufgrund der auf dem Briefumschlag vermerkten dreistelligen Zahl ein Bezug zu einer konkreten Straftat oder auch Ordnungswidrigkeit hergestellt werden kann. Von Seiten der Polizeiinspektion wurde mitgeteilt, daß zum Nachvollzug der Verwendung der Postwertzeichen in der Behörde die jeweilige Postsendung mit dem Aktenzeichen erfaßt wird. Vom vollständigen Aktenzeichen, das aus der Behördenkennziffer, der sechsstelligen Registriernummer, der Jahreszahl und einer Prüfziffer besteht, werden dafür ein Teil der Registriernummer und die Jahreszahl verwandt. Vom Amtsleiter wurde dabei versichert, daß durch den Vermerk dieses verkürzten Aktenzeichens auf dem Briefumschlag kein Rückschluß auf personenbezogene Daten des Empfängers bzw. auf den konkreten Sachverhalt möglich sei.
Im Ergebnis meiner datenschutzrechtlichen Prüfung habe ich dem Beschwerdeführer darüber informiert, daß kein datenschutzrechtlicher Verstoß festgestellt werden konnte. Der Polizeiinspektion habe ich mitgeteilt, daß ich die sichtbare Anbringung eines Teiles des Aktenzeichens auf dem Briefumschlag dennoch für nicht erforderlich halte. Dem wurde Rechnung getragen.

7.10 Erhebung und Verarbeitung von Daten im Rahmen der Verfolgung von Verkehrsordnungswidrigkeiten

Zur wirksamen Verfolgung von Verkehrsordnungswidrigkeiten muß der Halter immer mit den Tatdaten, wozu im besonderen bei Geschwindigkeitsüberschreitungen zur Ermittlung des Fahrers auch das Fahrerfoto zählt, konfrontiert werden. Stimmt der Fahrer nicht mit dem Halter überein, ist es erforderlich, den Kraftfahrzeughalter zum Fahrer zu befragen und ihm dazu wegen seiner späteren Zeugenschaft das Foto mit der abgebildeten Person zur Kenntnis zu geben. Seit 1996 wird deshalb in Thüringen nach einer Testphase bei einer Geschwindigkeitsüberschreitung dem Halter auf dem Anhörungsbogen das Tatfoto des Fahrers als Beweismittel übersandt. Zu damit verbundenen datenschutzrechtlichen Überlegungen (1. TB, 7.5.1) hat sich das zuständigen Innenministerium dahingehend geäußert, daß aufgrund der negativen Verkehrsunfallentwicklung in Thüringen und des überwiegenden öffentlichen Interesses an einer effektiven Verfolgung von Verkehrsordnungswidrigkeiten gegebenenfalls bestehende datenschutzrechtliche Bedenken zurückgestellt werden müssen. Im weiteren wird dies damit begründet, daß sich seit Einführung dieses Verfahrens die Anzahl der Einwendungen und Rückfragen bei der zentralen Bußgeldstelle erkennbar reduziert haben, so daß sich der erhoffte Effekt, die Betroffenen erkennen den Tatvorwurf eher bei unmittelbarer Vorlage des Beweismittels an, bestätigt hat. Durch technische und organisatorische Regelungen wird darüber hinaus gewährleistet, daß auf dem an den Halter übersandten Foto außer dem Fahrer keine weitere Personen abgebildet sind. Es liegen auch von den Betroffenen keinerlei datenschutzrechtlich begründete Einwendungen gegen diese Verfahrensweise vor.

Wirkt der Betroffene bei der Fahrerermittlung nicht mit, z. B. durch Aussageverweigerung, Nichtfolgeleistung einer Vorladung und wird er auch nicht zu Hause angetroffen, erfolgt im Rahmen der Fahrerermittlung die weitere Datenerhebung im Ordnungswidrigkeitsverfahren mittels eines Datenabgleichs mit Ausweis- oder Paßbildern in der Meldebehörde oder bei Dritten (z. B. Nachbarn). Meinem Vorschlag entsprechend soll künftig zur Informa-

tion der Betroffenen auf dem Anhörungsbogen der Hinweis aufgenommen werden, daß das Tatfoto, wenn der Halter sich nicht zum Vorwurf äußert oder keine Angaben zum Fahrer macht, mit dem Paß- und Personalausweisregister verglichen wird. Die Ermächtigung zum Datenabgleich ergibt sich aus § 22 Abs. 2 Nr. 1 bis 3 Paßgesetz (PaßG) bzw. § 2 b Abs. 2 Gesetz über Personalausweise. Danach dürfen Paß- bzw. Personalausweisbehörden anderen Behörden Daten aus dem Paßregister bzw. Personalausweisregister, wozu selbstverständlich auch die Fotos gehören, übermitteln, wenn die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen. Dies ist der Fall, wenn der Halter an der Fahrerermittlung nicht mitwirkt, da ein Datenabgleich in der Meldebehörde mit dem Fahrerfoto zweifellos einen geringeren Eingriff in das Selbstbestimmungsrecht der Betroffenen darstellt, als eine Befragung bei Dritten.

Nach längerer Prüfung und eingehenden Diskussionen zur datenschutzgerechten, inhaltlichen Gestaltung von Verwarnungsgeldangebots- und Anhörbögen bei Verkehrsordnungswidrigkeiten (1. TB, 7.5.1) hat nunmehr das Innenministerium durch Runderlaß an alle Polizeibehörden die notwendigen Veränderungen veranlaßt. Dies betraf insbesondere die eindeutige Festlegung von Pflicht- und freiwilligen Angaben. Desweiteren entfällt künftig aufgrund fehlender Erforderlichkeit die Erhebung einiger Daten.

7.11 Lichtbildernachweis in einem polizeilichen Auskunftssystem

Auf Nachfrage teilte mir das TIM mit, daß vorgesehen ist, ein digitales Lichtbildaufnahme- und Lichtbildverwaltungssystem für die Polizei des Landes Thüringen aufzubauen. Man verspricht sich davon eine Steigerung der Qualität der Täterlichtbilder, die sofortige Verfügbarkeit nach der Aufnahme und Erfassung für alle Polizeidienststellen des Landes sowie Recherchemöglichkeiten zur Bildvorlage unter Einhaltung datenschutzrechtlicher Bestimmungen bei verringertem Zeitaufwand. Im Rahmen der Arbeit mit dem Bilddatenbanksystem sollen personenbezogene Zugriffsberechtigungen erteilt und jeder Zugriff im Rechner entsprechend protokolliert werden. Mir ist zugesagt worden, das Pflichtenheft, das Gegenstand einer entsprechenden Ausschreibung sein soll. Ich werde diesen Vorgang auch weiterhin begleiten.

7.12 Videoüberwachung

Es ist abzusehen, daß der Einsatz von Videokameras auch im öffentlichen Bereich in Zukunft bundesweit zunehmen wird. Im Berichtszeitraum war ich mehrfach mit der Frage beschäftigt, unter welchen Voraussetzungen das Erheben, Verarbeiten und Nutzen der Videoaufnahmen zulässig ist. Ganz allgemein werden Videokameras installiert und Aufzeichnungen erstellt, um ein Objekt zu überwachen, Vorgänge zu dokumentieren, Beweismittel zu gewinnen sowie einen Abschreckungseffekt zu erreichen. Für die datenschutzrechtliche Beurteilung ist es von Bedeutung, ob die Videobeobachtung heimlich erfolgt oder aber deutliche Hinweise an alle Betroffenen erfolgen. Ebenso ist die ausschließlich für momentane Bilder genutzte Kamera „als verlängertes Auge“ von derjenigen zu unterscheiden, die das Beobachtete auch auf Videobändern mitzeichnet. Die Herstellung von Videoaufnahmen stellt in jedem Fall einen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen dar.

Ein großes Einsatzgebiet für Videokameras ist die Verkehrsüberwachung durch die Thüringer Verkehrspolizei. Die Geräte werden dabei während der Fahrt als auch im Stand z. B. zur Geschwindigkeits- und Abstandsüberwachung eingesetzt. Die erstellten Beweisbänder sind Beweisstücke im Sinne von § 147 StPO. In den Richtlinien für die polizeiliche Verkehrsüberwachung (StAnz. Nr. 29/1991 S. 595-599) ist bestimmt, daß die Video-Bänder

gelöscht werden können, wenn die Verwarnung wirksam geworden oder das Verfahren durch rechtskräftigen Bußgeldbescheid abgeschlossen oder eingestellt ist. Wie das TIM mir mitteilte, werden nicht verwertbare Aufnahmen sofort gelöscht. Die o. g. Richtlinie wird aber z. Zt. überarbeitet, so daß konkretere Regelungen zur Speicherungs- und Löschungsfrist zu erwarten sind.

In einem anderen Bereich hatte ich Presseartikeln entnommen, daß eine kreisfreie Stadt mehrere Wertstoffsammelplätze mit Videokameras überwachen läßt, weil dort häufig unerlaubte Müllablagerungen stattfinden würden.
Wie sich auf meine Anfrage hin heraus stellte, übernimmt die Abfallentsorgung eine GmbH, die zu 100% im Eigentum der Stadt liegt. Dieser Entsorger hatte eine private Sicherheitsfirma damit beauftragt, einen Wertstoffsammelplatz verdeckt mit einer Videokamera zu überwachen. Nicht aufgeklärt werden konnte meine Vermutung, daß der Entsorger nicht aus eigenem Antrieb heraus handelte, sondern vielmehr von der Stadt hierzu beauftragt wurde. Ordnungswidrigkeitsverfahren wurden aufgrund der erstellten Aufnahmen nicht eingeleitet.
Ich habe der Stadtverwaltung mitgeteilt, daß als Rechtsgrundlage für eine Videoüberwachung von Wertstoffsammelstellen zur Verhinderung unzulässiger Müllablagerungen § 26 Satz 1 Nr. 1 Thüringer Ordnungsbehördengesetz (ThürOBG) heranzuziehen ist. Danach können die Ordnungsbehörden Bildaufzeichnungen anfertigen, „soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß Gefahren für die öffentliche Sicherheit oder Ordnung entstehen.“ Zuvor sind aber alle Maßnahmen zu prüfen, die das informationelle Selbstbestimmungsrecht weniger beeinträchtigen (z. B. Aufstellen von Verbotsschildern, Stichprobenkontrollen durch Umweltamtmitarbeiter usw.). Im Rahmen des Verhältnismäßigkeitsgrundsatzes und des Übermaßverbotes sollte im Falle einer Videoüberwachung mit Hinweisschilder darauf aufmerksam gemacht werden. Allein dieser Hinweis könnte bereits eine abschreckende Wirkung haben.
Das TIM hat mir auf Anfrage mitgeteilt, daß es die Videoüberwachung für eine originäre staatliche Aufgabe halte und dem Funktionsvorbehalt von Art. 33 Abs. 4 GG unterfalle. Eine Übertragung von Videoüberwachungen von Wertstoffsammelplätzen auf Private hält das TIM für unzulässig. Es verwies hierzu auf die Rechtsprechung im Zusammenhang mit der Geschwindigkeitsmessung durch Private (1. TB, 7.5.3).

Im Nachgang zu einem Fußballspiel wandte sich ein Bürger an mich, der Videoaufzeichnungen von Polizeibeamten anläßlich eines Fußballspiels für unverhältnismäßig hielt und wollte wissen, ob eine derartige Vorgehensweise zulässig sei. Ich konnte ihm hierzu mitteilen, daß nach § 33 Abs. 1 PAG eine Ermächtigungsgrundlage für derartige Bild- und Tonaufnahmen besteht, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß Gefahren für die öffentliche Sicherheit und Ordnung entstehen.

In einem weiteren Fall stellte ich im Rahmen der datenschutzrechtlichen Kontrolle einer Hochschule fest, daß auf dem Campus an verschiedenen Stellen eine Videoüberwachungsanlage installiert wurde. Nach Angaben der Hochschulleitung wurde diese Maßnahme aufgrund von verschiedenen Vandalismusfällen notwendig. Neben „Live-Bildern“, die von den Kamerastandpunkten zum Pförtner übertragen werden, werden unter bestimmten Bedingungen auch regelmäßig Einzelstandbilder aufgezeichnet. Soweit keine Vorkommnisse während der Aufzeichnungsphase auftreten, werden die Aufzeichnungen am darauf folgenden Tag gelöscht (überspielt).
Wenn eine konkrete Gefahrenlage besteht, halte ich die Geländeüberwachung mittels einer Videoanlage zum Schutz von öffentlichen Einrichtungen an besonders gefährdeten Stellen für datenschutzrechtlich unbedenklich. Mangels einer spezialgesetzlichen Rechtsgrundlage ergibt sich die Zulässigkeit für die Videoüberwachung aus § 19 Abs. 1 ThürDSG. Im übrigen hat die

Hochschule auf meine Bitte hin an den Eingangspforten Hinweisschildern angebracht, die auf die Videoüberwachung hinweisen. Ich gehe davon aus, daß damit Vandalismusversuche bereits im Vorfeld verhindert werden können.

8. Verfassungsschutz

8.1 Kontrollbesuch beim Landesamt für Verfassungsschutz (TLfV)

Im Berichtszeitraum wurde im Thüringer Landesamt für Verfassungsschutz der Umgang mit personenbezogenen Daten im Rahmen von Sicherheitsüberprüfungen kontrolliert. Die erbetenen Auskünfte des TLfD dazu wurden durch das TLfV gegeben, und es wurde Einsicht in Sicherheitsüberprüfungsakten gewährt. Anlaß zu Beanstandungen in diesem Zusammenhang gab es nicht. Unabhängig davon bestehen jedoch nach wie vor zwischen dem TIM und mir unterschiedliche Auffassungen zu der Frage, wer als Betroffener zur Ausübung des Widerspruchsrechts nach § 37 Abs. 2 ThürDSG berechtigt ist. Während ich davon ausgehe, daß „Betroffener“ im Sinne des Sicherheitsüberprüfungsverfahrens nur die zu überprüfende Person ist, vertritt das TIM den Standpunkt, daß auch die einbezogenen Personen (Ehegatte, Lebenspartner) Widerspruch gemäß § 37 Abs. 2 ThürDSG erklären können. Falls ein Widerspruch von Seiten einer Auskunfts- oder Referenzperson erklärt wird, solle eine Trennung der Akte vorgenommen werden. Der Teil der Akte, der die Angaben der Auskunfts- bzw. Referenzperson beinhaltet, soll damit der Kontrolle durch den TLfD entzogen sein. Im übrigen soll die Akte dem TLfD zur Verfügung gestellt werden. Eine einvernehmliche Lösung bezüglich der unterschiedlichen Auffassungen zur Einsichtnahme des TLfD wurde nicht erreicht. Allerdings wurde andererseits auch das Kontrollrecht des TLfD bezüglich der Sicherheitsüberprüfungsakten im Berichtszeitraum nicht behindert oder eingeschränkt.

8.2 Sicherheitsüberprüfung

Bereits in meinem 1. TB hatte ich unter 8.1 darauf hingewiesen, daß es eines Sicherheitsüberprüfungsgesetzes bedarf, um Sicherheitsüberprüfungen, die bisher lediglich anhand von Richtlinien vorgenommen werden, auf eine eindeutige gesetzliche Grundlage zu stellen. Nachdem bislang kein Gesetzentwurf bekannt ist, möchte ich noch einmal an die Dringlichkeit der Verabschiedung eines Thüringer Sicherheitsüberprüfungsgesetzes erinnern.

9. Finanzen, Steuern, Rechnungsprüfung

9.1 Bereichsspezifische Regelungen in der Abgabenordnung (AO)

Wie im 1. TB (9.1.8) berichtet, war der BfD an das BMF herangetreten, um das datenschutzrechtliche Anliegen der Datenschutzbeauftragten des Bundes und der Länder zum Entwurf eines Abgabenordnungs-Änderungsgesetzes zu unterbreiten. Im Vorfeld des Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetzes (StMBG) waren die datenschutzrechtlichen Hinweise nicht berücksichtigt worden. Der aus Sicht des Datenschutzes erforderliche Änderungsbedarf der Abgabenordnung wurde in einer detaillierten Liste seitens des BfD dem BMF vorgelegt und hat zu einer Diskussion auf Bundesebene geführt. Das Ergebnis ist aber unbefriedigend, da die seitens der Datenschutzbeauftragten des Bundes und der Länder gemachten Vorschläge fast durchgängig abgelehnt wurden. Nach wie vor ist es aus datenschutzrechtlicher Sicht dringend erforderlich, vor allem den Umgang mit Daten, die dem Steuergeheimnis unterliegen, klarer zu regeln. Die Datenschutzbeauftragten des Bundes und der Länder werden weiterhin Vorschläge hierzu unterbreiten.

9.2 „Bescheidzustellung an Dritte“

Ein Petent hat mir folgendes datenschutzrechtliches Problem vorgetragen: Der an diesen Bürger von Seiten eines ARoV erlassene Bescheid hinsichtlich der Rückübertragung von Vermögenswerten wurde in vollständiger Form auch von diesem Bescheid betroffenen Dritten zur Verfügung gestellt. Diese Personen erhielten somit Kenntnis von Daten hinsichtlich des Eigentums, insbesondere Angaben über die die Interessen dieser Dritten nicht betreffenden Grundstücke des Beschwerdeführers. Zur datenschutzrechtlichen Klärung dieser Angelegenheit habe ich das ARoV um Mitteilung hinsichtlich der rechtlichen Grundlagen für die Übermittlung des Bescheides an dritte Personen gebeten. Aus meiner Sicht wäre zur Unterrichtung der betroffenen Dritten auch ein Auszug aus dem Bescheid ausreichend gewesen bzw. hätten schutzwürdige Daten des beschwerdeführenden Bürgers geschwärzt werden können. Nach § 29 Verwaltungsverfahrensgesetz (VwVfG) hat die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Darüber hinaus gilt für die Geheimhaltungsinteressen von Beteiligten in Verfahren im Verhältnis zueinander der § 30 VwVfG, hinsichtlich dessen die Beteiligten Anspruch darauf haben, daß ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden, von der Behörde nicht unbefugt offenbart werden. Die betreffende Behörde hat im Ergebnis der Prüfung des geschilderten Sachverhaltes eingeräumt, daß im vorliegenden Fall durch die Übersendung des kompletten Bescheides an betroffene Dritte diese Kenntnis von Grundstücksdaten erhalten haben, die die unmittelbaren Interessen dieser Dritten nicht berühren. Nach Mitteilung des Amtes handelte es sich dabei jedoch um einen bedauerlichen Ausnahmefall. Der hiermit festgestellte datenschutzrechtliche Verstoß in Form einer Übermittlung von personenbezogenen Daten an Unberechtigte wurde nach Mitteilung des Amtes zwischenzeitlich dadurch behoben, daß die Mitarbeiter ausdrücklich darauf hingewiesen wurden, bei allen Entscheidungen grundsätzlich eine Einzelfallprüfung durchzuführen, in welchem Umfang ein Bescheid den jeweiligen Verfahrensbeteiligten zugestellt wird, was eine geeignete Maßnahme darstellt, zukünftig die Einhaltung der datenschutzrechtlichen Bestimmungen sicherzustellen.

9.3 Kontrolle im Thüringer Landesamt zur Regelung offener Vermögensfragen (ThLARoV)

Die datenschutzrechtliche Kontrolle im ThLARoV führte aufgrund des Einsatzes von automatisierten Verfahren ohne die erforderliche datenschutzrechtliche Freigabe sowie wegen Mängeln bei der Führung von Personalakten zur datenschutzrechtlichen Beanstandung. Die Beanstandung der Personalaktenführung war darauf zurückzuführen, daß vorhandene Altunterlagen („Kaderakten“) grundsätzlich ohne Überprüfung eines unmittelbaren inneren Zusammenhangs der einzelnen Unterlagen mit den Dienstverhältnissen weitergeführt wurden. In den Personalakten waren auch Unterlagen enthalten, die nach § 97 Abs. 1 ThürBG nicht aufgenommen werden dürfen. Gesundheitszeugnisse, die wegen der enthaltenen sensiblen Daten nur in verschlossenen Umschlägen zur Personalakte genommen werden dürfen, waren offen abgeheftet. Auf anderen Unterlagen befanden sich zum Teil auch Namen mehrerer Betroffener, ohne daß die erforderliche Schwärzung erfolgt war. Es wurde zugesagt, daß meinen Forderungen im Rahmen der laufenden Personalaktenbearbeitung nachgekommen wird.
Weitere Datenschutzforderungen und Empfehlungen wurden zur Umsetzung von Sicherungsmaßnahmen am Gebäude aufgestellt. Diese wurden im Rahmen der Möglichkeiten umgesetzt bzw. in Angriff genommen. Zur Zugriffssicherung beim vorhandenen Datenverarbeitungssystem wurden den

Anforderungen zur Gestaltung des Paßworts durch eine entsprechende Hausverfügung nachgekommen. Alle erforderlichen Maßnahmen wurden ergriffen.

9.4 Kontrollen in der Finanzverwaltung

Im Berichtszeitraum wurden drei Finanzämter kontrolliert:
Bei einem Finanzamt führte der Einsatz von automatisierten Verfahren in der Personalverwaltung ohne die erforderlichen datenschutzrechtlichen Freigaben nach § 34 Abs. 2 ThürDSG und fehlende Meldungen zum Datenschutzregister sowie die Personalnebenaktenführung zu datenschutzrechtlichen Beanstandungen. Die Freigaben zu den automatisierten Verfahren und die Meldungen zum Datenschutzregister wurden zwischenzeitlich nachgereicht. Bezüglich der Führung von Personalnebenakten wurde unter Verweis auf den Erlaß des Thüringer Finanzministeriums (TFM) mitgeteilt, daß alle Unterlagen, die zur konkreten Aufgabenerfüllung nicht erforderlich sind, entnommen wurden. Zur Frage der Aufbewahrung von Lohnsteuerkarten des Statistikjahres 1992, die dem Finanzamt in keiner erkennbaren Ordnung zurückgegeben worden waren, wurde festgelegt, daß diese fünf Jahre nach den entsprechenden Bestimmungen aufzubewahren sind.

Durch eine Mitteilung in der Presse erhielt ich Kenntnis davon, daß von Seiten eines Thüringer Finanzamtes Steuerunterlagen eines Bürgers einem offensichtlich falschem Empfänger zugestellt worden waren. Es handelte sich bei diesen Steuerunterlagen um personenbezogene Daten, die dem Steuergeheimnis gemäß § 30 AO unterliegen. Diese unzulässige Datenübermittlung wurde von mir im Ergebnis der durchgeführten Kontrolle gemäß § 39 Abs. 1 i. V. m. § 9 Abs. 3 ThürDSG beanstandet. Das Finanzamt hat mir mitgeteilt, daß die Mitarbeiter des Finanzamtes nach diesem Vorfall erneut angewiesen wurden, der Überwachung des Postausganges besondere Aufmerksamkeit zu widmen und verstärkt darauf zu achten, daß Post an den richtigen Empfänger adressiert und abgesandt wird. Von Seiten der OFD wurde eine Verfügung zum Steuergeheimnis erlassen, die auf die Notwendigkeit der besonderen Sorgfalt beim Postausgang in den Finanzämtern hinweist, um zukünftig Verletzungen des Steuer- bzw. Datengeheimnisses in den Finanzämtern auszuschließen. Ich sehe diese Maßnahmen als geeignet an, den Datenschutz für die Zukunft zu gewährleisten.

Bei der Kontrolle eines weiteren Finanzamts wurden ebenfalls in der Personalverwaltung mehrere automatisierte Verfahren zur Verarbeitung personenbezogener Daten vorgefunden, die weder datenschutzrechtlich gemäß § 34 Abs. 2 ThürDSG freigegeben, noch zum Datenschutzregister gemeldet waren, was zur Beanstandung führte. Die erforderlichen Maßnahmen sind zwischenzeitlich realisiert worden. Diese Kontrolle hatte ich zum Anlaß genommen, drei zur Aufgabenerfüllung der Besteuerung bei allen Thüringer Finanzämtern eingesetzten automatisierten Verfahren näher zu beleuchten. Datenschutzrechtliche Freigaben und Registermeldungen waren vor Ort nicht bekannt. Bezeichnend für diese Kontrolle war, daß die datenschutzrechtliche Verantwortlichkeit beim Einsatz dieser drei zur Aufgabenerfüllung eingesetzten automatisierten Verfahren den Ansprechpartnern nicht bekannt war. Mittels des automatisierten Verfahrens IABV (Integriertes Automatisiertes Besteuerungsverfahren) erfolgt die Steuererhebung und -festsetzung. Das Verfahren wird zentral bei der OFD eingesetzt und verwaltet. Die Daten der Steuerpflichtigen werden in den Finanzämtern mittels Datenerfassungsgeräten aufgenommen und täglich per Standleitung zur OFD transferiert. Es wurden die Zugriffe und deren Protokollierung geprüft. Die erforderlichen technischen und organisatorischen Maßnahmen gemäß § 9 ThürDSG in diesem Zusammenhang waren gegeben.

Die Bewertung von Grundstücken zur Festsetzung der Grundsteuer, der Feststellung der Einheitswerte und der Berechnung der Einkommenssteuer erfolgt mittels des automatisierten Verfahrens ELF (Ersatzwirtschaftswerte für Land- und Forstwirtschaft). Zu den technischen und organisatorischen Sicherheitsmaßnahmen nach § 9 Abs. 2 ThürDSG wurden datenschutzrechtliche Forderungen aufgemacht, denen nachgekommen wurde.
Zur Bewertung des Grundvermögens wird in den Finanzämtern das automatisierte Verfahren BBT (Bewertungsverfahren Brandenburg/Thüringen) eingesetzt. Das Verfahren wird seit 1994 in Thüringen genutzt. Die Betreuung des lokalen Netzes, auf dem das Verfahren abgearbeitet wird, obliegt der OFD. Ein Sicherheitskonzept bzw. eine zusammenfassende Darstellung von den vorhandenen technischen und organisatorischen Sicherheitsmaßnahmen konnte nicht vorgelegt werden. Einzelne Festlegungen sind zwischenzeitlich erfolgt. Bezüglich der Log-in-Prozedur wird seitens der Finanzverwaltung noch geprüft, inwieweit die Anzahl der fehlerhaften Login-Versuche begrenzt und ein automatischer Paßwortwechsel nach vorgegebener Gültigkeitsdauer eingerichtet werden kann.
Zu den Akten der Bodenschätzungen waren Kopien von Auszahlungsanordnungen für die Entschädigung ehrenamtlicher Sachverständiger genommen worden, damit nachvollziehbar war, welcher Sachverständige beteiligt war. Daß aber aus der Auszahlungsanordnung auch die Kontonummer des Betroffenen und die Art und Weise der durchgeführten Dienstreise zu entnehmen war, stieß auf datenschutzrechtliche Bedenken wegen der Speicherung nicht erforderlicher personenbezogener Daten. Nach dem entsprechenden Hinweis wurde zugesagt, künftig nur noch die erforderlichen Daten, nämlich Name des Sachverständigen und Datum der Schätzung, in diesen Akten zu dokumentieren.
Im Ergebnis der Kontrolle habe ich das Finanzamt aufgefordert, sich unverzüglich über die in seiner Verantwortlichkeit liegenden datenschutzrechtlich relevanten Umstände zu informieren und die Einhaltung der datenschutzrechtlichen Vorschriften sicherzustellen. Im Nachgang wurde mit dem TFM und der OFD geklärt, daß, auch wenn die Nutzung eines Verfahrens vorgeschrieben ist und das Verfahren zentral eingesetzt wird, die nutzenden Finanzämter als speichernde Stellen im Sinne des § 3 Abs. 5 ThürDSG nicht von ihrer datenschutzrechtlichen Verantwortlichkeit befreit sind.

9.5 Verfolgung von „Steuersündern“

Im Wege der Beschwerde hatte sich ein Betroffener wegen der Verfahrensweise der Finanzbehörden, deren Verfolgung er sich ausgesetzt sah, an mich gewandt. Der Beschwerde lag folgender Sachverhalt zugrunde:
Unter dem Namen des Beschwerdeführers war im Freistaat Thüringen ein Gewerbe angemeldet worden. Da der Betroffene unter der angegebenen Adresse nicht auffindbar war, hatte das zuständige Finanzamt ein Adressenfeststellungsverfahren eingeleitet. Hierbei kam man auf den Betroffenen. Da Steuerschulden aufgelaufen waren, wurden ihm mehrere Steuerfestsetzungen, Mahnungen bis hin zu Vollstreckungsbescheiden durch verschiedene Finanzämter, auch verschiedener Bundesländer, im Rahmen der Amtshilfe zugestellt. Der Beschwerdeführer machte jeweils geltend, es könne sich nicht um ihn handeln, er übe kein Gewerbe aus, sondern befinde sich seit Jahren in einem festen Arbeitsverhältnis. Hierzu legte er eine an ihn adressierte Bescheinigung seines Arbeitgebers vor. Darüber hinaus seien ihm in der Vergangenheit die Ausweispapiere gestohlen worden. Im steuerstrafrechtlichen Ermittlungsverfahren, das gegen den Betroffenen eingeleitet worden war, erfolgte kurzerhand zunächst eine telefonische Anfrage der zuständigen Bußgeld- und Strafsachenstelle eines Thüringer Finanzamts beim Arbeitgeber nach Fehlzeiten. Dadurch erhoffte man sich Aufschluß darüber, ob Handlungen als Gewerbetreibender zu bestimmten Zeiten in anderen Bundesländern möglich gewesen sein könnten. Per Telefax wurde unter dem

Betreff „Strafverfahren gegen ...“ unter Angabe des Aktenzeichens sodann die begehrte Auskunft verlangt. Aus datenschutzrechtlicher Sicht war nichts dagegen einzuwenden, daß den Finanzämtern auch über Landesgrenzen hinweg im Wege der Amtshilfeersuchen die personenbezogenen Daten des Betroffenen übermittelt wurden. Dies ist nach der Abgabenordnung möglich. Die Anfrage an den Arbeitgeber jedoch begegnete aus datenschutzrechtlicher Sicht erheblichen Bedenken. Per Telefax wurde dem Arbeitgeber als unbeteiligtem Dritten übermittelt, daß ein Strafverfahren gegen den Betroffenen besteht. Hierbei handelt es sich um ein sensibles personenbezogenes Datum, dessen Übermittlung mangels einer konkreten Übermittlungsvorschrift an der Verhältnismäßigkeit zu messen ist. Danach muß die jeweilige Maßnahme unter Würdigung aller persönlichen und tatsächlichen Umstände des Einzelfalls zur Erreichung des angestrebten Zwecks geeignet und erforderlich sein. Dies konnte nicht schlüssig dargelegt werden. Allein die Vermutung, ein Beschuldigter könnte nicht die Wahrheit sagen, weil er dazu auch nicht verpflichtet ist, reicht nicht aus. Auch gilt im steuerstrafrechtlichen Ermittlungsverfahren die Unschuldsvermutung, bis eine Schuld nachgewiesen wird. Ein weniger eingriffsintensives Mittel wäre gewesen, dem Beschuldigten aufzugeben, eine Bestätigung seiner Abwesenheitszeiten beizubringen. Hätten sich daraus Anhaltspunkte für Zweifel an der Richtigkeit ergeben, wäre eine Nachfrage zur Überprüfung der Angaben zulässig gewesen. Eine zeitliche Abkürzung, die direkte Anfrage beim Arbeitgeber vorzunehmen, rechtfertigt dieses Vorgehen jedoch nicht. Auch das Vorbringen, der Arbeitgeber sei als Zeuge zu sehen, der zu wahrheitsgemäßen Angaben verpflichtet sei, konnte nicht überzeugen. Eine erforderliche Belehrung, die eine Zeugenvernehmung voraussetzt, war im übrigen nicht erkennbar. Ich habe die Übermittlung daher als Verstoß gegen die datenschutzrechtlichen Vorschriften beanstandet. Darüber hinaus wurde dem Arbeitgeber auch der Abschluß der Ermittlungen mitgeteilt. Auch dies begegnete erheblichen datenschutzrechtlichen Bedenken. Eine Zulässigkeit dieser erneuten Übermittlung von personenbezogenen Daten des Betroffenen über den Verfahrensausgang lag ebenfalls nicht vor. Es konnte nur davon ausgegangen werden, daß der Schaden, den der Betroffene durch die Anfrage beim Arbeitgeber möglicherweise erlitten hatte, mit dieser erneuten Übermittlung behoben werden sollte. Eine „Heilung“ der ursprünglich unzulässigen Übermittlung konnte dadurch jedoch nicht eintreten. Seitens der Finanzverwaltung wird zwar nach wie vor in Abrede gestellt, daß das Mittel unverhältnismäßig war. Sie beruft sich zum Vorgehen auf die Anwendung der „Anweisung für das Straf- und Bußgeldverfahren (Steuer) - AStBV (St)“, zu der zu bemerken ist, daß diese Anweisung nicht den Anforderungen an bereichsspezifische Regelungen in Gesetzesnormqualität genügt und daher keine Rechtsgrundlage für Eingriffe in das informationelle Selbstbestimmungsrecht darstellt. Meiner Forderung, durch geeignete Maßnahmen sicherzustellen, daß zukünftig unzulässige Datenübermittlungen unterbleiben, wurde seitens der Finanzverwaltung aber dergestalt nachgekommen, daß die Angelegenheit mit den Mitarbeitern erörtert und künftig eine behutsamere Formulierung bei der Nutzung der gesetzlichen Möglichkeiten im Strafverfahren zugesagt wurde.

9.6 Führung eines Fahrtenbuches durch Ärzte für steuerliche Zwecke

Im Kreis der Datenschutzbeauftragten des Bundes und der Länder wurde im Berichtszeitraum die datenschutzrechtliche Problematik bei der Führung eines Fahrtenbuches für steuerliche Zwecke diskutiert. Durch das Jahressteuergesetz 1996 wurde die ertragssteuerliche Behandlung der privaten Kfz-Nutzung sowie die Pauschalierung der Privat-PKW-Kosten für alle Einkunftsarten vereinheitlicht. Der private Nutzungsanteil eines zum Betriebsvermögen des Steuerpflichtigen gehörenden Kraftfahrzeugs oder der private Nutzungsanteil eines dem Arbeitnehmer vom Arbeitgeber zur Verfügung

gestellten Kraftfahrzeuges ist danach monatlich mit 1 v. H. des inländischen Listenpreises anzusetzen. Diese Anwendung der Pauschalregelung führt zwar zu einer erheblichen Steuervereinfachung, kann aber im Einzelfall zu einer deutlichen Steuermehrbelastung führen, denn eine Pauschalierung kann den Besonderheiten im Einzelfall nur unvollkommen Rechnung tragen. Als Ausnahme zu den Festlegungen des Jahressteuergesetzes 1996 kann der Steuerpflichtige daher die auf die Privatfahrten anfallenden tatsächlichen Kosten ansetzen, wenn er die für das Fahrzeug entstehenden Aufwendungen durch Belege und das Verhältnis der privaten zu den übrigen Fahrten durch ein Fahrtenbuch nachweist.
Der BfD hat mitgeteilt, daß das BMF ab 01.01.1998 bei Führung eines Fahrtenbuches für steuerliche Zwecke dazu von Ärzten die Angabe „des aufgesuchten Patienten - als „Geschäftspartner“ - zusätzlich zu der Angabe „Patientenbesuch“ - als „Reisezweck“ - fordert. Die im Rahmen einer Geschäfts- bzw. Dienstfahrt aufgesuchten Gesprächspartner haben aber ein durch § 203 StGB geschütztes Interesse an der Verschwiegenheit des Fahrtenbuchführenden. Dieses Interesse bezieht sich nicht nur auf den Inhalt des im Rahmen des Besuches geführten Gespräches, sondern kann bereits durch die Offenbarung der Tatsache, daß ein Besuch stattgefunden hat, verletzt werden. Bereits die Kenntnis vom stattgefundenen Besuch kann unbefugt im Sinne des § 203 StGB sein - es sei denn, der Besuchende hätte in diese Offenbarung eingewilligt bzw. der Fahrtenbuchführer wäre aufgrund besonderer Gesetze zur Offenbarung verpflichtet.
Da gesetzliche Regelungen, die diese Angaben für die ordnungsgemäße Führung eines Fahrtenbuches festlegen, nicht vorliegen, habe ich das TFM um Stellungnahme und Mitteilung zur Problematik gebeten.

9.7 Datenschutz bei der Ausstellung und Versendung von Lohnsteuerkarten

Das bislang in Thüringen verwendete Merkblatt über die Ausstellung und Übermittlung der Lohnsteuerkarten durch die Gemeinden enthielt keine eindeutige Regelung hinsichtlich der Zustellung von Lohnsteuerkarten für Ehegatten. Wie im 1. TB (9.1.2) berichtet, hatte ich gebeten, auf dieses Problem bei der Zustellung hinzuweisen und damit die gemäß § 9 Abs. 1 ThürDSG erforderlichen technischen und organisatorischen Maßnahmen zu treffen. Das TFM hat mich darüber informiert, daß hinsichtlich der Ausstellung und Übermittlung der Lohnsteuerkarten ein neuer Erlaß gefertigt wurde, in dem geregelt ist, die Lohnsteuerkarten von Ehegatten getrennt zuzustellen. In diesem Zusammenhang habe ich beim TFM weitere Informationen hinsichtlich der Handhabung der Ausstellung und Übermittlung der Lohnsteuerkarten eingeholt. Es wurde mitgeteilt, daß die Gemeinden dafür in erheblichem Umfang private Serviceunternehmen nutzen. Soweit Auftragsverarbeitung durch Private erfolgt, sind die Bestimmungen des § 8 ThürDSG zu beachten, d. h., der Auftraggeber bleibt für die Einhaltung des ThürDSG verantwortlich und hat mich darüber hinaus über diese Beauftragung zu unterrichten. Personenbezogene Daten auf der Lohnsteuerkarte sind nicht nur Name und Anschrift des Bürgers, sondern auch Steuerdaten wie Familienstand, Steuerklasse und Konfession. Gegenwärtig werden Gespräche mit dem TFM geführt, damit bis zur Vorbereitung des Druckes der Lohnsteuerkarten für 1999 (ab Mai 1998) alle Maßnahmen getroffen werden können, um sowohl den Datenschutz als auch das Steuergeheimnis gemäß § 30 AO zu gewährleisten.

9.8 Übermittlung von Fördermittelanträgen an Finanzamt

Ein Landratsamt bat mich um eine datenschutzrechtliche Beurteilung zur Frage, ob Daten von Empfängern von Wohnungsbaufördermitteln listenmäßig auf Anforderung an das Finanzamt zu übermitteln sind. Auf Anfrage bei der OFD hat diese mitgeteilt, daß gemäß § 93a AO die Bundesregierung

durch Rechtsverordnung Behörden verpflichten kann, Verwaltungsakte, die die Versagung oder Einschränkung einer steuerlichen Vergünstigung zur Folge haben oder die Subvention oder ähnliche Fördermaßnahmen darstellen, den Finanzbehörden mitzuteilen. Eine Benachrichtigungspflicht ergibt sich aus § 4 Mitteilungsverordnung. Danach haben Behörden Verwaltungsakte mitzuteilen, die den Wegfall oder die Einschränkung bei einer steuerlichen Vergünstigung zu Folge haben können. Da es sich bei den erlassenen Bewilligungsbescheiden um Verwaltungsakte handelt, die einen Einfluß auf die Gewährung von steuerlichen Vergünstigungen haben, habe ich mich der Meinung der OFD angeschlossen und dem Landratsamt mitgeteilt, daß sich aufgrund der bestehenden bereichsspezifischen Vorschriften keine datenschutzrechtlichen Einwände gegen eine listenmäßige Übermittlung der Fördermittelempfänger an das Finanzamt ergeben.

9.9 Einsichtsrecht des Rechnungshofs in Personalakten von Beamten

In meinem 1. TB (6.1.4) hatte ich die Diskussion im Kreise der Datenschutzbeauftragten von Bund und Ländern aufgegriffen, die Nutzung von Personalaktendaten durch den Rechnungshof normenklar zu regeln.
In der Stellungnahme der Landesregierung wurde dazu ausgeführt, daß § 95 der Landeshaushaltsordnung (LHO) eine ausreichende Rechtsgrundlage für die Vorlage der Akten im erforderlichen Umfang darstellt, soweit der Rechnungshof zum Vollzug seines gesetzlichen Auftrags Einsicht in Personalakten nehmen muß.
Es ist unbestritten, daß der Rechnungshof als selbständiges unabhängiges Organ der Finanzkontrolle einen uneingeschränkten Prüfungsauftrag der gesamten Haushalts- und Wirtschaftsführung des Landes hat. Dies schließt auch die Prüfung finanzwirksamer Vorgänge in Personalakten ein. Soweit sich der Rechnungshof beim Einsichtsrecht in Personalakten auf das Unerläßliche und unbedingt Notwendige beschränkt, werden keine datenschutzrechtlichen Bedenken erhoben. Mir ist bisher auch kein Fall bekannt geworden, um Kritik an der Prüfpraxis des Rechnungshofs zu üben. Gerade auch ein Gespräch im Landesrechnungshof machte deutlich, daß beim Umgang mit personenbezogenen Daten der Verhältnismäßigkeitsgrundsatz beachtet wird und Unterlagen vertraulicher Art, wie Gesundheitszeugnisse und Beurteilungen, nicht Gegenstand von Prüfungsvorgängen sind.

10. Justiz

10.1 Justizmitteilungsgesetz

Das im 1. TB (10.1) als noch ausstehende bereichsspezifische Regelung genannte Justizmitteilungsgesetz (JuMiG) liegt zwischenzeitlich vor (BGBl I 1997, S. 1430). Mit Inkrafttreten des JuMiG im Juni 1998 wird eine Lücke der bereichsspezifischen Regelungen geschlossen. Bis dahin sind auch die entsprechenden Verwaltungsvorschriften -Mitteilungen in Strafsachen (MiStra) und Mitteilungen in Zivilsachen (MiZi)- anzupassen. Die Datenschutzbeauftragten des Bundes und der Länder haben die Gelegenheit erhalten, zu den Verwaltungsvorschriften Stellung zu nehmen. Neben den allgemeinen datenschutzrechtlichen Anliegen, wie verschiedene sensible Mitteilungen von der Entscheidung durch hierfür qualifizierte Personen, nämlich Richtern und Staatsanwälten, abhängig zu machen und die Betroffenen von den Mitteilungen in Kenntnis zu setzen, scheint es mir aus den praktischen Erfahrungen (vgl. 10.16) erforderlich, auch konkrete Bestimmungen der Adressaten von Mitteilungen in Thüringen in den Verwaltungsvorschrift bereits zu berücksichtigen, um sicherzustellen, daß nur die zur Kenntnisnahme Befugten auf direktem Weg die Mitteilungen erhalten.

10.2 Beratungen zum Strafverfahrensänderungsgesetz (StVÄG 1996)

Im 1. TB (10.1) waren fehlende bereichsspezifische Regelungen im Bereich der Justiz dargestellt worden. Hierzu hatte die Landesregierung in ihrer Stellungnahme auf die Regelungskompetenz des Bundes und die Notwendigkeit, den Verwaltungsaufwand gering zu halten, hingewiesen. Eine Zuständigkeit des TMJE sei nur mittelbar, nämlich über die Mitwirkung im Bundesrat, gegeben. Ende 1996 wurde von der Bundesregierung erneut ein Gesetzentwurf für ein StVÄG 1996 vorgelegt. Er enthält Regelungen für die strafprozessuale Ermittlungstätigkeit und die Verwendung personenbezogener Daten, die in einem Strafverfahren erhoben sind, über die Öffentlichkeitsfahndung und die Inanspruchnahme der Medien, über die Erteilung von Aktenauskünften und Akteneinsichten für Justizbehörden, andere öffentliche Stellen und Private sowie die Übermittlung von Erkenntnissen für Forschungszwecke und die Bestimmung, unter welchen Voraussetzungen die Polizeibehörden künftig personenbezogene Informationen, die für Zwecke der Strafverfolgung erhoben worden sind, auch für präventiv-polizeiliche Zwecke verwendet werden dürfen. Die Erwartung der DSB des Bundes und der Länder, daß damit die Lücken von bereichsspezifischen Regelungen in zufriedenstellender Art und Weise geschlossen werden, haben sich nicht vollständig erfüllt. Dies vor allem deshalb, weil der Gesetzentwurf der Bundesregierung bereits in Teilbereichen den Vorgaben des Bundesverfassungsgerichts nicht gerecht wird und teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen zurückfällt, aber auch, weil er im Gesetzgebungsverfahren durch die Stellungnahme des Bundesrats noch weitergehende datenschutzrechtliche Verschlechterungen erfahren hat. Die Datenschutzbeauftragten des Bundes und der Länder haben sich auf der 53. Konferenz in der Entschließung zu „Beratungen zum StVÄG 1996“ (Anlage 10) gegen die gravierenden datenschutzrechtlichen Verschlechterungen gewandt und den Gesetzgeber aufgefordert, bei den anstehenden weiteren Beratungen des Gesetzentwurfs die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

10.3 Öffentliche Fahndung im Strafverfahren

Das Recht von Betroffenen auf informationelle Selbstbestimmung wird stets bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Beschuldigten, Verurteilten, Strafgefangenen und Zeugen eingeschränkt. Nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil bedarf es für alle Maßnahmen der öffentlichen Fahndung nach Personen einer normenklaren und dem Grundsatz der Verhältnismäßigkeit entsprechenden gesetzlichen Regelung. Eine solche fehlt bisher. Fahndungsmaßnahmen sind gegenwärtig durch die bundeseinheitlichen Verwaltungsvorschriften „Richtlinien über die Inanspruchnahme von Publikationsorganen zur Fahndung nach Personen bei der Strafverfolgung“ geregelt. Im vorliegenden Regierungsentwurf eines StVÄG 1996 finden sich zwar in den §§ 131 bis 131c StPO Regelungen, wobei jedoch Zweifel bestehen, ob diese den verfassungsrechtlichen Anforderungen genügen. Die zur Problematik der öffentlichen Fahndung im Strafverfahren aufgestellten Grundsätze und Forderungen wurden von der 51. Datenschutzkonferenz am 14./15. März 1996 zustimmend zur Kenntnis genommen (Anlage 2). Das TMJE sah für seinen Geschäftsbereich jedoch im Hinblick auf die zu erwartende Gesetzesänderung und die Tatsache, daß die bisher angewandte Verwaltungsvorschrift des TMJE vom 29. April 1991 ohnehin auf die Beachtung des Verhältnismäßigkeitsprinzips abstellt, keinen Anlaß, diese Grundsätze vorab umzusetzen.
Die Öffentlichkeitsfahndung im Internet als besondere Form der Öffentlichkeitsfahndung ist aus datenschutzrechtlicher Sicht wegen der weltweiten Abrufbarkeit für jedermann nicht unproblematisch. Bei einer Durchsicht der

im Internet durch das Thüringer Landeskriminalamt (LKA) eingestellten Fahndungen fand sich Ende des Jahres 1996 eine Fahndung wegen versuchten Mordes, bei dem der letzte Wohnsitz des Betroffenen angegeben war. Dies war aus meiner Sicht geeignet, besonders auf das Umfeld eines Betroffenen (unbeteiligte Familienangehörige, Nachbarn) weltweit aufmerksam zu machen. Auf Anfrage hat das LKA mitgeteilt, daß es meine Auffassung nach gesetzgeberischem Handlungsbedarf teilt. Die Einstellung der Fahndung im Internet erfolgt derzeit nach den „Richtlinien für die Inanspruchnahme von Publikationsorganen zur Fahndung bei Personen bei der Strafverfolgung“ in Verbindung mit Richtlinien zur Nutzung des Internet. Da der Wohnort des Betroffenen zwischenzeitlich durch die Angabe einer größeren Stadt als letzter Aufenthaltsort ersetzt wurde, so daß auch Belange Dritter/Unbeteiligter gewahrt werden, habe ich keine weiteren Bedenken bezüglich der konkret eingestellten Fahndung wegen versuchten Mordes als schwerwiegende Tat geltend gemacht.
In Anbetracht dessen, daß die Fahndungsdaten des LKA eines hohen Schutzes bezüglich ihrer Integrität bedürfen und somit mögliche Risiken für Manipulationen dieser Informationen weitgehend ausgeschlossen werden müssen, habe ich mich über die Einstellung der Informationen im Internet informiert. Es muß sichergestellt sein, daß lesende Zugriffe für alle Benutzer erlaubt ist, der schreibende Zugriff aber nur autorisierten Personen zustehen darf. Hierzu sind technische und organisatorische Maßnahmen gemäß § 9 Abs. 2 ThürDSG erforderlich, deren Umsetzung erfolgt.

10.4 DNA-Analyse - „Genetischer Fingerabdruck“

Durch das Strafverfahrensänderungsgesetz - DNA-Analyse („Genetischer Fingerabdruck“) - vom 17.03.1997 (BGBl I S. 534) wurde eine spezielle Rechtsgrundlage für molekulargenetische Untersuchungen an Blutproben oder sonstigen menschlichen Körperzellen im Strafverfahren geschaffen. Damit wurden die Voraussetzungen und Grenzen molekulargenetischer Untersuchungen in die StPO aufgenommen. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht. Für eine Nutzung der mittels DNA-Analyse gewonnenen Daten auch für andere Strafverfahren und deren Zugänglichmachung in abrufbaren Datenbanken haben die DSB mit der Entschließung der 53. Konferenz „Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke“ (Anlage 11) ergänzend eine spezielle gesetzliche Regelung in der StPO verlangt und konkrete Forderungen an die automatisierte Speicherung und Nutzung von DNA-Idenditätsdaten aufgestellt.

10.5 Zentrales Staatsanwaltschaftliches Verfahrensregister

Zu dem im 1. TB (10.5) berichteten, nach den §§ 474 ff. StPO vorgesehenen Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV) liegen zwischenzeitlich die in der Errichtungsanordnung angekündigten organisatorisch-technischen Leitlinien in der zwischen den Justizressorts abgestimmten Fassung vor. Die nach § 476 Abs. 5 StPO zu treffenden erforderlichen technischen und organisatorischen Maßnahmen nach § 9 BDSG, die in der Errichtungsanordnung zunächst nicht aufgenommen worden sind und den organisatorisch-technischen Leitlinien vorbehalten werden sollten, sind auch in diesen wiederum nicht enthalten. Vielmehr ist eine Bedrohungs- und Risikoanalyse angekündigt, die Grundlage für zu verwirklichende Sicherheitsmaßnahmen sein soll. Zu den organisatorisch-technischen Leitlinien habe ich gegenüber dem TMJE eine Stellungnahme abgegeben, die von dort aus an das BMJ und die übrigen Landesjustizverwaltungen zur Kenntnisnahme

weitergeleitet wurde, davon ausgehend, daß sie gebührende Beachtung finden wird. Bedenken habe ich auch zu folgenden Punkten geäußert:
Soweit über die in Ausnahmefällen wegen besonderer Eilbedürftigkeit möglichen Eilanfragen hinaus telefonische und fernschriftliche Anfragen vorgesehen sind, besteht ein hohes Risiko, daß die anfragende Person nicht berechtigt sein könnte. Es fehlt deshalb eine erforderliche Berechtigungsprüfung. Die aus meiner Sicht zu unbestimmte Formulierung, daß für die Übertragung von Mitteilungen und Anfragen an das Verfahrensregister die „allgemein zugänglichen Übertragungsdienste verwendet werden, wobei entsprechende Sicherheitsmaßnahmen vorgesehen werden", müßten durch konkrete Festlegungen von Sicherheitsmaßnahmen ergänzt werden. Erfreulicherweise wird eine aus datenschutzrechtlicher Sicht erforderliche Verschlüsselung der Daten auf dem Übertragungsweg im Rahmen der Bedrohungs- und Risikoanalyse nicht von vornherein ausgeschlossen. Die weitere Prüfung wird zeigen, ob der besonderen Schutzbedürftigkeit der zu übermittelnden Daten hinreichend Rechnung getragen wird. Jedenfalls soll das Zentrale Staatsanwaltschaftliche Verfahrensregister erst dann in Betrieb genommen werden, wenn alle erforderlichen Bestimmungen vorliegen.

10.6 Entwurf eines Vierten Gesetzes zur Änderung des Bundeszentralregisters (4. BZRÄndG)

Im 1. TB (10.8) war dargestellt worden, daß die Eintragung der Schuldunfähigkeit in das Bundeszentralregister aus datenschutzrechtlicher Sicht bedenklich ist, da nicht ersichtlich ist, ob es sich um eine dauernde oder nur vorübergehende Schuldunfähigkeit gehandelt hat. Schuldunfähige sind damit gegenüber Schuldfähigen benachteiligt, weil für die Eintragungen bei Schuldunfähigen bislang keine entsprechenden Tilgungsfristen bestehen. Durch den nunmehr vorliegenden Entwurf eines Vierten Gesetzes zur Änderung des Bundeszentralregisters (Stand: 15.02.1997), zu dem ich gegenüber dem TMJE Stellung genommen habe, wird diese Problematik einer Regelung zugeführt, die die datenschutzrechtlichen Bedenken weitgehend ausräumt. Der Gesetzesentwurf enthält auch begrüßenswerte Regelungen zu Berichtigungs- und Nachberichtspflichten sowie Bestimmungen zur Protokollierung der erteilten Auskünfte. Meine Anregung, den Kreis der Abrufberechtigten im automatisierten Abrufverfahren (§ 21 4. BZRÄndG) ausdrücklich auf bestimmte Stellen zu beschränken, wurde seitens des TMJE aufgegriffen. Der Fortgang des Beratungsverfahrens wird weiterhin aus datenschutzrechtlicher Sicht begleitet.

10.7 Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren/Videoaufzeichnungen von Zeugenvernehmungen

Überlegungen des Bundesgesetzgebers und eine begonnene öffentliche Diskussion, moderne Technik, insbesondere in Form von Videoaufnahmen zur Wahrheitsfindung und zum Zeugenschutz in gerichtlichen Verfahren, nun auch bei Gericht zuzulassen, werfen vielfältige datenschutzrechtliche Aspekte auf. In Anbetracht dessen, daß bisher der unmittelbare Eindruck von Zeugen bei seiner mündlichen Aussage maßgeblich war und in möglicherweise folgenden Verfahren nur auf schriftliche Protokolle zurückgegriffen werden konnte, liegt der Einsatz insbesondere auch von Videotechnologie in gerichtlichen Strafverfahren sowohl im Interesse der Wahrheitsfindung als auch im Interesse der betroffenen Zeugen, daß diese nicht jeweils erneut eventuell nach langer Zeit zum selben Gegenstand nochmals aussagen müssen. Als aus datenschutzrechtlicher Sicht wichtiges Kriterium für die Zulassung der Bild-Ton-Aufzeichnung bei Vernehmungen im Strafverfahren stellt sich auch der Aspekt der guten Dokumentation als besonderes Anliegen der Praxis dar. Nicht zu vergessen ist jedoch, daß die einmal gemachte Aussage

sodann unbegrenzt oft in genau derselben Art und Weise immer wieder abgespielt werden kann. Die Beurteilung des Beweiswerts einer Bild-Ton-Aufzeichnung wird jedoch deutlich verbessert. In einer Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben die DSB (Anlage 16) in diesem Zusammenhang wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts gefordert.

10.8 „Großer Lauschangriff“

Unter der Bezeichnung „Großer Lauschangriff“ wird schon seit geraumer Zeit im Kreise der Datenschutzbeauftragten über das Vorhaben der Einführung der elektronischen Überwachung von Wohn- und Geschäftsräumen zum Zwecke der Beweismittelgewinnung in Strafverfahren diskutiert. Von der Mehrheit der Datenschutzbeauftragten wird die damit erforderliche Änderung des Artikel 13 GG mit den entsprechenden gesetzlichen begleitenden Regelungen der Änderung der Strafprozeßordnung als erheblicher Eingriff in das Persönlichkeitsrecht des einzelnen aus grundsätzlichen Erwägungen abgelehnt. Ich bin der Auffassung, daß der Staat zur Bekämpfung schwerer Kriminalität in die Lage versetzt werden muß, ggf. das Mittel der akustischen Überwachung einsetzen zu können. Bereits in der 52. Datenschutzkonferenz (Anlage 9) haben die Datenschutzbeauftragten 10 Forderungen erhoben, die auch von mir unterstützt werden:

1. Im Grundgesetz selbst ist festzulegen, daß
   - der Einsatz technischer Mittel zur Wohnraumüberwachung nur zur Verfolgung schwerster Straftaten, die im Hinblick auf ihre Begehungsform oder Folgen die Rechtsordnung nachhaltig gefährden und die im Gesetz einzeln bestimmt sind und
   - nur auf Anordnung eines Kollegialgerichts

   erfolgen darf.
2. Die Maßnahme darf sich nur gegen den Beschuldigten richten. Erfolgt ein Lauschangriff in der Wohnung eines Dritten, müssen konkrete Anhaltspunkte die Annahme rechtfertigen, daß sich der Beschuldigte in der Wohnung aufhält. In allen Fällen muß die durch Tatsachen begründete Erwartung vorliegen, daß in der überwachten Wohnung zur Strafverfolgung relevante Gespräche geführt werden.
3. Das Mittel der Wohnungsüberwachung darf nur dann angewandt werden, wenn andere Methoden zur Erforschung des Sachverhalts erschöpft oder untauglich sind. Bei einem Lauschangriff in Wohnungen dritter Personen bedeutet dies auch, daß die Maßnahme nur durchgeführt werden darf, wenn aufgrund bestimmter Tatsachen anzunehmen ist, daß ihre Durchführung in der Wohnung des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts des Täters führen wird.
4. Das Zeugnisverweigerungsrecht von Berufsgeheimnisträgern und Personen, die aus persönlichen Gründen zur Verweigerung des Zeugnisses berechtigt sind, muß gewahrt werden.
5. Die Dauer der Maßnahme wird zeitlich eng begrenzt. Auch die Möglichkeit der Verlängerung der Maßnahme ist zu befristen.
6. Eine anderweitige Verwendung der erhobenen Daten (Zweckänderung) ist weder zu Beweiszwecken noch als Ermittlungsansatz für andere als Katalogdaten zulässig.

   Personenbezogene Erkenntnisse aus einem Lauschangriff dürfen zur Abwehr von konkreten Gefahren für gewichtige Rechtsgüter verwendet werden.
7. Wenn sich der ursprüngliche Verdacht nicht bestätigt, sind die durch den Lauschangriff erhobenen Daten unverzüglich zu löschen.

8. Die Betroffenen müssen unverzüglich und vollständig über die Durchführung der Maßnahme informiert werden, sobald dies ohne Gefährdung des Ermittlungsverfahrens möglich ist.
9. Eine Verfahrenssicherung durch den Zwang zur eingehenden Begründung und durch detaillierte jährliche Berichtspflichten der Staatsanwaltschaft für die Öffentlichkeit ähnlich den gerichtlichen Wire-Tap-Reports in den USA einschließlich einer Erfolgskontrolle ist vorzusehen. Anhand der Berichte ist jeweils - wegen der Schwere des Eingriffs - in entsprechenden Fristen zu überprüfen, ob die gesetzliche Regelung weiterhin erforderlich ist.
10. Die effektive Kontrolle der Abhörmaßnahme und der Verarbeitung und Nutzung der durch sie gewonnenen Erkenntnisse durch Gerichte und Datenschutzbeauftragte ist sicherzustellen.

Zwischenzeitlich ist der Entwurf eines Gesetzes zur Änderung des Grundgesetzes (Artikel 13 GG) (Drucksache 13/8650) eingebracht. Problematisch hierbei ist, daß danach derartige technische Mittel schon eingesetzt werden dürfen, wenn nur die Vermutung besteht, daß sich der Beschuldigte in einer bestimmten Wohnung aufhält.

Zu Personen, wie Ärzten, Rechtsanwälten, Geistlichen, Abgeordneten und Journalisten besteht ein besonderes Vertrauensverhältnis, so daß diese ein Zeugnisverweigerungsrecht haben. Räumlichkeiten, in denen diese in § 53 StPO genannten Personen ihren Beruf ausüben, müssen von vornherein abhörfrei bleiben.

10.9 Zentrale europäische Datenbanken, in denen gerichtliche Streitfälle gesammelt werden

Zweifellos kann interessant sein, zu wissen, ob jemand irgendwo in Europa wegen einer Streitfrage in einer Zivil- oder Handelssache nach dem Brüsseler Übereinkommen vom 27.09.1968 ein Gericht angerufen hat. Nach einem Vorschlag, eine entsprechende Datenbank für erhobene Klagen und die diesbezüglichen Entscheidungen einzurichten, erhielt ich die Gelegenheit, zu den dafür beabsichtigten Übermittlungen von personenbezogenen Daten Stellung zu nehmen. Die Übermittlung personenbezogener Daten durch Thüringer Gerichte an die Datenbankverwaltung müßte unter der Voraussetzung des § 21 ThürDSG erfolgen. Danach ist die Übermittlung personenbezogener Daten zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG (Zweckänderung) zulassen würde. Diese Voraussetzungen wären gegeben, sobald eine entsprechende Rechtsvorschrift vorliegt. Zu den vorgesehenen zu übermittelnden Daten hatte ich jedoch nach der geltenden Rechtslage erhebliche Bedenken. Was personenbezogenen Daten von verfahrensbeteiligten Privatpersonen angeht, könnte sich für die Betroffenen die Situation ergeben, daß sie Anfragen aus dem gesamten europäischen Bereich ausgesetzt sein könnten, weil die Aufnahme der vollen Adresse in die Datenbank vorgesehen war. Eine Bereitstellung von personenbezogenen Daten zum unbegrenzten Abruf für jedermann wäre aber ein erheblicher Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen, den der Zweck, Interessierten die Möglichkeit einzuräumen, vergleichbare Verfahren feststellen zu können, nicht rechtfertigen kann. Die Einstellung in diese zentrale europäische Datenbank dürfte danach nur erfolgen, wenn eine konkrete Einwilligung der Betroffenen vorliegt. Es ist mir nicht bekannt, ob die Überlegungen weiter verfolgt wurden.

10.10 Gesetz über das Versorgungswerk der Rechtsanwälte (ThürRAVG)

Schon frühzeitig erhielt ich die Gelegenheit, zum Referentenentwurf eines Gesetzes über das Versorgungswerk der Rechtsanwälte im Freistaat Thüringen aus datenschutzrechtlicher Sicht Stellung zu nehmen. Ich hatte dazu verschiedene Änderungen vorgeschlagen. Diese betrafen insbesondere die Konkretisierung der für die Feststellung der Mitgliedschaft sowie Art und Umfang der Beitragspflicht oder der Versorgungsleistung erforderlichen Auskünfte und die Erforderlichkeit der Erhebung der personenbezogenen Daten beim Betroffenen selbst. Im parlamentarischen Verfahren erhielt ich nochmals die Gelegenheit, die datenschutzrechtlichen Aspekte vorzutragen, die im ThürRAVG vom 31. Mai 1996 (GVBl S. 70) insgesamt Berücksichtigung fanden.

10.11 Einsatz automatisierter Verfahren im Justizbereich

Auch im Geschäftsbereich des TMJE hält die Automatisierung der Geschäftsstellen weiter Einzug.

10.11.1 MEGA

Für den Bereich der ordentlichen Gerichtsbarkeit kommt MEGA (Abkürzung für „Mehrländer-Gerichts-Anwendung“) zur Anwendung. MEGA ist ein von den Bundesländern Brandenburg, Schleswig-Holstein und Thüringen gemeinsam neu entwickeltes EDV-Programm, das in der Justiz die vollständige Einbindung der Arbeitsplätze von Richtern und Rechtspflegern, Aktenverwaltung und Schreibdienst verwirklicht. Auf meine Bitte um Beteiligung wurden mir verschiedene Konzeptionsentwürfe zur Kenntnis gegeben, die jedoch für eine abschließende datenschutzrechtliche Bewertung noch nicht ausgereicht haben. Auch habe ich die Gelegenheit einer Demonstration der Anwendung vor Ort erhalten. Mittels dieses Verfahrens, mit dem Verfahrensdaten und neu anfallende Daten (Wiedervorlage, Termine oder Zeugen) verarbeitet werden, wird auch die gesamte Aktenregistratur übernommen. Der Kanzleibereich wird durch automatisierte Bereitstellung von Mitteilungsformularen unterstützt. Darüber hinaus ermöglicht es Verfahrensauskünfte, Verfügungsvorbereitungen sowie den Einsatz von spezieller juristischer Software. Das Verfahren werde ich weiterhin aus datenschutzrechtlicher Sicht begleiten, sobald mir weitere Unterlagen insbesondere auch zu den organisatorischen und technischen Maßnahmen vorliegen.
Im 1. TB (10.12) wurde die datenschutzrechtliche Problematik von Ehescheidungsverbundurteilen und deren weitestgehende Lösung durch entsprechende Hinweise der Personalstellen als anfordernde Stellen dargelegt. Mit der Ausstattung der Thüringer Gerichte mit EDV (MEGA) wird nun auch seitens der Gerichte nochmals gegenüber der Betroffenen darauf hingewiesen, daß Ehescheidungsverbundurteile auch als Auszüge oder Teilausfertigungen erteilt werden, was bereits bei den genutzten Computerprogrammen als Fußnoten automatisch im entsprechenden Ausdruck Berücksichtigung findet.

10.11.2 SIJUS-Straf-StA

Der Einsatz des Verfahrens SIJUS-Straf-StA bei den Staatsanwaltschaften des Landes wurde in den Grundzügen im Rahmen einer durchgeführten Kontrolle bei einer Staatsanwaltschaft geprüft. Über das dort bislang nur teilweise angewandte Verfahren werden die Aufgaben der Führung von staatsanwaltschaftlichen Registern, Strafverfolgungsstatistik sowie die Geschäftstellenverwaltung erledigt. Das Verfahren bietet auch die bisher noch nicht genutzte Möglichkeit der Kommunikation mit externen anderen Regi-

stern und Stellen, etwa mit dem Bundeszentralregister und Polizeidienststellen. Den im Ergebnis der Kontrolle festgestellten datenschutzrechtlichen Mängeln, wie fehlende eigene Benutzerkennungen für jeden einzelnen Nutzer und Protokollierung der fehlerhaften LOGIN-Versuche, wurde nachgekommen. Die noch offenen Fragen, vor allem der Protokollierungsmöglichkeit sämtlicher Zugriffe, der Verschlüsselung personenbezogener Daten bei der Datenübermittlung sowie die Möglichkeit der Nutzung nicht näher bezeichneter Freifelder wird weiterhin mit der Generalstaatsanwaltschaft und dem TMJE erörtert.
Zu der gesamten Problematik haben die Datenschutzbeauftragten des Bundes und der Länder auf der 53. Konferenz vom 17./18.04.1997 eine Vorlage des Arbeitskreise Justiz zu „Datenschutzrechtlichen Forderungen zum Einsatz von automatisierten Staatsanwaltschaftlichen Informationssystemen“ (Anlage 18) zustimmend zur Kenntnis genommen. Ich habe dieses Themenpapier, das eine gute Arbeitsgrundlage im Hinblick auch auf den Einsatz des Verfahrens SIJUS-Straf-StA darstellt, zu einem Meinungsaustausch zu den aufgeführten datenschutzrechtlichen Aspekten dem TMJE zugeleitet.

10.11.3 Geschäftsstellenlösung der Justizvollzugsanstalten

Im 1. TB (10.11.2) hatte ich die automatisierte Geschäftsstellenlösung für die Justizvollzugsanstalten angesprochen. Im Rahmen einer im Berichtszeitraum durchgeführten Kontrolle in einer Justizvollzugsanstalt konnte ich den Einsatz in der Praxis, obwohl dort erst seit 4 Wochen ein Probelauf stattfand, kontrollieren. Hinsichtlich des Dateiinhalts ergaben sich keine Bedenken. Bei den in die angezeigten Masken einzutragenden Daten handelte es sich im wesentlichen um die Angaben zu einem Gefangenen, die auch auf dem Wahrnehmungsbogen als Kernstück der Gefangenpersonalakte einzutragen sind. Bezüglich der Datensicherheit ergaben sich nach meinem derzeitigen Erkenntnisstand ebenfalls keine Bedenken. Zu der Forderung einer Zugriffsbeschränkung für die einzelnen Bediensteten nach dem jeweiligen Aufgabengebiet wird die Prüfung und Diskussion im Hinblick darauf, daß aus datenschutzrechtlicher Sicht auch nur ein eingeschränkter Zugriff auf die Gefangenenpersonalakten zulässig sein kann, fortgeführt.

10.12 Kontrollkompetenz des TLfD bei Gerichten

§ 37 Abs. 4 ThürDSG bestimmt, daß die Gerichte der Kontrolle durch den TLfD nur soweit unterliegen, als sie in Verwaltungsangelegenheiten tätig werden. Im Vorfeld einer angekündigten Kontrolle bei einem Amtsgericht - Grundbuchamt- wurde seitens des TMJE geltend gemacht, daß Bereiche der Rechtspflege, die von Rechtspflegern in sachlicher Unabhängigkeit oder von Richtern wahrgenommen werden, ebensowenig wie Tätigkeiten in Vorbereitung bzw. Vollziehung der rechtspflegerischen Entscheidungen der Richter und Rechtspfleger erfolgen, nicht kontrolliert werden können, was aus meiner Sicht unbestritten ist. Daß sich dies jedoch nach Auffassung des TMJE auch auf die gesamte zur Unterstützung dieser rechtspflegerischen Tätigkeit eingesetzten EDV beziehen soll, kann ich nicht vorbehaltlos akzeptieren. Im Hinblick auf den Einsatz von automatisierten Verfahren, mittels deren auch reine Verwaltungstätigkeiten erledigt werden können, würde dies bedeuten, daß diese auch bei Datensicherungsmaßnahmen gänzlich meiner Kontrolle entzogen wären, sobald auch Rechtspflegern und Richtern Zugriffe gewährt werden oder mit diesen Verfahren auch irgendein der Rechtspflegetätigkeit zuzuordnender Bereich zusätzlich erledigt werden kann. Daß meinerseits datenschutzrechtliche Kontrollen nur in den Bereichen durchgeführt werden, die auch meiner Zuständigkeit unterliegen, versteht sich von selbst. Aus Gründen der Rechtssicherheit ist es aber auch für die zu kontrollierenden Stellen in der Justiz aus meiner Sicht dringend geboten, daß für zukünftige datenschutzrechtliche Kontrollen ein Katalog darüber vorliegt,

welche konkreten Bereiche und Tätigkeiten entweder der Rechtspflege oder der Verwaltungstätigkeit zuzuordnen sind. Auch wenn nur die Verwaltungsangelegenheiten der Gerichte der Kontrolle des TLfD unterliegen, so sind die Gerichte dennoch nicht davon entbunden, in eigener Zuständigkeit auch in den der Rechtspflege unterfallenden Angelegenheiten die Einhaltung der datenschutzrechtlichen Vorschriften sicherzustellen. Die Bestellung von behördeninternen Datenschutzbeauftragten erscheint mir daher unerläßlich. Um die eingangs genannte angekündigte Kontrolle bei dem Amtsgericht-Grundbuchamt durchführen zu können, habe ich mich daher auf die unstreitigen der Verwaltungstätigkeit zuzuordnenden Bereiche beschränkt.
Im Nachgang zur Kontrolle wurde ein behördlicher Datenschutzbeauftragter bestellt. Zu beanstanden war die Personalaktenführung, da die vorhandenen Personalakten auch nicht erforderliche Bestandteile enthielten. Hierzu zählten z. B. Kopien alter Personalbögen, zahlungsbegründende Unterlagen wie Geburtsurkunden von Kindern, Heiratsurkunden usw., die sich nur in Vergütungsakten befinden sollten oder nach § 97 Abs. 5 ThürBG getrennt aufzubewahrende Fragebögen zur persönlichen Eignung. Eine entsprechende Überarbeitung ist erfolgt. Darüber hinaus ist den Personalakten ein Vorblatt mit der Angabe der enthaltenen Unterlagen sowie ein Verzeichnis der Neben- und Teilakten, das den Betroffen Aufschluß darüber gibt, wo sich welche weiteren ihn betreffende Personalunterlagen befinden, um ihnen die Ausübung des Einsichtsrechts in die vollständige Personalakte nach § 100 Abs. 1 ThürBG zu erleichtern, vorgeheftet worden. Mit der Erarbeitung dieser Blätter war bereits vor der Kontrolle begonnen worden. Die datenschutzrechtlichen Empfehlungen im Bereich der Personalverwaltung, insbesondere zur Arbeitszeiterfassung und Telefongebührenerfassung wurden umgehend umgesetzt. Die nach § 9 Abs. 3 ThürDSG erforderlichen technischen und organisatorischen Maßnahmen, die verhindern, daß Unbefugte auch bei der Aufbewahrung, dem Transport und der Vernichtung auf personenbezogene Daten zugreifen können, wurden getroffen. Eine Sicherung gegen unbefugtes Entfernen von Metallcontainern, in denen zur Vernichtung bestimmte Unterlagen aufbewahrt werden, wurde unverzüglich vorgenommen.

10.13 Telefonüberwachungsmaßnahmen

Der Katalog der Straftaten, die eine Telefonüberwachung nach § 100a StPO erlauben, ist in der Vergangenheit mehrfach, zuletzt mit dem Verbrechensbekämpfungsgesetz, erweitert worden.
So sehr Telefonüberwachungen für eine wirksame Verbrechensbekämpfung notwendig sein mögen, so notwendig erscheint es auch, den tatsächlichen Erfolg zu prüfen, um das Persönlichkeitsrecht im Ausgleich hierfür zu stärken. Mit Erlaß des TMJE im Februar 1996 wurde die Einführung von Berichtspflichten bei der Überwachung des Fernmeldeverkehrs im Freistaat Thüringen umgesetzt. Danach sind jährlich von der Generalstaatsanwaltschaft die Anzahl der Verfahren und deren Zuordnung nach den in § 100a StPO aufgeführten Katalogstraftaten zu berichten. Für 1996 ergaben sich insgesamt 22 Verfahren. Presseveröffentlichungen in diesem Zusammenhang habe ich zum Anlaß genommen, mich bei einer Staatsanwaltschaft im Rahmen einer datenschutzrechtlichen Kontrolle vom Umgang mit Unterlagen zu Telefonüberwachungsmaßnahmen insbesondere zur Einhaltung der Löschfristen nach § 100b Abs. 6 StPO zu informieren. Dem TLfD wurden in diesem Zusammenhang Auskünfte zu allen Fragen erteilt. In einer entsprechenden Hausverfügung wurden darüber hinaus klarstellende Hinweise im Geschäftsbereich gegeben.

10.14 Täter-Opfer-Ausgleich und Datenschutz

Auf der Grundlage der Richtlinie des TMJE zur Förderung des Täter-Opfer-Ausgleichs in Thüringen (JMBl I 1994, S. 109) war seitens des TMJE beab-

sichtigt, im Rahmen eines Pilotprojektes den Täter-Opfer-Ausgleich (TOA) unter wissenschaftlicher Begleitung einer Fachhochschule durchzuführen. Der TOA soll den Rechtsfrieden, der durch eine Straftat gestört ist, wiederherstellen helfen. Vorrangiges Ziel des TOA ist das Bemühen um einen Ausgleich mit dem Geschädigten. Zur sachgemäßen Vorbereitung der zu führenden Gespräche zwischen Tätern und Opfern müssen daher den Schlichtern personenbezogene Daten zur Verfügung gestellt werden. Vor der Durchführung dieses Pilotprojektes hat mich das TMJE um Stellungnahme gebeten. Die Zulässigkeit der Übermittlung ist nach folgenden Gesichtspunkten zu bewerten: Zunächst liegt eine Aufgabenerfüllung der Staatsanwaltschaft als übermittelnde Stelle nach § 22 Abs. 1 Nr. 1 ThürDSG vor. Nach Abwägung, daß kein überwiegendes schutzwürdiges Interesse an dem Ausschluß der Übermittlung des betroffenen Opfers nach § 22 Abs. 1 Nr. 2 ThürDSG anzunehmen ist, da die Durchführung des Täter-Opfer-Ausgleichs auch im Interesse des Opfers an einer Wiedergutmachung zu sehen ist, kann auch dies als Zulässigkeitsgrund herangezogen werden. In Anbetracht dessen, daß der Bundesrat in seiner Stellungnahme zum Entwurf des StVÄG 96 die Prüfung einer Erforderlichkeit einer entsprechenden gesetzlichen Regelung angeregt hat, habe ich es bis zum Vorliegen eines entsprechenden Ergebnisses für zulässig erachtet, auch vorher schon Opferdaten an die zur Durchführung des TOA beauftragten privaten Stellen zu übermitteln. Der Umfang der Daten ist jedoch auf das zur Aufgabenerfüllung bei Einleitung der Durchführung des Täter-Opfer-Ausgleichs erforderliche Maß zu beschränken. Es darf sich daher nur um wenige Daten handeln, die notwendig sind, die Einwilligung des betroffenen Opfers zur Teilnahme zu erhalten.

10.15 Weitergabe personenbezogener Daten an gemeinnützige Einrichtungen

Die datenschutzrechtliche Problematik der Datenübermittlung im Zusammenhang mit der Entrichtung von Geldern an gemeinnützige Einrichtungen durch Beschuldigte bzw. Angeklagte wurde bereits im 1. TB (10.7) dargestellt. Die Landesregierung hatte in ihrer Stellungnahme hierzu die Bedenken grundsätzlich geteilt, man verschließe sich nicht grundsätzlich dem Vorschlag des TLfD. Auf meine Nachfrage zum aktuellen Stand der Diskussion wurde in der Folge seitens des TMJE mitgeteilt, es erscheine weder erforderlich noch unter praktischen Gesichtspunkten durchführbar, bei der Zuweisung von Geldauflagen weiter zu anonymisieren. Nachdem ich mein Unverständnis hierzu geäußert hatte, wurde nach einer im Sinne aller Beteiligten Lösung gesucht. Im Ergebnis der Prüfung der Realisierungsmöglichkeiten durch das TMJE im Hinblick auf die zu schaffenden Voraussetzungen bei den Gerichtskassen verständigte man sich darüber, daß vertretbar erscheint, dem Betroffenen nur die Wahlmöglichkeit einzuräumen, entweder an die Staatskasse zu deren Gunsten oder verbunden mit der Einwilligung zur Übermittlung der personenbezogenen Daten an eine gemeinnützige Einrichtung zu bezahlen. Aufgrund der Wahlmöglichkeit wird bei dieser Variante dem informationellen Selbstbestimmungsrecht weitgehend Rechnung getragen.

10.16 Postsendungen von Staatsanwaltschaften und Gerichten an kommunale Stellen

Im Berichtszeitraum wurde ich auch darauf aufmerksam gemacht, daß von Staatsanwaltschaften den kommunalen Behörden üblicherweise verschiedene Vorgänge aus Strafverfahren gesammelt, in einem Umschlag, allgemein adressiert, z. B. an die „Stadtverwaltung“ übersandt werden. Da die enthaltenen Vorgänge jedoch jeweils unterschiedliche Ämter innerhalb der Kommunalverwaltung betrafen, mußte der Sammelumschlag in der zentralen Poststelle geöffnet werden, um die Vorgänge an die zuständigen Ämter zu leiten.

Einerseits sind hier die empfangenden Behörden aufgerufen, sicherzustellen, daß nicht unbefugt personenbezogene Daten zur Kenntnis genommen werden, andererseits bleibt den Mitarbeitern der Poststelle jedoch nichts anderes übrig, als die einzelnen Vorgänge jeweils zuzuordnen und damit zwangsläufig personenbezogene Daten zur Kenntnis zu nehmen.
Ein weiteres Problem besteht auch, wenn einer kommunalen Behörde ein Gerichtsfach zur Verfügung steht. Auch hier sollte sichergestellt sein, daß die einzelnen Vorgänge ohne Möglichkeit der Kenntnisnahme durch Unbefugte der zuständigen Stelle zugeleitet werden kann.
Das TMJE hat zwischenzeitlich den Geschäftsbereich gebeten, durch geeignete Maßnahmen sicherzustellen, daß künftig Postsendungen mit personenbezogenen Daten an die jeweils zuständigen Ämter der Verwaltungsbehörden in gesonderten und verschlossenen Briefumschlägen - ggf. aus Kostengründen nochmals in Sammelumschlägen an die jeweiligen Verwaltungsbehörden verpackt - versandt werden. Damit ist dem datenschutzrechtlichen Anliegen Rechnung getragen.

Mitteilung zum Wählerverzeichnis

Im 1. TB (5.2.6.2) hatte ich berichtet, daß Wahlämter im Zusammenhang mit der Mitteilung von Wahlausschlußgründen zum Teil vollständige Beschlüsse des Vormundschaftsgerichts oder auch mehrseitige Urteilsschriften erhalten hatten. In diesem Berichtszeitraum habe ich mich weiter über eingehende Mitteilungen von Wahlrechtsausschlüssen informiert. Die Mitteilung von Wahlausschlußgründen richtete sich nach Nr. 12a der Verwaltungsvorschrift Mitteilungen in Strafsachen. Die dort enthaltenen Vorgaben waren jedoch seitens des mitteilenden Stellen nicht beachtet worden. Obwohl der zuständigen Verwaltungsbehörde lediglich die Tatsache der rechtskräftigen Verurteilung ohne Angaben der rechtlichen Bezeichnung der Tat und ohne Angabe der angewendeten Strafvorschriften mitzuteilen ist, wurden Kopien von vollständigen Urteilen mit unzulässigen Daten, wie Namen von Zeugen und Opfern, aber mitunter ohne die erforderlichen Daten, nämlich Rechtskraftsvermerk und Angabe des Endes des Verlustes der Amtsfähigkeit und Wählbarkeit übersandt. Darüber hinaus waren erhebliche Unsicherheiten bezüglich der Adressierung der Mitteilungen festzustellen. Das Meldeamt als funktional zuständige Stelle und zuständig für die Eintragung im Melderegister und Erstellung des Wählerverzeichnisses war in den wenigsten Fällen konkret genannt. Auf meine Anregung hin wurde ein Formblatt für Mitteilungen in Strafsachen erarbeitet, in dem nur noch die erforderlichen und zulässigen Angaben für die kommunalen Verwaltungsbehörden möglich sind. Meinen Anregungen ist damit in vollem Umfang nachgekommen worden.

10.17 Datenschutz im Strafvollzug

Im 1. TB (10.11) war auch darauf hingewiesen worden, daß es bislang immer noch an bereichsspezifischen Datenschutzregelungen für den Strafvollzug fehlt. Zwischenzeitlich liegt ein Referentenentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes vor. Der Referentenentwurf enthält einige datenschutzrechtliche Vorschriften, in einzelnen Punkten reichen diese jedoch nicht aus. Ich habe gegenüber dem TMJE insbesondere zu folgenden Punkten Stellung genommen:
Die Einbeziehung des Datenschutzbeauftragten in den Kreis der von der Überwachung des Schriftwechsels ausgenommenen Institutionen wurde ausdrücklich begrüßt, zumal vom Grundsatz her, wie in § 11 ThürDSG niedergelegt, eine ungehinderte Kontaktaufnahme mit dem TLfD möglich sein sollte. Nicht berücksichtigt durch den Entwurf ist allerdings die Problematik der Antwortschreiben, was in anderem Zusammenhang seitens des TLfD aufgegriffen wurde.

Die Problematik des Zugriffs der Strafvollzugsbediensteten auf die Gefangenenpersonalakte, die besonders sensible Daten über die Betroffenen enthält, wird zwar an die Aufgabenerfüllung geknüpft, die Aufgabenerfüllung wird jedoch seitens der Justiz sehr global gesehen. Hier ist zu befürchten, daß durch die Aufgabe der Verfolgung des Strafvollzugsziels eine Allgemeinzuständigkeit eines jeden Vollzugsbediensteten gesehen wird, so daß eine Beschränkung des Zugriffs auf die Gefangenenpersonalakte nicht eindeutig geregelt wird. Seitens des TLfD wird die Auffassung vertreten, daß die Einsicht funktionsgebunden erfolgen kann. Dies darf nicht durch den Verweis auf eine Globalvorschrift (Vollzugsziel) relativiert werden. Um dies zu gewährleisten, erscheint es auch als besonders wichtig, daß nicht nur Gesundheitsakten und Krankenblätter getrennt von anderen Unterlagen zu führen und besonders zu sichern sind. Auch beispielsweise Unterlagen über psychologische, psychiatrische, psychotherapeutische und sozialtherapeutische Behandlungen sollten so behandelt werden. Eine Einsichtnahme muß sorgfältig dokumentiert werden, Möglichkeit der Nachprüfung der Zulässigkeit zu gewährleisten.

Im Ergebnis der im 1. TB (10.11.1, 10.11.3) geschilderten Probleme im Justizvollzug konnten verschiedene datenschutzrechtliche Verbesserungen erreicht werden:

- Die Einrichtung einer zentralen Auskunftsstelle, bei der eine Speicherung der alten Gefangenenpersonalakten aus DDR-Zeiten zunächst seitens des TMJE angestrebt war, wird zwischenzeitlich aus Kosten- und Haushaltsgründen nicht mehr für vertretbar gehalten. Jedoch werden die alten Akten, die nur für Auskünfte oder Bestätigungen für die Betroffenen benötigt werden, in verschiedenen Justizvollzugsanstalten ausreichend gesichert gelagert.
- Im Hinblick auf die erwartete Änderung des Strafvollzugsgesetzes wird die Beschränkung der Einsichtnahme in die Gefangenenpersonalakten weiterhin aus datenschutzrechtlicher Sicht gefordert. Zwischenzeitlich wird zur Überprüfung der Erforderlichkeit in den Justizvollzugsanstalten eine Protokollierung der Einsicht in Gefangenenpersonalakten vorgenommen.
- Hinsichtlich der Namensschilder an den Haftraumtüren ist das TMJE den Forderungen des TLfD soweit entgegengekommen, daß, bis zur Ausstattung aller Justizvollzugsanstalten mit umklappbaren Schildern, die Namensschilder an den Haftraumtüren bei Besuchen von Privatpersonen abzudecken sind.
- Die Problematik der Briefüberwachung von Schreiben des TLfD an Gefangene ist im Vorgriff auf die kommende Novelle geregelt worden.
- Das TMJE hatte an mich die Problematik der Erhebung und Speicherung von Besucherdaten durch Justizvollzugsanstalten herangetragen. In den Justizvollzugsanstalten des Freistaats Thüringen wurden Name, Vorname, Zeitpunkt des Besuches und teilweise auch die Anschrift von Besuchern auf einem Besuchsschein oder einer Besuchskarte vermerkt. Die Besuchscheine wurden nach Erledigung, die Besuchskarten nach Entlassung oder Verlegung des Gefangenen zu den Gefangenenpersonalakten genommen und 30 Jahre aufbewahrt. Diese Speicherdauer der Besucherdaten begegnete Bedenken. Zum Schutz des informationellen Selbstbestimmungsrecht der betroffenen Besucher müßten diese zumindest wissen, daß ihre Daten einer Speicherung unterliegen. Das TMJE hat meine Anregung, auf den Besuchsscheinen einen Hinweis für die Besucher aufzunehmen, daß die Daten gespeichert werden, aufgegriffen. Gleichzeitig wird ein Besucher mittels eines an den Pforten der Justizvollzugsanstalt ausgehängten Merkblatts mit konkreten Ausführungen zur Speicherung von Besucherdaten hingewiesen. Zur Abkürzung der Speicherdauer erfolgt zwei bis drei Jahre nach Entlassung von Gefangenen eine Überprü-

fung der Gefangenenpersonalakten auf die Erforderlichkeit des Inhalts von Besucherdaten und ggf. eine Löschung. Dieses Vorgehen ist aus meiner Sicht akzeptabel.

10.18 Kontrolle einer Staatsanwaltschaft

Im Ergebnis einer durchgeführten Kontrolle bei einer Staatsanwaltschaft wurde eine Beanstandung ausgesprochen wegen fehlender datenschutzrechtlicher Freigaben von automatisierten Verfahren, ungenügender Gebäudesicherung sowie Mängeln bei der Personalaktenführung, weil sich in den Personalakten mitunter doppelte und nicht erforderliche Unterlagen befanden. Datenschutzforderungen und -empfehlungen ergaben sich vor allem im organisatorischen und technischen Bereich, wegen noch ausstehender Datenschutzregistermeldungen sowie zum Einsatz des Verfahrens SIJUS-Straf-StA (siehe 10.11.2). Besonders auffällig waren vor dem Dienstgebäude Metall-Container abgestellt, die deutlich sichtbar mit dem Hinweis auf den Inhalt versehen waren. Diese standen dort für die Entsorgung von Aktenmaterial durch eine beauftragte Firma bereit. Eine Unterbringung im Gebäude war aus baulichen Gründen nicht möglich. Die mit einem Einhängeschloß versehenen Container hätten jedoch problemlos von jedem Passanten weggerollt werden können. Von einer Beanstandung konnte abgesehen werden, weil umgehend eine Sicherung erfolgte. Auf zunächst keinerlei Verständnis stieß die Forderung zur Sicherung von genutzten Einzelplatz-PCs durch Paßworte. Eine Dienstanweisung für die Benutzung von Personalcomputern für dienstliche Zwecke im Geschäftsbereich des TMJE, bereits aus dem Jahr 1995, regelt jedoch die Paßwortfrage.
Erhebliche Mängel wurden in der Personalverwaltung festgestellt. In den Personalakten befanden sich doppelte und nicht erforderliche Unterlagen. Soweit Personalakten den Abteilungsleitern zur Erstellung von Beurteilungsentwürfen ausgehändigt wurden, stieß dies auf erhebliche datenschutzrechtliche Bedenken, da die Abteilungsleiter nicht zum Kreis der zugangsberechtigten Personen nach § 97 Abs. 3 ThürBG zählen.
Automatisierte Verfahren zur Verarbeitung der personenbezogenen Daten der Mitarbeiter waren nicht freigegeben. Insbesondere bezüglich der Telefondatenerfassung war keine Erforderlichkeit der datenschutzrechtlichen Freigabe gesehen worden, da man Gesprächsdaten nicht den personenbezogenen Daten zuzuordnen wußte. Die festgestellten datenschutzrechtlichen Mängel sind zwischenzeitlich behoben.

10.19 Entsorgung „alter“ Diktatkassetten einer Staatsanwaltschaft

Im Berichtszeitraum wurden mir Diktatkassetten übergeben, auf denen sich u. a. Diktate von Anklageschriften, Vernehmungsprotokollen und Einstellungsverfügungen befanden. In einem Gespräch bei der betreffenden Staatsanwaltschaft konnte nicht geklärt werden, wie, wann und durch wen eine Entsorgung alter Diktatkassetten der Staatsanwaltschaft erfolgt ist. Der Fund von bespielten, nicht gelöschten Kassetten zeigte, daß keine oder unzureichende Maßnahmen getroffen worden waren, um zu verhindern, daß Unbefugte auf die Tonträger Zugriff haben konnten, worin ein Verstoß nach § 9 ThürDSG lag. Ich habe dies nach § 39 Abs. 1 ThürDSG beanstandet und die Staatsanwaltschaft aufgefordert, durch geeignete Maßnahmen sicherzustellen, daß künftig nur Diktatkassetten entsorgt werden, die zuvor gelöscht wurden. Auch habe ich die Anregung gegeben, durch dienstliche Regelungen Festlegungen zum Umgang mit Tonträgern, die personenbezogene Daten enthalten, zu treffen, um einen Zugriff durch Unbefugte auszuschließen. Die betreffende Staatsanwaltschaft hat durch eine interne Hausverfügung dieser Forderung Rechnung getragen und veranlaßt, daß alle vorhandenen unter den Mitarbeitern ausgegebenen Diktatkassetten ihrer Zahl nach erfaßt wurden, um deren Bestand erforderlichenfalls überprüfen zu können. Das TMJE hat

darüber hinaus eine Regelung für alle Dienststellen der Justizverwaltung zur Aussonderung und Vernichtung von Diktatkassetten getroffen. Durch die getroffenen organisatorischen Maßnahmen sehe ich die Beanstandung als ausgeräumt an.

10.20 Datenschutz im Notariat

Ein Bürger hatte sich mit der Bitte um Überprüfung folgenden Sachverhalts an mich gewandt: Ihm war im Zuge des Kaufs eines Grundstücks eine notarielle Urkunde zugesandt worden, in der eine Vielzahl von Käufern mit Name, Geburtsdatum und Anschrift sowie des entsprechend festgesetzten Kaufpreises zur Gebührenberechnung angegeben war. Zwar waren die Kaufpreise mit Deckfarbe überpinselt gewesen, jedoch hätte es keines großen Aufwandes bedurft, die Kaufpreise wieder sichtbar zu machen. Seitens des Notars wurde eingeräumt, die Urkunde wäre auch ohne die Geburtsdaten der Käufer und ohne die Angaben der Kaufpreise zu beurkunden gewesen. Darüber hinaus hätte jedem einzelnen Käufer ein entsprechender Auszug nur mit seinen personenbezogenen Daten gefertigt werden können. Die Übermittlung personenbezogener Daten der anderen Käufern an einen einzelnen Käufer war daher nicht erforderlich. Ich gehe davon aus, daß durch die Auswertung der Angelegenheit mit den Mitarbeitern des Notariats die geeigneten Maßnahmen getroffen wurden, so daß künftig solche datenschutzrechtlichen Verstöße vermieden werden.

10.21 Datenübermittlungen der Notare an die Gemeinden

Aus dem Kreis der Datenschutzbeauftragten der Länder wurde ich auf die Problematik von der Mitteilungspflicht nach § 28 Abs. 1 Satz 1 Baugesetzbuch (BauGB) und anderer Rechtsvorschriften aufmerksam. Sinn und Zweck der Datenübermittlung ist, den Gemeinden die Prüfung des Bestehens oder Nichtbestehens eines Vorkaufsrechts zu ermöglichen. Ein Vorkaufsrecht kommt dann u. a. in Betracht, wenn sich das Grundstück in einem ausdrücklich durch Satzung bestimmten entsprechenden Gebiet liegt (§ 25 BauGB) oder in den Fällen des § 24 BauGB, in denen Gebiete auf andere Art und Weise festgelegt sind. Dies erfordert jedoch nicht, daß der Gemeinde grundsätzlich sämtliche in einem Kaufvertrag über ein Grundstück enthaltenen Regelungen zur Kenntnis gelangen. In Betracht käme ein zweistufiges Verfahren, das auch von der Notarkammer Thüringen unterstützt wird. So sollten zunächst einer Gemeinde lediglich die Angaben aus dem Kaufvertrag mitgeteilt werden, die zur Prüfung über das Bestehen oder Nichtbestehen des Vorkaufsrechts notwendig sind, nämlich die Lage des Grundstücks, die Angabe der Beteiligten sowie der Kaufpreis im Hinblick auf die hiervon abhängig zu erhebende Gebühr gemäß § 10 Thüringer Kommunalabgabengesetz für die auszustellende Bescheinigung, mit der der Verzicht auf die Ausübung des Vorkaufsrechts seitens der Gemeinde erklärt wird. Erst wenn ein Vorkaufsrecht in Betracht kommt, sollte auf Anfrage der vollständige Kaufvertrag übermittelt werden.

11. Gesundheits- und Sozialdatenschutz

11.1 Neues Transplantationsrecht

Im Berichtszeitraum wurde nach längerer Diskussion im Transplantationsgesetz geregelt, unter welchen Voraussetzungen Organe Verstorbener entnommen und verpflanzt werden dürfen. Außer der juristischen und ethischen Frage, ab welchem Zeitpunkt ein Mensch als tot anzusehen ist, war im Rahmen des Gesetzgebungsverfahrens bis zuletzt offen, ob materielle Voraussetzung für die Zulässigkeit der Organentnahme ausschließlich die ausdrückliche Zustimmung des Betroffenen (enge Zustimmungslösung) sein soll oder

aber bei einer fehlenden Äußerung des Betroffenen ersatzweise die Zustimmung der nächsten Angehörigen bzw. einer Person, auf die die Entscheidung des Betroffenen zu Lebzeiten von diesem übertragen wurde (erweiterte Zustimmungslösung), ausreicht. Aus datenschutzrechtlicher Sicht hätte die „enge Zustimmungslösung“ - also die ausdrückliche Zustimmung des Organspenders - den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet, weil niemand gezwungen wird, seine ablehnende Haltung dokumentieren oder gar Dritten offenbaren zu müssen, wenn keine Transplantation gewünscht wird. Hierauf hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 14./15. März 1996 (Anlage 1) hingewiesen. Der Bundestag hat sich letztlich für die erweiterte Zustimmungslösung entschieden. Das Transplantationsgesetz vom 05.11.1997 (BGBl I S. 2631) ist am 01.12.1997 in Kraft getreten.

11.2 Sozialhilfedatenabgleichsverordnung (SozhiDAV)

Schon durch das Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms (FKPG) vom 23.06.1993 wurde in § 117 Bundessozialhilfegesetz (BSHG) die Rechtsgrundlage zum Erlaß einer Rechtsverordnung geschaffen, wonach die Sozialhilfeträger untereinander sowie die Sozialhilfeträger mit der Bundesanstalt für Arbeit und den Trägern der gesetzlichen Unfall- und Rentenversicherungen regelmäßig Daten über erbrachte Sozialleistungen abgleichen können. Die Aufnahme solcher umfangreichen Datenabgleichsmöglichkeiten in das BSHG erfolgte unter kritischer Begleitung der Datenschutzbeauftragten des Bundes und der Länder (1. TB, Anlage 3). Erst vier Jahre später wurde von der Bundesregierung ein Entwurf einer Sozialhilfedatenabgleichsverordnung nach § 117 Abs. 1 und 2 BSHG vorgelegt.

Der Verordnungsentwurf sieht vor, daß alle Sozialämter sowie die Bundesanstalt für Arbeit und die Renten- und Unfallversicherungsträger einen standardisierten Datensatz mit den Angaben über Name, Geburtsdatum, Geburtsort, Nationalität, Geschlecht, Anschrift und Versicherungsnummer an eine zentrale Vermittlungsstelle bei der Datenstelle der Rentenversicherungsträger (DSRV) regelmäßig übermitteln. Dort wird verglichen, ob Sozialleistungen auch von anderen Sozialleistungsträgern bezüglich derselben Person im gleichen Leistungszeitraum gezahlt worden sind. Ist das nicht der Fall, erfolgt eine Nullmeldung. Sofern auch Leistungen eines anderen Sozialleistungsträgers im gleichen Zeitraum erbracht worden sind, wird dies den beteiligten Stellen in einer Rückmeldung mitgeteilt. Allerdings kann hieraus allein noch nicht ein unzulässiger Doppelbezug von Sozialleistungen angenommen werden, da durchaus der Betroffene beispielsweise eine kleine Rente beziehen kann, die jedoch gegenüber dem Sozialamt angegeben worden ist und auf die Sozialhilfe angerechnet wird. Es muß also vom Sozialleistungsträger in der Regel dann erst ermittelt werden, ob ein Leistungsmißbrauch vorliegt.

Bei diesem Verfahren handelt es sich um einen nicht unerheblichen Eingriff in das informationelle Selbstbestimmungsrecht, das am Grundsatz der Verhältnismäßigkeit zu messen ist. Daher hielte ich einen Totalabgleich aller aktuellen Leistungsbezieher nur dann für verhältnismäßig, wenn konkrete Anhaltspunkte für einen erheblichen und flächendeckenden Sozialleistungsmißbrauch vorliegt und weniger einschneidende Möglichkeiten zu keinem Erfolg bei der Bekämpfung des Sozialleistungsmißbrauchs geführt haben. Deshalb habe ich gegenüber dem TMSG die Auffassung vertreten, daß in der Verordnung bei der Auswahl der Abgleichsfälle und des Abgleichszeitraums keine verbindliche Einbeziehung aller Sozialhilfeleistungsempfänger, die aktuell Sozialhilfe erhalten, vorgeschrieben werden sollte, sondern eine Ermessensregelung aufgenommen wird. Damit wäre sichergestellt, daß nur solche Personen in den Abgleich einbezogen werden, bei denen Anhaltspunkte für einen Mißbrauch vorliegen. Die Datenschutzbeauftragten von

Bund und Ländern sind sich einig, daß hier ein Nachweis, daß Sozialleistungsmißbrauch im großen Stil erfolgt, nicht erbracht worden ist. Dies beruht bisher größtenteils auf Vermutungen. Daher habe ich zusätzlich empfohlen, in die Verordnung eine Regelung aufzunehmen, die es erlaubt nachzuvollziehen, in wievielen Fällen und mit welchem finanziellen Ergebnis die übermittelten Datensätze zur Reduzierung des Leistungsmißbrauches genutzt werden konnten. Ich wende mich nicht gegen eine notwendige Einschränkung des Datenschutzes von Sozialhilfeempfängern, wenn dies zur Verhinderung und Aufdeckung von Sozialleistungsmißbrauch tatsächlich erforderlich ist. Allerdings darf eine solche einschneidende Maßnahme auch nicht ohne konkrete Anhaltspunkte erfolgen und dabei pauschal einer ganzen Bevölkerungsgruppe undifferenziert die Vertrauenswürdigkeit abgesprochen werden. Die Sozialhilfedatenabgleichsverordnung vom 21.01.1998 (BGBl I S. 103) ist mit Wirkung vom 01. Januar 1998 in Kraft getreten. Die von mir ggü. dem TMSG angeregte Ermessensregelung zur Durchführung von Totalabgleichen nur bei entsprechenden Anhaltspunkten wurde nicht aufgenommen. Eine Eingrenzung des Umfangs der Abgleiche erfolgt nur bei mangelnder technischer Ausstattung der Sozialhilfeträger. Eine Vorschrift für eine Erfolgskontrolle wurde ebenfalls nicht aufgenommen. Allerdings ist zwischenzeitlich auf Drängen des BfD vom Bundesministerium für Gesundheit ein wissenschaftliches Sozialforschungsinstitut mit der erfolgskontrollierenden Begleitung der Einführung des Sozialhilfedatenabgleichs beauftragt worden.

Parallel zu diesem konkreten Datenabgleichsverfahren hat eine Arbeitsgruppe der Arbeits- und Sozialministerkonferenz von Bund und Ländern Vorschläge erarbeitet, inwieweit ein zusätzlicher Datenaustausch bei Sozialleistungen zum effektiveren Mitteleinsatz und zur Verhinderung von Sozialleistungsmißbrauch eingeführt werden könnte. Die Datenschutzbeauftragten von Bund und Ländern haben in einer gemeinsamen Entschließung vom 20.10.1997 (Anlage 14) 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. Die Arbeits- und Sozialministerkonferenz hat diese Bedenken aufgegriffen und die Bundesregierung um Prüfung der Umsetzbarkeit der Vorschläge unter Einbeziehung des Gesprächsangebots der Datenschutzbeauftragten gebeten. Die weitere Entwicklung wird abzuwarten sein.

11.3 Landesrechtliche Ausführungsvorschriften zum Pflegeversicherungsgesetz und deren Anwendung

Das am 01. Januar 1995 in Kraft getretene Pflegeversicherungsgesetz (PflegeVG) verpflichtet in Artikel 1, § 9 SGB XI die Länder zur Vorhaltung einer leistungsfähigen, zahlenmäßig ausreichenden und wirtschaftlichen pflegerischen Infrastruktur. Das soll zum einen durch eine Landespflegeplanung geschehen. Zum anderen sollen bestimmte Investitionsaufwendungen öffentlich gefördert werden. Darüber hinaus wurde mit Artikel 52 PflegeVG ein Sonderinvestitionsprogramm für die neuen Länder aufgelegt. Zur Umsetzung dieser Vorgaben bedurfte es landesrechtlicher Regelungen, an deren Erarbeitung ich im Vorfeld durch das TMSG beteiligt worden bin. Der Entwurf des Thüringer Ausführungsgesetzes zum Pflegeversicherungsgesetz (ThürAGPflegeVG) enthielt in § 14 Auskunftspflichten der Träger der Pflegeeinrichtungen, der Pflegeversicherung, der privaten Versicherungsunternehmen sowie des Medizinischen Dienstes an das TMSG zu Zwecken der Planung und Investitionsförderung. Hierzu habe ich u. a. gefordert, daß weder Daten von Pflegebedürftigen noch Angaben von Angehörigen der Pflegebedürftigen und der ehrenamtlichen Helfer personenbezogen übermittelt werden dürfen. Für eine personenbezogene Übermittlung dieser mitunter

sensiblen Daten besteht im Rahmen der Pflegeplanung und Investitionsförderung keine Notwendigkeit. Außerdem habe ich angeregt, festzuschreiben, daß die personenbezogenen Daten über Pflegedienste und Einrichtungen bei den Landkreisen und kreisfreien Städten ausschließlich für Planungszwecke im Bereich der Pflegeversicherung verwendet werden. Meine Anregungen wurden übernommen. Das ThürAGPflegeVG vom 20.06.1996 (GVBl 1996, S. 97 ff.) ist am 01.07.1996 in Kraft getreten. Auch bei der aufgrund des ThürAGPflegeVG zu erlassenden Verordnung zur Durchführung des Thüringer Gesetzes zur Ausführung des Pflegeversicherungsgesetzes (ThürAG-PflegeVG-DVO) vom 12.12.1996 (GVBl. 1996, S. 62) wurde ich beteiligt.

Bei der Umsetzung der Regelungen im Zusammenhang mit der Erstellung des örtlichen Pflegeplanes nach § 3 Abs. 1 ThürAGPflegeVG wandte sich ein Pflegedienst an mich mit der Frage, ob es zulässig sei, daß vom zuständigen Landratsamt die Qualifikationsnachweise und die Arbeitsverträge der Pflegekräfte angefordert werden. Nach § 3 Abs. 2 Nr. 4 ThürAGPflegeVG-DVO sind für eine Bewerbung im Rahmen des Teilnahmewettbewerbs zur Erstellung des örtlichen Pflegeplanes der Nachweis über die Anzahl der beschäftigten Kräfte, deren Qualifikation und vertragliche Wochenarbeitszeit sowie über die Anzahl der sozialversicherungspflichtigen Beschäftigungsverhältnisse vorzulegen. Die Vorlage derartiger Unterlagen erscheint zur Entscheidung über die Aufnahme in den örtlichen Pflegeplan und damit über die Gewährung von Landesmitteln grundsätzlich erforderlich, da die Länder nach § 9 SGB XI für die Vorhaltung einer leistungsfähigen, zahlenmäßig ausreichenden und wirtschaftlichen pflegerischen Versorgungsstruktur verantwortlich sind und eine entsprechende Überprüfung von Zahl und Qualifikation der tatsächlich eingesetzten Pflegekräfte möglich sein muß. Allerdings handelt es sich dabei um Personaldaten über die Beschäftigten der Anbieter, so daß ein entsprechender Schutz, insbesondere eine strenge Zweckbindung, zu beachten ist. Eine Erforderlichkeit zur Vorlage der Arbeitsverträge der Beschäftigten in vollem Umfang ist § 3 Abs. 2 Nr. 4 ThürAGPflege-DVO nicht zu entnehmen. Hierfür ist es ausreichend, wenn Kopien der Arbeitsverträge vorgelegt werden, bei denen die nicht erforderlichen personenbezogenen Angaben geschwärzt sind. Zum Nachweis der Qualifikation reicht es aus, wenn die entsprechenden Nachweise beim Landratsamt vorgelegt werden und nach Sichtung und Prüfung dem Anbieter wieder zurückgegeben werden. Sofern im Einzelfall Zweifel am Vorliegen der Voraussetzungen bestehen sollten, können diese Unterlagen im Einzelfall beim jeweiligen Arbeitgeber durch Mitarbeiter des Sozialamts bzw. im Rahmen der Rechnungsprüfung durch Mitarbeiter der Rechnungsprüfungsstellen eingesehen werden. Über meine rechtliche Bewertung habe ich das zuständige Landratsamt sowie das TMSG informiert. Das Landratsamt hat mir mitgeteilt, daß im Rahmen des weiteren Teilnahmewettbewerbs nach meinen Hinweisen verfahren worden ist. Darüber hinaus hat das TMSG in einem Rundschreiben die zuständigen Stellen entsprechend informiert und um zukünftige Beachtung gebeten.

11.4 Dritte Verordnung über die Pauschalförderung nach dem Krankenhausgesetz

Vom TMSG wurde mir der Entwurf einer Dritten Verordnung über die Pauschalförderung nach dem Krankenhausgesetz (3. ThürKHG-PVO) zur Stellungnahme vorgelegt. Darin war u. a. vorgesehen, daß die Jahrespauschalen nicht mehr wie bisher nach der Planbettenzahl sowie der Versorgungsstufe bestimmt werden sollen, sondern anhand der Zahl der abgeschlossenen Behandlungsfälle. Damit lag es durchaus nahe, daß im Rahmen der Beantragung und Ausreichung der Fördermittel sowie im Zuge der Kontrolle der gemachten Angaben personenbezogene Daten aus dem Krankenhausbereich dem Krankenhausträger zur Vorlage gebracht werden müßten. In meiner

Zuständigkeit liegt nicht die Bewertung von Förderprinzipien aber der rechtmäßige Umgang mit personenbezogenen Daten. Aus diesem Grunde habe ich angeregt, in die 3. ThürKHG-PVO ausdrücklich aufzunehmen, daß zur Festsetzung und Überprüfung der Jahrespauschale von den Krankenhäusern nur anonymisierte Daten übermittelt werden dürfen. Dies fand in der 3. ThürKHG-PVO vom 09. Dezember 1997 (GVBl. S. 518) Berücksichtigung, womit die datenschutzrechtlichen Bedenken ausgeräumt sind.

11.5 Kontrolle eines Universitätsklinikums

Im Berichtszeitraum wurde eine Kontrolle in einem Universitätsklinikum durchgeführt. Neben der Überprüfung der technisch-organisatorischen Maßnahmen zum Schutz der Patientendaten wurden auch die Auswirkungen des Einsatzes eines automatisierten Patientenverwaltungssystems aus datenschutzrechtlicher Sicht kontrolliert. Obwohl keine Verstöße gegen datenschutzrechtliche Vorschriften festgestellt wurden, habe ich eine Reihe von Empfehlungen zur Verbesserung des Patientendatenschutzes abgegeben, die zwischenzeitlich im Rahmen des Möglichen umgesetzt worden sind.

Das Klinikum hatte seit kurzem ein Patientenverwaltungssystem eingeführt. Damit erfolgt die Patientenaufnahme sowie die Abrechnung automatisiert. In einigen Kliniken ist das System auch zur Patientenverwaltung auf den einzelnen Stationen eingesetzt. Wie bereits durch meine Kollegen in anderen Bundesländern, wurde auch in Thüringen bei der Überprüfung der Aufnahmeprozedur mit diesem System festgestellt, daß systemseitig Daten vom Patienten abgefragt werden, die zum Teil nicht erforderlich sind. So wurde z. B. nach dem Familienstand des Patienten gefragt. Für den Fall, daß im Rahmen der Behandlung eine Einwilligungserklärung des Ehepartners erforderlich ist, reicht die Angabe verheiratet/nicht verheiratet aus. Die Tatsache, ob jemand verwitwet, geschieden oder getrennt lebend ist, ist in diesem Zusammenhang unerheblich. Im Formular war auch routinemäßig die Tätigkeit und der Arbeitgeber des Hauptversicherten einzutragen. Eine Erforderlichkeit hierfür ergibt sich jedoch nur dann, wenn die Krankenhausbehandlung aufgrund eines Arbeitsunfalles erfolgt, um Kontakt mit der zuständigen Berufsgenossenschaft zur Leistungsabrechnung aufnehmen zu können. Eine Notwendigkeit der Abfragefelder „Pseudonym“, „VIP“, „Organspender“ und „Konfession“ war ebenfalls nicht erkennbar. Auch nach dem neuen Transplantationsgesetz (11.1) besteht keine Pflicht, die Eigenschaft als Organspender gegenüber dem behandelnden Krankenhaus zu offenbaren. Schließlich hat auch die Angabe der Religionszugehörigkeit keine Auswirkung auf die Behandlung. Sofern es um die Frage der Klinikseelsorge geht, wäre zu fragen, ob eine solche gewünscht ist. Erst wenn dies zutrifft, wäre die Frage nach der Konfession des gewünschten Klinikseelsorgers als notwendig anzusehen. Das Klinikum hat aufgrund meiner Hinweise in einer Dienstanweisung festgelegt, daß die betreffenden Datenfelder bei der Aufnahme nicht benutzt werden bzw. die Angaben freiwillig sind (Konfession bzw. Personalien der Angehörigen) oder aber nur in bestimmten Konstellationen abgefragt werden (Arbeitgeber nur bei Unfällen). Dies sehe ich jedoch nur als eine Übergangslösung an, da die Gefahr besteht, daß diese Daten versehentlich abgefragt werden, obwohl keine Erforderlichkeit besteht. Dieses Beispiel zeigt deutlich, daß beim Einsatz elektronischer Datenverarbeitung verarbeitende Stellen oftmals vorgefertigte Softwareprodukte einsetzen, die jedoch nicht den geltenden Vorschriften für die Einzelanwendung entsprechen.

Schließlich waren die Zugriffsrechte der Mitarbeiter zum Zeitpunkt der Kontrolle nicht auf das für die jeweilige Aufgabenerfüllung erforderliche Maß beschränkt. Nach meinen entsprechenden Hinweisen wurde zwischenzeitlich in einer überarbeiteten Version diese Beschränkung der Zugriffsrechte vorgenommen.

11.6 Krankenhäuser als Wettbewerbsunternehmen nach § 26 ThürDSG

Aus Anfragen von Krankenhäusern habe ich entnommen, daß häufig Unsicherheiten bei der Frage bestehen, welche datenschutzrechtlichen Vorschriften in Krankenhäusern zu beachten sind. Soweit es um die Patientendaten geht, haben alle Krankenhäuser unabhängig von ihrer Trägerschaft (Land, Landkreis, Stadt, Private oder Kirchen) die Vorschriften des Thüringer Krankenhausgesetzes (ThürKHG) zu beachten. Als öffentliche Stellen nach § 2 Abs. 1 ThürDSG sind auch solche Krankenhäuser anzusehen, die in einer privatrechtlichen Rechtsform betrieben werden und deren Mehrheitsgesellschafter eine öffentliche Stelle ist. Soweit jedoch öffentliche Stellen am Wettbewerb teilnehmen, sind auf sie nach § 26 ThürDSG die materiellen Vorschriften des BDSG über nicht-öffentliche Stellen anzuwenden. Von den Vorschriften des ThürDSG sind lediglich diejenigen über die Kontrollbefugnisse des TLfD anwendbar. Von Bedeutung ist die Einordnung als Wettbewerbsunternehmen insbesondere deshalb, weil Wettbewerbsunternehmen keine Meldungen zum Thüringer Datenschutzregister nach § 12 ThürDSG an den TLfD abgeben müssen.

Ich gehe bei Krankenhäusern, die öffentlichen Stellen des Landes gemäß § 2 Abs. 1 ThürDSG sind, grundsätzlich von einer Wettbewerbssituation nach § 26 ThürDSG aus. Dies gilt auch für Universitätskliniken. Zwar erfüllen Universitätskliniken auch Funktionen, die von anderen Krankenhäusern nicht erbracht werden. Neben den Leistungen der Krankenversorgung haben sie Aufgaben der Forschung und Lehre zu erfüllen, die jedoch nicht die überwiegende Zweckbestimmung darstellen. Nach 26.1 VVThürDSG ist bei mehreren Tätigkeitsfeldern die teilweise dem Wettbewerb unterfallen und teilweise nicht dem Wettbewerb unterfallen, auf die überwiegende Zweckbestimmung abzustellen. Da bei einer Universitätsklinik überwiegend Leistungen der Krankenversorgung erbracht werden, ist von einer Wettbewerbssituation auszugehen. Gleiches gilt auch für die Landesfachkrankenhäuser für Psychiatrie und Neurologie bei denen nur ein geringer Teil der Patienten zwangsweise eingewiesen wird und zum überwiegenden Teil die Patienten sich die im Wettbewerb zueinander stehenden Krankenhäuser selbst aussuchen können. Diese Auffassung vertritt auch das TMSG.

11.7 Bekenntnisfreiheit und Datenschutz im Krankenhaus

Aufgrund meiner Ausführungen zur Übermittlung von Daten zur Religionszugehörigkeit von Patienten im Krankenhaus im 1. TB (11.3.4), wurde ich gebeten, die von mir „favorisierte negative Bekenntnisfreiheit eines Patienten im Krankenhaus“ nochmals zu überdenken. Es sollte danach dem Patienten freigestellt sein, ob er Angaben zu seiner Konfession machen will oder nicht. Um dies sicherzustellen, wurde angeregt, die Krankenhäuser zu verpflichten, entsprechende Fragen an den Patienten zur Konfessionszugehörigkeit zu stellen. Ich habe dazu mitgeteilt, daß keinesfalls eine Verfahrensweise favorisiert wurde, sondern ich lediglich auf die grundrechtlich garantierte negative Bekenntnisfreiheit nach Artikel 4 Abs. 1 Grundgesetz hingewiesen habe. Selbstverständlich bestehen keine Bedenken gegen eine Erhebung der Religionszugehörigkeit zum Zweck der Weitergabe an die Klinikseelsorge, sofern der Patient seine Einwilligung nach einer Information über die Freiwilligkeit erteilt hat.

Davon zu unterscheiden ist jedoch die mögliche Verpflichtung des Krankenhauses, überhaupt die Krankenhausseelsorge einzuschalten und hierzu entsprechende Erhebungen beim Patienten durchzuführen. Das ist keine Frage des Datenschutzes und müßte beispielsweise durch die Krankenhausträger erfolgen. Deshalb habe ich den betreffenden Kirchenvertreter an das TMSG

als oberste Rechtsaufsicht im Krankenhausbereich vermittelt. Wie mir bekannt ist, wird derzeit zwischen dem TMSG und dem TIM eine Mitteilung an die Krankenhäuser in öffentlicher Trägerschaft vorbereitet, die vorsehen soll, daß der Wunsch des Patienten bezüglich einer Krankenhausseelsorge sowohl im positiven wie im negativen Sinn zu respektieren ist. In einer solchen Mitteilung könnten auch die datenschutzrechtliche Fragen zusammenfassend dargestellt werden. Darin wäre u. a. klarzustellen, daß die Erhebung der Konfessionszugehörigkeit nur mit Einwilligung des Patienten zulässig ist, wobei dieser auf die Freiwilligkeit seiner Angaben und die ausschließliche Zweckbestimmung der Weiterleitung dieses Datums an den zuständigen Seelsorger informiert werden muß. Kann der Patient nicht befragt werden und ist die Religionszugehörigkeit dem Krankenhaus bekannt, so ist auf den mutmaßlichen Willen des Patienten abzustellen, der insbesondere auch durch Befragung von Angehörigen ermittelt werden kann. Ich gehe davon aus, daß mit einer entsprechenden Mitteilung auch dem Anliegen der Kirchen an einer Ermöglichung ihrer Arbeit im Krankenhaus ausreichend Rechnung getragen werden kann.

11.8 Datensicherungsmaßnahmen beim Versand von Gewebeproben

Daß der Datenschutz nicht nur eine unzulässige Erhebung, Verarbeitung und Nutzung von Daten bzw. eine Kenntnisnahme personenbezogener Daten durch unbefugte Personen verhindern soll, sondern auch dazu dient, personenbezogene Daten vor Verlust zu schützen, zeigt ein Fall, den ich der Presse entnommen habe. Dort war unter der Überschrift „Verschlampte Krebs-Tests: Wenn man sich auf die Post verläßt ...“ zu lesen, daß von einem Krankenhaus bei mehreren entnommenen Gewebeproben von Patienten nach dem Versand mit einfacher Postsendung auf dem Postweg verlorengegangen waren. Solche Gewebeproben sind Patientendaten i. S. v. § 27 Abs. 2 Satz 2 ThürKHG, da es sich dabei um Einzelangaben über die persönlichen Verhältnisse bestimmter Patienten aus dem Bereich der Krankenhäuser handelt. Selbst wenn, wie im Regelfall, die Gewebeproben nicht den Namen und sonstige personenbezogene Angaben getragen haben, sondern mit einer Verweisnummer versehen wurden, handelt es sich um solche Informationen über den Patienten, die nach durchgeführter Analyse anhand der Verweisnummer im Krankenhaus wieder dem einzelnen Patienten zugeordnet werden. Kommt die Gewebeprobe abhanden, so sind auch diese personenbezogenen Angaben verloren. Daher sind nach § 27 Abs. 10 ThürKHG durch das Krankenhaus die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Beachtung der in den Absätzen 1 bis 9 enthaltenen Bestimmungen zu gewährleisten. Dazu gehört insbesondere auch der Erhalt der personenbezogenen Daten.

Das betreffende Krankenhaus hat auf meine Anfrage hin mitgeteilt, daß die Gewebeproben in einer Spezialverpackung mit einfacher Postsendung an ein Labor versandt wurden. Diese Verfahrensweise entsprach den genannten Anforderungen nicht, da mangels einer lückenlosen Dokumentation (Postausgangsbuch, Dokumentation über den Verbleib bei der Post AG) eine Nachverfolgung der Proben erheblich erschwert bzw. ausgeschlossen wird. Aufgrund des Vorfalls hat das Krankenhaus sein Verfahren dahingehend geändert, daß die Gewebeproben zukünftig durch einen Paketdienst transportiert werden, bei dem sowohl die Übergabe als auch alle weiteren Zwischenstationen lückenlos aufgezeichnet werden.

11.9 Archivierung von Krankenakten

Krankenhäuser haben die Akten ihrer Patienten auch nach Abschluß der Behandlung für eine bestimmte Zeit sicher aufzubewahren. Dies erfolgt sowohl im Interesse des Patienten als auch im Interesse des Krankenhauses und des behandelnden Arztes, der beispielsweise bei möglichen Haftungsprozessen die Möglichkeit haben muß, nachzuweisen, welche Diagnosen er gestellt bzw. therapeutische Maßnahmen er auf welcher Wissensgrundlage angeordnet hat. Dementsprechend legen die ärztlichen Berufsordnungen und spezialgesetzliche Regelungen wie z. B. die Strahlenschutzverordnung Mindestzeiten für die Aufbewahrung von Krankenunterlagen fest. In einer Dienstanweisung hatte ein Krankenhaus in Anlehnung an die Verjährungsfrist des BGB eine Aufbewahrungsfrist von abgeschlossenen Krankenakten auf dreißig Jahre festgelegt und gleichzeitig angeordnet, daß ältere Akten zu vernichten sind. Sofern im Einzelfall ein besonderes Interesse für die Forschung und Lehre besteht, sollte von einer Vernichtung abgesehen werden. Im Rahmen einer Kontrolle wurde festgestellt, daß unter Hinweis auf die Notwendigkeit der Nutzung der Akten für Forschungszwecke generell noch alle Akten, die länger als dreißig Jahre abgeschlossen waren, im Krankenhaus aufbewahrt worden waren. Eine generelle Aufbewahrung aller Akten über die vorgeschriebenen Aufbewahrungsfristen hinaus ist nach § 27 Abs. 9 ThürKHG nicht zulässig. Die Akten wurden in erster Linie zum Zweck der Krankenbehandlung angelegt. Nach Abschluß der Krankenhausbehandlung und Ablauf einer angemessenen Frist besteht keine Notwendigkeit mehr, daß ohne weiteres auf diese Unterlagen im Rahmen des Krankenhausgesetzes zugegriffen werden muß. Sofern Unterlagen für Forschungszwecke benötigt werden, können in den Krankenhäusern vorhandene Unterlagen nach den Grundsätzen von § 27 Abs. 4 ThürKHG innerhalb des Krankenhauses (ggf. auch durch externe Forscher) genutzt werden. Diese Forschungsklausel, die u. a. die Pflicht zur frühestmöglichen Anonymisierung der Unterlagen enthält, gilt jedoch nur dann, wenn die Patientendaten noch nicht nach § 27 Abs. 9 ThürKHG zu löschen sind. Nach Ablauf der Aufbewahrungsfristen ergeben sich aus dem Archivrecht die rechtlichen Rahmenbedingungen , um sowohl den Interessen der Forscher als auch den berechtigten Interessen der Patienten am ordnungsgemäßen Umgang mit ihren Gesundheitsdaten gerecht zu werden. Die weitere Aufbewahrung von Krankenunterlagen bedarf einer besonderen Betrachtung, wenn es sich um eine wissenschaftliche Forschungseinrichtung handelt. Konkret stellte sich mir diese Frage bei einem Universitätsklinikum. Wegen dem besonderen Forschungsinteresse an den dort vorhanden Krankenunterlagen und weil die potentiellen Nutzer überwiegend aus dem Klinikum selbst kommen, beabsichtigt das Klinikum, ein eigenes Krankenaktenarchiv auf der Grundlage von § 5 Thüringer Archivgesetz (ThürArchivG) einzurichten. Hierzu muß von der Universität eine eigene Archivsatzung erlassen werden. Dabei wird darauf zu achten sein, daß nur diejenigen Patientenakten dauerhaft archiviert werden, die für die Forschung von Bedeutung sind. Weil es sich um besonders sensible Akten handelt, muß dabei auch eine Begrenzung des Personenkreises erfolgen, der mit diesen Akten umgehen darf, wobei sich der Kreis grundsätzlich nur auf die der Schweigepflicht unterliegenden Ärzte erstrecken sollte. Aus datenschutzrechtlicher Sicht ist eine solche Archivierung ärztlicher Unterlagen im Klinikum gegenüber einer Aufbewahrung im Staatsarchiv zu bevorzugen, da dies insoweit unter dem Schutzbereich der ärztlichen Schweigepflicht erfolgt. Das Klinikum hat mir zugesagt, mich bei diesen weiteren Verfahrensschritten zu beteiligen.

11.10 Externe Archivierung von Krankenhausakten/Mikroverfilmung

Die gesetzlichen Aufbewahrungspflichten für Krankenakten sowie die technische Möglichkeit, den Archivierungspflichten auch dadurch nachzukommen, daß ein platzsparender Mikrofilm erstellt wird und die eigentliche Akte vernichtet werden könnte, führen sowohl bei Krankenhäusern als auch bei entsprechenden Dienstleistungsunternehmen zu Überlegungen, ob diese Datenverarbeitungsvorgänge auch außerhalb von ärztlichen Behandlungseinrichtungen durchgeführt werden können. Da in Krankenakten sensible personenbezogene Daten enthalten sind, die überdies durch die Vorschriften des Strafgesetzbuches (§ 203) sowie der Landeskrankenhausgesetze geschützt sind, ist ein Umgang mit diesen Daten durch nicht zum Krankenhaus gehörendes Personal nur unter sehr eingeschränkten Voraussetzungen möglich. Die Datenschutzbeauftragten des Bundes und der Länder haben sich zunehmend mit Anfragen zu beschäftigen, unter welchen Voraussetzungen Verarbeitungen außerhalb der ärztlichen Behandlungseinrichtungen noch als zulässig anzusehen sind. Dabei sind die rechtlichen Rahmenbedingungen in den einzelnen Bundesländern aufgrund der unterschiedlichen Landeskrankenhausgesetze differenziert zu betrachten. Die Mikroverfilmung von Krankenhausakten durch ein Privatunternehmen ist nach § 27 Abs. 5 Satz 2 ThürKHG erlaubt, wenn das Krankenhaus sicherstellt, daß beim Auftragnehmer besondere technisch-organisatorische Schutzmaßnahmen eingehalten werden und solange keine Anhaltspunkte dafür bestehen, daß durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden. Bei dieser Vorschrift handelt es sich um eine Befugnisnorm, die eine Offenbarung von Patientenakten zum Zweck der Mikroverfilmung an Mitarbeiter des Unternehmens erlauben. Es gilt hier allerdings die Einschränkung, daß keine Anhaltspunkte bestehen, daß schutzwürdige Belange von Patienten beeinträchtigt werden. Sofern die Akten zum Zweck der Mikroverfilmung aus dem Krankenhaus gegeben werden, entfällt der Gewahrsam der Krankenanstalt nach § 97 Abs. 2 Satz 2 StPO. Das hat zur Folge, daß die Krankenakten den Beschlagnahmeschutz verlieren, den sie bei Aufbewahrung im Krankenhaus genießen. Deshalb wird in diesen Fällen regelmäßig ein entgegenstehendes Interesse des Patienten anzunehmen sein, so daß eine Mikroverfilmung durch Dritte nur innerhalb des Krankenhauses als zulässig anzusehen ist. Nach Angaben der Landeskrankenhausgesellschaft, besteht derzeit bei den Thüringer Krankenhäusern kein Bedürfnis, diese Mikroverfilmung bzw. die Archivierung von Krankenunterlagen außerhalb der Krankenhäuser vorzunehmen.

Für eine Archivierung von Krankenakten außerhalb der Krankenhäuser gibt es keine entsprechenden Regelungen im Thüringer Krankenhausgesetz. Die allgemeinen Vorschriften über die Datenverarbeitung im Auftrag nach § 8 ThürDSG können jedoch eine Offenbarung von Unterlagen, die der ärztlichen Schweigepflicht unterliegen, nicht erlauben. Sofern eine Einwilligung der betroffenen Patienten nicht vorliegt, kommt für eine Aufbewahrung dieser Unterlagen bei einem externen Archivierungsunternehmen lediglich eine sogenannte „Container-Lösung“ (5.2.9) in Betracht, bei der es dem aufbewahrenden Unternehmer nicht möglich ist, Kenntnis vom Inhalt der jeweiligen Akten zu nehmen.

11.11 Krankenakte im Krankenhaus verlegt

Eine Patientin eines Thüringer Krankenhauses wandte sich mit der Bitte an mich, ihr beim Auffinden ihrer Krankenakte behilflich zu sein, da sie diese im Rahmen einer weiteren ärztlichen Behandlung benötigte. Meine Überprüfung der Angelegenheit ergab, daß die Krankenakte unter einem falschen Vornamen im Archiv des Krankenhauses abgelegt worden war. Dadurch

bedingt erhielt die Patientin bei ihren Nachfragen die Auskunft, daß ihre Akte nicht vorliege. Obwohl in diesem Fall keine Stellen außerhalb des Krankenhauses Kenntnis vom Inhalt der Akte nehmen konnten, lag eine Beeinträchtigung der Rechte der Patientin vor, da ein erforderlicher Zugriff auf die Unterlagen über einen längeren Zeitraum nicht möglich war. Ich habe daraufhin das Krankenhaus aufgefordert, die Unterlagen so aufzubewahren, daß jederzeit unter dem zutreffenden Namen auf sie zugegriffen werden kann.

11.12 Einsichtsrecht des Patienten in Krankenhausakten

Im Rahmen einer Eingabe hatte ich mich mit der Frage zu beschäftigen, unter welchen Voraussetzungen und in welchem Umfang Patienten Einsicht in die zu ihrer Behandlung angelegten Krankenakten erhalten können. Der Petent war nach seinen Angaben Ende der fünfziger und Mitte der sechziger Jahre zwei Mal - nach seiner Ansicht zu Unrecht - zwangsweise in eine Nervenklinik eingewiesen worden. Zwischenzeitlich hatte er einen Antrag auf berufliche Rehabilitierung gestellt und dabei erfahren, daß im betreffenden Krankenhaus eine Krankenakte über ihn existiert. Nachdem er schriftlich einen Antrag auf Akteneinsicht gestellt hatte, fand ein Termin im Krankenhaus statt, bei dem ihm ein Arzt auszugsweise aus seiner Krankenakte vorgelesen hatte. Ein unmittelbarer Einblick in die Akte wurde ihm aus Gründen des Datenschutzes verweigert. Die von ihm vermuteten Bescheinigungen über die Zwangseinweisungen befanden sich nach Angaben des Arztes nicht in der Krankenakte. Nach § 27 Abs. 8 ThürKHG hat der Patient auf einen Antrag hin Anspruch auf kostenfreie Auskunft über die zu seiner Person gespeicherten Daten. Daraus ist abzuleiten, daß der mündige Patient grundsätzlich ein Recht darauf hat, zu erfahren, welche Aufzeichnungen über ihn im Rahmen einer Krankenhausbehandlung erstellt worden sind. Nach § 27 Abs. 8 Satz 3 ThürKHG ist vorgesehen, daß die Auskunft im Einzelfall durch einen Arzt vermittelt werden soll, soweit dies mit Rücksicht auf den Gesundheitszustand des Patienten dringend geboten ist. Sinn dieser Regelung ist die Absicht, dem einsichtnehmenden Patienten, der in der Regel nicht über den medizinischen Sachverstand verfügt, die ärztliche Dokumentation in ihrer vollen Tragweite zu erläutern. So könnte z. B. die Eintragung einer Verdachtsdiagnose, die sich jedoch nicht bestätigt hat, beim Patienten zu falschen Schlüssen führen. Nach § 27 Abs. 8 Satz 3 ThürKHG ist eine Beschränkung der Auskunft hinsichtlich ärztlicher Beurteilungen oder Wertungen zulässig. Hier ist durch den Arzt im Einzelfall eine Abwägung zwischen dem informationellen Selbstbestimmungsrecht und dem therapeutischen Interesse des Patienten vorzunehmen. Soweit Unterlagen aus den Krankenakten als Nachweis in einem Rehabilitierungsverfahren benötigt werden, besteht die Möglichkeit, daß der Patient die Krankenhausärzte gegenüber der Rehabilitierungsbehörde von der ärztlichen Schweigepflicht entbindet und diese die erforderlichen Unterlagen in Kopie der Rehabilitierungsbehörde übergeben. Dabei wäre allerdings auch möglich, daß ärztliche Beurteilungen oder Wertungen, die die Voraussetzungen nach § 27 Abs. 8 Satz 4 ThürKHG erfüllen, auf den Kopien geschwärzt werden. Evtl. in den Akten vorhandene personenbezogene Daten Dritter müssen geschwärzt werden, da sich der Auskunftsanspruch nicht auf diese Daten erstreckt. Das Krankenhaus habe ich auf diese Rechtslage hingewiesen. Dieses hat mitgeteilt, daß gegen eine entsprechende Erstattung der Kosten für Kopien und Porto die gewünschten Kopien zur Verfügung gestellt werden. Den Petenten habe ich ebenfalls über diese Verfahrensmöglichkeiten informiert, womit seinem Anliegen in angemessener Weise Rechnung getragen sein dürfte.

11.13 Chipkarten im Gesundheitswesen

Bereits in meinem 1. TB (11.10) habe ich die Aktivitäten im Bereich des Gesundheitswesens zur Einführung von Chipkartenanwendungen sowie die hierzu von den Datenschutzbeauftragten des Bundes und der Länder geforderten Rahmenbedingungen dargestellt. Auch im Berichtszeitraum hat ein intensiver Meinungsaustausch zwischen den Datenschutzbeauftragten und der Arbeitsgemeinschaft „Karten im Gesundheitswesen“ stattgefunden. In der Arbeitsgemeinschaft sind bundesweit Verbände, Institutionen und Unternehmen vertreten, die eine gewisse Standardisierung der Technik bei den Kartenprojekten - auch auf europäischer Ebene - anstreben. Im Rahmen dieses Meinungsaustausches wurde in zahlreichen Punkten Übereinstimmung bei der Beurteilung der Rahmenbedingungen für den Einsatz von Chipkartenanwendungen erzielt. Dazu zählt u. a., daß die Verwendung von Chipkarten im Gesundheitswesen (mit Ausnahme der Krankenversichertenkarte nach § 291 SGB V) ausschließlich auf freiwilliger Basis erfolgt und der Betroffene jederzeit die Möglichkeit haben muß, vom Inhalt der gespeicherten Daten Kenntnis zu nehmen. Einvernehmen besteht auch bzgl. der Notwendigkeit zur Schaffung der technischen Voraussetzungen, um sicherzustellen, daß keine unbefugten Dritten Einsicht in die auf der Karte gespeicherten Daten bekommen (vgl. hierzu die allgemeinen Anforderungen an die Datensicherheit beim Einsatz von Chipkarten unter 15.9). Zwischenzeitlich sind weitere Pilotprojekte, wie z. B. die medizinische Patientenkarte bei der Kassenärztlichen Vereinigung Koblenz gestartet worden, die den Vorgaben der Entschließungen der Datenschutzkonferenzen weitgehend entspricht (das Problem des sozialen Drucks zur Verwendung der Karte stellt sich hier wegen der geringen Zahl der Teilnehmer nicht). Andere bereits begonnene Pilotprojekte wurden nicht weiter verfolgt. Mittlerweile ist eine gewisse Tendenz dahingehend zu beobachten, daß die freiwilligen Patientenchipkarten lediglich einen eingeschränkten Datensatz wie z. B. Blutgruppe, Rhesusfaktor, Allergien, Impfungen usw. enthalten. Dies wird durch Absprachen auf der Ebene der G7-Staaten unterstrichen, die sich auf einen einheitlichen Patienten-Datensatz (Patient Data Set) geeinigt haben, der in allen Gesundheitskartensystemen als Mindestangabe enthalten sein sollte. Dieser Datensatz umfaßt neben reinen Notfallangaben auch Angaben über Erkrankungen, Allergien und Medikamente, deren Kenntnis bei einer ärztlichen Behandlung notwendig sind, um das Eintreten eines Notfalls oder einer ernsten Komplikation möglichst zu vermeiden. Ergänzend soll eine sogenannte Health Professional Card (HPC) entwickelt werden, die Ärzten oder medizinischem Personal über elektronische Verfahren den Zugriff auf Patientendaten der Patientenchipkarten aber auch über Datennetze auf Patientendaten in Arztpraxen und Krankenhäusern ermöglichen soll. Durch den Einsatz von geeigneter Sicherheitssoftware muß dabei sichergestellt werden, daß nur hierzu berechtigte Angehörige von Heilberufen und deren Hilfspersonal (Health Professionals) Zugriff auf sensible medizinische Daten bekommen können. Auch im Zusammenhang mit der Nutzung von medizinischen Datennetzen und telemedizinischen Anwendungen (z. B. Übertragung von Operationen über das ISDN-Netz) stellen sich ähnliche Fragen wie bei Chipkartenanwendungen. So ergibt sich auch hier insbesondere das Problem, welche technischen Vorkehrungen getroffen werden müssen, um auszuschließen, daß Unbefugte Zugriff auf die durch § 203 StGB besonders geschützten medizinischen Daten bekommen können.

11.14 Vorlage eines polizeilichen Führungszeugnisses für die Zulassung als Vertragsarzt

Bereits in meinem 1. TB (11.11.2) hatte ich darüber berichtet, daß das von der Kassenärztlichen Vereinigung Thüringen nach wie vor für die Zulassung als Vertragsarzt geforderte Behördenführungszeugnis zur unmittelbaren

Übersendung an die Behörde auf die derzeit gültige Rechtsgrundlage des § 18 Abs. 2 b Ärzte-ZV nicht gestützt werden kann. Da von Fachseite ein Behördenführungszeugnis gemäß § 30 Abs. 5 BZRG aber weitgehend für erforderlich gehalten wird, hat das BMG nunmehr den Entwurf einer fünften Verordnung zur Änderung der Zulassungsverordnung für Vertragsärzte vorgelegt, gegen den ich aus datenschutzrechtlicher Sicht keine Bedenken mehr habe.

11.15 Umgang mit Kassenarztverzeichnis

Im Berichtszeitraum wurde die Frage erörtert, welchen Personen Angaben aus dem bei der Kassenärztlichen und Kassenzahnärztlichen Vereinigungen (KV bzw. KZV) nach § 95 SGB V zu führenden Arztregister zugänglich gemacht werden können. Als mögliche Adressaten kommen die übrigen Kassenärzte im Einzugsbereich der KV und KZV, die gesetzlichen Krankenkassen, die gesetzlich Krankenversicherten oder auch Rettungsleitstellen in Betracht. Die Bekanntgabe der Namen, Anschriften, Facharztbezeichnung, Sprechzeiten und Telefonnummern der Kassenärzte an die Krankenkassen sowie auf Einzelanfrage an die gesetzlich Krankenversicherten halte ich nach den Vorschriften des SGB V für zulässig. Ebenso ist die Bekanntgabe der Daten an diejenigen Rettungsleitstellen zu beurteilen, die die Einsätze der am ärztlichen Notfalldienst teilnehmenden Ärzte koordinieren. Für eine Übermittlung an alle übrigen Kassenärzte oder gar Veröffentlichung der Angaben, besteht jedoch keine gesetzliche Grundlage, weshalb dies nur mit Einwilligung der betroffenen Ärzte zulässig wäre, falls eine Erforderlichkeit hierfür überhaupt zu begründen wäre. Bei den personenbezogenen Daten der Vertragsärzte wie z. B. Name, Anschrift, Facharztbezeichnung, Sprechzeiten oder Telefonnummer handelt es sich auch um Sozialdaten im Sinne von § 67 Abs. 1 SGB X, weil diese von der KV als einer im SGB genannten öffentlich-rechtlichen Vereinigung (§ 35 Abs. 1) im Hinblick auf die in § 95 SGB V vorgesehene Pflicht zur Führung des Arztregisters erhoben wurden. Das ergibt sich im übrigen auch aus § 285 SGB V. Da die Krankenkassen an der Erfüllung des Sicherstellungsauftrages mitwirken, haben sie einen Anspruch, zu erfahren, ob in ihrem Bereich die vertragsärztliche Versorgung tatsächlich sichergestellt ist. Deshalb ist eine Übermittlung der Ärzteliste an die Krankenkassen nach § 69 Abs. 1 Nr. 1 SGB X und § 285 Abs. 3 i. V. m. Abs. 1 Satz 1 Nr. 2 SGB V zulässig. Auch eine Übermittlung im Einzelfall auf Anfrage von Versicherten durch die Krankenkassen ist zur Aufgabenerfüllung der Krankenkassen nach § 69 Abs. 1 Nr. 1 SGB X erforderlich, da diese nach § 17 SGB I die Pflicht haben, darauf hinzuwirken, daß jeder Berechtigte die ihm zustehenden Sozialleistungen in zeitgemäßer Weise, umfassend und schnell erhält sowie der Zugang zu den Sozialleistungen möglichst einfach gestaltet wird. Eine Rechtsgrundlage für die Übermittlung dieser Liste durch die KV an die übrigen Vertragsärzte ist jedoch weder dem Sozialgesetzbuch zu entnehmen, da die Vertragsärzte nicht als Leistungsträger anzusehen sind, noch aus § 59 Bundesmantelvertrag-Ärzte ersichtlich, da dort lediglich geregelt ist, daß die KV den Krankenkassen ein Verzeichnis zur Verfügung stellt, jedoch nicht die Vertragsärzte als Empfänger nennt. Es besteht allenfalls die Möglichkeit, die Vertragsärzte in eine entsprechende Datenübermittlung einwilligen zu lassen, wobei diese vorher auf den Zweck und die Freiwilligkeit der Übermittlung hingewiesen werden müssen. Demgegenüber ist die Übermittlung der Daten an eine Rettungsleitstelle, die die Einsätze des ärztlichen Notfalldienstes koordiniert, zur Erfüllung des Sicherstellungsauftrages nach § 75 SGB V erforderlich. Deshalb ergibt sich die Zulässigkeit der Datenübermittlung aus § 285 Abs. 3 i. V. m. Abs. 1 Satz 1 Nr. 2 SGB V. Eine Erforderlichkeit der Übermittlung von Vertragsarztdaten an Rettungsleitstellen, in deren Bereich der betreffende Arzt nicht niedergelassen ist, ist aber nicht ersichtlich.

11.16 Meldebögen der Landestierärztekammer Thüringen

In einer Anfrage wurde ich auf die von der Landestierärztekammer Thüringen verwendeten Meldebögen zur Anmeldung bei der Tierärztekammer aufmerksam gemacht. Darin werden außer den Angaben zur Person, Praxisanschrift, tierärztlichen Prüfung, Approbation und Fachgebietsbezeichnungen auch Angaben über die Mitgliedschaft beim Versorgungswerk, die Höhe der bisherigen Kammerbeiträge, die Versandanschrift für das Deutsche Tierärzteblatt sowie in einem weiteren Erhebungsbogen detaillierte Angaben zur Haupt- und Nebentätigkeit der Ärzte angefordert. Dabei werden u. a. die Namen von Mitinhabern einer Gemeinschafts- bzw. Gruppenpraxis oder des Arztes, bei dem der Meldende als Assistent tätig ist sowie die Beschäftigungsverhältnisse mit Kliniken oder Instituten erfragt. Auf Nachfrage zur Erforderlichkeit dieser Angaben teilte die Landestierärztekammer mit, daß dies zur Ermittlung des Fort- und Weiterbildungsbedarfs sowie zur Ermittlung geeigneter Gutachter notwendig sei. In der aufgrund des Thüringer Heilberufegesetzes (HeilberG) erlassenen Satzung der Landestierärztekammer Thüringen wird der Tierarzt nach § 3 verpflichtet, Angaben über Personalien, Ort und Art seiner Tätigkeit sowie Nachweise über seine Qualifikation einzureichen, wobei der von der Landestierärztekammer vorgegebene Meldebogen verwendet werden soll. Von dieser Meldepflicht sind jedoch die detaillierten Angaben im Meldebogen nicht erfaßt. Solange keine Pflichten zur detaillierten Meldung in der Satzung der Landestierärztekammer bzw. dem HeilberG aufgenommen sind, können diese Angaben von den Kammermitgliedern nur mit deren Einwilligung erhoben und gespeichert werden, wobei die Betroffenen hierauf hinzuweisen sind. Die Landestierärztekammer hat zwischenzeitlich im Meldebogen diejenigen Angaben, die von den Mitgliedern freiwillig erhoben werden, als solche gekennzeichnet und eine entsprechende Einwilligungserklärung am Ende des Formulars aufgenommen. Einem der nächsten Rundbriefe soll eine Erklärung beigelegt werden, mit der die Kammermitglieder ihre nachträgliche Einwilligung zur Erhebung und weiteren Verarbeitung der im Meldebogen erhobenen Daten erteilen können. Darin werden sie auf den Zweck der Erhebung und Speicherung sowie auf die Freiwilligkeit und die Möglichkeit des jederzeitigen Widerrufs hingewiesen. Gleichzeitig beabsichtigt die Kammer sich darum zu bemühen, in einer Novellierung des HeilberG sowie der Satzung auf eine normenklare Konkretisierung derjenigen Daten zu drängen, zu deren Angabe die Kammermitglieder verpflichtet sind.

11.17 Automatisierte Datenverarbeitung bei der AOK

Im Berichtszeitraum habe ich die automatisierte Datenverarbeitung bei der AOK-Thüringen überprüft. Die Datenverarbeitung erfolgt dergestalt, daß die jeweiligen Geschäftsstellen mit einem zentralen Rechenzentrum über Datenleitungen verbunden sind. Im Rechenzentrum habe ich eine datenschutzrechtliche Kontrolle durchgeführt, um mich über die technischen und organisatorischen Maßnahmen zum Schutz der Sozialdaten zu informieren. Dabei habe ich entsprechend der Sensibilität der verarbeiteten Daten insgesamt ausreichende technische und organisatorische Schutzmaßnahmen vorgefunden. Ich konnte darüber hinaus den einen oder anderen Hinweis zur Verbesserung der Schutzmaßnahmen geben, was zwischenzeitlich auch umgesetzt wurde. So fehlte zum Zeitpunkt der Kontrolle z. B. ein Konzept über Maßnahmen im Katastrophenfall, d. h. eine Möglichkeit im Falle eines Brandes oder des sonstigen Ausfalls des zentralen Rechners innerhalb kürzester Zeit mit den aufbewahrten Sicherungskopien einen Notbetrieb zu gewährleisten. Dies wurde ebenfalls umgesetzt.

Zum Zeitpunkt der Kontrolle war ein privatisierter Rechenbetrieb mit der Datenverarbeitung beauftragt. Nach § 80 Abs. 5 SGB X ist das dann mög-

lich, wenn beim Auftraggeber ansonsten Störungen im Betriebsablauf auftreten oder die Aufgaben beim Auftragnehmer erheblich kostengünstiger besorgt werden können. Nach dem Inkrafttreten des Zweiten SGB-Änderungsgesetzes wurde als zusätzliche Voraussetzung in § 80 Abs. 5 SGB X festgelegt, daß nicht der gesamte Datenbestand des Auftraggebers beim Auftragnehmer gespeichert werden darf. Zwischen der AOK, dem TMSG und dem TLfD haben Gespräche zu den Möglichkeiten der Umsetzung dieser zusätzlichen Voraussetzung stattgefunden. Im Ergebnis wurde zwischenzeitlich das Rechenzentrum in die Organisation der AOK-Thüringen eingegliedert, so daß die Vorschriften der Auftragsdatenverarbeitung nicht mehr zur Anwendung kommen.

11.18 Automatisierte Abrechnung durch die Krankenkassen

Im Berichtszeitraum wurden zahlreiche datenschutzrechtliche Fragen im Zusammenhang mit der im Gesundheitsreformgesetz und Gesundheitsstrukturgesetz festgelegten automatisierten Abrechnung der gesetzlichen Krankenkassen mit den Leistungserbringern erörtert. In § 295 SGB V werden die Kassenzahnärzte und Kassenärzte verpflichtet, die Abrechnungsunterlagen maschinenlesbar an ihre Kassenärztliche bzw. Kassenzahnärztliche Vereinigung zu übermitteln, die diese ebenfalls maschinenlesbar den Krankenkassen zu Abrechnungszwecken zu übermitteln haben. Entsprechende Pflichten zur maschinenlesbaren Übermittlung von Abrechnungsdaten an die Krankenkassen treffen nach § 300 SGB V die Apotheken, § 301 SGB V die Krankenhäuser und nach § 302 SGB V die sonstigen Leistungserbringer (z. B. Optiker, Rettungsdienste etc.). Die gesetzlichen Vorschriften sehen jeweils vor, daß die Einzelheiten zum Datenträgeraustausch zwischen den Spitzenverbänden der Kassen und der Leistungserbringer einvernehmlich durch Vereinbarungen bzw. gemeinsam erstellte Richtlinien geregelt werden. Diese Vereinbarungen wurden zwischenzeitlich alle getroffen bzw. ersatzweise durch das Bundesschiedsamt festgelegt. Bis Ende 1997 war der automatisierte Datenträgeraustausch größtenteils noch nicht angelaufen, was u. a. mit technischen Schwierigkeiten begründet wird. Nach dessen Einführung werde ich mich über die Einhaltung der hierzu geltenden datenschutzrechtlichen Vorschriften informieren.

11.18.1 Datenträgeraustausch zwischen Krankenkassen und Zahnärzten

Der Gesetzgeber hat in § 295 Abs. 2 SGB V festgelegt, daß die Kassenärztlichen Vereinigungen den Krankenkassen die für die Abrechnung erforderlichen Angaben fallbezogen nicht jedoch versichertenbezogen auf maschinell verwertbaren Datenträgern übermitteln sollen. Damit wurde der Tatsache Rechnung getragen, daß es sich bei den Arztabrechnungen um einen sehr sensiblen Datenbestand handelt, der beim Normalfall einer Abrechnung nicht beliebig und systematisch durch die Krankenkassen ausgewertet werden soll. Die Einzelheiten sollten nach § 275 Abs. 3 SGB V von den Spitzenverbänden der Krankenkassen und den Kassenärztlichen Bundesvereinigungen in einer Vereinbarung geregelt werden. Zwischen der Kassenzahnärztlichen Bundesvereinigung und den Spitzenverbänden der Krankenkassen kam keine einvernehmliche Vereinbarung zustande. Daraufhin wurde vom zuständigen Bundesschiedsamt eine Vereinbarung durch Schiedsspruch festgelegt. Dieser Schiedsspruch berücksichtigte jedoch nicht in ausreichendem Maße die Vorgaben des § 295 Abs. 2 SGB V. Die Identität des einzelnen Versicherten war den Abrechnungsdaten mit relativ geringem Aufwand aus einem Vergleich der Leistungs- mit den Versichertendatensätzen zu entnehmen, weil beide Datensätze identische Angaben enthalten. Das hätte eine versichertenbezogene Abrechnung bedeutet, was aber nach § 295 Abs. 2 SGB V gerade unzulässig ist. Nachdem sich die Datenschutzbeauftragten des Bundes und der Länder für eine Reduzierung der zu übermittelnden Angaben sowohl im

Versichertendatensatz wie auch im fallbezogenen Leistungsdatensatz ausgesprochen haben, haben die gesetzlichen Krankenkassen dies in entsprechenden Protokollnotizen umgesetzt und so die Möglichkeit der Zusammenführung beider Datensätze erheblich verringert. Lediglich der Verband der Angestelltenkrankenkassen verhielt sich zunächst abwartend. Nach einer entsprechenden Aufforderung durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Anlage 6) hat auch dieser die Vereinbarung unterzeichnet.

Aufgrund der im Zusammenhang mit der Datenträgeraustauschvereinbarung zwischen Kassen und Kassenzahnärztlicher Bundesvereinigung erörterten Probleme haben auch Gespräche auf Bundesebene zwischen den Datenschutzbeauftragten einerseits und Kassen und Kassenärztlicher Bundesvereinigung andererseits begonnen, um die Datenträgeraustauschvereinbarung im Arztbereich in entsprechender Weise zu verändern. Die Gespräche dazu sind noch nicht abgeschlossen.

11.18.2 ICD-10-Code zur Abrechnung ungeeignet

Sowohl bei der Abrechnung zwischen den Krankenkassen und den Ärzten nach § 295 SGB V wie auch bei der Abrechnung zwischen den Krankenkassen und den Krankenhäusern nach § 301 SGB V ist vorgesehen, daß den Krankenkassen die Diagnosen nach dem sogenannte ICD-10-Code mitgeteilt werden. Dabei handelt es sich nicht um eine Verschlüsselung, die dem Leser die Kenntnisnahme der Diagnose unmöglich macht, weil die Krankheiten, die sich hinter den einzelnen Diagnoseschlüsseln verbergen, jedermann über entsprechende Verzeichnisse zugänglich sind. Zweck der Regelung sollte vielmehr sein, das Abrechnungsgeschehen durch vereinheitlichte Merkmale transparent aber auch auswertbar zu machen. Dabei hat sich bei der praktischen Umsetzung gezeigt, daß der ICD-10-Code, der ursprünglich von der Weltgesundheitsorganisation zu statistischen Zwecken entwickelt wurde, für Abrechnungszwecke in seiner bestehenden Form ungeeignet ist. Hauptkritikpunkte aus datenschutzrechtlicher Sicht waren, daß für bestimmte, häufig vorkommende Diagnosen teilweise zu wenig Aufschlüsselungen existierten und andererseits seltene, beispielsweise nur in tropischen Gegenden vorkommende Krankheiten (z. B. W 58 Krokodilbiß) sehr detailliert dargestellt werden. Vielfach enthielten die Schlüssel zudem keine Diagnosen im engeren Sinne, sondern Rückschlüsse auf bestimmte Verhaltens- und Lebensweisen als Ursache von Krankheiten (z. B. W 39 - Verletzung beim Abrennen von Feuerwerkskörpern oder V 86 - Verletzung bei Benutzung eines geländegängigen Spezialfahrzeugs). Durch die bindende Verpflichtung der Benutzung dieses Diagnoseschlüssels bestand die Gefahr, daß ein verfälschtes Bild vom Patienten gezeichnet wird bzw. über die Diagnose hinaus nicht erforderliche Angaben über den Patienten gespeichert werden. Aufgrund der hierzu geführten öffentlichen Diskussion haben die Kassenärztliche Bundesvereinigung sowie die Spitzenverbände der Krankenkassen und die Deutsche Krankenhausgesellschaft vereinbart, die Pflicht zur Verwendung des ICD-10-Codes für zwei Jahre auszusetzen und den Katalog umfassend zu überarbeiten. Dies ist noch nicht abgeschlossen.

11.18.3 Technisch-organisatorische Anforderungen an die Datenübermittlung

Da die Abrechnungsunterlagen zukünftig von den Leistungserbringern den Krankenkassen aufgrund der Vereinbarungen nach den §§ 295 Abs. 3, 300 Abs. 3, 301 Abs. 3 und 302 Abs. 2 SGB V in maschinenlesbarer Form zur Verfügung gestellt werden sollen, haben sich die Krankenkassen entschlossen, für den Transport dieser dann in elektronischer Form vorliegenden Abrechnungsunterlagen sich u. a. der bestehenden Telekommunikationsinfra-

struktur zu bedienen. Da sich jeder Versicherte aufgrund der freien Arztwahl grundsätzlich im gesamten Bundesgebiet ärztlich behandeln lassen kann, ist hierbei zu berücksichtigen, daß die gesetzlichen Krankenkassen mit allen Abrechnungsstellen der Leistungserbringer kommunizieren können müßten. Zu diesem Zweck sollen sogenannte Datenannahme- und -verteilstellen eingerichtet werden, die die Datensätze nach den jeweiligen Datenträgeraustauschvereinbarungen an die zuständige Krankenkasse weiterleiten. Diese Funktion der Datenannahme und -verteilstellen soll in Thüringen für die AOK Thüringen deren Rechenzentrum übernehmen. Von anderen Krankenkassen war geplant, mit dieser Aufgabe ein Privatunternehmen zu beauftragen. Angesichts der Sensibilität und dem großen Umfang der zu übermittelnden Daten sind bei der Übermittlung besondere Anforderungen an die Datensicherheit nach § 78a SGB X zu stellen. Sofern die Daten über öffentliche Leitungen übertragen werden, sind diese mit einem geeigneten kryptographischen Verfahren zu verschlüsseln (vgl. hierzu Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09. Mai 1996; Anlage 4). Hierüber habe ich die meiner Kontrolle unterliegenden Krankenkassen hingewiesen. Die AOK Thüringen beabsichtigt bei Einführung des automatisierten Abrechnungsverfahrens die Daten kryptographisch zu verschlüsseln sowie mit einer digitalen Signatur versehen, so daß der Absender eindeutig identifiziert und die Integrität der übermittelten Daten festgestellt werden kann.

11.18.4 Löschung der Abrechnungsdaten

Mit der Einführung des automatisierten Abrechnungsverfahrens wurden auch die gesetzlichen Aufbewahrungsfristen dieser Daten in § 304 SGB V neu geregelt. Danach sind die Abrechnungsdaten spätestens nach zwei Jahren zu löschen, wobei die Frist mit dem Ende des Geschäftsjahres beginnt, in dem Leistungen gewährt oder abgerechnet wurden. Auf Anfrage bei der Kassenärztlichen Vereinigung Thüringen (KVT) nach der Einhaltung dieser Fristen wurde mitgeteilt, daß in einer Vielzahl von Fällen diese Zweijahresfrist überschritten wurde. Dies betreffe insbesondere die Fälle, die im Rahmen von Wirtschaftlichkeitsprüfungen als Vergleichsfälle zu noch bei den Sozialgerichten anhängigen Streitfällen benötigt würden. Ich habe daraufhin gegenüber der KVT klargestellt, daß die gerichtliche Überprüfung einzelner Abrechnungsfälle nicht dazu führen kann, daß der gesamte Abrechnungsdatenbestand bis zum rechtskräftigem Abschluß aller Verfahren entgegen den kurzen Löschungsfristen von § 304 SGB V aufbewahrt wird. Sofern im Rahmen der Wirtschaftlichkeitsprüfung nach § 106 SGB V Vergleichsgruppen gebildet werden müssen, sollte geprüft werden, ob eine Nutzung anonymisierter Daten ausreichend ist. Die KVT hat mir mitgeteilt, daß nur jeweils diejenigen versichertenbezogenen Daten herangezogen werden, welche zur Durchführung von Verfahren der Wirtschaftlichkeitsprüfung benötigt werden. Dabei sind diese Daten nur nach Mitgliedern, Familienversicherten und Rentnern aufgeschlüsselt. Damit soll eine ausreichende Anonymisierung erreicht sein.

11.19 Falsch verstandene Auftragsdatenverarbeitung durch die AOK

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, daß Ende 1994 durch die AOK Thüringen Adreßdaten einer größeren Anzahl von Versicherten an ein Privatunternehmen übermittelt worden sein sollen, ohne daß es hierfür eine Rechtsgrundlage gibt. Meine Überprüfung der Angelegenheit bei der AOK Thüringen ergab, daß zum Jahresende 1994 ein AOK-interner Club für „Junge Leute“ aufgelöst wurde. Zweck dieses Clubs war es u. a. Gutscheine für Präventionsangebote nach § 20 SGB V auszugeben. Zum Zeitpunkt der Auflösung des Clubs existierte auf Bundesebene ein Privatun-

ternehmen, das ähnliche Angebote für AOK-Mitglieder bereithielt. Die AOK Thüringen beabsichtigte, den Mitgliedern des bisherigen AOK-Clubs die Möglichkeit aufzuzeigen, dem neuen Club beizutreten. Allerdings hat sie aus Kostengründen nicht ihre Clubmitglieder selbst angeschrieben und auf die Möglichkeit einer Mitgliedschaft beim neuen Club hingewiesen. Vielmehr beauftragte die AOK das Unternehmen, das den „Nachfolgeclub“ betrieb mit der Information der Clubmitglieder über diese Möglichkeit. Die AOK ging dabei davon aus, daß es sich hierbei um eine Auftragsdatenverarbeitung handelt. Solche Datenverarbeitungen im Auftrag sind nach dem Sozialgesetzbuch unter der Voraussetzung zulässig, daß ohne einen solchen Auftrag bei der AOK Störungen im Betriebsablauf auftreten können oder die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden. Letzteres mag zwar durchaus der Fall gewesen sein, doch lagen bereits die Grundvoraussetzungen für eine Auftragsdatenverarbeitung nicht vor. Eine solche kommt nur dann in Betracht, wenn es sich um eine technische Abwicklung von Datenverarbeitungsvorgängen handelt, ohne daß dem Auftragnehmer eine eigene Aufgabe mit Entscheidungsbefugnissen übertragen wird. Nur in diesem Fall wird vom Gesetz der Auftragnehmer nicht als Dritter und damit die Weitergabe der Daten nicht als Übermittlung angesehen. Im konkreten Fall enthielt die Vereinbarung außer dem allgemeinen Hinweis, daß Adreßdaten verarbeitet werden sollen, keinerlei Ausführungen zum Zweck und Gegenstand des Auftragsverhältnisses. Eine diesbezügliche Vereinbarung konnte von der AOK Thüringen nicht vorgelegt werden. Es war daher davon auszugehen, daß die Adreßdaten dem Privatunternehmen ohne die Auferlegung einer Zweckbindung, beispielsweise zur einmaligen Information über die Möglichkeit zum Beitritt in den neu gegründeten Club, übermittelt wurden. Schriftliche Weisungen der AOK zur Abwicklung des Auftrags konnten ebenfalls nicht vorgelegt werden, so daß auch insoweit davon ausgegangen werden mußte, daß solche Weisungen überhaupt nicht ergangen sind und die Adreßdaten vom neuen Club für eigene Zwecke genutzt oder weiterübermittelt werden konnten. Ich mußte daher feststellen, daß die Sozialdaten durch die AOK ohne eine Rechtsgrundlage an ein Privatunternehmen übermittelt wurden. Diesen Verstoß gegen die datenschutzrechtlichen Vorschriften des Sozialgesetzbuches habe ich formell beanstandet und die AOK aufgefordert, zukünftig die Beachtung datenschutzrechtlicher Vorschriften in diesem Bereich sicherzustellen. Die AOK teilte mit, daß hier die Belange des Datenschutzes nicht im ausreichendem Maße berücksichtigt wurden und daher die Mitarbeiter nochmals über die Einhaltung der Sozialdatenschutzvorschriften aufgeklärt worden sind.

11.20 Zweckfremde Nutzung von Sozialdaten?

Im Spätsommer 1996 war Presseberichten zu entnehmen, daß Mitarbeiter der AOK Thüringen solchen Taxiunternehmern, die ihre Mitgliedschaft bei der AOK Thüringen aufkündigten mit einem Ausschluß aus der Teilnahme an der Versorgung mit Krankentransportleistungen nach § 133 SGB V gedroht haben sollen. Diese Vermutungen legten den Schluß nahe, daß die AOK Thüringen Sozialdaten der bei ihr versicherten Taxiunternehmer zweckwidrig genutzt haben könnte. Eine Nachfrage bei der AOK Thüringen hat ergeben, daß regelmäßig bei Kündigungen Mitarbeiter der AOK versuchen, die Mitglieder zum Verbleib in der AOK zu bewegen. Diese Mitgliederhaltearbeit sei zufällig in zeitlichem Zusammenhang mit den Verhandlungen mit den Taxiunternehmern gefallen. Allerdings seien hierbei Mitarbeiter anderer Abteilungen der AOK tätig gewesen. Bei den Betroffenen hätte daher der Eindruck entstehen können, es bestehe ein kausaler Zusammenhang zwischen der weiteren Mitgliedschaft in der AOK und dem Abschluß von Verträgen zur Durchführung von Krankentransportleistungen. Das von mir in dieser Sache als oberste Rechtsaufsichtsbehörde einbezogene TMSG hat den Vorgang durch den Landesprüfdienst der Sozialversicherung geprüft und die

Angaben der AOK Thüringen bestätigt. Ich habe danach keinen Anlaß zu weiteren Maßnahmen gesehen, da eine zweckwidrige Nutzung von Versichertendaten der Taxiunternehmer nicht nachweisbar war.

Zum generellen Problem der Schaffung einer Befugnis für die Gesetzlichen Krankenkassen zur Erhebung und Speicherung personenbezogener Daten zu Werbezwecken habe ich bereits im 1. TB (11.2.1) ausgeführt, daß die Datenschutzbeauftragten des Bundes und der Länder gegenüber dem zuständigen Bundesministerium für Gesundheit die Forderung erhoben haben, § 284 Abs. 1 SGB V um eine Datenerhebungsbefugnis zur personenbezogenen Werbung zu ergänzen. Obwohl zwischenzeitlich einige Änderungen am SGB V erfolgt sind, ist eine solche Datenerhebungsbefugnis nicht aufgenommen worden. Damit wurden die Möglichkeiten nicht genutzt, die nach wie vor bestehende Unsicherheiten über die Zulässigkeit der Erhebung und Speicherung personenbezogener Daten zur Werbung neuer Versicherter zu beseitigen.

11.21 Zu großer Verteiler beim Notarzteinsatzprotokoll

Im Berichtszeitraum wurde ich darüber informiert, daß von Mitarbeitern einer Krankenkasse Durchschläge von Notarzteinsatzprotokollen im Zusammenhang mit der Abrechnung von Rettungsdiensteinsätzen verlangt werden, bei denen der Verunglückte noch an der Unfallstelle bzw. auf dem Transport in das Krankenhaus verstirbt. In diesem Fall erfolgt eine Einweisung in ein Krankenhaus und die damit verbundene Übergabe einer Durchschrift des Notarzteinsatzprotokolls an den behandelnden Arzt nicht. Neben dem Namen und den Adreßdaten des Betroffenen erfolgen auf dem Notarzteinsatzprotokoll Aufzeichnungen zu Erstbefund und zu Verletzungen. Als Begründung für diese Verfahrensweise hat die Krankenkasse auf Nachfrage mitgeteilt, daß eine Leistungspflicht der Krankenkasse für einen derartigen Einsatz nur dann besteht, wenn der Patient noch lebend an der Unfallstelle vom Notarzt angetroffen wird. Ansonsten handele es sich um einen Fehleinsatz, dessen Kosten nicht von der Krankenkasse erstattet werden. Weil es diesbezüglich in der Vergangenheit Schwierigkeiten gegeben habe, den genauen Todeszeitpunkt festzustellen, sollte die Vorlage der Kopie des Notarzteinsatzprotokolls zur Feststellung einer möglichen Leistungspflicht der Krankenkasse herangezogen werden. Da im Notarzteinsatzprotokoll Angaben enthaltenen sind, die der ärztlichen Schweigepflicht unterliegen und eine Rechtsgrundlage, die die Übermittlung an einen nicht-ärztlichen Mitarbeiter der Krankenkasse erlaubt, nicht besteht, ist diese Verfahrensweise unzulässig. Die Krankenkasse hat daraufhin auf die Anforderung derartiger Notarzteinsatzprotokolle verzichtet.

In diesem Zusammenhang teilte die Krankenkasse mit, daß derartige Notarzteinsatzprotokolle in nicht-anonymisierter Form bei der Deutschen Rettungsflugwacht (DRF) vorliegen und regelmäßig zu Abrechnungszwecken verwendet werden (1. TB, 11.7). Auch insoweit gibt es keine Rechtsgrundlage für eine Durchbrechung der ärztlichen Schweigepflicht. Insbesondere nach § 302 Abs. 2 SGB V und der hierzu erlassenen Richtlinie ist nur die Weitergabe der ärztlichen Verordnung einer Krankenbeförderung zulässig, nicht jedoch die Mitteilung von Diagnosen oder Gesundheitsdaten des Patienten an die Krankenkasse. Ich habe das TIM als Aufgabenträger der Luftrettung darauf hingewiesen, die Verfahrensweise bei der Luftrettung dahingehend umzustellen, daß der DRF als Leistungserbringer vom Notarzt lediglich ein anonymisierter Durchschlag des Notarzteinsatzprotokolls zu Qualitätssicherungszwecken übermittelt wird. Das TIM hat daraufhin umgehend mit der DRF vereinbart, daß neben der ärztlichen Verordnung überhaupt kein Durchschlag des Notarzteinsatzprotokolls mehr der DRF übergeben werden soll.

11.22 Prüfung einer Beratungsstelle des MDK

Der Medizinische Dienst der Krankenversicherung (MDK) hat nach den §§ 275 ff. SGB V die Aufgabe, für die gesetzlichen Krankenkassen gutachterliche Stellungnahmen in bestimmten Einzelfällen durchzuführen. Da der MDK im Regelfall mit Daten umgeht, die der ärztlichen Schweigepflicht unterfallen, bedarf es beim Umgang mit diesen Daten besonderer Sorgfalt. Anläßlich einer Kontrolle in einer Beratungsstelle des MDK Thüringen habe ich die Praxis der Vorlage von ärztlichen Unterlagen und Auskünften durch die beauftragenden Kassen beim MDK überprüft. Danach wird nach Erteilung des Gutachtenauftrags der Leistungserbringer (Arzt oder Krankenhaus) von der Krankenkasse angeschrieben und die Beauftragung des MDK mitgeteilt. Gleichzeitig erfolgt die Aufforderung zur Übersendung der Unterlagen direkt an den MDK. Dies entspricht der Regelung des § 276 Abs. 2 SGB V, wonach die Leistungserbringer verpflichtet sind, Sozialdaten im Rahmen eines Gutachtenauftrags unmittelbar, d.h. ohne Kenntnisnahme durch die Krankenkasse zu übermitteln. Daß die Krankenkasse nach § 276 Abs. 1 SGB V dem MDK alle zur Begutachtung erforderlichen Unterlagen vorzulegen hat, steht der Verpflichtung des Leistungserbringers zur unmittelbaren Übermittlung der Unterlagen an den MDK nicht entgegen. Sobald der Gutachtenauftrag erteilt ist, gilt nämlich § 276 Abs. 2 SGB V, d.h. die Pflicht der Krankenkasse zur Vorlage der Unterlagen bezieht sich nur auf die zum Zeitpunkt der Auftragserteilung bei der Kasse vorhandenen Unterlagen. Die Krankenkasse darf jedoch nicht nach Auftragserteilung die Vorlage weiterer medizinischer Unterlagen vom Leistungserbringer zur Weiterleitung an den MDK verlangen, wenn sie Kenntnis vom Inhalt nehmen kann. Hierfür besteht auch keinerlei Erforderlichkeit. Wie bereits im 1. TB (11.2.4) angekündigt, habe ich auch den Umfang der Datenerhebungen bei gutachtlichen Stellungnahmen nach § 275 SGB V sowie den Umfang der Ergebnisübermittlung an die auftraggebende Krankenkasse überprüft. So habe ich beispielsweise im Rahmen eines Arbeitsunfähigkeitsgutachtens festgestellt, daß bei der Berufsanamnese die Tatsache des Schulabschlusses nach der 8. Klasse erfaßt war. Im weiteren Gutachten wurde jedoch auf diese Feststellung in keiner Weise mehr eingegangen. Vom MDK wurde erklärt, daß dieses Datum zu einer üblichen Berufsanamnese gehöre. Das vollständige Gutachten ist in diesem Fall an die Krankenkasse auf der Grundlage nach § 277 SGB V übermittelt worden. Allerdings ist in § 277 SGB V lediglich bestimmt, daß der MDK der Krankenkasse das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund mitzuteilen hat. Ob im o. g. Beispiel der Schulabschluß im Rahmen der Berufsanamnese aus medizinischer Sicht tatsächlich eine Auswirkung auf die medizinische Begutachtung (es ging um ein Magengeschwür und eine Bronchitis) haben kann, ist aus rein datenschutzrechtlicher Sicht möglicherweise schwer zu beurteilen. Gerade deshalb wäre zu überlegen, ob bestimmte Angaben, die für den Gesamteindruck des Arztes erforderlich sind, aber zu einer Ergebnismitteilung an die Kasse nicht gebraucht werden, lediglich beim MDK gespeichert werden. Nach der bisherigen Verfahrensweise wäre das jedoch nur mit einem erheblichen manuellen Aufwand möglich. Das vom Medizinischen Dienst der Spitzenverbände (MDS) zur Verfügung gestellte Datenverarbeitungssystem „ISmed“ läßt bisher nur den vollständigen Ausdruck des Gutachtens zu. Im Rahmen einer Überarbeitung dieses Systems wurde dem MDS von Datenschutzseite nahegelegt, eine solche differenzierte Gutachtenspeicherung bzw. -ausgabe zu integrieren. Den MDK Thüringen habe ich aufgefordert, sich im Rahmen von innerbetrieblichen datenschutzrechtlichen Schulungen die ärztlichen Gutachter regelmäßig mit dem Abgrenzungsproblem zu befassen, welche Angaben über den Befund noch erforderlich im Sinne von § 277 SGB V sind und welche Angaben hiervon nicht mehr gedeckt werden. Damit soll sichergestellt werden, daß keine unzulässige Datenübermittlung an die Kassen erfolgt.

11.23 Einsicht des MDK in Krankenhausakten

Im Berichtszeitraum wurde ich mit der Frage beschäftigt, unter welchen Voraussetzungen die Krankenhäuser befugt bzw. verpflichtet sind, den Krankenkassen bzw. dem MDK Krankenunterlagen zu Prüfzwecken zur Verfügung zu stellen.

Abbau der Fehlbelegung

Am 01.01.1995 ist § 17a Krankenhausfinanzierungsgesetz (KHG) in Kraft getreten. Darin wird bestimmt, daß die Krankenkassen insbesondere durch gezielte Einschaltung des MDK daraufhin hinwirken, daß Fehlbelegungen (Patienten liegen unnötig oder unnötig lange im Krankenhaus) vermieden und bestehende Fehlbelegungen zügig abgebaut werden. Zu diesem Zweck darf der MDK Einsicht in die Krankenunterlagen nehmen. Nicht von § 17a KHG gedeckt sind sogenannte „Stichtagserhebungen", bei denen an einem bestimmten Tag durch Mitarbeiter des MDK landesweit in allen Krankenhäusern die Krankenakten von sämtlichen Patienten geprüft werden, die an einem bestimmten Tag stationär behandelt worden waren. Das KHG enthält außer der Verpflichtung zur gezielten Einschaltung des MDK keine näheren Bestimmungen, unter welchen Bedingungen der MDK Krankenunterlagen einsehen bzw. anfordern kann. Solche Regelungen sind in den §§ 275 ff. SGB V enthalten. Bereits aus der Formulierung „gezielte Einschaltung des MDK" in § 17a Abs. 2 KHG ist zu entnehmen, daß keine flächendeckende allgemeine Prüfung von Krankenunterlagen durch den MDK möglich ist, sondern in Anlehnung an die Regelungen der §§ 275, 276 SGB V und unter Beachtung des Verhältnismäßigkeitsgrundsatzes nur eine fallbezogene Prüfung in begründeten Einzelfällen vorgenommen werden darf.

Die Landeskrankenhausgesellschaft übergab mir Mitte 1997 den Entwurf einer Vereinbarung zwischen den Verbänden der Krankenkassen und der Landeskrankenhausgesellschaft nach § 112 Abs. 1 SGB V zur Prüfung. Darin sollte ein Verfahren zur Konkretisierung der gezielten Einschaltung des MDK nach § 17a KHG festgelegt werden. Da es sich bei den Krankenunterlagen um solche Daten handelt, die der ärztlichen Schweigepflicht (§ 2 Berufsordnung der Landesärztekammer Thüringen/§ 203 StGB) unterliegen, bedarf die Einsichtnahme und Weitergabe dieser Daten einer gesetzlichen Grundlage. Der Landeskrankenhausgesellschaft habe ich mitgeteilt, daß eine Vereinbarung nach § 112 SGB V keinen Gesetzesrang hat und damit keine Befugnis zur Offenbarung von Patientendaten an den MDK darstellen kann. Maßstab hierfür können die §§ 275 und 276 SGB V sein. Allerdings ist eine solche Vereinbarung geeignet, Kriterien aufzustellen, bei welchen Konstellationen im Einzelfall anlaßbezogen Einsicht in Krankenunterlagen durch den MDK genommen werden soll. Sofern die Prüfergebnisse im Rahmen der Pflegesatzverhandlungen für zukünftige Zeiträume von Bedeutung sind, dürfen diese Angaben ausschließlich in anonymisierter Form verwendet werden. Die Landeskrankenhausgesellschaft hat meine Anregungen weitgehend übernommen. Allerdings bestand von den Kassen zunächst keine Bereitschaft, eine derartige Vereinbarung abzuschließen. Vielmehr wurde der MDK von den Kassen beauftragt, in einigen Thüringer Krankenhäusern Fehlbelegungsprüfungen durchzuführen. Die Prüfungen wurden zwischenzeitlich ausgesetzt. Zwischen den Kassen und der Landeskrankenhausgesellschaft wird derzeit über den Abschluß einer Rahmenempfehlung verhandelt, die das Verfahren zur Prüfung der Erforderlichkeit von stationärer Behandlung in Thüringer Krankenhäusern festlegen soll.

Überprüfung im Rahmen der Abrechnung

Im Rahmen der Abrechnung der Krankenhausleistungen mit den Krankenkassen ist derzeit häufig streitig, ob die abgerechnete Leistung tatsächlich erforderlich war bzw. in der entsprechenden Form erbracht worden ist. In diesen Fällen beauftragen die Krankenkassen den MDK , eine gutachterliche Stellungnahme abzugeben. Die Kassen fordern das Krankenhaus auf, z. B. Operations- und Krankenhausentlassungsberichte in den jeweiligen Fällen dem MDK zur Begutachtung zu übersenden. Von einem Thüringer Krankenhaus wurde diese Praxis als nicht rechtmäßig angesehen. MDK und Krankenhaus haben mich um eine Stellungnahme zur Auslegung des § 275 Abs. 1 Satz 1 Nr. 1 SGB V gebeten. In dieser Vorschrift wird bestimmt, daß die Krankenkassen verpflichtet sind, „wenn es nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist, bei Erbringung von Leistungen, insbesondere zur Prüfung von Voraussetzung, Art und Umfang der Leistung eine gutachtliche Stellungnahme des Medizinischen Dienstes der Krankenversicherung“ einzuholen. Ist der MDK von der Krankenkasse beauftragt, so sind die Leistungserbringer und damit auch die Krankenhäuser nach § 276 Abs. 2 Satz 1 SGB V verpflichtet, „Sozialdaten“ auf Anforderung des Medizinischen Dienstes unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist. Das Krankenhaus argumentierte, daß die Voraussetzungen des § 275 Abs. 1 Satz 1 Nr. 1 SGB V „bei Erbringung von Leistungen“ keinesfalls eine Rechnungsprüfung nach Abschluß der Behandlung beinhalten könne. Damit entfalle die Rechtsgrundlage für die Übermittlung von Patientendaten und einer Übermittlung der Unterlagen stehe die ärztliche Schweigepflicht entgegen. Dies hat in dem betreffenden Fall dazu geführt, daß aufgrund der Verweigerung der geforderten Unterlagen die Krankenkasse ihrerseits die Zahlung verweigert hat und die Angelegenheit jetzt dem zuständigen Sozialgericht zur Entscheidung vorliegt. Aus dem Wortlaut des § 275 Abs. 1 Satz 1 Nr. 1 SGB V ist jedoch nicht abzuleiten, daß eine Beauftragung des MDK nur bis zum Abschluß der Behandlung im Krankenhaus möglich ist. Andernfalls hätte dies im Gesetz einschränkend formuliert werden müssen. Aber auch aus dem Sinn und Zweck der Vorschrift ergibt sich kein anderes Ergebnis. Die Krankenkassen sollen durch den medizinischen Sachverstand des MDK in die Lage versetzt werden, die Erforderlichkeit und den Umfang von im Krankenhaus erbrachten medizinischen Leistungen beurteilen zu können. Häufig ergeben sich für die Krankenkassen erst im Rahmen der Abrechnung Anhaltspunkte dafür, daß eine medizinische Leistung nicht oder nicht im erbrachten Umfang erforderlich war. Würde man eine Überprüfung durch den MDK nur vor Abschluß der Krankenhausbehandlung zulassen, so würde diese Kontrollmöglichkeit in vielen Fällen leerlaufen. Die Formulierung „bei Erbringung“ umfaßt daher auch noch einen Zeitraum nach Abschluß der Behandlung in dem die Abrechnung stattfindet. Nicht mehr vom Wortlaut erfaßt sind jedoch nachträgliche Rechnungsprüfungen, wenn eine Abrechnung bereits erfolgt ist (z. B. um Material für Budgetverhandlungen zu sammeln).

Wie bereits erwähnt, bedarf es zur Einschaltung des MDK konkreter Anhaltspunkte durch die Krankenkassen im jeweiligen Einzelfall. Liegen die Voraussetzungen vor, so ist das Krankenhaus als Leistungserbringer nach § 276 Abs. 2 Satz 1 SGB V verpflichtet, die Krankenunterlagen im erforderlichen Umfang unmittelbar an den MDK zu übermitteln. Obwohl in § 276 Abs. 2 Satz 1 SGB V geregelt ist, daß die Leistungserbringer „Sozialdaten“ an den MDK übermitteln, sind hier Patientendaten gemeint, da erst mit der Erhebung der Daten durch den MDK diesen der Status von Sozialdaten zufällt. Hier liegt ein redaktionelles Versehen des Gesetzgebers vor. § 276 SGB V setzt jedoch voraus, daß nur solche Unterlagen vom Krankenhaus an den MDK übermittelt werden dürfen und müssen, soweit dies für die gut-

achtliche Stellungnahme und Prüfung erforderlich ist. Daher sind im Anforderungsschreiben der Krankenkassen bzw. des MDK nähere Angaben über den Gegenstand und Umfang der Begutachtung zu machen, um den Leistungserbringer in die Lage zu versetzen, auch nur die erforderlichen Unterlagen zu übersenden. Diese Auffassung wurde auch vom TMSG geteilt, das ich in dieser Frage um eine Stellungnahme gebeten habe.

11.24 Gemeinsame Nutzung von Daten durch Krankenkasse und Pflegekasse

Durch das PflegeVG wurde bestimmt, daß bei jeder Krankenkasse eine Pflegekasse errichtet wird, die nach § 46 Abs. 2 SGB XI eine eigene rechtsfähige Körperschaft des öffentlichen Rechts mit Selbstverwaltung ist. Damit sind zwei rechtlich selbständige Institutionen errichtet worden, zwischen denen kein beliebiger Austausch der Sozialdaten erfolgen darf. Der Tatsache, daß für die Aufgabenerfüllung sowohl der Krankenkasse als auch der Pflegekasse in vielen Fällen dieselben Daten erforderlich sind, hat die Vorschrift des § 96 Abs. 1 SGB XI Rechnung getragen. Danach können die Spitzenverbände der Pflegekassen und der Krankenkassen gemeinsam und einheitlich festlegen, daß die verbundenen Pflege- und Krankenkassen bestimmte Daten gemeinsam verarbeiten und nutzen können. Die Festlegung dieses gemeinsamen Datenkatalogs soll unter Beteiligung des BfD und des Bundesministeriums für Arbeit und Sozialordnung erfolgen. Am Verfahren zur Erarbeitung des Katalogs wurden vom BfD die Landesbeauftragten für den Datenschutz (LfD) einbezogen. Als schwierig hat sich dabei erwiesen, daß anstatt der eigentlich wünschenswerten abschließenden Festlegung der Datenarten, die sowohl die Krankenkasse wie auch die bei ihr errichtete Pflegekasse für ihre Aufgaben benötigen, wegen der vielfältigen Fallgestaltungen und der bundesweit unterschiedlichen Datenverarbeitungsverfahren oft nur zusammengefaßte Oberbegriffe (wie z. B. „Beitragsdaten“) allgemeingültig festgelegt werden können. Es wurde daher eine erste Version für eine Übergangszeit bis Ende 1998 festgelegt. Eine zumindest teilweise Präzisierung der Datenarten sollte nach Auffassung der Datenschutzbeauftragten in einer überarbeiteten Fassung angestrebt werden. Die Tatsache der Aufnahme der Datenarten in den Katalog führt aber nicht automatisch dazu, daß Einzeldaten von der jeweils anderen Kasse genutzt werden dürfen, ohne daß eine Erforderlichkeit zur Aufgabenerfüllung besteht. Sofern die Pflegekasse beispielsweise auf die Grunddaten eines 20-jährigen im Rahmen der gemeinsamen Verarbeitung und Nutzung zugreifen könnte, darf sie es dennoch erst dann, wenn es zum Vollzug des Pflegeversicherungsgesetzes im konkreten Fall (z. B. Antrag auf Pflegeleistungen 50 Jahre später) erforderlich ist. Unabhängig von dem nach § 96 Abs. 1 SGB XI festzulegenden Datenkatalog gilt nach § 96 Abs. 2 SGB XI bei der Übermittlung von Daten, die den Krankenkassen oder Pflegekassen von einem Arzt oder sonstigen Schweigeverpflichteten zugänglich gemacht worden sind, daß solche der ärztlichen Schweigepflicht unterliegenden Daten nur unter den Voraussetzungen des § 76 SGB X ausgetauscht werden dürfen. Sofern demnach keine ausdrücklich gesetzliche Erlaubnis hierfür besteht, bedarf es zu diesem Datenaustausch der ausdrücklichen Einwilligung des Versicherten. Bevor der Datenkatalog festgelegt worden war, erhielt ich von einem Pflegedienst eine Anfrage, aufgrund welcher Rechtsgrundlagen eine Datenübermittlung zwischen Krankenkasse und Pflegekasse zulässig sei. Dem Pflegedienst gegenüber habe ich die Auffassung vertreten, daß aufgrund von § 93 SGB XI die Datenschutzvorschriften der §§ 67 SGB X gelten. Nach § 69 Abs. 1 Nr. 1 SGB X hielt ich einen Datenaustausch zwischen der Krankenkasse und der Pflegekasse für zulässig, soweit dies für die Erfüllung einer gesetzlichen Aufgabe des jeweils anderen Sozialleistungsträgers erforderlich ist.

11.25 Kontrolle eines Versorgungsamtes

In der Versorgungsverwaltung des Landes werden eine Vielzahl von Sozial- und Gesundheitsdaten von Versorgungsempfängern und Schwerbehinderten erhoben und verarbeitet. Daher führte ich eine Kontrolle durch, um mir ein Bild darüber zu verschaffen, wie dort mit diesen sensiblen Angaben umgegangen wird. Obwohl keine datenschutzrechtlichen Verstöße festgestellt wurden, die Anlaß für eine Beanstandung gegeben hätten, wurden eine Reihe von Forderungen zur Verbesserung der Datensicherheit erhoben, die alle nach der Prüfung durch die Versorgungsverwaltung umgesetzt wurden. Hierzu zählen insbesondere die Verbesserung der EDV-Sicherheit durch Anbringen von Diskettenschlössern an Einzel-PC sowie die Einschränkung der Zugangsberechtigung zu dem in einem besonders gesicherten Raum untergebrachten Zentralrechner. Da die Akten in den einzelnen Büros nicht in Schränke weggeschlossen werden, richtete sich mein Augenmerk darauf, den Zugang Dritter zu den Räumen und damit die Möglichkeit der Kenntnisnahme vom Inhalt der Unterlagen auszuschließen. In diesem Zusammenhang wurden bei der Ausgabe der Büroschlüssel durch den Pförtner an die Mitarbeiter Schlüsselkarten eingeführt, um auszuschließen, daß Unbefugte sich einen entsprechenden Schlüssel geben lassen. Außerdem wurde die Reinigung der Räume in die Arbeitszeit verlegt.

Bei der Durchsicht der verwendeten Antragsformulare fiel auf, daß diese in vielen Fällen noch nicht den geänderten sozialdatenschutzrechtlichen Vorschriften angepaßt waren. Insbesondere fehlten die Hinweise, aufgrund welcher Rechtsgrundlage und zu welchem konkreten Zweck die Datenerhebung erfolgt. Bei einem Großteil der im Versorgungsamt gestellten Anträge, wird vom Antragsteller die Einwilligung verlangt, daß das Versorgungsamt Auskünfte bei seinen behandelnden Ärzten einholt. Diese Schweigepflichtsentbindungserklärungen waren teilweise so abgefaßt, daß die Versorgungsverwaltung bei allen Ärzten anfragen konnte, die im Zusammenhang mit der beantragten Leistung den Antragsteller behandelt haben. Dem Antragsteller war es dabei nicht möglich, Einschränkungen bezüglich einzelner Ärzte oder Krankheiten vorzunehmen, um beispielsweise zu verhindern, daß dem Versorgungsamt Befunde über eine psychische Erkrankung mitgeteilt werden, die für die Anerkennung als Schwerbehinderten überhaupt nicht erforderlich sind (vgl. auch 11.26). Die Vordrucke wurden entsprechend meinen Hinweisen überarbeitet.

Im Rahmen der Kontrolle ist auch zutage getreten, daß keine klare Regelung der Zuständigkeitsverteilung zwischen dem Landesversorgungsamt und den drei Versorgungsämtern existiert. Dies hat auch Auswirkungen auf datenschutzrechtliche Sachverhalte. Nur eine für die Erledigung der Verwaltungsaufgabe zuständige Stelle darf die erforderlichen personenbezogenen Daten erheben. Hierbei bestehen insbesondere nach der am 01.07.1994 in Kraft getretenen Kreisgebietsreform hinsichtlich der örtlichen Zuständigkeit einige Unsicherheiten. Als Grundlage für die Arbeit des Landesversorgungsamtes sowie der Ämter für Soziales und Familie (Versorgungsämter) dient die Anordnung über die Errichtung, den Sitz und den Zuständigkeitsbereich des Landesamtes für Soziales und Familie (Landesversorgungsamt) sowie der Ämter für Soziales und Familie (Versorgungsämter) vom 13.05.1991 (GVBl. S. 102). Im dortigen § 4 ist bestimmt, daß die Aufgabenverteilung zwischen dem Landesamt für Soziales und Familie und den Ämtern für Soziales und Familie noch gesondert geregelt wird. Das ist aber nur durch einen vorläufigen Organisationsplan geschehen. Darin werden keinerlei Aussagen zur örtlichen Zuständigkeit gemacht. Auf Nachfrage hat das TMSG mitgeteilt, daß der Entwurf einer Thüringer Verordnung über die Zuständigkeiten der Versorgungsverwaltung und der Hauptfürsorgestelle gegenwärtig zwischen

den Ministerien abgestimmt wird. Da dies schon über ein Jahr zurückliegt, erwarte ich eine baldige Regelung der Zuständigkeiten.

Auch zum Schutz der Daten der Mitarbeiter waren einige Hinweise zu geben. So wurde beispielsweise in einem Arbeitsbereich festgestellt, daß zwar die Abrechnung für die geführten privaten Telefongespräche um die letzten drei Ziffern verkürzt aufgezeichnet und dem Mitarbeiter übergeben wurden. Allerdings wurde in dieser Organisationseinheit so verfahren, daß ein Mitarbeiter die Begleichung der Rechnung mit der Abrechnungsstelle für die Kollegen übernahm. Dieser gab sie jedoch dann nicht, wie zu vermuten wäre, den jeweiligen Mitarbeitern zurück, sondern heftete sie in einem allen Kollegen zugänglichen Ordner ab. So entstand eine umfangreiche Sammlung der Telefongespräche des jeweiligen Mitarbeiters, bei der zwar nicht erkennbar war, wen der Betreffende jeweils angerufen hat, aus dem jedoch ablesbar war, an welchen Tagen wie oft und wie lange der jeweilige Kollege telefoniert hatte. Man wußte offenbar nicht, was mit den Abrechnungsbelegen nach Zahlung des Betrages zu tun ist und heftete sie in ordentlicher Behördenmanier ab. Ich habe die Stelle aufgefordert, die Abrechnung den jeweiligen Mitarbeitern zurückzugeben oder falls diese sie nicht mehr benötigen, zu vernichten. Das Versorgungsamt hat daraufhin die Verfahrensweise entsprechend umgestellt.

11.26 Nachweis einer Schweigepflichtsentbindung durch die Versorgungsverwaltung

Von Thüringer Krankenhäusern wurde ich im Berichtszeitraum mit der Frage konfrontiert, ob bei der Anforderung von Patientenunterlagen durch die die Versorgungsverwaltung die vom Patienten abgegebene Schweigepflichtsentbindungserklärungen im Original bzw. in Kopie vorgelegt werden müssen. Bei den Vertretern der Krankenhäusern bestand Unsicherheit darüber, ob nicht ohne einen entsprechenden Nachweis die Gefahr besteht, daß eine Offenbarung von Gesundheitsdaten möglicherweise in unzulässigem Umfang erfolgt. Eine häufige Fallkonstellation ist der beim Versorgungsamt gestellte Antrag auf Anerkennung einer Schwerbehinderung. In derartigen Fällen stellt der Patient einen Antrag auf Gewährung einer Sozialleistung, für dessen Entscheidung es maßgeblich auf die Beurteilung medizinischer Sachverhalte ankommt. Mit der Antragstellung wird in aller Regel vom Betroffenen eine Einwilligungserklärung zur Beiziehung von über ihn bei Ärzten vorhandenen medizinischen Unterlagen verlangt, soweit es zur Bearbeitung des Antrags erforderlich ist. In diesem Zusammenhang ist festzuhalten, daß der Arzt letztlich entscheiden muß, ob eine Entbindung von der Schweigepflicht bezüglich einzelner zu übermittelnder Angaben vorliegt. Je konkreter die Anforderung erfolgt, desto einfacher dürfte es dem Arzt fallen, dem Ersuchen nachzukommen, wobei bei Vorliegen einer konkreten Anforderung im Regelfall auf die Versicherung des Versorgungsamts vertraut werden darf, eine entsprechende Schweigepflichtsentbindung liege vor.

Ausgangspunkt für die Zulässigkeit derartiger Datenübermittlungen von den Krankenhäusern an die Versorgungsverwaltung ist die durch § 203 StGB geschützte ärztliche Schweigepflicht. Eine Offenbarung ist außer in gesetzlich ausdrücklich geregelten Fällen nur dann zulässig, wenn der Betroffene wirksam hierin eingewilligt hat. Ob diese Voraussetzung erfüllt ist, hat grundsätzlich der um Auskunft gebetene Arzt zu prüfen. Zu differenzieren ist danach, ob die Schweigepflichtsentbindungserklärung hinreichend konkret erfolgt, um dem Arzt eine Einschätzung zu ermöglichen, welche Angaben gegenüber dem Versorgungsamt ohne Verletzung der Schweigepflicht gemacht werden dürfen. Andererseits ist danach zu fragen, in welcher Form der Nachweis der Entbindungserklärung zu erfolgen hat. Beide Aspekte stehen in einem direkten inneren Zusammenhang. Je konkreter die Entbindungserklä-

rung hinsichtlich bestimmter Erkrankungen und Behinderungen und die darauf bezugnehmende Anforderung von Auskünften ist, desto eher kann der Arzt beurteilen, ob die Übermittlung bestimmter Unterlagen von der Entbindungserklärung gedeckt ist. Damit fällt es ihm auch leichter, sich auf die Versicherung der öffentlichen Stelle zu verlassen, die entsprechende Entbindungserklärung liege tatsächlich vor. In dem Anforderungsschreiben sind deshalb so genau wie möglich diejenigen Angaben zu benennen, die für die Antragsbearbeitung erforderlich sind. Zwar ist für das Versorgungsamt vielfach aus den Angaben des Betroffenen im Antrag nicht erkennbar, über welche Unterlagen der jeweilige Arzt verfügt. Deshalb sollte dem Arzt beispielsweise durch die Angabe der dem Antrag zugrunde liegenden Behinderung die Beurteilung ermöglicht werden, ob einzelne seiner Unterlagen für die behördliche Entscheidung von Bedeutung sind. Sofern es sich um ein Massenverfahren handelt, sollte dem Anforderungsschreiben regelmäßig der Text der vorformulierten Schweigepflichtsentbindungserklärung, den der Betroffene unterschrieben hat, beigefügt werden. Da bei solchen Einwilligungserklärungen außerdem die Möglichkeit bestehen muß, die Schweigepflichtsentbindung nur auf bestimmte Erkrankungen bzw. auf einzelne Ärzte zu beschränken, ist auch diese Information für den mit dem Auskunftsersuchen konfrontierten Arzt zur Einschätzung seiner Befugnis von Bedeutung. Außerdem ist die Einwilligungserklärung so zu formulieren (z. B. durch Bezugnahme auf die im Antrag angegebenen Ärzte), daß klar erkennbar wird, bei welchen Ärzten durch das Versorgungsamt nachgefragt werden darf. Sofern von den so ermächtigten Ärzten auch dort vorliegende Befunde anderer Ärzte im erforderlichen Umfang übermittelt werden sollen, ist dies ebenfalls ausdrücklich in die Einwilligungserklärung aufzunehmen. Sind diese Anforderungen erfüllt, kann sich der Arzt im Regelfall auf die Versicherung durch das Versorgungsamt verlassen, ohne damit den Rahmen der durch die Einwilligungsklärung des Patienten geschaffenen Befugnis zur Offenbarung ärztlicher Daten zu überschreiten. Hat der Arzt jedoch aufgrund besonderer Anhaltspunkte begründete Zweifel, daß der Patient eine derartige Entbindungserklärung gegenüber dem Versorgungsamt erteilt hat bzw. hegt er Zweifel am Umfang der Entbindungserklärung, könnte im Einzelfall auch eine Kopie der unterschriebenen Entbindungserklärung verlangt werden. Als Absicherung der Ärzte wäre auch denkbar, daß im Rahmen einer weiteren Behandlung der Patient selbst befragt wird, ob er mit der Übersendung der entsprechenden Unterlagen an das Versorgungsamt einverstanden ist. Diese Fälle dürften jedoch die Ausnahme bilden, da außerhalb von besonderen Konstellationen sich der Arzt auf die Versicherung der öffentlichen Stelle verlassen darf. Eine gewisse Absicherung für den Arzt stellt auch der Umstand dar, daß Mitarbeiter der Versorgungsämter für den Fall, daß sie die Übermittlung von Krankenunterlagen durch den Arzt mit der unwahren Behauptung erschleichen, eine entsprechende Schweigepflichtsentbindung liege vor, nach § 85 Abs. 2 Nr. 1 SGB X mit einer Freiheitsstrafe von bis zu einem Jahr oder Geldstrafe bestraft werden können. Diese Auffassung habe ich dem TMSG sowie der Landeskrankenhausgesellschaft mitgeteilt.

11.27 Zuverlässigkeitsprüfung von Heimträgern und Heimleitern

Anfang 1997 ist das Zweite Gesetz zur Änderung des Heimgesetzes (HeimG) in Kraft getreten. Darin wurde die Anzeigepflicht zum Betreiben von Heimen, in denen alte Menschen sowie Pflegebedürftige oder behinderte Volljährige aufgenommen werden auch auf sogenannte Kurzzeitpflegeheime erstreckt. Aus diesem Anlaß hat die zuständige Versorgungsverwaltung neue Anzeigeformulare entwickelt. Darin wird eine Vielzahl von Angaben über die wirtschaftliche Situation des Heimträgers sowie über die Qualifikation und die Zuverlässigkeit des leitenden Personals abgefragt. Ein Wohlfahrtsverband hat mir diese Anzeigeformulare vorgelegt und dabei Zweifel an der datenschutzrechtlichen Zulässigkeit einzelner Angaben geäußert. Insbeson-

dere erschienen ihm die Fragen im Rahmen einer Selbstauskunft über den Stand der Darlehens- und Hypothekenkonten des Heimträgers sowie den Stand sonstiger Konten und die Angabe des Geburtsnamens der Mutter ungerechtfertigt zu sein. Die Angaben zur wirtschaftlichen Situation des Heimträgers haben jedoch in § 7 Abs. 1 HeimG, wonach die Unterlagen zur Finanzierung der Investitionskosten vorzulegen sind, eine gesetzliche Grundlage. Außerdem ist durch § 6 Nr. 1 HeimG geregelt, daß der Heimträger die notwendige Zuverlässigkeit, insbesondere wirtschaftliche Leistungsfähigkeit zum Betrieb des Heims, besitzen muß. Darüber hinaus ist der Heimträger nach § 9 HeimG zur Auskunft über diese Angaben verpflichtet. Meine Nachfrage beim Landesversorgungsamt zur Erforderlichkeit der Angabe des Geburtsnamens der Mutter ergab erstaunliches. Gestützt auf § 6 HeimG i. V. m. § 2 Heimpersonalverordnung, der die Eignungsvoraussetzung des Heimleiters bestimmt, wurde die Auffassung vertreten, daß zur Überprüfung der Zuverlässigkeit des Heimträgers in persönlicher Hinsicht eine unbeschränkte Auskunft aus dem Bundeszentralregister nach § 41 BZRG angefordert wird, zu deren Beantragung die Angabe des Geburtsnamens der Mutter erforderlich sei. Richtig ist zwar, daß für eine Auskunft aus dem Bundeszentralregister das Geburtsdatum der Mutter zur eindeutigen Identifizierung erforderlich sein kann. Allerdings stellt die Anforderung einer unbeschränkten Auskunft nach § 41 eine unverhältnismäßige Maßnahme dar. Da mit der Erteilung einer unbeschränkten Auskunft, die den gesamten Inhalt des Registers zu einer Person enthält, ein nicht unerheblicher Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen verbunden ist, sind in § 41 Abs. 1 BZRG diejenigen Behörden abschließend aufgezählt, denen im überwiegenden öffentlichen Interesse diese umfassenden Auskünfte zur Kenntnis gebracht werden dürfen. Die Versorgungsämter sind in diesem abschließenden Katalog nicht genannt. Es kommt hier lediglich die Vorlage eines Führungszeugnisses nach § 31 BZRG in Betracht. Wie sich aus 3.1 der 2. BZRGVwV ergibt, ist bei einem Verfahren auf Antrag oder im Interesse des Betroffenen regelmäßig kein Führungszeugnis nach § 31 BZRG durch die Behörde einzuholen, sondern dem Betroffenen aufzugeben, ein Führungszeugnis zur Vorlage bei einer Behörde nach § 30 Abs. 5 BZRG zu beantragen. Bei dem Anzeigeverfahren nach § 7 HeimG liegt ein Verfahren vor, das im Interesse des Betroffenen erfolgt. Daher ist der Antragsteller vom Versorgungsamt aufzufordern, ein Führungszeugnis zunächst selbst beim Meldeamt zur Vorlage bei der Heimaufsicht zu beantragen. Erst wenn diese Aufforderung erfolglos geblieben ist, liegen die Voraussetzungen vor, unter denen das Versorgungsamt selbst ein Führungszeugnis nach § 31 BZRG beantragen kann. Mit dem Landesversorgungsamt und dem TMSG konnte Einvernehmen erzielt werden, daß diese gestufte Verfahrensweise auch Niederschlag in den Anzeigeformularen findet.

11.28 Antragsgestaltung für die Gewährung von Eingliederungshilfen

In einer Eingabe wurde ich gebeten, zu prüfen, inwieweit die Verfahrensweise zur Erhebung, Bearbeitung und Gewährung von Eingliederungshilfen gemäß §§ 39, 40 BSHG, insbesondere hinsichtlich der genutzten Vordrucke und Erläuterungen den datenschutzrechtlichen Anforderungen genügen. Im konkreten Fall handelte es sich um die Antragstellung auf Eingliederungshilfe zur Berechnung der Höhe der sogenannten häuslichen Ersparnis für die Ganztagsbetreuung eines schulpflichtigen Kindes beim Besuch einer Spezialschule für Körperbehinderte. Geregelt wird das Verfahren dazu im BSHG. Im Rahmen der „erweiterten Hilfe“ nach § 43 BSHG ist den Eltern eines Behinderten, der das 21. Lebensjahr noch nicht vollendet hat und dem eine Hilfe zu einer angemessenen Schulbildung (z. B. Besuch einer besonderen Förderschule) gewährt wird, lediglich eine Beteiligung in Höhe der für die Sicherstellung des Lebensunterhaltes in der Einrichtung entstehenden Kosten

zuzumuten. Die Nachfrage beim zuständigen Landesamt für Soziales und Familie ergab, daß die Berechnung der Höhe des Kostenbeitrages, wie vom Gesetzgeber vorgegeben (§ 43 Abs. 2 S. 2 BSHG), auf der Grundlage der Ersparnis vom Lebensunterhalt unter Berücksichtigung der Einkommens- und Vermögensverhältnisse, der Dauer der Unterbringung und der Art und Höhe der Leistung, die die Familie regelmäßig für den Hilfsempfänger zu erbringen haben, erfolgt. Grundlage ist eine beim Landessozialamt vorliegende Kostentabelle, in der nach Gegenüberstellung des Einkommens des Hilfeempfängers und der unterhaltspflichtigen Personen mit dem geltenden Bedarfssatz für Hilfeempfänger die berechneten monatlichen Einsparungen in Abhängigkeit vom Betreuungszeitraum ausgewiesen werden. Übersteigt das bereinigte Einkommen den Bedarfsatz eines entsprechenden Sozialhilfeempfängers um mehr als 100 % ist in jedem Fall der Höchstbetrag (z. B. 100 % des maßgeblichen Sozialhilferegelsatz bei der ganzjährigen Unterbringung und Versorgung in der Einrichtung) von den Eltern als monatliche Ersparnis zu zahlen. Zur Berechnung des bereinigten Einkommens hat gegenwärtig der Hilfeempfänger bzw. dessen Sorgeberechtigter einen allgemeinen Sozialhilfeantrag, in dem die persönlichen Verhältnisse des Kindes und der Eltern, die Familien-, Einkommens-, Vermögens- und Wohnverhältnisse aller im Haushalt lebenden Personen sowie Daten von allen unterhaltspflichtiger Angehöriger zu offenbaren sind, beim Landessozialamt abzugeben. Dies ist aus datenschutzrechtlicher Sicht in den Fällen unverhältnismäßig, wenn bereits aufgrund entsprechend hoher Einkünfte der Eltern erkennbar ist, daß die Einkünfte unter Berücksichtigung der im Sozialbereich abzugsfähigen Beträge weit über den Sozialhilfesätzen liegen. Ich habe daraufhin das Landessozialamt gebeten, die bisherigen Regelungen und Vordrucke dahingehend zu ändern, daß bei einer erkennbaren Überschreitung der entsprechenden Einkommensgrenze nur noch die tatsächlich erforderlichen Daten von den Antragstellern abgefordert werden. Neben datenschutzrechtlichen Gründen hätte dies auch eine Entlastung der Verwaltung und eine Reduzierung des Aufwandes und der Nachweisführung ihrer Einkommens- und Vermögensverhältnisse durch die Betroffenen zur Folge. Das Landesamt für Soziales und Familie hat meine Empfehlungen aufgegriffen und beabsichtigt das Antragsformular für Hilfen nach §§ 39, 40 und 43 BSHG entsprechend zu ändern. Daneben soll den Unterhaltspflichtigen künftig zunächst nur der zu zahlende Höchstbetrag mitgeteilt werden mit dem Hinweis, unter welchen Voraussetzungen eine Reduzierungen des Elternbeitrages möglich ist und, daß in diesen Fällen eine Offenbarung aller Einkommens- und Vermögensverhältnisse des Antragstellers sowie der Unterhaltsverpflichteten erforderlich wird. Diese Änderungsvorschläge wurden zwischenzeitlich dem TMSG zur Bestätigung vorgelegt.

11.29 Gegenseitige Beauftragung der Träger der gesetzlichen Rentenversicherung mit der Versichertenbetreuung

Die gesetzlichen Rentenversicherungsträger (z. B. BfA und LVAen) sind eigenständige Sozialleistungsträger, die nur über die bei ihnen versicherten Personen Sozialdaten gespeichert haben. Sofern daher der Versicherte Auskünfte zu seinem Versicherungskonto benötigt, mußte er sich bisher an den zuständigen Rentenversicherungsträger wenden. Da oftmals Versicherte in den Zuständigkeitsbereich eines anderen Rentenversicherungsträgers umziehen oder an unterschiedlichen Orten leben und arbeiten, entstand das Bedürfnis, den Versicherten die Möglichkeit einzuräumen, auch bei den eigentlich nicht zuständigen Rentenversicherungsträgern Auskünfte über das Versichertenkonto zu erhalten und diese erläutert zu bekommen. Hierzu haben die Landesversicherungsanstalten und die Bundesversicherungsanstalt für Angestellte (BfA) Vereinbarungen über „die gegenseitige Beauftragung nach § 88 SGB X mit der Erstellung, Anforderung, Aushändigung und Erläuterung von Versicherungsverläufen, Rentenauskünften, Lückenauskünften und

Auskünften über Beitragserstattungen sowie über die dafür erforderliche Bearbeitung und Nutzung von Sozialdaten im Auftrag nach § 80 SGB X“ abgeschlossen. Danach wird allen Rentenversicherungsträgern technisch die Möglichkeit eingeräumt, auf die Versichertenkonten der jeweils unzuständigen Rentenversicherungsträger zum Zweck der Beauskunftung und Erläuterung bei Anfragen des Versicherten zuzugreifen. Die Einrichtung eines derartigen Abrufverfahrens ist rechtlich zulässig. Es stellte sich lediglich die Frage, ob es sich um ein automatisiertes Abrufverfahren nach § 79 SGB X handelt oder ob es als Datenverarbeitung im Auftrag anzusehen ist. Ich habe gegenüber der LVA Thüringen die Auffassung vertreten, daß ich die reine Auskunftserteilung sowie die allgemeine Erläuterung als Auftragsdatenverarbeitung nach § 80 i. V. m. § 88 SGB X ansehe. Sowohl bei einer Einordnung des Verfahrens als Auftragsdatenverarbeitung wie als automatisiertes Abrufverfahren kommt angesichts der Zugriffsmöglichkeiten auf eine sehr große Anzahl der Rentendaten von Versicherten der Umsetzung von technisch-organisatorischen Maßnahmen nach § 78a SGB X zum Schutz dieser Daten eine zentrale Bedeutung zu. Gegenüber der LVA Thüringen habe ich es als notwendig angesehen, daß folgende Maßnahmen vorgesehen werden:

- Begrenzung der Anzahl der zur Dialognutzung zugelassenen Mitarbeiter auf das erforderliche Maß,
- technische Beschränkung der Zugriffsmöglichkeiten der zugelassenen Mitarbeiter auf das zu ihrer Aufgabenerfüllung erforderliche Maß,
- Unterweisung und datenschutzrechtliche Sensibilisierung der zugelassenen Mitarbeiter,
- Identitätsprüfung des Antragstellers anhand eines Lichtbildausweises,
- Schriftlichkeit des Antrags (formularmäßig),
- sichere Identifizierung und Authentisierung,
- Protokollierung der EDV-Zugriffe sowohl beim zuständigen als auch beim anfordernden Rentenversicherungsträger und
- stichprobenmäßige Kontrolle, daß für protokollierte Zugriffe ein Antrag vorliegt sowie auf Gleichlauf der beiden Protokolle.

Die LVA Thüringen hat daraufhin eine Dienstanweisung zu den organisatorischen Vorkehrungen zum Schutz der Sozialdaten bei der Dialogisierung des Datenaustausches innerhalb der gesetzlichen Rentenversicherung vorgelegt, die im wesentlichen die formulierten Anforderungen regelt. So werden die Zugriffsrechte auf bestimmte Mitarbeiter beschränkt, wobei die Vergabe der Zugriffsrechte nur mit Zustimmung des behördeninternen Datenschutzbeauftragten möglich ist. Darüber hinaus ist vorgesehen, daß sich der Auskunftssuchende bei der Vorsprache ausweisen muß und sein Auskunftsersuchen durch Unterschrift dokumentiert wird. Schließlich sind sowohl beim anfragenden wie auch beim angefragten Rentenversicherungsträger die einzelnen Abrufe zu protokollieren. Die Zugriffe werden vom behördeninternen Datenschutzbeauftragten überprüft, um ggf. mißbräuchliche Abfragen (z. B. ohne Auskunftsersuchen des Versicherten) feststellen zu können.

12. Statistik

12.1 Einführung einer Strafverfolgungsstatistik im Freistaat Thüringen

Die Strafverfolgungsstatistik stellt zweifellos ein wichtiges Instrument für die Bewältigung der den Landesjustizverwaltungen, Staatsanwaltschaften und Gerichten gestellten Aufgaben im strafrechtlichen Bereich dar. Mit Hilfe der veröffentlichten Tabellen der Strafverfolgungsstatistik lassen sich Fragen bezüglich der Sanktionsentwicklung nach Kategorien beantworten und bewerten. Sie ermöglichen anhand der erfaßten Delikte und ausgesprochenen Sanktionen exakte Vorgaben für die zukünftig notwendige Gesetzesent-

wicklung. Obwohl die Strafverfolgungsbehörden diese Übersichten zur Überprüfung, ob bestehende Verfahrens- oder Sanktionsarten sich als tauglich erwiesen haben bzw. von der gerichtlichen und staatsanwaltschaftlichen Praxis akzeptiert werden, benötigen, gibt es bisher keine entsprechende konkrete Rechtsgrundlage. Wie schon im 1. TB (12.) ausgeführt, vertrete ich die Ansicht, daß über 13 Jahre nach dem Volkszählungsurteil der sogenannte Übergangsbonus für die Neueinführung von Erhebungen nicht mehr in Anspruch genommen werden kann. Um dennoch bis zur Verabschiedung einer einheitlichen bundesgesetzlichen Regelung die notwendigen statistischen Aussagen zu erhalten, wurde auf der Grundlage des Thüringer Statistikgesetzes (ThürStatG) nach einer den Forderungen des Datenschutzes und der Statistik gerecht werdenden Übergangslösung gesucht. Diese bot sich darin, daß künftig die Staatsanwaltschaften verpflichtet werden, in ihrem Geschäftsbereich, auf der Grundlage der vorliegenden Daten, eine Geschäftsstatistik zu erstellen. In der entsprechenden Verwaltungsvorschrift mußte daher ausdrücklich aufgenommen werden, daß es sich um eine Sekundärstatistik handelt und eine Übermittlung von Einzeldaten an andere Stellen unzulässig ist. Die einzelnen Staatsanwaltschaften bleiben daher für diese Daten, die in die Statistik einfließen, als Auftraggeber speichernde Stellen. Das Thüringer Landesamt für Statistik (TLS) bereitet lediglich aus wirtschaftlichen Gründen sowie zur Vereinfachung der Arbeiten und Entlastung der Staatsanwaltschaften die Daten als Auftragnehmer der jeweiligen Staatsanwaltschaften statistisch auf. Andere Stellen können deshalb nur anonymisierte Daten erhalten. Das TMJE hat die datenschutzrechtlichen Hinweise übernommen. Gegen die nunmehr vorliegende Fassung einer Verwaltungsvorschrift zur Anordnung der Strafverfolgungsstatistik bestehen aus datenschutzrechtlicher Sicht keinerlei Bedenken.

12.2 Führung „Zentraler Register“

In den Kommunen nehmen die Bestrebungen zu, für statistische oder Planungszwecke die in den Verwaltungen vorliegenden verschiedensten Datenbestände zum Aufbau von fachübergreifenden zentralen Registern zu nutzen. Um die Auswertung der Daten jederzeit aktuell nach den unterschiedlichsten Kriterien, insbesondere für kleinräumige Gliederungen, zu ermöglichen, ist der Aufbau entsprechender Register (z. B. Grundstücks- oder Gebäudedateien) beabsichtigt, in denen eine objektkonkrete Fortschreibung der Merkmale erfolgen soll.
Aus datenschutzrechtlichen Gründen ist diese Verfahrensweise äußerst bedenklich, weil durch die Verknüpfung und Vorratshaltung der personenbezogenen Daten solche Stellen Zugang zu Verwaltungsdaten erhalten, die sie entsprechend der Zweckbestimmung der Daten (überwiegend für Verwaltungsverfahren) nicht bekommen dürften. Nicht unerheblich sind dabei die ständig wachsenden Bedürfnisse nach immer fundierterem und umfassenderem Datenmaterial unter den Bedingungen der raschen Entwicklung der technischen Möglichkeiten, die zwangsläufig dazu führen, die Datenbestände durch weitere Verknüpfungen mit allen möglichen - adreßbezogenen - Verwaltungsdaten ständig zu vervollständigen. Im Ergebnis würden „gläserne Grundstücke“ mit allen „grundstücksbezogenen“ (im Einzelfall somit personenbezogenen) Daten entstehen, aus denen Daten zur Infrastruktur (wie Wasser- und Abwasseranschluß, Gas, Fernwärme, Abfallentsorgung), Daten zur Eigentumsform und Bewertungsdaten (wie Sanierungsstand, Bodenwerte, Kaufpreis), zur Nutzung, Größe und Ausstattung bis hin zu detaillierten Daten über die Bewohner (wie Bevölkerungsdaten, Angaben zur sozialen Zusammensetzung, zur Belegungsbindung) oder zur gewerblichen Nutzung (Art und Größe des Gewerbebetriebes) entnommen werden können. Da bei einer Vielzahl der Daten durch entsprechendes „Zusatzwissen“ oder auch durch Aufnahme weiterer Merkmale (z. B. einer Wohnungsnummer) eine Zuordnung und damit Bestimmbarkeit von Personen gegeben sein dürfte,

bestehen aufgrund der gegenwärtig geltenden Rechtsvorschriften auf dem Gebiet des Datenschutzes und der Statistik begründete Zweifel an der Zulässigkeit der Zusammenführung und objektkonkreten Fortschreibung von Verwaltungsdaten aus den verschiedensten Bereichen der öffentlichen Verwaltung innerhalb einer Behörde. Diese Form der zentralen Datenspeicher dürfte nach meiner Auffassung dem vom Bundesverfassungsgericht aufgestellten Grundsatz der informationellen Gewaltenteilung, wonach aus der Einheit der Kommunalverwaltung aufgrund der Zweckbindung der Daten keine informationelle Einheit abgeleitet werden kann, widersprechen.

Gemäß § 23 ThürStatG können Kommunen zur Wahrnehmung ihrer Selbstverwaltungsaufgaben Statistiken durch Satzung anordnen. Dabei sind die in § 25 i. V. m. § 9 Abs. 2 und § 15 Abs. 3 ThürStatG an eine amtliche Statistik gestellten Anforderungen zu beachten. Danach sind zur Durchführung einer Statistik nähere Bestimmungen zu treffen über die Art der Erhebung, den Kreis der zu Befragenden, die sonstigen Auskunftsstellen, die durch Erhebungsmerkmale zu erfassenden Sachverhalte, die Hilfsmerkmale, den Berichtszeitraum, den Berichtszeitpunkt, die Häufigkeit der Erhebung sowie die Art und den Umfang der Auskunftspflicht. Da für den Aufbau und die Pflege obiger Register regelmäßig alle möglichen Sachdaten aus dem Verwaltungsvollzug genutzt werden sollen, fehlt die vom Bundesverfassungsgericht im Volkszählungsurteil geforderte Normenklarheit als Voraussetzung für die Einschränkung des informationellen Selbstbestimmungsrechts der Bürger. Im Gegensatz zu den herkömmlichen Statistiken, bei denen Hilfsmerkmale (Ordnungs- und Adreßdaten) dazu dienen, die Zuordnung der Daten bis zum Abschluß der Prüfung auf Schlüssigkeit und Vollständigkeit zu erhalten und diese anschließend gemäß § 15 Abs. 3 ThürStatG zu löschen, soll gerade bei einer objektkonkreten Fortschreibung von Daten, z. B. in einem Gebäuderegister, dieser Bezug erhalten bleiben. Diese weitere Speicherung ist nach den Statistikgesetzen nur bei wiederkehrenden statistischen Erhebungen möglich, soweit die Hilfsmerkmale künftig zur Bestimmung des Kreises der zu Befragenden benötigt werden, nicht jedoch zur Aktualisierung vorhandener Einzeldatensätze.
In Anlehnung an § 10 Abs. 3 Bundesstatistikgesetz (BStatG) stellt das ThürStatG in § 15 Abs. 4 als kleinste territoriale Einheit, auf die sich dauerhaft Einzeldatensätze beziehen dürfen und somit als tiefste Aggregationsstufe für regional gegliederte statistische Einzeldatensätze auf die Ebene von Blockseiten (z. B. Straßenzüge) ab. Es ist deshalb davon auszugehen, daß für die Führung von objektbezogenen Registern das ThürStatG keine entsprechende Rechtsgrundlage bildet. Soweit keine spezialgesetzlichen Regelungen anwendbar sind, gilt aber für die Speicherung, Veränderung und Nutzung von Daten innerhalb der Verwaltung § 20 ThürDSG. Danach ist das Speichern, Verändern oder Nutzen personenbezogener Daten, zu denen auch Gebäudedaten zählen können, zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgabe erforderlich ist und es für Zwecke erfolgt, für die die Daten erhoben sind. Unabhängig davon, daß gemäß § 24 ThürStatG Statistikstellen nicht mit der gleichzeitigen Wahrnehmung nicht-statistischer Aufgaben des Verwaltungsvollzugs betraut werden dürfen, wozu auch Planungsaufgaben zählen, ist zu beachten, daß sich die Dauer der Speicherung von Verwaltungsdaten aus ihrer Erforderlichkeit für die Aufgabenerfüllung ergibt, für die sie erhoben wurden. Eine unbestimmte „Datenvorratshaltung“ ist unzulässig, ebenso wie eine weitere Speicherung für Planungs- oder statistische Zwecke, da sie für diese Zwecke regelmäßig nicht erhoben wurden (Zweckbindung). Eine Verarbeitung für andere Zwecke liegt nur dann nicht vor, wenn die Daten - solange sie für die Verwaltungsaufgaben, für die sie erhoben wurden, noch benötigt werden - zur Erstellung von Geschäftsstatistiken innerhalb der speichernden Stelle genutzt werden. Die Führung von Registern (wie Grundstücks- oder Gebäuderegister) bei den Statistikstellen der Kommunen ist aber keine Geschäfts-

statistik im Sinne des ThürStatG. Eine Zusammenführung von objektkonkreten Einzeldaten aus den verschiedensten Verwaltungsbereichen und deren dauerhafte Speicherung und Aktualisierung für einen noch nicht näher bestimmten statistischen Zweck widerspricht dem statistischen Gebot einer möglichst frühzeitigen Anononymisierung statistischer Einzelangaben. Aufgrund der geltenden Rechtsvorschriften erscheint es deshalb mit den Bestimmungen des ThürStatG sowie dem ThürDSG unvereinbar, für Planungs- oder statistische Zwecke, objektkonkret Daten aus den verschiedensten Verwaltungsbereichen auf Dauer an einer Stelle innerhalb der Verwaltung zusammenzuführen und fortzuschreiben. Da mir zwischenzeitlich von einer Kommune eine Satzung zur Führung einer sogenannten „statistischen Gebäudedatei“ vorliegt, habe ich mich zur Frage der Zulässigkeit der Führung objektkonkreter zentraler kommunaler Register mit den Datenschutzbeauftragten des Bundes und der Länder ausgetauscht. Dabei wurden von diesen, wie auch vom zuständigen TIM die von mir geäußerten Bedenken geteilt. Ich habe deshalb die Rechtsaufsichtbehörde gebeten, die Satzung nochmals hinsichtlich ihrer Vereinbarkeit mit datenschutzrechtlichen Bestimmungen zu überprüfen. Darüber hinaus habe ich auch der Kommune meine Auffassung zum Aufbau eines zentralen Datenspeichers mitgeteilt. Da sich bei der gleichzeitig durchgeführten Kontrolle ergab, daß die Umsetzung der Satzung bisher nicht erfolgte, besteht gegenwärtig meinerseits noch kein unmittelbarer weiterer Handlungsbedarf. Wegen ihrer grundsätzlichen Bedeutung werde ich diese Problematik im Hinblick auf die Einhaltung datenschutzrechtlicher Bestimmungen weiterverfolgen.

13. Bildung, Wissenschaft und Forschung

13.1 Datenerhebung im Rahmen der Schulgesundheitspflege

In meinem 1. TB (13.1.3) hatte ich auf die noch ausstehende Rechtsverordnung des Ministers für Soziales und Gesundheit im Einvernehmen mit dem Kultusminister zur Schulgesundheitspflege gemäß § 55 Thüringer Schulgesetz (ThürSchulG) hingewiesen. In der Stellungnahme der Landesregierung war ausgeführt worden, daß diese Rechtsverordnung voraussichtlich 1996 erlassen werden sollte. Wie mir bekannt ist, liegt im TMSG aber bislang nur ein Referentenvorentwurf vor. Im Interesse aller Beteiligten wäre es wünschenswert, wenn der Erlaß der Verordnung in absehbarer Zeit erfolgen würde.

13.2 Schulpflichtüberwachung durch Schulamt?

Aufgrund eines Hinweises hatte ich davon erfahren, daß ein Schulamt sich am Schuljahresende von allen Schulen im Zuständigkeitsbereich die Schülerdaten von allen Schulabgängern auf Diskette übermitteln ließ, die ihre Vollzeitschulpflicht noch nicht erfüllt hatten. Zusätzlich wurden zu Beginn des nächsten Schuljahres die Berufsschulen im Zuständigkeitsbereich aufgefordert, die Schülerdaten von allen Anfangsklassen auf Diskette an das Schulamt zu übermitteln. Im Schulamt erfolgte dann ein Datenabgleich zwischen beiden Dateien. Die Eltern derjenigen Schüler, die im Ergebnis des Abgleiches nicht in der aktuellen Berufsschuldatei enthalten waren, wurden vom Schulamt unter Hinweis auf die noch bestehende Berufsschulpflicht aufgefordert, gegenüber dem Schulamt nachzuweisen, daß entweder eine Schule außerhalb des Zuständigkeitsbereichs besucht wird oder aber die Berufsschulpflicht aus den in § 22 ThürSchulG genannten Gründen ruht. Wenn daraufhin der Nachweis nicht erfolgte, wurde der Vorgang an das Landratsamt als untere staatliche Verwaltungsbehörde übergeben. Ich hatte mich in der Sache an das TKM gewandt und darauf hingewiesen, daß die Kenntnis der o. g. Schülerdaten zur Erfüllung der in der Zuständigkeit des Schulamtes liegenden Aufgaben im Regelfall nicht erforderlich ist. Die mir

vom Schulamt zuvor genannte Auffassung, wonach das Schulamt gemäß §§ 17 ff. ThürSchulG die Erfüllung der Schulpflicht überwacht, konnte ich nicht teilen. Vielmehr ist die Erfüllung der Schulpflicht gemäß § 17 Abs. 6 ThürSchulG vom Schulleiter und den Lehrern zu überwachen. Weiterhin haben nach § 23 Abs. 3 ThürSchulG die Eltern und die mit der Erziehung und Pflege Schulpflichtiger beauftragten Personen für die Einhaltung der Berufsschulpflicht zu sorgen. Gemäß § 23 Abs. 4 ThürSchulG haben darüber hinaus Ausbildende und Arbeitgeber sowie die von ihnen Beauftragten auf die Schulpflicht der Berufsschulpflichtigen hinzuwirken. Der Schulleiter trifft nach § 24 Abs. 2 ThürSchulG im Einvernehmen mit dem zuständigen Schulamt die Entscheidung über die zwangsweise Schulzuführung und beantragt die Durchführung beim örtlich zuständigen Landkreis oder der örtlich zuständigen kreisfreien Stadt. Eine Beteiligung an der Schulpflichtüberwachung besteht für das Schulamt ausdrücklich nur insoweit, als es gemäß § 18 Abs. 2 Satz 3 ThürSchulG auf Antrag beurlauben und nach § 22 Abs. 2 ThürSchulG bei Vorliegen der dort genannten Voraussetzungen den Schulpflichtigen im Einzelfall von der Berufsschulpflicht befreien kann. In beiden Fällen handelt es sich aber ausschließlich um Bescheide auf Antrag. Das ThürSchulG trifft also hier konkrete Aussagen zur Verantwortlichkeit des Schülers, der Eltern, des Lehrers, des Schulleiters und des Auszubildenden zur Überwachung der Schulpflicht. Da im Ergebnis die Schulpflichtüberwachung nicht Aufgabe des Schulamtes ist und eine regelmäßige Datenübermittlung der Schulen an das Schulamt in Anwendung des § 57 Abs. 1 und 4 ThürSchulG unzulässig ist, bat ich das TKM, zu veranlassen, sich für die Einstellung dieses Verfahrens einzusetzen. Der Sachverhalt wurde daraufhin vom TKM überprüft und eine Einstellung dieser Verfahrensweise veranlaßt.

13.3 Datenerhebungen der Kirchen zur Planung des Religionsunterrichts

Nach Artikel 7 Abs. 3 Satz 2 GG wird der Religionsunterricht in Übereinstimmung mit den Grundsätzen der Religionsgemeinschaft erteilt. Zur Planung des Einsatzes von Religionslehrern benötigen die Kirchen daher Angaben über die Zahl der jeweils an den Schulen für das Fach Religionsunterricht eingesetzten Lehrer sowie der jeweils daran teilnehmenden Schüler. In diesem Zusammenhang wurde die Frage erörtert, unter welchen Voraussetzungen und in welchem Umfang die staatlichen Schulen für die Kirchen personenbezogene Daten erheben und übermitteln dürfen. Dabei wurde mir ein Erhebungsbogen zur anonymen Erfassung der am Religionsunterricht teilnehmenden Schüler vorgelegt, der gleichzeitig namentlich die Religionslehrer ausweist, die an der betreffenden Schule Religionsunterricht erteilen. Da es keine spezialgesetzliche Rechtsgrundlage zur Übermittlung der Personaldaten der Lehrer durch die Schulen an die Kirchen gibt und auch hier der Grundsatz der Erhebung beim Betroffenen gilt, wurden im Ergebnis der Gespräche zwischen dem TKM und den Kirchen die Erhebungsbögen getrennt. Sofern es um die Erfassung der Religionsunterricht erteilenden Lehrer geht, wurden eigene Personalbögen entworfen, die die Kirchen den Schulen zur Weiterleitung an die Lehrer übergeben. Dabei ist es den Lehrern freigestellt, entsprechende Angaben zu machen und über die Schule an die jeweilige Kirche zurückzugeben. Bezüglich des Schülererhebungsbogens konnte ich einige Hinweise geben, um die Vorschriften des Statistikgeheimnisses einzuhalten. Hierzu gehört insbesondere, daß eine Übermittlung der gewonnenen Daten durch die Statistikstelle des TKM in zusammengefaßter Form erfolgt, so daß keine Rückschlüsse auf einzelne Schüler möglich sind.

13.4 Hochschuleinrichtung - öffentlich-rechtliches Wettbewerbsunternehmen?

Im Rahmen der Klärung einer Eingabe wurde von einer Hochschuleinrichtung die Auffassung vertreten, aufgrund ihrer Forschungstätigkeit als öffentlich-rechtliches Wettbewerbsunternehmen zu gelten mit der Konsequenz, daß bei der datenschutzrechtlichen Bewertung nicht die Bestimmungen des ThürDSG zum Umgang mit personenbezogenen Daten anzuwenden sind, sondern das Bundesdatenschutzgesetz. Begründet wurde dies insbesondere damit, daß im Bereich der Forschung die Hochschule als Wettbewerber auf dem „Forschungsmarkt“ auftritt, da wissenschaftliche Institute auch außerhalb der Hochschulen gegen Honorar damit befaßt sind, Forschungsaufträge wie den vorliegenden zu erledigen. Private und Hochschulen ständen folglich in einem Konkurrenzverhältnis auf dem „Wissenschaftsmarkt“. Diese Auffassung kann ich nicht teilen. Aus den einschlägigen Kommentierungen zum Bundesdatenschutzgesetz ist zu entnehmen, daß die besonderen Vorschriften für öffentlich-rechtliche Wettbewerbsunternehmen ausschließlich zur Vermeidung von Wettbewerbsverzerrung im Hinblick auf eine wirtschaftliche Benachteiligung aufgenommen wurden. Allein die Tatsache, daß wissenschaftliche Institute für Dritte tätig werden, ist kein Kriterium für die Einordnung als öffentlich-rechtliches Wettbewerbsunternehmen im datenschutzrechtlichen Sinn. Entscheidend ist der wirtschaftliche Aspekt und nicht allein die Tatsache des Wettbewerbes und der Möglichkeit, daß die Aufgaben auch von nicht-öffentlichen Stellen wahrgenommen werden können. Als öffentliche Unternehmen sind solche staatlichen Einheiten zu betrachten, die sich wirtschaftlich betätigen. Demgegenüber ist es erklärte Zielstellung der wissenschaftlichen Forschungstätigkeit an Hochschulen, zusammen mit der Lehre und dem Studium die Wissenschaften und Künste zu pflegen und zu entwickeln (§ 4 ThürHG). Dabei ist es unerheblich, ob dies von Dritten finanziert oder unterstützt wird. Im übrigen kann davon ausgegangen werden, daß wissenschaftliche Arbeiten an Hochschulen regelmäßig nicht im Rahmen eines unter wirtschaftlichen Gesichtspunkten durchgeführten Ausschreibungsverfahren, an dem sich uneingeschränkt öffentliche und nicht-öffentliche Stellen beteiligen können, vergeben werden. Aus o. g. Gründen sind, soweit nicht an Hochschulen spezialgesetzliche Datenschutzregelungen gelten, die Bestimmungen des ThürDSG einschlägig.

13.5 Kontrolle einer Hochschule

Im Berichtszeitraum erfolgte eine datenschutzrechtliche Kontrolle in einer Hochschule im Bereich Studentenverwaltung. Dabei wurde von mir beanstandet, daß sowohl für die zur Anwendung kommende Studentenverwaltungsdatei als auch für das Telefondatenerfassungssystem keine schriftlichen Verfahrensfreigaben gemäß § 34 Abs. 2 ThürDSG vorgelegt werden konnten. Ebenso wurden beide Verfahren nicht in einem Anlagen- und Verfahrensverzeichnis nach § 10 ThürDSG dokumentiert. Die Hochschule hat zwischenzeitlich das Erforderliche zur Beseitigung der datenschutzrechtlichen Mängel veranlaßt. Weiterhin ist auf dem Gelände der Hochschule an Punkten, für die eine konkrete Gefahrenlage besteht, eine Videoanlage zur Geländeüberwachung installiert. Da die Kameras nicht unmittelbar erkennbar sind, vertrat ich gegenüber der Hochschule die Auffassung, daß auf die Videoüberwachung hinzuweisen ist. Entsprechende Hinweisschilder wurden inzwischen am Haupteingang und an anderen wegweisenden Stellen des Geländes angebracht. Schließlich wurde die von der Hochschule geforderte Beifügung eines Lebenslaufes zum Antrag auf Einschreibung kritisiert. Weder gibt es hierzu eine spezialgesetzliche Grundlage noch konnte eine allgemeine Erforderlichkeit zur Aufgabenerfüllung der Hochschule begründet werden. Zukünftig wird deshalb kein Lebenslauf mehr verlangt, sondern

ausschließlich die für die Aufnahme des Studiums erforderlichen Informationen zum Bildungsgang erfragt.

13.6 Von Schimmelpilzen der Gattung Rhizopus, Mucor, Aspergillus fumigatus und flavus, Penicilium, Epicoccum sowie Modadium befallene Akten

In der Eingabe eines Bürgers beschwerte sich dieser darüber, daß seiner Bitte um Akteneinsicht in seine Hochschulunterlagen aus früherer DDR-Zeit aus Restaurierungsgründen von Seiten der Hochschule vorläufig nicht entsprochen wurde. Grundsätzlich bestimmt Art. 6 Abs. 4 ThürVerf, daß nach Maßgabe der Gesetze jedem neben dem Aktenauskunftsrecht auch ein Einsichtsrecht in die ihn betreffenden Akten zusteht. Deshalb hatte ich mich an die Hochschulleitung gewandt und um Erläuterung gebeten, welche Restaurierungsgründe gegen die Einsicht des Beschwerdeführers in seine Unterlagen sprechen. Im Ergebnis wurde mir mitgeteilt, daß aufgrund von ungünstigen Lagerbedingungen im Hochschularchivraum ein Teil des Aktenbestands von Schimmelpilzen befallen war. Da der Bürger aber auf seinem Einsichtsrecht bestand, konnte ich erreichen, daß die Benutzungssperre der von Schimmelpilzen befallenen Aktenbestände für ihn auf eigene Verantwortung aufgehoben wurde. Ich wurde aber von der Hochschule gebeten, den Beschwerdeführer auf die gesundheitlichen Risiken während der Benutzungsdauer hinzuweisen. Inzwischen sind die Schimmelpilze vernichtet und die Akten in andere Räume umgelagert worden, so daß jedenfalls aus gesundheitlichen Gründen nichts mehr gegen die Einsichtnahme in die Akten spricht.

13.7 Nutzung von Jugendgerichtshilfeakten zu Forschungszwekken

Im Zusammenhang mit einem vom TMJE in Zusammenarbeit mit dem TMSG in Auftrag gegebenen Forschungsprojekt zur „Praxis der Untersuchungshaftvermeidung nach den §§ 71 und 72 Jugendgerichtsgesetz (JGG)“ waren datenschutzrechtliche Fragen beim Umgang mit Jugendgerichtshilfeakten erörtert worden. Im Rahmen des Forschungsprojekts sollen durch Mitarbeiter der mit der Durchführung des Forschungsprojekts beauftragten Hochschule sowohl Gespräche mit Richtern, Staatsanwälten, Jugendgerichtshelfern, Vollzugsbeamten sowie Mitarbeitern sozialer Dienste geführt werden als auch ausgewählte Akten der Jugendgerichtshilfe der Thüringer Jugendämter ausgewertet und bestimmte Angaben auf anonymisierte Listen übertragen werden. Die Interviews mit Richtern, Staatsanwälten usw. erfolgen ohne namentliche Nennung der Jugendlichen. Darüber hinaus war beabsichtigt, die Auswertungen der Jugendgerichtshilfeakten in anonymisierter Form zu speichern und zu nutzen, so daß sich insoweit keine datenschutzrechtlichen Probleme stellten. Allerdings werden durch die Einsichtnahme in die Jugendgerichtshilfeakten den Mitarbeitern der Hochschule personenbezogene Daten übermittelt. Eine Anwendung der datenschutzrechtlichen Vorschriften des Sozialgesetzbuches ist bezüglich der Unterlagen der Jugendgerichtshilfe aufgrund von § 61 Abs. 3 SGB VIII nicht möglich, da insoweit ein abschließender Verweis auf die Vorschriften des JGG vorliegt. Im JGG sind aber keine datenschutzrechtlichen Vorschriften enthalten. Daher findet für die Jugendämter, soweit sie die Aufgaben der Jugendgerichtshilfe wahrnehmen, das ThürDSG Anwendung. Nach § 21 Abs. 1 i. V. m. § 20 Abs. 2 Satz 1 Nr. 9 ThürDSG ist eine Übermittlung an die Mitarbeiter der Hochschule möglich, soweit es zur Durchführung einer wissenschaftlichen Forschung erforderlich ist und das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Einer Übermittlung steht auch nicht § 24 ThürDSG

entgegen, da grundsätzlich davon auszugehen ist, daß der Jugendgerichtshelfer - anders als der Mitarbeiter im Bereich der Jugendhilfe - nicht als besonderer Berufsgeheimnisträger nach § 203 StGB anzusehen ist. Das ergibt sich bereits aus seiner Funktion im Jugendgerichtsverfahren, wonach er die Persönlichkeit, Entwicklung sowie die Umwelt des Jugendlichen zu erforschen und darüber dem Gericht zu berichten hat. Bei der Prüfung, ob der Forschungszweck nicht auf andere Weise erreicht werden kann, sind aber zur Minimierung des Eingriffs in das Persönlichkeitsrecht der Jugendlichen auch weniger einschneidende Verfahrensmöglichkeiten zu prüfen. In Betracht kommt dabei zunächst, daß die Jugendlichen bzw. deren Erziehungsberechtigte ihre Einwilligung für die Teilnahme an dem entsprechenden Projekt erteilen. Als weitere Möglichkeit kommt in Betracht, daß die Mitarbeiter des Jugendamtes im Auftrag und auf Kosten des Forschungsträgers die Anonymisierung der Akten nach dessen Kriterien vornehmen. Schließlich wäre auch zu prüfen, ob ein zuvor besonders verpflichteter Mitarbeiter des Forschungsträgers die Anonymisierungsarbeiten mit den Akten durchführt und anschließend aus dem Projekt ausscheidet. Damit könnte sichergestellt werden, daß aufgrund der Aktenkenntnis auch anonymisierte Datensätze im weiteren Forschungsvorhaben nicht „wiedererkannt“ werden.

13.8 Staatsvertrag über ein gemeinsames Krebsregister der neuen Bundesländer und Berlins

Das Krebsregistergesetz (KRG) des Bundes sieht vor, daß bis zum 01.01.1999 in allen Bundesländern bevölkerungsbezogene Krebsregister eingeführt werden, sofern dort noch keine solchen existieren. Hierzu sind in den Bundesländern Ausführungsgesetze zu erlassen. Wie bereits im 1. TB (13.3.2) berichtet, wird in den neuen Bundesländern und Berlin das zentrale Krebsregister der ehemaligen DDR aufgrund eines Verwaltungsabkommens vom 23.12.1994 fortgeführt. Es ist erfreulich, daß sich zwischenzeitlich die beteiligten Ländern auf den Entwurf eines Staatsvertrages über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen (GKR) geeinigt und auf den Erlaß gleichlautender Ausführungsgesetze verzichtet haben. Damit ist sichergestellt, daß verbindliche, für alle beteiligten Länder gleichermaßen geltende Rahmenbedingungen zur Fortführung des GKR geschaffen werden. Im Rahmen der Erarbeitung des Staatsvertragsentwurfs wurden die Datenschutzbeauftragten der beteiligten Länder jeweils einbezogen und konnten ihre Vorstellungen aus datenschutzrechtlicher Sicht einbringen. Der Staatsvertrag wurde Ende November 1997 unterzeichnet. Mit der Verabschiedung der jeweiligen Zustimmungsgesetze dürfte innerhalb des ersten Halbjahres 1998 zu rechnen sein, so daß die gesetzliche Verpflichtung zur Schaffung von landesrechtlichen Grundlagen zum 01.01.1999 eingehalten werden dürfte.

13.9 Bestandsaufnahme der Asbestsituation in Thüringen

Im Rahmen eines Forschungsvorhabens „Bestandsaufnahme der Asbestsituation in Thüringen“ war zum Zweck der wissenschaftlichen Forschung auf dem Gebiet der Feststellung des vorhandenen Gefährdungspotentials sowie zur Ableitung langfristiger Aufgaben zur Sanierung der bebauten Umwelt und der sicheren Endverbringung des Gefahrenstoffes beabsichtigt, zunächst in ausgewählten Gemeinden landesweit bauwerks- und baustoffspezifische Daten zu erheben. Zielstellung war dabei die Aufstellung einer landesweiten Gefahrenstoffdatenbank als Basismaterial für die wissenschaftliche Arbeit und die Anfertigung kartographischer und tabellarischer Gefahrstoffdokumentationen. Um den datenschutzrechtlichen Belangen bei der Erhebung, Verarbeitung und Nutzung der Daten Rechnung zu tragen, wurde ich von der Forschungsstelle frühzeitig in das Verfahren einbezogen. Aufgrund einer

fehlenden Rechtsgrundlage für die Erhebung der erforderlichen Daten wurde die Form und der Umfang der Erhebung sowie die möglichen Auswertungsverfahren unter dem Aspekt der Nutzung von Daten aus öffentlichen Quellen und der freiwilligen Mitwirkung von Haus- und Grundstückseigentümer erarbeitet. Es wurde Einvernehmen darüber erzielt, daß für die notwendigen Planungs- und Forschungsaufgaben eine Bestandsaufnahme der Asbestsituation auf der Grundlage einer nicht objektkonkreten sondern straßenzug- bzw. quartierbezogenen Datenmenge ausreicht. Damit wurde ein Kompromiß gefunden, um einerseits dem Planungs- und Forschungsvorhaben die notwendige Erhebung, Verarbeitung und Nutzung einer breiten Datenbasis zu ermöglichen, ohne andererseits die Persönlichkeitsrechte der Eigentümer in unverhältnismäßiger Weise zu beeinträchtigten. Gleichzeitig stellt diese Verfahrensweise sicher, daß ein Mißbrauch der Daten aufgrund der faktischen Anonymisierung der Einzelangaben ausgeschlossen werden kann.

13.10 Anwendung des ThürDSG in Archiven

In meine Kontrolltätigkeit wurden im Berichtszeitraum auch Archive einbezogen. Ich konnte dabei feststellen, daß dort im Hinblick auf die Einhaltung datenschutzrechtlicher Bestimmungen bei der Verwahrung und Benutzung von Archivgut verantwortungsbewußt mit allen Unterlagen, die personenbezogene Daten enthalten, umgegangen wird. Bemerkenswerte datenschutzrechtliche Mängel wurden in keinem Fall festgestellt. Als spezialgesetzliche Regelung findet für den Umgang mit Archivgut das ThürArchivG Anwendung. Als Archivgut gelten dabei Unterlagen, die für Verwaltungsaufgaben nicht mehr benötigt werden, deren Archivwürdigkeit nach § 12 ThürArchivG festgestellt wurde und die vom zuständigen öffentlichen Archiv übernommen wurden. Im Rahmen von Kontrollen habe ich allerdings in Einzelfällen bei Kommunalarchiven festgestellt, daß bereits bei der Aufbewahrung von Zwischenarchivgut der Verwaltung gemäß § 14 Abs. 3 ThürArchivG hinsichtlich der weiteren Nutzung dieser Unterlagen nach archivrechtlichen Bestimmungen verfahren wird. Dort wurde vernachlässigt, daß die Aufbewahrung ausschließlich im Auftrag der abgebenden Stelle erfolgt, die aber weiterhin die volle Verantwortung über die Benutzung der Unterlagen behält. Ich habe in diesen Fällen die betreffenden Stellen auf die Rechtslage hingewiesen. Bei der Prüfung eines Landesarchivs stellte sich heraus, daß für archivarische Zwecke automatisierte Such- und Finddateien mit teilweise sehr detaillierten personenbezogenen Angaben zum Inhalt des Archivgutes angelegt worden waren. Anläßlich einer gemeinsamen Beratung von Archivaren bei der obersten Aufsichtsbehörde war die Auffassung vertreten worden, daß die staatlichen Archive nicht als speichernde öffentliche Stellen im Sinne der ThürDSGRegVO betrachtet werden könnten. Daten in Archivbeständen würden von den Archiven weder selbst erhoben, noch verändert oder inhaltlich verarbeitet werden. Da die Daten lediglich für innerdienstliche, insbesondere für arbeitsorganisatorische und statistische Zwecke genutzt werden und im übrigen die Nutzung von personenbezogenen Daten in Archiven nach dem ThürArchivG geregelt sei, war man davon ausgegangen, daß eine Meldung gegenüber dem Datenschutzregister unterbleiben könnte. Dies nahm ich zum Anlaß, mit der zuständigen obersten Landesbehörde Fragen des Umfangs von Finddateien sowie zur Abgabe von Datenschutzregistermeldungen zu erörtern. Im Ergebnis wurde vom TMWK die Erforderlichkeit der Führung teilweise sehr detaillierter Finddateien mit personenbezogenen Daten aufgrund der Aufgabenstellung der Archive zur Erschließung und Bereitstellung des Archivgutes für die weitere Benutzung bestätigt. Gleichzeitig wurde festgestellt, daß für staatliche oder kommunale Archive die Bestimmungen des ThürDSG gelten, soweit nicht hinsichtlich des Umgangs mit Archivgut spezialgesetzliche Regelungen des ThürArchivG vorgehen. Das betreffende Archiv wurde aufgefordert, kurzfristig alle automatisierten Datei

mit personenbezogenen Daten dem TLfD zum Datenschutzregister gemäß § 3 ThürDSRegVO zu melden, was zwischenzeitlich erfolgte.

14. Wirtschaft, Verkehr, Wohnungswesen, Umwelt

14.1 Gesetz zur Änderung des Rechts der Architekten und Ingenieure

Vom TMWI wurde mir der Entwurf eines Thüringer Gesetzes zur Änderung des Rechts der Architekten und Ingenieure zur Stellungnahme aus datenschutzrechtlicher Sicht zugesandt. Darin war u. a. vorgesehen, in einem neuen Architektengesetz Regelungen zur Führung einer Architektenliste und die Beauskunftung hieraus aufzunehmen. Dabei sollten inhaltlich die Vorschriften des bestehenden Ingenieurkammergesetzes zur Liste der Beratenden Ingenieure übernommen werden. Zu begrüßen war, daß in den Regelungen abschließend diejenigen Daten genannt werden, die in die Architektenliste bzw. die Liste der Beratenden Ingenieure eingetragen werden. Auskunft aus der Liste soll jedermann erhalten, ohne daß ein berechtigtes Interesse geltend gemacht werden muß. Das hielt ich angesichts des eingeschränkten Datensatzes für vertretbar. Sofern jedoch Auskunft über eine Vielzahl nicht namentlich bezeichneter Architekten bzw. beratender Ingenieure begehrt wird oder eine Veröffentlichung der Liste beabsichtigt ist, soll dies nur zulässig sein, sofern der Betroffene nicht widersprochen hat. Da Widerspruchsrechte in der Regel dann leerlaufen, wenn auf solche Rechte nicht hingewiesen wird, habe ich gefordert, eine Regelung aufzunehmen, wonach die Betroffenen auf dieses Widerspruchsrecht hingewiesen werden müssen. Schließlich habe ich angeregt, eine normenklare Rechtsgrundlage zur Übermittlung von Daten von der Architektenkammer bzw. der Ingenieurkammer an das zuständige Versorgungswerk aufzunehmen. Meine Änderungsvorschläge wurden vom TMWI aufgegriffen und sind im Thüringer Gesetz zur Änderung des Rechts der Architekten und Ingenieure vom 13.06.1997 (GVBl. 97, 210 ff) berücksichtigt worden, das am 14.06.1997 in Kraft getreten ist.

14.2 Thüringer Verordnung über den Gebrauchtwaren-, Edelmetall- und Altmetallhandel, über Auskunfteien, Detekteien, Reisebüros und die Vermittlung von Unterkünften

Zur dem in der Überschrift genannten Verordnungsentwurf bat mich das TMWI um eine datenschutzrechtliche Stellungnahme. Nach dieser Verordnung hat u. a. der Gebrauchtwaren-, Edelmetall- und Altmetallhandel die Pflicht zur Führung eines Geschäftsbuchs, in dem verschiedene Angaben über die An- und Verkäufe von gehandelten Gegenständen sowie über Käufer und Verkäufer einzutragen sind. Nach Prüfung der Verordnung teilte ich dem Ministerium mit, daß für die Aufzeichnung der Ausweisnummer des Käufers und des Verkäufers im Geschäftsbuch keine Erforderlichkeit gegeben ist und deshalb darauf verzichtet werden sollte. Mein Hinweis wurde entsprechend berücksichtigt.

14.3 Verwaltungsvorschrift zu § 34 a GewO und der Bewachungsverordnung

Das TMWI bat mich um eine datenschutzrechtliche Stellungnahme zum Entwurf einer Verwaltungsvorschrift zu § 34 a GewO und zur Bewachungsverordnung. In der Verwaltungsvorschrift wird näher festgelegt, welche Voraussetzungen ein Bewachungsgewerbetreibender und seine Beschäftigten erfüllen müssen, um von der zuständigen Behörde eine Gewerbeerlaubnis zu erhalten. So hatte ich das TMWI neben einigen begrifflichen Klarstellungen u. a. darauf hingewiesen, daß dem Betroffenen ein Anhörungsrecht gemäß § 28 Abs. 1 ThürVwVfG zusteht und dieses Recht nicht einer Ermessensent-

scheidung der prüfenden unteren Gewerbebehörde unterliegt. Dies sollte auch ausdrücklich in die Verwaltungsvorschrift aufgenommen werden. Alle von mir vorgebrachten Konkretisierungs- und Änderungsvorschläge wurden vom TMWI umgesetzt.

14.4 Bewerberliste der Bezirksschornsteinfeger

Der Zentralverband der Deutschen Schornsteinfeger e. V. bat mich um Beantwortung der Frage, ob datenschutzrechtliche Bedenken bestehen, wenn an alle Schornsteinfeger des jeweiligen Gebietes eine Liste mit Vornamen, Namen und Rangstichtag derjenigen Bewerber, die sich als Bezirksschornsteinfeger bestellen lassen wollen, versendet wird. Nach § 22 Abs. 1 Nr. 1 erster Halbsatz ThürDSG ist die Übermittlung an eine nicht-öffentliche Stelle u. a. zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist. Diese Erforderlichkeit ergibt sich aber weder aus dem Schornsteinfegergesetz noch aus der Verordnung über das Schornsteinfegerwesen. Weiterhin ist zwar eine Übermittlung nach § 22 Abs. 1 Nr. 2 ThürDSG zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten darlegt, allerdings darf der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung haben. Solange bei einer listenmäßigen Übermittlung nicht ausgeschlossen werden kann, daß diese Übermittlung schutzwürdigen Interessen einzelner Betroffener entgegenstehen, ist diese ebenfalls nicht zulässig. Das TLVwA bestätigte meine Einschätzung, daß eine Übermittlung der Bewerberlisten nicht erforderlich ist. Die Listen würden sowohl vom Vorstand als auch vom Gesellenausschuß der Schornsteinfegerinnung überwacht. Außerdem könne bei berechtigtem Interesse der Bewerber jederzeit Einsicht in die Liste genommen werden. Im übrigen stünden einem Bewerber, der geltend macht, in seinen Rechten verletzt zu sein, der Klageweg offen. Der Zentralverband wurde von mir über das Ergebnis unterrichtet.

14.5 Veröffentlichungen von Handelsregisterdaten im Internet

Von verschiedenen Industrie- und Handelskammern (IHK) war geplant, aus Gründen einer Erweiterung ihres Serviceangebots, Handelsregisterdaten in das Internet einzustellen. Dies widerspricht der Regelung des § 125 Abs. 1 FGG i. V. m. § 9 Abs. 1 HGB, wonach zwar jedem die Einsicht in das Handelsregister gestattet ist, die Register aber bewußt dezentral im Zuständigkeitsbereich des jeweiligen Amtsgerichts geführt werden. Ich habe deshalb die Thüringer IHK darauf aufmerksam gemacht, daß bei einer Veröffentlichung der örtlichen Register im Internet nicht mehr zu kontrollieren wäre, wer auf die Daten zugreift und wie diese weiter verarbeitet oder genutzt werden. Technisch wäre es ohne Probleme möglich, auf diese Weise ein bundesweites Handelsregister zu erstellen. In einem Beschluß des BGH zur Frage, ob eine Mikroverfilmung des gesamten Handelsregisterbestands zulässig ist, wird ausgeführt, daß diese „Übermittlung personenbezogener Daten das informationelle Selbstbestimmungsrecht der Betroffenen in einem wesentlich größeren Ausmaß als die bisher mögliche Einsicht in das Handelsregister berührt“ und „deshalb einer hinreichenden Rechtsgrundlage“ bedarf. Nach meiner Auffassung wäre bei einer Einstellung der Handelsregisterdaten in das Internet das informationelle Selbstbestimmungsrecht in einem noch stärkeren Maße tangiert. Gegen die Veröffentlichung der Mitteilungen des Amtsgerichts über Neueintragungen, Veränderungs- und Löschungsmeldungen der IHK in das Internet bestehen aber keine datenschutzrechtlichen Bedenken. Ich gehe davon aus, daß alle Handelsregisterdaten, die gemäß § 10 Abs. 1 HGB in den Bekanntmachungsblättern veröffentlicht werden, auch in das Internet eingestellt werden können.

14.6 Übermittlung von Gewerbeanzeigen an die AOK

Gemäß § 14 Abs. 5 Nr. 7 GewO darf die zuständige Behörde regelmäßig Daten der Gewerbeanzeigen „an die allgemeine Ortskrankenkasse für den Einzug der Sozialversicherungsbeiträge und für die Weiterleitung an die anderen in ihrem Zuständigkeitsbereich tätigen Krankenkassen“ übermitteln (§§ 28 h und 28 i SGB IV). Aufgrund des seit 01.01.1996 herrschenden Krankenkassenwahlrechts bestehen aus datenschutzrechtlicher Sicht gegen diese Übermittlungen Bedenken. Ich halte es mit dem informationellen Selbstbestimmungsrecht des Gewerbetreibenden nicht für vereinbar, die Daten aus der Gewerbeanzeige an eine Stelle zu übermitteln, von der zunächst nicht bekannt ist, ob sie diese Daten zur Erfüllung ihrer Aufgaben überhaupt benötigt. Außerdem verschafft sich die AOK gegenüber den anderen Krankenkassen damit einen zeitlichen Informationssprung, indem etwa frühzeitig Kontakte mit dem Gewerbebetrieb aufgenommen und gezielte Mitgliederwerbung betrieben werden kann. Den anderen Krankenkassen gehen die entsprechenden Informationen dann erst später zu. Eine mögliche Lösung wäre die Übermittlung an eine neutrale Stelle (z. B. die Gewerbeanzeigebehörden selbst), die die Gewerbeanzeigen an die Kassen weiterleitet. In jedem Fall ist eine Änderung des § 14 Abs. 5 Nr. 7 GewO erforderlich. Auf meine diesbezügliche Anfrage hin hat das TMSG meine Bedenken geteilt, aber darauf hingewiesen, daß ein kostenrelevanter Datenaustausch zu vermeiden sei. Soweit mir bekannt ist, soll zwischen dem Bundesministerium für Gesundheit und dem Bundesministerium für Wirtschaft eine diesbezügliche Ressortabstimmung mit dem Ziel einer Gesetzesänderung eingeleitet worden sein.

14.7 Änderung straßenverkehrsrechtlicher Vorschriften

Obwohl die Mitgliedstaaten verpflichtet waren, der Umsetzung der 2. EG-Führerscheinrichtlinie sowie anderer notwendiger Neuregelungen im Straßenverkehrsbereich bis spätestens ab 1. Juli 1996 nachzukommen, wird nunmehr mit dem Inkrafttreten des Gesetzes zur Änderung des Straßenverkehrsgesetzes (StVG) und anderer Gesetze erst zum 01.07.1998 gerechnet. Die datenschutzrechtlichen Bedenken gegen die Einführung eines zentralen Fahrerlaubnisregisters mit fast 50 Millionen Datensätzen wurden im Gesetzgebungsverfahren nicht aufgegriffen. Lediglich in einigen Detailfragen enthält der zuletzt eingebrachte Gesetzentwurf der Bundesregierung datenschutzrechtliche Verbesserungen. Selbst wenn das Gesetz zum 01.07.1998 in Kraft tritt, so bedeutet dies ein Nebeneinander der örtlichen- und des zentralen Fahrerlaubnisregisters von bis zu acht Jahren. Datenschutzrechtlich zu begrüßen ist aber der Umstand, daß auf die zunächst geplante Doppelspeicherung der Führerscheininhaber in beiden Registern zwischenzeitlich verzichtet wird. Positiv an dem bestehenden Änderungsentwurf hervorzuheben ist auch die nun getroffene Regelung, daß bei der Wiedererteilung oder der Entziehung der Fahrerlaubnis die bisher nach § 52 Abs. 2 BZRG gegebene Möglichkeit des zeitlich unbegrenzten Zugriffs der Fahrerlaubnisbehörden auf strafrechtliche Verurteilungen, die im BZR und im VZR gelöscht sind (1. TB, 14.2.3), jetzt zufriedenstellend korrigiert wurde. Insgesamt bin ich aber nach wie vor von der Notwendigkeit eines zentralen Fahrerlaubnisregisters im Sinne eines überwiegenden Allgemeininteresses nicht überzeugt. Mit der Errichtung eines zentralen Registers besteht jederzeit die Möglichkeit, ein umfassendes elektronisches Überwachungssystem, nicht nur für den Verkehrsbereich, zu schaffen. In Zukunft werden Abgleiche mit dem bereits vorhandenen Verkehrszentralregister sowie dem zentralen Fahrzeugregister durch die mit diesem Zentralregister über automatisierte Abrufverfahren verbundenen öffentlichen Stellen möglich sein. Darüber hinaus erhalten mit Inkrafttreten der Änderung des StVG die hierfür zuständigen öffentlichen Stellen der EU-Mitgliedstaaten Zugriff auf das zentrale Fahrerlaubnisregi-

ster. Die Schaffung eines europäischen Verkehrszentralregisters, das der Kontrolle durch die Landesdatenschutzbeauftragten entzogen wäre, könnte dann am Ende dieser Entwicklung stehen.

14.8 Kontrolle einer Führerscheinstelle

Im Berichtszeitraum wurde eine Führerscheinstelle der datenschutzrechtlichen Prüfung unterzogen. Dabei wurde neben allgemeinen technischen und organisatorischen Mängeln festgestellt, daß die Führerscheinakten ohne belastenden Inhalt in verschließbaren Schränken aufbewahrt wurden, während aus Platzgründen die Akten mit belastendem Inhalt in offenen Regalen gelagert waren. In den Akten mit belastendem Inhalt sind u. a. ausführliche medizinisch-psychologische Gutachten (MPU-Gutachten), die meistens hochsensible medizinische und psychologische Daten (Anamnesen, Labordaten etc.) über den Betroffenen enthalten. Ich hatte der Führerscheinstelle dringend empfohlen, diese Führerscheinakten in verschließbaren Schränken aufzubewahren, zumal die MPU-Gutachten den Akten nicht in verschlossenen Umschlägen beigefügt waren. Die Führerscheinstelle sah zunächst die Erforderlichkeit für die zu treffenden Maßnahmen nicht, ist jedoch zwischenzeitlich meiner Empfehlung gefolgt und bewahrt die Akten in verschließbaren Schränken auf, wobei die MPU-Gutachten in verschlossenen Umschlägen beigefügt werden.

Außerdem hatte ich die im Landratsamt getroffene Anweisung für den Umgang mit eingehender Post beanstandet. Darin war geregelt, daß alle Posteingänge von der zuständigen Poststelle geöffnet, registriert und nach den jeweiligen Zuständigkeitsbereichen über die Amtsleiter an die Sachbearbeiter weitergeleitet werden. Die Post wurde dann per Boten unverschlossen zwischen den mehrere Kilometer voneinander getrennten Gebäuden transportiert. Da die für die Führerscheinstelle eingehende Post auch besonders sensible Daten (MPU-Gutachten, BZR- und VZR-Auskünfte) enthält, verletzt die Postverteilung insoweit die Vorschriften des § 9 Abs. 3 ThürDSG. Danach sind von der Stelle Maßnahmen zu treffen, die verhindern, daß Unbefugte bei der Bearbeitung, dem Transport und der Vernichtung auf Daten zugreifen können. In der Verwaltungsvorschrift zum Vollzug des ThürDSG wird unter 9.3 näher ausgeführt, daß eingehende Schreiben an Stellen, die besonders sensible Daten verarbeiten, ungeöffnet an den Adressaten weiterzuleiten sind. Entsprechendes gilt auch für den Postverkehr innerhalb einer Behörde. Die Dienst- und Geschäftsanweisung wurde in dieses Punkten entsprechend geändert. Für die Weiterleitung der Post werden zwischen Post- und Führerscheinstelle jetzt verschlossene Transportbehälter benutzt.

Zusätzlich hatte ich die Führerscheinstelle darauf hingewiesen, daß die auf den aus der DDR stammenden Karteikarten von Fahrerlaubnisinhabern gespeicherte Personenkennzahl, nach der Übernahme von erforderlichen Daten gemäß § 16 Abs. 1 Nr. 2 ThürDSG zu löschen ist. Dies wurde zugesichert.

14.9 Kein „Wiederholungstäterregister“ von Parksündern

Im 1. TB (14.2.2) habe ich berichtet, daß ich eine regelmäßige Speicherung von Wiederholungsfällen bei Verstößen im ruhenden Straßenverkehr mangels einer Rechtsgrundlage für unzulässig halte. Eine seinerzeit durchgeführte Nachfrage bei verschiedenen Ordnungsämtern ergab, daß Daten aus Ordnungswidrigkeitenverfahren ausschließlich zu Rechnungsprüfungszwekken aufbewahrt werden, jedoch nicht zur Mehrfachtäterahndung herangezogen werden. Im Berichtszeitraum habe ich erfahren, daß in einer kreisfreien Stadt Fahrzeughalter aufgrund von wiederholten Parkverstößen aufgefordert worden sein sollen, ein MPU-Gutachten zu ihrer Fahreignung beizubringen. Daraufhin habe ich mir die Verfahrensweise im Umgang mit Daten von

Parksündern im betreffenden Ordnungsamt genauer angesehen. Zur Abwicklung der Verkehrsordnungswidrigkeiten im ruhenden Verkehr wird ein EDV-Verfahren eingesetzt. Nach Feststellen des Parkverstoßes durch die Außendienstmitarbeiter wird das Kfz-Kennzeichen, die Tatzeit, der Tatort sowie der Tatbestand in ein tragbares Erfassungsgerät eingegeben und die Daten nach Rückkehr im Ordnungsamt auf eine Feststation des Zentralrechners überspielt. Von dort aus werden in regelmäßigen Abständen Disketten an das Kraftfahrtbundesamt nach Flensburg geschickt, um den Namen und die Anschrift des Halters zu erfragen. Da es bei den Verkehrsordnungswidrigkeiten relativ kurze Verjährungsfristen gibt (in der Regel 3 Monate), habe ich diese Verfahrensweise akzeptiert, obwohl eine Halterabfrage für die Fälle nicht notwendig wäre, in denen die Halter ihr Verwarnungsgeld zeitnah bezahlen. Nach Auskunft des Ordnungsamtes würden aber auch bereits getätigte Überweisungen kurz vor Ablauf der Verjährungsfrist widerrufen, um nach Eintritt der Verjährung das Verwarnungsgeld letztlich nicht bezahlen zu müssen. Würde erst zu diesem Zeitpunkt eine Halterabfrage erfolgen, käme das Ergebnis möglicherweise zu spät. Erfolgt also die Zahlung innerhalb von drei Wochen nach der Tat, werden die Daten aus dem Computer gelöscht. Wird nicht bezahlt, erfolgt eine schriftliche Verwarnung an den zwischenzeitlich über das Kraftfahrtbundesamt ermittelten Halter, wobei ein Anhörungsbogen vom Halter auszufüllen und an das Ordnungsamt zurückzusenden ist. Die Gestaltung dieses Anhörungsbogens wurde auf meine Forderung hin zwischenzeitlich vom Ordnungsamt umgestaltet. Insbesondere sind diejenigen Angaben, die freiwillig erfolgen, als solche nunmehr ausdrücklich gekennzeichnet, um beim Betroffenen nicht den Eindruck zu erwecken, er sei zu diesen Angaben verpflichtet. Kommt es zu einer schriftlichen Verwarnung, wird im Ordnungsamt ein schriftlicher Vorgang angelegt. Die Ablage dieser Vorgänge erfolgt nicht nach Namen, sondern nach fortlaufenden Nummern, so daß bei der Vielzahl der Vorgänge eine systematische Auswertung in Papierform mit vertretbarem Aufwand nicht möglich ist. Bis zum rechtskräftigen Abschluß des Verfahrens können jedoch über das EDV-Programm bei Eingabe des Namens alle Verwarnungen oder Bußgelder, die noch nicht bezahlt worden sind, aufgerufen werden. Sofern es zu einem rechtskräftigen Bußgeldbescheid kommt, das Bußgeld aber wiederum nicht vom Betroffenen bezahlt wird, bleiben die zugehörigen Angaben ggf. bis zum Ablauf der Vollstreckungsverjährung (nach drei Jahren) andernfalls bis zur Vollstreckung des Bußgeldes in diesem Verfahren abrufbar. Begründet wurde das vom Ordnungsamt mit der Notwendigkeit, den Eingang von Zahlungen bei der Stadtkasse den einzelnen Verfahren zuordnen zu können. Zusammengefaßt heißt das: Wer ein „Knöllchen“ bekommen hat und das Verwarnungsgeld innerhalb von drei Wochen an die Stadt zahlt, wird nur vorübergehend in einem EDV-Verfahren gespeichert. Dagegen erfolgt eine längere und zusammengefaßte Speicherung bei denjenigen, die ihre Verwarnungsgelder und später Bußgelder trotz Feststellung der Rechtmäßigkeit der Forderung nicht bezahlen.

Von dem Ordnungsamt werden mehrfache Verstöße gegen Vorschriften des ruhenden Verkehrs nicht zu einer möglichen Erhöhung eines Verwarnungsgeldes in einem Wiederholungsfall herangezogen. Dies wäre auch nicht zulässig, da das Verwarnungsverfahren ein summarisch vereinfachtes Verfahren darstellt, bei dem Schuld oder Unschuld des Betroffenen nicht geprüft wird. Nach der Rechtsprechung des Bundesverwaltungsgerichts können allerdings hartnäckige und wiederholte Verstöße gegen Vorschriften im ruhenden Verkehr Zweifel an der Eignung zum Führen von Kraftfahrzeugen begründen. Hierzu wird vom Ordnungsamt bei Vorliegen gehäufter Verstöße gegen die Parkvorschriften eine Mitteilung an die Führerscheinstelle im selben Amt gegeben, daß Zweifel an der Eignung des Betroffenen zum Führen von Kraftfahrzeugen bestehen. Dabei wird ausschließlich auf nicht vollstreckte rechtskräftige Bußgeldbescheide zurückgegriffen. Fälle nicht be-

zahlter Verwarnungsgelder bzw. noch nicht rechtskräftig abgeschlossene Bußgeldverfahren bleiben hierbei unberücksichtigt. Weil es sich bei den Bußgeldern im Zusammenhang mit Verstößen gegen Vorschriften des ruhenden Verkehrs um Verfehlungen handelt, die nicht ins Verkehrszentralregister eingetragen werden, erscheint es fraglich, ob Eignungsbedenken systematisch aus einem EDV-Verfahren genutzt werden dürfen, das lediglich noch zur Abwicklung von nicht vollstreckten Bußgeldbescheiden diese Angaben enthält. Da es sich hierbei wohl nur um Ausnahmefälle handeln dürfte, habe ich insoweit gegenüber dem Ordnungsamt meine Bedenken zurückgestellt, wenn sichergestellt ist, daß eine Mitteilung an die Führerscheinstelle nur bei gehäuften, durch rechtskräftige Bußgeldbescheide geahndete Parkverstöße erfolgt.

14.10 Der „Kuckuck“ mit der Schuldnerkralle

Wie aus einem Presseartikel zu erfahren war, haben einige Gemeinden und Städte in der Bundesrepublik Deutschland, und so auch in Thüringen, „das Auto“ zum Eintreiben von Schulden entdeckt. Bei der „Schuldnerkralle“ handelt es sich um eine aus Metall bestehende Vorrichtung, die um den Reifen eines Kfz montiert wird und jede Weiterfahrt verhindert. Um Schäden an dem Fahrzeug bei einem Wegfahrversuch zu vermeiden, wird in der Regel ein deutlich sichtbarer Aufkleber und/oder ein Pfandsiegel auf die Scheibe der Fahrertür angebracht. Ich habe gegenüber dem TIM vertreten, daß durch die Pfändung eines im öffentlichen Straßenraum abgestellten Kfz diese Vollstreckungsmaßnahme gegen den Halter des Fahrzeugs durch das sichtbare Anlegen der „Schuldnerkralle“ sowie das Anbringen des Pfandsiegels insoweit öffentlich gemacht wird, als diejenigen Personen, die das Fahrzeug und dessen Halter kennen, Kenntnis von dieser Vollstreckungsmaßnahme erhalten können. Diese Maßnahme ist deshalb geeignet, das Ansehen der Person herabzusetzen und stellt durch die sogenannte „Prangerwirkung“ einen Eingriff in das Persönlichkeitsrecht dar. Eine solche Maßnahme halte ich jedoch nur dann für gerechtfertigt, wenn sie auf gesetzlicher Grundlage (§ 286 Abs. 2 AO i. V. m. § 38 ThürVwZVG) erfolgt und verhältnismäßig ist. Mit anderen Worten, wenn nicht mit Kanonen auf Spatzen geschossen wird. Sind demnach andere dem Wert der Forderung entsprechende Vermögensgegenstände vorhanden, stellt der Einsatz der Schuldnerkralle wegen einer geringfügigen Forderung eine unzulässige Überpfändung dar, die auch die damit verbundene Einschränkung des Persönlichkeitsrechts nicht rechtfertigt und aus datenschutzrechtlicher Sicht unzulässig wäre. Der Verhältnismäßigkeitsgrundsatz gebietet es ebenfalls, daß im Rahmen der Ermessensausübung durch den Vollstreckungsbeamten die für das informationelle Selbstbestimmungsrecht des Schuldners mildeste Vollstreckungsart gewählt wird, d. h. der Einsatz der Schuldnerkralle mit der damit verbundenen Bloßstellung nur dann erfolgen darf, wenn auf keine Gegenstände zugegriffen werden kann, die sich nicht im öffentlichen Raum befinden. Das TIM hat mir mitgeteilt, daß es meine datenschutzrechtliche Bewertung bezüglich des Einsatzes der Schuldnerkralle teilt.

14.11 Fahrgastbefragung zur Ermittlung der Reiseweite im Ausbildungsverkehr

Ich wurde durch einen Presseartikel auf den Fragebogen eines Verkehrsbetriebs aufmerksam, der im Zusammenhang mit der Beantragung von ermäßigten Monatskarten im Ausbildungsverkehr ausgeteilt wurde. Weder dem Fragebogen noch anderen Informationsquellen in den Ausgabestellen war zu entnehmen, ob es sich um eine freiwillige oder zwangsweise Erhebung handelt und welche Rechtsvorschriften diese erlaubt oder anordnet. Hintergrund für die Erhebung ist die Tatsache, daß ein Verkehrsunternehmen eine erhöhte Ausgleichszahlung vom Land erhält, wenn es nachweisen kann, daß der

zugrundeliegende Durchschnittswert der Beförderungsweite um mehr als 25 % nach oben abweicht. Gemäß § 45a Personenbeförderungsgesetz (PBefG) - in der Fassung der Bekanntmachung vom 8. August 1990 (BGBl I, S. 1690) hat ein Verkehrsunternehmen einen Anspruch auf Ausgleich, wenn ihm durch den Verkauf von ermäßigten Zeitkarten im Ausbildungsverkehr ein Verlust entsteht. Nach Angaben des Verkehrsbetriebes wurde der vorliegende Erhebungsbogen vom TMWI überprüft und genehmigt. Das TMWI ging davon aus, daß die Fahrgastbefragung zum Nachweis der Abweichung von der mittleren Reiseweite gemäß § 3 Abs. 5 Personenbeförderungsausgleichsverordnung (PBerfAusglV) - vom 2. August 1977 (BGBl I, S. 1460) erforderlich sei. Da sich aus den o. g. Rechtsgrundlagen unmittelbar keine Erhebungsbefugnis ergibt und auch die Voraussetzungen des § 28 BDSG (Erhebung nach Treu und Glauben) als Auffangvorschrift nicht vorlagen, weil kein Hinweis auf die Freiwilligkeit angebracht war, wurde die Durchführung der Fahrgastbefragung von mir beanstandet. Der Verkehrsbetrieb stellte daraufhin die Fragebogenaktion unmittelbar ein und ich stimmte zu, daß die bisher bereits ausgefüllten Fragebogen bis zu einer endgültigen rechtlichen Klärung verschlossen aufbewahrt wurden. Es wurde vorgeschlagen, den Namen, die Anschrift und die Unterschrift von den Daten über die Ein- und Ausstiegshaltestelle zu trennen und die Teile mit einer Codenummer zu versehen, damit ein nachträgliches Zusammenführen und eine Prüfung im Einzelfall jederzeit möglich wäre, die eigentlich benötigte Streckenlänge zwischen der Ein- und Ausstiegshaltestelle aber ohne Personenbezug ausgewertet werden kann.

Zur Durchführung einer zukünftigen Fahrgastbefragung hat der Verkehrsbetrieb den Entwurf des neugestalteten Antragsformulars zur datenschutzrechtlichen Prüfung übersandt. Ich habe gefordert, den Betroffenen Hinweise zum Ausfüllen des Erhebungsbogens zu geben, insbesondere, daß die Daten nicht für andere Zwecke verarbeitet oder genutzt werden dürfen. Außerdem habe ich verlangt, in die Tarifbestimmungen eine entsprechende Verpflichtung mit aufzunehmen, wonach die Antragsteller von Monatskarten im Ausbildungsverkehr die Angaben auf dem Fragebogen auszufüllen haben. Die Anregungen werden bei der nächsten Fragebogenauflage berücksichtigt.

14.12 Datenübermittlung zwischen Wohnungsgesellschaft und Sozialamt

Im 1. TB (14.3.6) hatte ich für die Datenübermittlung zwischen einer Wohnungsgesellschaft und dem Sozialamt bei Mietschuldnern gefordert, daß der Mieter auf die Möglichkeit eines Widerspruchs gegen die Übermittlung seiner personenbezogenen Daten an das Sozialamt hingewiesen wird. Zwischenzeitlich werden alle Mietschuldner der Wohnungsgesellschaft, die sich in einem größeren Mietrückstand befinden, über § 28 BDSG als Rechtsgrundlage für die bevorstehende Datenübermittlung an das Sozialamt unterrichtet. Gleichzeitig wird diesen Mietern eine 14-tägige Frist eingeräumt, dieser Datenübermittlung zu widersprechen. Ich habe die Wohnungsgesellschaft darüber hinaus nochmals darauf hingewiesen, daß vorab zu prüfen ist, ob überhaupt Anhaltspunkte für eine Hilfsbedürftigkeit des Mieters vorliegen.

14.13 Aushang einer Hausordnung in einem Familienübergangshaus

Mir lag eine Eingabe vor, wonach sich der Mieter eines Hauses dagegen wehrte, daß in seinem Haus eine Hausordnung ausgehängt wurde, aufgrund deren Inhalt die Bewohner als Sozialhilfeempfänger offenbart wurden. Problematisch war es deshalb, weil es sich um ein Familienübergangshaus handelt, in dem die Bewohner nur eine vorübergehende Wohnberechtigung

erhalten und somit keine dauerhaften Mietverhältnisse bestehen, jedoch aufgrund der teilweise langen Aufenthaltsdauer (z. T. über Jahre) am Gebäude bzw. an den Wohnungen die Briefkästen- und Klingelschilder die Namen der Bewohner tragen. Da es sich um ein Gebäude einer kommunalen Wohnungsgesellschaft handelte, zahlte das Sozialamt dem Eigentümer entsprechende Nutzungsentgelte für den Wohnraum und die Betriebskosten. Nach Prüfung der im Hausflur angebrachten und somit im beschränkten Maß öffentlich zugänglichen Hausordnung fand ich die Angaben des Petenten zum Inhalt bestätigt. Ich habe daraufhin der Stadtverwaltung mitgeteilt, daß nach meiner Auffassung der Inhalt und das öffentliche Aushängen der Hausordnung durchaus geeignet sind, Dritten gegenüber Daten unbefugt zu offenbaren. Die Hausordnung enthielt Einzelangaben über persönliche und sachliche Verhältnisse der Bewohner in der Form, daß unmißverständlich darüber informiert wurde, daß es sich bei den Bewohnern um Personen handelt, die obdachlos sind und deshalb vom Ordnungsamt in dieses Familienübergangshaus eingewiesen wurden. Im Gegensatz zu üblichen Obdachloseneinrichtungen, in denen die Benutzer ständig wechseln und sich im Regelfall nur stundenweise darin aufhalten, wohnen im Übergangshaus die eingewiesenen Personen als Nutzer von Übergangswohnungen für einen unbestimmten Zeitraum. Dementsprechend werden die Bewohner ordnungsgemäß melderechtlich erfaßt sowie postalisch, in Einzelfällen sogar telefonisch, dieser Anschrift zugeordnet. Daneben werden die Namen der Bewohner auf den Briefkästen, Klingeln oder Wohnungstüren dokumentiert. Dies führt dazu, daß die Hausordnung aufgrund ihres Inhaltes personenbezogene Daten offenbart. Da sie in dem Gebäude öffentlich ausgehängt wird, so daß jeder Besucher Kenntnis von dem darin enthaltenen Daten nehmen kann, stellt die Bekanntmachung eine Datenübermittlung im Sinne des ThürDSG dar. Allein aus dem Inhalt der Hausordnung ergibt sich aufgrund der Bezeichnung und Zuordnung des Gebäudes und der darin enthaltenen Regelungen, daß es sich um Bewohner handelt, die Sozialleistungen nach den Bestimmungen des Sozialgesetzbuches zur Sicherung eines menschenwürdigen Daseins sowie zum Ausgleich besonderer Belastung des Lebens empfangen. Eine Übermittlung dieser Daten ist nur im Rahmen der gesetzlichen Bestimmungen unter Beachtung der Erforderlichkeit zulässig. Ich habe deshalb empfohlen, künftig nur noch den Hausbewohnern persönlich die Hausordnung zu übergeben. Soweit man es darüber hinaus für erforderlich hielt, sollte man darüber hinaus einen Auszug der Hausordnung im Gebäude anbringen unter der Maßgabe, daß darin Informationen, aus denen sich der soziale Status der Hausbewohner ergeben könnte, nicht enthalten sind. Meiner Empfehlung entsprechend wurde von der Stadtverwaltung festgelegt, daß die bisherige Hausordnung nicht mehr zum Aushang gelangt.

14.14 Führung von Wohnungskarteikarten

Bis Ende 1989 führten die Gemeinden zum Zweck der Wohnraumlenkung und der Wohnungsbestandsfortschreibung Wohnraumkarteien. In den Kreisen bildeten diese die Grundlage für den Datenspeicher Wohnungspolitik. In meinem 1. TB (14.3.1) hatte ich bereits darauf hingewiesen, daß ich den weiteren Umgang mit diesen Unterlagen in der Folgezeit überprüfen werde. Die nunmehr durchgeführten Kontrollen in kleineren Städten und Gemeinden ergab, daß dort aufgrund fehlender weiterer Aufgaben die Karteien zwischenzeitlich, soweit keine Archivierung erfolgte, vernichtet wurden. In einer kreisfreien Stadt waren demgegenüber nur die Unterlagen, die dem privaten Bereich betrafen 1991/1992 ausgesondert und dem Kommunalarchiv übergeben worden. Die übrigen Wohnungskarteikarten des ehemaligen Datenspeichers Wohnungspolitik wurden zur Nachweisführung über den belegungsgebundenen Wohnraum zur Umsetzung des Thüringer Gesetzes über die Gewährleistung von Belegungsrechten im kommunalen Wohnungsbau weiterhin genutzt. Nicht mehr erforderliche Daten, insbesondere hinsichtlich

der Angaben früherer Mieter und weiterer Hinweise zur Wohnungsvergabe waren zwar gestrichen (gesperrt) jedoch nicht gelöscht worden. Da aufgrund des Thüringer Belegungsrechtegesetzes (ThürBelRechtG) vom 8. Dezember 1995 (GVBl S. 360) ohnehin der Umfang der belegungsgebundenen Wohnungen ab 1996 wesentlich reduziert werden sollte, hatte man bisher von einer weiteren Aussonderung der nicht mehr benötigten Karteikarten abgesehen. Zum Zeitpunkt der Kontrolle stand der Beschluß des Stadtrates zur konkreten Benennung der künftigen belegungsgebundenen Wohnungen gemäß § 3 ThürBelRechtG noch aus. Im Ergebnis meiner Prüfung wurde deshalb festgelegt, daß unmittelbar nach der Beschlußfassung die Aussonderung der Kartei (was zwischenzeitlich bereits erfolgt ist) dahingehend vorgenommen wird, daß künftig darin nur noch Karteikarten für den belegungsgebundenen Wohnraum zur gesetzlich vorgeschriebenen Nachweisführung enthalten sind. Die nicht mehr benötigten Unterlagen sollten dem Archiv übergeben werden. Gleichzeitig wurde gefordert, die alten Karteikarten durch neue, ohne Übernahme der gesperrten Daten, zu ersetzen.

14.15 Erarbeitung von Mietspiegeln

In Vorbereitung der Erstellung von Mietspiegeln in Thüringen hatte mich das TMWI gebeten, hierzu aus datenschutzrechtlicher Sicht Stellung zu nehmen. Ich habe die Verantwortlichen der Landkreise und der größeren Kommunen darauf hingewiesen, daß die Erarbeitung und Veröffentlichung eines sogenannte einvernehmlich festgestellten Mietspiegels als Ergebnis einer Verhandlung von Interessenvertretern der Vermieter und Mieter mit und ohne Beteiligung der Gemeinde datenschutzrechtlich unproblematisch ist, solange ausschließlich aggregierte und nicht mehr einer einzelnen konkreten Wohnung zuordenbare Daten genutzt werden. Verständigen sich die Interessenvertreter auf der Grundlage des ihnen jeweils vorliegenden eigenen Datenmaterials bei bestimmten Wohnungsgruppen auf „von - bis Spannen“ zur Miethöhe, werden personenbezogene Daten nicht offenbart und das Recht auf informationelle Selbstbestimmung der Mieter als auch der Vermieter nicht beeinträchtigt. Da nur Durchschnittswerte veröffentlicht werden und sogenannte „Ausreißermieten“ unberücksichtigt bleiben, können aus diesen Angaben im Einzelfall für einen speziellen Vermieter oder Mieter nicht der Mietpreis oder bestimmte Vermögensverhältnisse abgeleitet werden. Datenschutzrechtlich relevant ist demgegenüber die Erstellung eines sogenannten repräsentativen Mietspiegels. Das ergibt sich daraus, daß nicht auf bereits aggregierte Daten von Wohnungsgesellschaften zurückgegriffen wird, sondern zur Wahrung der Repräsentativität in jedem Fall zusätzliche Erhebungen bei sonstigen privaten Vermietern erforderlich werden. Werden personenbezogene Einzelangaben von Mietern oder Vermietern an Dritte übermittelt oder durch Dritte erhoben, verarbeitet oder genutzt, sind die einschlägigen datenschutzrechtlichen Bestimmungen zu beachten. Eine Rechtsgrundlage für eine zwangsweise Erhebung dieser Daten existiert nicht. Aus den Auffangvorschriften zum Datenschutz ergibt sich, daß ohne eine entsprechende Rechtsnorm die Erhebung, Verarbeitung und Nutzung der Daten nur auf freiwilliger Grundlage erfolgen kann. Da der Mieter im Regelfall eine schutzwürdiges Interesse am Ausschluß der Übermittlungen haben wird, wäre eine Übermittlung der Daten von Seiten des Vermieters ohne Einwilligung des Mieters nicht zulässig. Gemäß § 22 ThürStatG können unter bestimmten Bedingungen die Gemeinden für die Wahrnehmung ihrer Aufgaben im Rahmen ihrer Zuständigkeiten und Befugnisse Statistiken durchführen. Hierfür sind auf Gemeindeebene zur Erstellung repräsentativer Mietspiegel entsprechende Satzungen zu beschließen, so daß auch eine Auskunftspflicht der Mieter bzw. der Vermieter angeordnet werden kann. Dadurch wird auch für die Erhebung der Daten dem rechtsstaatlichen Gebot der Normenklarheit Rechnung getragen. Zu beachten ist, daß die einzelnen Datensätze der statistischen Geheimhaltung unterliegen und dementsprechend

nur in anonymisiertem, aggregiertem Zustand des Mietspiegel veröffentlicht werden dürfen. Eine Nutzung der Einzeldaten zur Fortschreibung sowie zur Benennung von Vergleichswohnungen ist selbstverständlich unzulässig. Gleichfalls verbietet sich ohne Zustimmung der betroffenen Mieter und Vermieter die Führung von objektkonkreten Datenbanken, da hierzu keine entsprechende Rechtsvorschrift besteht.

14.16 Datenübermittlung für Vermessungszwecke

Ein Thüringer Bürger hat im Berichtszeitraum die Frage an mich herangetragen, ob es datenschutzrechtlich zulässig sei, zur Durchführung des Einmessungsverfahrens die Anzeige der abschließenden Fertigstellung nach § 79 Abs. 1 ThürBO mit personenbezogenen Daten des Bauherrn von der unteren Bauaufsichtsbehörde an das Katasteramt zu übermitteln. Da keine Spezialvorschrift existiert, die eine Verpflichtung der unteren Bauaufsichtsbehörde enthält, wie beschrieben zu verfahren, beurteilt sich die Angelegenheit nach den §§ 21 Abs. 1, 20 Abs. 2 Ziffer 3 ThürDSG. Die Übermittlung war hier zur Erfüllung der Aufgaben des Katasteramtes erforderlich, da die Führung des Liegenschaftskatasters Aufgabe des Katasteramtes ist und die Errichtung eines Bauwerkes die Notwendigkeit der Aufnahme dieses Bauwerkes in das Kataster mit sich bringt. Meines Erachtens wird man gemäß § 20 Abs. 2 Ziffer 3 ThürDSG davon ausgehen können, daß es offensichtlich ist, daß dies im Interesse des Betroffenen liegt und kein Grund zu der Annahme besteht, daß er in Kenntnis der anderen Zwecke seine Einwilligung verweigern würde. Auf diese Weise kann sichergestellt werden, daß er von seiner Verpflichtung nach § 11 Abs. 2 ThürKatG Kenntnis erhält, als Gebäudeeigentümer dem Katasteramt die für die Führung des Liegenschaftskatasters erforderlichen Angaben zu machen und die entsprechenden, in seinem Besitz befindlichen Unterlagen vorzulegen. Ich habe dem Anfragenden deshalb mitgeteilt, daß dieses Verfahren keinen datenschutzrechtlichen Bedenken unterliegt.

14.17 Erhebungen von personenbezogenen Daten bei Zweckverbänden

Zahlreiche Eingaben von Bürgern erreichten mich im Zusammenhang mit den von den Zweckverbänden, und hier insbesondere den Wasser- und Abwasserzweckverbänden, erhobenen personenbezogenen Daten zur Berechnung von Beiträgen und Gebühren. In der Regel werden die betroffenen Eigentümer von den Zweckverbänden angeschrieben und um das Ausfüllen der beigefügten Erhebungsbögen, sogenannte Selbstauskunftsbögen, gebeten. Verschiedene Zweckverbände fordern vom Eigentümer zusätzlich noch die Beifügung von Kopien des Grundbuchauszuges sowie den Lageplan des Grundstücks. Einige Zweckverbände weisen vorsorglich darauf hin, daß die vom Bürger erteilten Auskünfte stichprobenartig durch Abgleiche mit dem Liegenschaftskataster auf ihren wahrheitsgemäßen Inhalt überprüft werden. Bei der datenschutzrechtlichen Prüfung von Fragebögen stellte ich häufig fest, daß der Betroffene entgegen den Bestimmungen des § 19 Abs. 3 ThürDSG nicht auf die Rechtsvorschriften hingewiesen wird, die ihn zur Auskunft verpflichten. Wenn diese Aufklärungspflicht von Seiten des Zweckverbandes unterblieben ist, muß ein solcher Hinweis nachgeholt werden. Weitergehende Rechtsfolgen lassen sich aber hieraus nicht ableiten. Insbesondere wird die Zulässigkeit der Erhebung sowie die nachfolgende Verarbeitung der personenbezogenen Daten damit nicht beeinträchtigt, wenn die Angaben aufgrund einer Rechtsgrundlage erhoben wurden, die zur Auskunft verpflichtet. Eine detaillierte Überprüfung der Angaben auf verschiedenen Fragebögen hat teilweise ergeben, daß aus den erlassenen Satzungen der Erhebungsgrund verschiedener personenbezogener Daten nicht hervorgeht. Wenn die Erforderlichkeit der Erhebung eines bestimmten Datums

nicht gegeben ist, kann der Betroffene deshalb nicht verpflichtet werden, diese Auskunft zu erteilen. Hat in diesem Falle der Zweckverband nicht auf die Freiwilligkeit der Angaben hingewiesen bzw. muß der Betroffene davon ausgehen, daß er zur Angabe dieser Daten verpflichtet ist, so war die Erhebung dieses Datums unzulässig und muß gemäß § 16 Abs. 1 Nr. 1 ThürDSG gelöscht oder gemäß § 15 Abs. 1 Nr. 2 ThürDSG gesperrt werden.

Als Rechtsgrundlage für die Erhebung der personenbezogenen Daten zur Berechnung von Beiträgen und Gebühren sind § 2 und §§ 7 ff. Thüringer Kommunalabgabengesetz (ThürKAG) in Verbindung mit der jeweiligen vom Zweckverband erlassenen Satzung maßgeblich. Die Forderung einiger Zweckverbände nach Beifügung von weiteren Kopien, wie des Grundbuchauszuges oder des Lageplanes, ist in § 7 Abs. 14 ThürKAG geregelt. Die Grundstückseigentümer werden hierin „dazu verpflichtet, auf Verlagen der beitragsberechtigten Körperschaft die für die Berechnung der Vorauszahlung, Vorschüsse und Beiträge erheblichen Tatsachen vollständig und wahrheitsgemäß offenzulegen und die ihnen bekannten Beweismittel anzugeben.“ Die Mitwirkungspflicht des Betroffenen wird in § 15 Abs. 1 Nr. 3a ThürKAG in Verbindung mit § 97 Abs. 2 Abgabenordnung (AO) konkretisiert. Entsprechend § 97 Abs. 1 AO kann der Zweckverband von den Betroffenen die Vorlage von Büchern, Aufzeichnungen und anderen Urkunden verlangen. Dieses soll aber nach Abs. 2 nur verlangt werden, wenn der Vorlagepflichtige eine Auskunft nicht erteilt hat, wenn die Auskunft unzureichend ist oder Bedenken gegen ihre Richtigkeit bestehen. Ich habe deshalb gegenüber den betroffenen Zweckverbänden vertreten, daß nur in Fällen, in denen begründete Zweifel an der Richtigkeit der im Erhebungsbogen gemachten Angaben bestehen, Kopien, z. B. des Grundbuchauszuges und des Lageplanes, verlangt werden können und der Auskunftspflichtige die dabei entstehenden Kosten tragen muß. Eine prinzipielle Erforderlichkeit regelmäßig Grundbuchauszüge u. ä. auf eigene Kosten vorlegen zu müssen, sehe ich nicht.

Klärungsbedarf bestand auch zu der Frage, ob die Einsichtnahme in das entsprechende Liegenschaftskataster durch den Zweckverband, ohne daß der Betroffene hiervon Kenntnis erlangt hat, zulässig ist. Hierzu ist auszuführen, daß jeder, der ein berechtigtes Interesse darlegt, das Liegenschaftskataster und seine Unterlagen gemäß § 9 Abs. 1 Thüringer Katastergesetz (ThürKatG) einsehen sowie Auskunft daraus erhalten kann. Weiterhin können gemäß § 10 Abs. 1 ThürKatG Daten aus dem Liegenschaftskataster regelmäßig an Behörden und sonstige öffentliche Stellen übermittelt werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.

14.18 Datenerhebung bei der Abfallentsorgung

Entsorgungspflichtige Körperschaften im Sinne des § 3 Abs. 2 Abfallgesetz (AbfG) sind gemäß § 2 Abs. 1 Thüringer Abfallwirtschafts- und Altlastengesetz (ThAbfAG) die Landkreise und kreisfreien Städte. Sie können durch Satzung gemäß § 4 ThAbfAG festlegen, wie ihnen die Abfälle zu überlassen sind und erheben als Gegenleistung für die Inanspruchnahme ihrer öffentlichen Einrichtung Benutzungsgebühren nach den Vorschriften des Thüringer Kommunalabgabengesetzes. Im Bestreben, eine immer gleichmäßigere und gerechtere Lastenverteilung bei der Müllentsorgung zu erreichen, werden immer neue Verfahren entwickelt, die gleichfalls Veränderungen bei der Erhebung und Verarbeitung von Daten der Anschluß- bzw. Benutzungspflichtigen bei der Abfallentsorgung nach sich ziehen. In der letzten Zeit ist deshalb eine Zunahme von Anfragen und Eingaben betroffener Bürger zu Fragen der Datenerhebung und -verarbeitung im Rahmen der Umsetzung von Abfallsatzungen und Abfallgebührensatzungen festzustellen. Als Ursachen stellen sich insbesondere mißverständliche bzw. nicht normenklare Regelun-

gen oder fehlende Definitionen in den Satzungen ebenso wie nicht rechtzeitige oder mangelhafte Information der Betroffenen heraus. Darüber hinaus werden mitunter in Satzungen Bestimmungen, Verfahren oder Vordrucke aufgenommen, bei denen sich mangels einer vorherigen Prüfung erst später bei der praktischen Umsetzung datenschutzrechtliche Probleme ergeben. Nicht selten zeigt sich auch bei der Bearbeitung entsprechender Anfragen und Beschwerden, daß der jeweilige behördeninterne Datenschutzbeauftragte bis zu diesem Zeitpunkt nicht oder nur unzureichend über das jeweilige Verfahren in Kenntnis gesetzt wurde und mit der automatisierten Verarbeitung personenbezogener Daten die datenschutzrechtliche Freigabe gemäß § 34 Abs. 2 ThürDSG und die Datenschutzregistermeldung, nach § 3 Abs. 1 ThürDSRegVO teilweise noch ausstehen.

Überwiegend werden in den Abfall- und Abfallgebührensatzungen als Adressaten und Auskunftspflichtige die Grundstückseigentümer bestimmt und zur Berechnung der Gebühren die Anzahl der auf den Grundstücken gemeldeten Einwohner zugrunde gelegt. Mitunter fordern deshalb die in den Landkreisen für die Abfallgebührenberechnung zuständigen Stellen von den Meldeämtern der Gemeinden regelmäßig aus den Melderegistern Einzeldaten aller Einwohner ab. Dies würde jedoch der Führung eines zweiten Melderegisters entsprechen, obwohl regelmäßig die Abfallbehörde nur die Einzeldaten der Gebührenzahler (z. B. Eigentümer) benötigt. Darüber hinaus würde die regelmäßige Datenübermittlung von den Meldebehörden der Gemeinden an die Abfallbehörden der Landkreise gegen § 29 Abs. 5 ThürMeldeG verstoßen, wonach regelmäßige Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen nur zulässig sind, sofern dies durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zwecks der Übermittlung, der Datenempfänger und der zu übermittelnden Daten bestimmt ist. Soweit ich dies in der Praxis festgestellt habe, wurde gefordert, die regelmäßige personenbezogene Datenübermittlung von den Meldeämtern einzustellen und statt dessen den Gebührenstellen nur noch die Anzahl der jeweils unter dieser Anschrift gemeldeten Personen mitzuteilen.

Aufgrund des im Kreislaufwirtschafts- und Abfallgesetz verwendeten Begriffes „private Haushaltungen“, der dort in unterschiedlichen Regelungen bei der Entsorgung als Unterscheidungskriterium für die Herkunft des Abfalls und nicht zur Definition konkreter Personengruppen (Haushalte) verwendet wird, stellen einige Satzungen bei der Berechnung von Vorhaltemengen und Gebühren z. B. statt auf den Eigentümer/Mieter auf „Haushalte“ ab. Es fehlt aber jeweils eine für die Betroffenen nachvollziehbare eindeutige Definition für den Begriff des „Haushaltes“. Dies stellt sich aber häufig erst in der Praxis heraus, wenn widersprüchliche Aussagen von Eigentümern (oder Gleichgestellten) /Pächtern oder Mietern vorliegen. Durch zusätzliche Befragungen sollen dann die fehlenden Daten erhoben werden. Dies kann letztlich, wie in einem Fall bekannt wurde, dazu führen, daß in einer Gemeinde nur die im Melderegister gespeicherten „Kernfamilien“ (Ehepaare und deren unter gleicher Anschrift gemeldeten Kinder bis zum 27. Lebensjahr) als „Haushalte“ betrachtet und bei der Gebührenberechnung zugrunde gelegt wurden, was z. B. bei nichtehelichen Lebensgemeinschaften zu einer Vielzahl von Einsprüchen führte, weil diese im Melderegister nicht erfaßt sind.

Datenschutzrechtlich bedenklich ist insbesondere die mangelnde Normenklarheit, d.h. wenn in Abfall- und Abfallgebührensatzungen der Umfang und die Auskunftspflicht der Anschluß-, Benutzungs- und Gebührenpflichtigen nicht eindeutig festgelegt wird. Dies verunsichert die Betroffenen hinsichtlich ihrer Pflichten und führt im Ergebnis häufig zu einer Mehrfacherhebung von Daten, weil z. B. Mieter und Eigentümer teilweise sogar sich widersprechende Angaben machen. Desweiteren kann diese Verfahrensweise eine über das Erfordernis hinausgehende Datenerhebung und eine Datenvorratshaltung

zur Folge haben. In Einzelfällen erhalten diese Daten auch mehrere Stellen gleichzeitig (z. B. Landratsamt, Eigenbetrieb der Abfallwirtschaft, privater Entsorgungsbetrieb), ohne daß deren Kenntnis dort in jedem Fall zur Aufgabenerfüllung erforderlich wäre. Soweit ich dies festgestellt habe, wurde von den entsprechenden Stellen die Einhaltung der datenschutzrechtlichen Bestimmungen gefordert.

Zunehmend kommen im Freistaat Thüringen computergestützte Müllerfassungssysteme zur Anwendung. Als Vorteil dieser Systeme werden insbesondere die höhere Kostengerechtigkeit für den einzelnen Bürger sowie die Einschränkung von Verwaltungskosten genannt. Nicht unerwähnt bleiben darf aber, daß soweit die Benutzung der Spezialmüllcontainer nicht durch eine „anonyme“ Gebührenzahlung durch den Einwurf von Gebührenmarken oder der Abbuchung eines Guthabens von einer Chipkarte erfolgt, bei diesen Verfahren zusätzliche Daten wie Entsorgungszeitpunkt, Müllmenge und Entsorger (z. B. Nummer der Chipkarte) im Identifikationsgerät des Müllcontainers gespeichert werden. Soweit diese Daten ausschließlich und zweckgebunden der Müllgebührenberechnungsstelle übergeben werden und die Entsorgungsfirma aus den Daten nicht konkret entnehmen kann, wer der Benutzungspflichtige (Chipkartenbesitzer) ist, bestehen gegen dieses Verfahren grundsätzlich keine Bedenken. Selbstverständlich sind diese Einzeldaten spätestens nach Rechnungslegung und Ablauf der Einspruchsfrist zu löschen. In jedem Fall ist eine Zuordnung des Abfalls zu einem Benutzungspflichtigen nach Abgabe an den Entsorgungsbetrieb etwa durch Kennzeichnung oder Registrierung der Abfallbehältnisse (z. B. Müllsack) unverhältnismäßig und deshalb auszuschließen.

14.19 Datenübermittlung aus dem Emissionskataster an eine Stadtverwaltung

Aufgrund einer Anfrage hatte ich mich mit der Zulässigkeit von Datenübermittlungen aus dem bei der Thüringer Landesanstalt für Umwelt geführten Emissionskataster an eine Kommune zum Zwecke der Erstellung eines Energiekonzepts zu beschäftigen. Das Emissionskataster enthält Einzelangaben über Art, Menge, räumliche und zeitliche Verteilung und die Austrittsbedingungen von Luftverunreinigungen bestimmter Anlagen und Fahrzeuge und wird insbesondere auch für Planungsaufgaben geführt. Hinsichtlich der Datenübermittlung aus dem Kataster an andere Stellen gibt es keine spezialgesetzlichen Regelungen. Nach der allgemeinen Verwaltungsvorschrift zum Bundes-Imissionsschutzgesetz (BImSchG) - in der Fassung der Bekanntmachung vom 14. Mai 1990 (BGBl I, S. 880) können für Untersuchungen in belasteten Schwerpunktbereichen gemäß 4.1 der Vorschrift auch Darstellungen (tabellarisch bzw. kartographisch) mit höherer (als 1 km mal 1 km) räumlicher Auflösung erforderlich sein, so daß die Übermittlung von Einzeldaten an andere Stellen zur Aufgabenerfüllung im Rahmen der Zweckbestimmung der Daten (als Grundlage für Planungsaufgaben) mangels einer speziellen Rechtsvorschrift in Anwendung der Bestimmungen des § 21 Abs. 1 ThürDSG zulässig ist. Entsprechend dem Grundsatz der Verhältnismäßigkeit ist jedoch vor der Übermittlung von Einzeldaten zu prüfen, inwieweit Daten bzw. Karten mit einem entsprechend kleinem Raster zur Aufgabenerfüllung bereits ausreichen. Sollten sich dabei die Notwendigkeit der Übermittlung von Einzeldaten ergeben, ist von der Kommune zu gewährleisten, daß eine Verarbeitung oder Nutzung dieser Daten gemäß § 21 Abs. 3 ThürDSG ausschließlich für den konkreten Zweck erfolgt, für den die Daten übermittelt wurden und die Einzelangaben gelöscht werden, sobald es der Zweck erlaubt. Selbstverständlich darf in den Planungsunterlagen (z. B. Konzeptionen) selbst oder gar in Veröffentlichungen kein Rückbezug auf personenbezogene Daten möglich sein. Soweit eine Verarbeitung und Nut-

zung der Daten durch einen Dritten im Auftrag der Kommune vorgesehen wird, sind die Regelungen des § 8 ThürDSG zu beachten.

14.20 Dorfbiotopkartierung in Thüringen

In einer Eingabe wurde ich darauf aufmerksam gemacht, daß bis 1999 alle Dörfer und Kleinstädte im Freistaat Thüringen aus Gründen der Landschaftsplanung sowie des Arten- und Biotopenschutzes kartiert werden sollen. Da von dieser Kartierung auch Privatgrundstücke betroffen sind, bestehen bei einigen Grundstückseigentümern Bedenken und Rechtsunsicherheiten hinsichtlich der Zulässigkeit des Betretens und Erfassens dieser Grundstücke durch die hierfür zuständigen Stellen. Ich hatte dem Beschwerdeführer mitgeteilt, daß gegen das Betreten der Grundstücke zunächst keine Bedenken bestehen, da diese Duldungspflicht in § 47 Vorläufiges Thüringer Naturschutzgesetz (VorlThürNatG) geregelt ist. Gleichwohl hatte ich mich an das TMLNU gewandt und um Auskunft gebeten, welche personenbezogene Daten von den Grundstückseigentümern erhoben werden und auf welcher rechtlichen Grundlage dies geschieht. In seiner Stellungnahme hat das TMLNU ausgeführt, daß der gesetzliche Auftrag zur Biotopkartierung sich unmittelbar aus § 18 Abs. 2 VorlThürNatG ergibt. Nach der Rechtsprechung begründen Biotopkartierungen mangels unmittelbarer Rechtswirkung nach außen gegenüber den Grundstückseigentümern kein Rechtsverhältnis. Mit anderen Worten ergeben sich für die Eigentümer keine unmittelbaren Rechtsfolgen, insbesondere werden keine Eigentümerrechte beeinträchtigt. Das Erheben von Grundstücksdaten zum Zwecke einer allgemeinen Biotopkartierung sei deshalb zulässig. Aus datenschutzrechtlicher Sicht gehe ich davon aus, daß die erhobenen Daten sich zwar auf einzelne Personen beziehen, diese jedoch nicht ohne weiteres identifizierbar sind. Aus der Kartieranleitung geht nicht hervor, daß Namen und Anschriften von Grundstückseigentümern erfaßt werden, sondern die Lage der Biotope lediglich anhand von topographischen- und Katasterkarten sowie mit Hilfe von Luftbildaufnahmen durch die Vergabe von Flächennummern verzeichnet wird. Selbst wenn nicht auszuschließen ist, daß die Lage von Biotopen einzelnen Eigentümern zuzuordnen ist, werden die Kartierungen aufgrund § 18 Abs. 2 VorlThürNatG und mit Kenntnis des Betroffenen erhoben. Da die in § 19 Abs. 1-3 ThürDSG geforderten Voraussetzungen für eine Erhebung erfüllt sind, bestehen gegen die Biotopkartierungen meinerseits keine Bedenken.

14.21 Kontrolle des ökologischen Landbaus durch private Stellen

Landwirtschaftliche Betriebe, die ökologischen Landbau betreiben, müssen sich nach der Verordnung (EWG) Nr. 2092/91 einem Kontrollverfahren unterwerfen, um ihre Erzeugnisse in der Kennzeichnung oder Werbung als ökologisch beim Verbraucher anbieten zu dürfen.
Der Freistaat Thüringen bedient sich dabei, wie dies auch in anderen Bundesländern der Fall ist, privater Kontrollstellen. Dafür sind in Thüringen zur Zeit 11 private Kontrollstellen tätig. Zugelassen und überwacht werden die Kontrollstellen von der Thüringer Landesanstalt für Landwirtschaft (TLL). Für die Kontrollstellen gelten die Vorschriften des 3. Abschnitts des BDSG sowie die in der Verordnung (EWG) Nr. 2092/91 genannten datenschutzrechtlichen Bestimmungen, wonach keinen anderen Personen als den für den landwirtschaftlichen Betrieb verantwortlichen und den zuständigen staatlichen Stellen Einblick in die Informationen und Daten, von denen sie bei ihrer Kontrolltätigkeit Kenntnis erlangen, gegeben werden darf. Ich habe gegenüber dem TMLNU die Auffassung vertreten, daß die von den privaten Kontrollstellen erhobenen und gespeicherten personenbezogenen Daten der geprüften Betriebe in der gleichen Weise zu schützen sind, wie dies bei einer öffentlichen Stelle der Fall wäre (Aufsicht, Kontrolle, strafrechtliche Folgen bei einer Pflichtverletzung, usw.). Ich halte es deshalb für geboten, alle Per-

sonen, die für die jeweilige private Kontrollstelle tätig werden, nach dem Verpflichtungsgesetz zu verpflichten. Die so verpflichteten Mitarbeiter machen sich dann bei einer Verletzung der Verschwiegenheitspflicht in der gleichen Weise wie Amtsträger strafbar. Die nach dem Verpflichtungsgesetz zuständige Behörde hat jeden Mitarbeiter einzeln zu verpflichten. Die Verpflichtung des Kontrollstellenleiter reicht allein nicht aus, da dieser für das Verhalten seiner ihm nachgeordneten Mitarbeiter nicht verantwortlich gemacht werden kann. Die Thüringer Landesanstalt für Landwirtschaft hat mir mitgeteilt, daß zwischenzeitlich die Kontrollstellenleiter gemäß einer vom TMLNU erlassenen Anordnung des TMLNU (ThürStAnz Nr. 46/1997 S. 2186) durch das TMLNU nach § 1 VerpflichtungsG verpflichtet werden. Die übrigen Mitarbeiter der privaten Kontrollstellen werden auf der Grundlage der „Thüringer Verordnung über die Zuständigkeit für die Verpflichtung von nichtbeamteten Personen nach dem Verpflichtungsgesetz vom 30. August 1996“ (GVBl. Nr. 14 S. 167) durch das TLL verpflichtet. Zur Niederschrift über die förmliche Verpflichtung der Kontrolleure kommt ein vom TMLNU erstelltes Formblatt zur Anwendung.

15. Technischer und organisatorischer Datenschutz

15.1 Entwicklungen und Tendenzen der Informations- und Kommunikationstechnik

Die Informations- und Kommunikationstechnik (IuK) bestimmt wesentlich die Arbeitswelt aber zunehmend auch die Privatsphäre. Der Umgang mit Computern ist zu einem Allgemeingut geworden und nicht mehr auf nur wenige Experten beschränkt.
Die Ausstattung der Arbeitsplätze und privater Haushalte mit eigener Computerintelligenz sowie integrierter Netzanbindung und die Ausweitung von Online-Anwendungen unter Einbindung des Internet prägen die heutige IuK-Infrastruktur.
Anfang dieses Jahrzehnts etablierten sich in der Verwaltung und der Wirtschaft zunehmend Client-Server-Systeme. Mitarbeiter von Fachbereichen konnten an ihrem Arbeitsplatz sowohl auf ihren PC wie auch auf einen zentralen Server zugreifen.
Das Rechenzentrum in seiner bisherigen Form, als abgeschlossene Einheit, scheint überholt zu sein. Viele der einst so starren zentralen Rechenzentren sind zwischenzeitlich durch viele kleine Zentralen an lokalen Standorten abgelöst worden. Mit dieser Entwicklung vollzog sich zwangsläufig auch eine weitgehende Dezentralisierung der zuvor zentral vorgehaltenen Daten. Sowohl in der Verwaltung als auch in der Wirtschaft müssen die benötigten Informationen jederzeit am gewünschten Ort zur Verfügung stehen. Um diese Anforderungen zu realisieren, werden verstärkt Großrechner als leistungsstarke Server in heterogene Netzwerke eingebunden. Hiermit versucht man die Vorteile einer zentralen Verwaltung mit der Flexibilität von Client-Server-Systemen zu verbinden, wobei zwei sich ergänzende Konzepte zur Verfügung stehen. Zum einen handelt es sich um die als Informations-Sharing bezeichnete gemeinsame Nutzung von Informationen über mehrere Rechner hinweg und zum anderen um die direkte Integration von Speichersystemen in das Netzwerk.
Verstärkt setzt sich der Trend zur Auftragsdatenverarbeitung, zum Outsourcing und zur Fernwartung (15.10) fort.
Inwieweit sich gegenüber der bisherigen PC-Technik die neuen sogenannten Netzcomputer (NC) durchsetzen, wird sich zukünftig zeigen. Diese einfachen Rechner haben einen Internet-Anschluß und beziehen sowohl ihre Software als auch ihre Daten direkt über das Internet. Diese sehr starke Bindung an das Netz soll mittels preiswerter und bedienerfreundlicher Geräte durchgesetzt werden. Anwendungen wie beispielsweise eine Textverarbeitung holt sich der NC über das Netz. Auf einem zentralen Speicher im Netz legt er auch

seine Daten wieder ab. Hier können datenschutzrechtliche Gesichtspunkte unmittelbar berührt sein. Das Ablegen personenbezogener Daten auf der Festplatte eines Internetservers ist datenschutzrechtlich nicht unbedenklich. Hier muß u. a. genau der Zugriffsmodus analysiert werden.

Ein wesentliches Merkmal unserer Informationsgesellschaft zeigt sich in ihrer grenzenlosen Kommunikation. An offene Netze kann sich jeder anschließen. Insbesondere die mobile Datenkommunikation wird nach Einschätzung vieler Experten massiv zunehmen. Die heutigen GSM-Netze (Global Standard for Mobile Communikation) werden bisher noch zu 95 bis 98 Prozent nur für reine Sprachkommunikation genutzt. Prognosen besagen, daß bis zum Jahre 2000 25 Prozent der Kommunikation in den Netzen reiner Datenverkehr sein werden. Der Zugriff auf Datennetze über Handy wird sich zunehmend durchsetzen, insbesondere für Geschäftsreisende und Außendienstmitarbeiter. Mit einem datenfähigen GSM-Handy, einem mobilen PC sowie einer PC-Card, welche den Computer mit dem Handy verbindet, kann heute schon der mobile Online-Zugriff auf Daten, die im Behörden-, Firmen-, Homerechner oder in internationalen Netzen zur Verfügung stehen, erfolgen. Mittels Telefax (15.12), E-Mail, WWW kann man somit an jeden beliebigen Ort der Erde, ob im Auto, im Zug oder beim Kunden, online gehen.

Das Internet ist zum Medium für alle geworden. Dieser Freiheit des einzelnen steht allerdings ein nur begrenzter Schutz seiner persönlichen Daten gegenüber. Zum einen fehlen weiterhin noch international wirksame rechtlich bindende Regeln in der virtuellen Welt. Zum anderen bestehen aufgrund unzureichender technischer und organisatorischer Sicherheitsmaßnahmen Gefahren insbesondere durch Abhör- und Manipulationsrisiken sowohl bei stationärer als auch bei mobiler Kommunikation. Hier gilt noch immer das Prinzip, jeder Benutzer muß seine Daten selbst vor Angriffen schützen. Dieser Schutz muß sich sowohl auf die übermittelten Daten als auch auf die auf dem lokalen Rechner, der am Internet angeschlossen ist, gespeicherten Daten erstrecken. Schlagzeilen machen neue Technologien, welche beim Aufruf von Web-Seiten durch die Benutzer das automatische Laden von aktiven Programmkomponenten auf deren EDV-System ermöglichen. Die Codeausführung bleibt dem Benutzer zumeist verborgen. Neben vielen nützlichen Aspekten können sich aber durch den gezielten Einsatz bösartiger Programme auch erhebliche Gefahren für Datenschutz und Datensicherheit ergeben (15.13).

Der PC als Kommunikationszentrale forciert das Zusammenwachsen von Informationstechnologie und Unterhaltungselektronik. Der Begriff „Tele“ wird zunehmend zur Vorsilbe für Arbeit, Einkaufen, Banking, Medizin und weitere Aktivitäten. Täglich werden digitale Computersysteme mit immer kleineren, leistungsfähigeren und preiswerteren elektronischen Bausteinen für neue Anwendungen eingesetzt. Parallel zu dieser Entwicklung steigt die Abhängigkeit der Gesellschaft, der Wirtschaft und auch des einzelnen Bürgers von der Funktionsfähigkeit und Sicherheit dieser Technik. Angesichts dieser Entwicklung stellt sich verschärft die Frage, ob die hiermit verbundenen Gefahren für das Recht auf informationelle Selbstbestimmung des einzelnen noch beherrschbar sind. Das sich mit der digitalen Technik auch in zunehmenden Maße Chancen zum Schutz der Privatsphäre des einzelnen ergeben, zeigen Veröffentlichungen der Datenschutzbeauftragten des Bundes und der Länder zum Einsatz „Datenschutzfreundlicher Technologien“ (15.6). Gemeint sind Technologien, die einen umfassenden Datenschutz der Anwender durch ein weitgehend anonymes Nutzen der IuK ermöglichen, um somit der Gefahr des Mißbrauchs personenbezogener Daten zu begegnen. Es geht um die Durchsetzung des Prinzips der Datenvermeidung zumindest der Datensparsamkeit sowie um die Anonymisierung und Pseudonymisierung bei der Erhebung und Verarbeitung personenbezogener Daten, einschließlich deren Nutzung.

Auch der Einsatz von modernen Sicherheitsmechanismen führt zu einem wesentlich verbesserten Schutz der Privatsphäre und erhöhter Datensicherheit. Die Verschlüsselung von Daten (15.7.2), das digitale Signieren von elektronischen Dokumenten (15.7.3, 15.8), der verstärkte Einsatz von intelligenten Chipkarten (15.9) zur Realisierung von Sicherheitsfunktionen können hierfür beispielhaft genannt werden. Das Einbeziehen solcher sicherheitsrelevanter Schlüsseltechnologien in vorhandene und zukünftige Verfahren der IuK können die Quellen für neue, innovative Anwendungslösungen sein, in denen datenschutzrechtliche Erfordernisse und Forderungen quasi automatisch von vornherein schon einbezogen sind.
Mit dem neuen Signaturgesetz (15.8) wurde auch aus rechtlicher Sicht eine grundlegende Basis für die Verbindlichkeit digitaler Willensäußerungen und Online-Transaktionen mittels sicherer digitaler Signaturen geschaffen.

15.2 Corporate Network (CN) der Landesverwaltung

15.2.1 Einführung

Der Aufbau eines CN für die Verwaltungseinrichtungen des Freistaats Thüringen am Standort Erfurt u. a. unter Einbeziehung des Landesverwaltungsamtes erfolgt auf der Grundlage eines entsprechenden Beschlusses der Landesregierung aus dem Jahre 1996. Die Realisierung und der Betrieb des CN obliegt dem TIM.
Unter einem CN versteht man ein eigenständiges, geschlossenes Kommunikationsnetz, in dem Sprach-, Daten- und Bildübertragung über dafür gemeinsam genutzte Übertragungswege realisiert werden. Die bisher unterschiedlichen Kommunikationsnetze und die Trennung von Sprach- und Datenübertragung werden damit aufgehoben. Letztendlich wird eine weitestgehende Unabhängigkeit von öffentlichen kommerziellen Netzbetreibern erzielt.
Schon in meinem 1. TB (15.5.1) habe ich zum CN Stellung bezogen und auf hiermit verbundene mögliche Gefahren aus der Sicht des Datenschutzes hingewiesen sowie Empfehlungen für die Einhaltung datenschutzrechtlicher Vorschriften gegeben. Der gesetzliche Auftrag in § 1 ThürDSG, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, ist auch beim CN grundsätzlich zu beachten und in alle Überlegungen einzubeziehen.
CN unterliegen dem Telekommunikationsgesetz (TKG). Dieses verpflichtet gemäß § 87 den Betreiber von Telekommunikationsanlagen, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen, angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze

- des Fernmeldegeheimnisses und personenbezogener Daten,
- der programmgesteuerten Systeme gegen unerlaubte Zugriffe,
- gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen und
- gegen äußere Angriffe und Einwirkungen von Katastrophen

zu treffen. Dabei ist der Stand der technischen Entwicklung zu berücksichtigen. Erfaßt werden alle zum Erbringen der Telekommunikationsdienste betriebenen Telekommunikations- und Datenverarbeitungssysteme.
Am 01.04.1997 wurden die TK-Anlagen der Ressorts und des Landesverwaltungsamtes im Verbund Erfurt-Weimar (Stadtnetz) zusammengeschaltet. Damit wurde in der ersten Ausbaustufe des CN die Sprachkommunikation im Stadtnetz realisiert. Im III. Quartal 1997 erfolgte der infrastrukturelle Ausbau des CN, mit dem Ziel, die technischen Voraussetzungen für die Datenkommunikation zu schaffen. Die in den Ressorts hierfür installierten technischen Komponenten (Sprach-Datenmultiplexoren) ermöglichen jetzt, neben der Sprach-, auch die Datenkommunikation über die gleichen Festverbindungen zu realisieren. Parallel zum Ausbau des Stadtnetzes, erfolgt der weitere Ausbau des bisherigen Landesdatennetzes zu einem Weitverkehrsnetz (WAN) im CN, mit dem Ziel, auch die hier vorhandenen Festverbindungen sowohl zur

Daten- als auch zur Sprachkommunikation zu nutzen. Die Anbindung des Stadtnetzes an das WAN erfolgt über den Datennetzknoten im TMSG. Desweiteren wird über diesen Knoten eine zentrale und abgesicherte Verbindung zwischen CN und Internet eingerichtet.
Parallel zur Weiterentwicklung des CN werden auf seiner Grundlage Dienste bereitgestellt, wie beispielsweise der elektronische Postdienst (E-Mail). Die Landesverwaltung bildet hierfür einen privaten X.400 - Verwaltungsbereich (PRMD) (1. TB, 15.5.2). Die Datenkommunikation innerhalb des PRMD erfolgt über das CN der Landesverwaltung. Für diese elektronische Nachrichtenkommunikation wurde im TLRZ eine X.400 - Landeskopfstelle auf der Basis der Kommunikationssoftware Microsoft-Exchange-Server eingerichtet. Die Landeskopfstelle fungiert als Zentralpostamt, indem sie den ressortübergreifenden und den von außerhalb des PRMD eingehenden externen Nachrichtenverkehr an die entsprechenden Mail-Server der einzelnen Ressorts vermittelt sowie die aus den PRMD abgehenden Nachrichten weiterleitet. In den angeschlossenen Ressorts sind hierfür eigenständige MS-Exchange-Server installiert, welche in der Regel sachgebiets- und benutzerorientierte Postfächer enthalten, auf die entsprechend ihrer Befugnisse die jeweiligen Benutzer mit ihrem PC (Client) Zugriff besitzen und somit Nachrichten empfangen, versenden und bearbeiten können.
Weitere Dienste werden über das CN im Rahmen des Intranet der Landesverwaltung angeboten. Unter einem Intranet versteht man ein behörden- oder unternehmensinternes Netzwerk (privates Corporate Network) das Internetprodukte und -technologien nutzt, aber im Gegensatz zum Internet gegenüber der Außenwelt vor unbefugtem Zugriff weitestgehend abgeschottet ist. Kennzeichnend ist der Einsatz von sogenannten Web-Servern zur Bereitstellung von Informationen sowie der lokale Einsatz entsprechender Browser-Software für den Zugriff auf diesen Servern. Somit ist es möglich, Informationen und Anwendungen bereitzustellen, auf die über die am CN angeschlossenen Rechner die Benutzer mittels eines lokalen Web-Browsers zugreifen können, unabhängig davon, unter welchem Betriebssystem der Rechner läuft. Computer unterschiedlichster Größe - von Mainfraime über PC bis zum Notebook - können in einem solchen Kommunikationsnetz eingebunden werden.
Im Rahmen der Intranetfunktionalität werden derzeit Informationen für die Dienste eines elektronischen Telefonbuchs, Meldungen der Deutschen Presseagentur (DPA) und die Parlamentsdokumentation des Thüringer Landtages bereitgestellt.

15.2.2 Sprachkommunikation im CN

Die TK-Anlagen der Ressorts einschließlich des Thüringer Landesverwaltungsamtes sind über eine zentrale Telekommunikationsanlage (zTK-Anlage) zu einem TK-Anlagenverbund zusammengeschaltet. Standort der zTK-Anlage ist das TMSG.
TK-Anlagen sind technische Einrichtungen, mit denen auch personenbezogene Daten automatisiert verarbeitet und das Verhalten sowie die Leistung der Mitarbeiter kontrolliert werden können. Die datenschutzrechtlichen Aspekte, welche beim Einsatz von TK-Anlagen zu beachten sind, habe ich schon in meinem 1. TB (15.7) dargelegt und auch hierzu über festgestellte Mängel beim Betrieb einer TK-Anlage berichtet (1. TB, 15.14.4). Aus datenschutzrechtlicher Sicht sind nicht nur die Beachtung des Schutzes des nicht öffentlich gesprochenen Wortes und die aktivierten einzelnen Leistungsmerkmale relevant, sondern auch welche Daten von der zentralen TK-Anlage erfaßt und verarbeitet werden und welche Funktionen - auch ungenutzte - diese TK-Anlage bietet. Die für den Betrieb solcher Anlagen erforderlichen Regelungen und Sicherheitsmaßnahmen müssen auch möglichen Manipulationen Rechnung tragen, welche aufgrund der eingesetzten Digitaltechnik

durch logische Zugriffe auf Verbindungen oder Endeinrichtung gegeben sein können.
Über die zTK-Anlage werden alle Gespräche geleitet, die von außerhalb in das CN eingehen sowie die innerhalb des CN zwischen den angeschlossenen Einrichtungen geführt werden. Nach Aussage des TIM führt die zTK-Anlage derzeit nur Vermittlungsfunktionen aus. Eine Erhebung und Verarbeitung personen- und verbindungsbezogener Daten wäre jedoch auf Anforderung der Ressorts (beispielsweise zur Gebührenermittlung) problemlos realisierbar.
Bereits in einer grundsätzlichen Stellungnahme zum von einer Arbeitsgruppe des Interministeriellen Ausschusses für Informationstechnik (IMA-IT) im Juni 1995 vorgelegten Konzept zum Aufbau eines CN wurden die mit einer Sprachkommunikation im CN verbundenen Gefährdungen und datenschutzrechtlichen Erfordernisse dargelegt (1. TB, 15.5.1).

Der TLfD hat rechtzeitig mit dem TIM, als verantwortlichem Betreiber des CN, Kontakt aufgenommen, um hinreichende Detailinformationen zu den vorgesehenen TK-Leistungsmerkmalen und Sicherheitsmaßnahmen zu erhalten.
Für den Betrieb einer CN-Sprachkommunikation sind nachfolgende datenschutzrechtliche Gesichtspunkte aus meiner Sicht bedeutsam und zu beachten:

1. Für die ressortübergreifende Sprachkommunikation ist eine Betriebsordnung erforderlich, welche den technologischen, verfahrenstechnischen und organisatorischen Ablauf regelt und die Transparenz des TK-Verfahrens gewährleisten soll. Desweiteren ist ein Sicherheitskonzept unverzichtbar.
2. Die zTK-Anlage ist vor unbefugtem Zugriff und vor einer möglichen Manipulation ihrer Konfigurationsparameter zu schützen, um Beeinträchtigungen des Persönlichkeitsrechts der Mitarbeiter als auch externer Gesprächsteilnehmer auszuschließen.
3. Weitergehende datenschutzrechtliche Erfordernisse sind zu beachten, wenn Ressorts eine zentrale Gebührenabrechnung für ihre bisher dezentral erfaßten Verbindungsdaten und ermittelten Gebühren wünschen. In diesem Fall müssen zusätzliche Maßnahmen zum Schutz der Daten vor unberechtigtem Zugriff und mißbräuchlicher Nutzung ergriffen sowie die Mitbestimmung der Personalräte der betroffenen Stellen beachtet werden.
4. Aus datenschutzrechtlicher Sicht sind bei ressortübergreifenden Leistungsmerkmalen die Leistungsmerkmale -Aufschalten- in bestehende Verbindungen und - Rufumleitung - eines ankommenden Gesprächs auf eine andere Nebenstelle nicht unbedenklich. Diese Merkmale sind nur vertretbar, wenn nachfolgende Einschränkungen beachtet werden. Ein Aufschalten in aktive Gespräche darf nur durch die zentrale Vermittlung möglich sein und nur, um externe Anrufe anzukündigen, deren Entgegennahme keinen Aufschub duldet. Das Aufschalten muß durch einen zwangsläufig erzeugten, nicht unterdrückbaren Signalton den Teilnehmern angezeigt werden. Es ist dafür Sorge zu tragen, daß der nicht betroffene Teilnehmer des Gesprächs keine Informationen über den externen Anrufer und den Anlaß des Gespräches erfährt, es sei denn, der Betroffene erteilt hierzu seine Einwilligung. Das Leistungsmerkmal Rufumleitung darf ausschließlich durch den betroffenen Teilnehmer geschaltet und aktiviert werden.
5. Für die Betreuung der zentralen TK-Anlage muß ein fachlich kompetenter Techniker zur Verfügung stehen, unter dessen fachlicher Betreuung die Anlage betrieben und administriert wird und der sich auch für die Einhaltung sicherheitstechnischer Belange verantwortlich zeichnet.
6. Die vorgesehene Fernwartung ist auf das unumgängliche Maß zu beschränken. Im Sicherheitskonzept sind die hierfür erforderlichen konkre-

ten Sicherheitsmaßnahmen auszuweisen. Insbesondere sind hierfür eine sichere Identifikation und Authentifikation des Wartungspersonals und eine entsprechende Protokollierung der durchgeführten Aktivitäten notwendig (15.10).

Das TIM sicherte die Realisierung meiner Forderungen zu. Das Sicherheitskonzept sollte nach ersten Aussagen im April 1997 vorliegen. Der Entwurf für eine Betriebsordnung wurde mir zur Stellungnahme zugeleitet. Meine hierzu gegebenen Hinweise wurden in dem überarbeiteten Entwurf berücksichtigt bzw. sollen anderweitig sichergestellt werden.
Das bisher noch ausstehende Sicherheitskonzept soll nach Angaben des TIM in das zu erarbeitende Gesamtsicherheitskonzept des CN einbezogen werden. Ich erachte eine kurzfristige Umsetzung für geboten.
Für die bisherige jeweilige dezentrale Vermittlung vor Ort wurde vom TIM eine zentrale Auskunfts- und Telefonvermittlung für alle angeschlossenen Einrichtungen auf der Basis eines rechnergestützten Telefonverzeichnisses eingerichtet. Zugriff auf das automatisierte Telefonverzeichnis besitzen nur befugte Mitarbeiter. Die Aktualisierung der hierzu vorgehaltenen personenbezogenen Daten erfolgt entsprechend der belegbaren Anforderungen der Ressorts. Desweiteren wurde ein elektronisches Telefonbuch (ETB) aufgebaut, das auf einem WEB-Server im TLRZ vorgehalten wird und auf das die Benutzer der CN-Datenkommunikation im Rahmen der bereitgestellten Intranetfunktionalität lesend zugreifen können und somit auch lokal hiervon Kopien ausdrucken oder elektronisch auf externe Datenträger speichern können. Das ETB enthält ausgewählte Datenfelder des zentralen Telefonverzeichnisses und wird ausgehend von diesen aktualisiert. Die Aktualisierung des zentralen Telefonverzeichnisses und des ETB erfolgt nur durch befugte Mitarbeiter (Administratoren). Hinsichtlich des vorgesehen Datenumfangs für das ETB bat ich das TIM um nähere Erläuterungen für die Erforderlichkeit zur Speicherung und Übermittlung des Vornamens und der Amtsbezeichnung. Gemäß § 19 Abs. 1 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben erforderlich ist. Eine diesbezügliche Erforderlichkeit zur Speicherung des Vornamens und der Amtsbezeichnung der Bediensteten im ETB kann ich nicht erkennen. Desweiteren regte ich an, eine entsprechende Richtlinie für eine einheitliche inhaltliche Verfahrensweise zur Darstellung der Ressorts im ETB zu erlassen.
Eine abschließende Stellungnahme des TIM bezüglich meiner o. g. Empfehlungen steht noch aus.

15.2.3 Datenkommunikation im CN

Gemäß § 9 ThürDSG haben öffentliche Stellen, die im Rahmen des ThürDSG personenbezogene Daten verarbeiten, die technischen und organisatorischen Datensicherungsmaßnahmen zu treffen, um die Ausführungen der Vorschriften des ThürDSG zu gewährleisten. Aus datenschutzrechtlicher Sicht ist es somit erforderlich, daß jede Stelle vor Anschluß und Nutzung des CN grundlegend klären muß:

1. ob und unter welchen Bedingungen das CN für die Übermittlung personenbezogener Daten genutzt werden darf,
2. inwieweit das Internet einbezogen werden soll,
3. welche Maßnahmen zu ergreifen sind, um die im internen Bereich in automatisierter Form vorgehaltenen personenbezogene Daten vor externen Angriffen über das CN bzw. aus dem Internet zu schützen.

Als Maßstab für die Schutzwürdigkeit der personenbezogenen Daten ist deren Sensibilität ausschlaggebend. Hierbei sollte sich an dem von mir empfohlenen Schutzstufenkonzept (1. TB, 15.3) orientiert werden.
Das Thüringer Datenschutzgesetz schreibt in § 20 vor, daß personenbezogene Daten nur für die Zwecke genutzt werden dürfen, für die sie erhoben

worden sind. Bei der komplexen Vernetzung der Landesverwaltung ist deshalb zu beachten, daß die sachliche und örtliche Zuordnung der automatisiert vorgehaltenen Datenbestände der angeschlossenen Stellen weiterhin transparent nachvollziehbar sein muß. Eine Nutzung der CN-Infrastruktur, um auf Datenbestände anderer öffentlicher Stellen zuzugreifen, darf nur im Ausnahmefall erfolgen, wenn eine entsprechende Rechtsvorschrift dies erlaubt. Grundsätzlich ist also ein solcher Zugriff auszuschließen und steht unter Erlaubnisvorbehalt.

Die Vertraulichkeit und die Integrität der über das Kommunikationsnetz übertragenen Daten sowie der in den vernetzten Systemen gespeicherten Daten wird dadurch gefährdet, daß durch unbefugte Zugriffe die Möglichkeit besteht, Daten unbemerkt zur Kenntnis zu nehmen, abzuziehen und ggf. auch zu manipulieren. Daraus leiten sich folgende grundlegenden Forderungen zur Gewährleistung des Datenschutzes ab:

1. Die Möglichkeiten zur Nutzung des CN sind nach dem Grundsatz der Erforderlichkeit festzulegen. Hierzu ist eine Analyse des Kommunikationsbedarfs der anzuschließenden Stelle erforderlich, wobei auch geprüft werden sollte, ob der angestrebte Zweck nicht schon durch den Anschluß eines isolierten Rechners erreicht werden kann.
2. Verbindungswünsche sind auf ihre Zulässigkeit zu prüfen. Es sollte der Grundsatz gelten, daß alle Datenverbindungen, die nicht explizit erlaubt wurden, verboten sind.
3. Verbindungen und Dienste, die sich nicht aus dem Aufgabenprofil der Stelle begründen lassen, sind, sofern möglich, durch technische Maßnahmen zu unterbinden. Nutzungsverbote allein werden regelmäßig hierfür nicht ausreichen.
4. Zur Abwehr unbefugter Zugriffe bzw. von Angriffen sind entsprechend dem Stand der Technik angemessene technische und organisatorische Maßnahmen zur Informationssicherheit zu realisieren.

Ich verweise weiter hierfür auf die „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ (1. TB, Anlage 30) sowie auf entsprechende Empfehlungen im BSI-Grundschutzhandbuch.

Die Komplexität des CN und die voraussichtliche Vielzahl angeschlossener lokaler Netze bzw. interner Rechner erfordert sowohl einen besonders gesicherten Übergang zwischen den ressortinternen Bereichen und dem CN sowie zwischen diesem und dem Internet. Es ist insbesondere darauf zu achten, daß außer solchen gesicherten Übergängen/Anschlüssen keine weiteren Verbindungen von Rechnern interner Netze, die am CN angeschlossen sind, beispielsweise über Modem oder ISDN, zu öffentlichen Netzen bestehen bzw. solche auf Ausnahmen beschränkt sind. Ausnahmen dürfen nur in begründeten Einzelfällen und nach entsprechender Prüfung, ob auch die hiermit verbundenen Gefahren (Bedrohungen) beherrschbar sind, genehmigt werden.

Um Gefährdungen für den Schutz personenbezogener Daten weitestgehend auszuschließen, sind Sicherheitskonzepte erforderlich, die auch Anforderungen des Datenschutzes angemessen berücksichtigen. Neben einem ressortübergreifenden zentralen Sicherheitskonzept für das zukünftige CN-Kommunikationsnetz, einschließlich des vorgesehenen Übergangs zum Internet, sind ressortbezogene Sicherheitskonzepte seitens der angeschlossenen Stellen erforderlich. Hierbei sind ausgehend von organisatorischen Festlegungen die technischen Sicherheitsmaßnahmen zu treffen. Grundsätzlich ist zu beachten, daß bei einer Verarbeitung von personenbezogenen Daten unterschiedlicher Sensibilität, die im Sicherheitskonzept aufgeführten Maßnahmen sich an den Daten mit dem höchsten Schutzbedarf orientieren müssen. Aus datenschutzrechtlicher Sicht ist ein Anschluß von Stellen an das CN ohne angemessene organisatorische und technische Sicherheitsmaßnahmen nicht zulässig. Bereiche, die besonders sensible Daten verarbeiten, müssen besonders abgeschottet werden. In der Regel sollten hier nur separate Netze eingesetzt werden. Das Risiko eines möglichen Schadens, der auch erhebli-

che materielle und nicht abschätzbare immaterielle Schäden zur Folge haben könnte, muß auf ein verantwortbares Maß verringert werden.
Der Einsatz von Firewall-Systemen kann nur ein Teil, wenn auch wesentlicher Bestandteil umfassender Sicherheitsmaßnahmen zum Zugangs- und Zugriffsschutz sein. Der alleinige Einsatz von Firewall-Systemen gewährleistet noch keine hinreichende Sicherheit. So kann z. B. mit einer Firewall nicht der Schutz der Integrität oder der Vertraulichkeit der Daten gewährleistet werden.
Die Erfahrungen auf dem Gebiet der IT-Sicherheit besagen, daß mit technischen Maßnahmen allein sich nicht alle Sicherheits- und Risikoaspekte hinreichend berücksichtigen und somit abdecken lassen. Sicherheitslösungen sind keine starren Systeme, sie müssen dynamisch dem Stand der Technik angepaßt werden. Analytische Untersuchungen zeigen, daß die eigenen Mitarbeiter bzw. die Benutzer ein wesentlicher Faktor für die Sicherheit des zu schützenden Systems darstellen. Die mit den vergebenen Zugriffsrechten „eingeschränkte Handlungsfreiheit“ stößt nicht immer auf eine positive Resonanz. Wichtig ist es deshalb, die Benutzer als aktive und sicherheitsbewußte Mitarbeiter in die Sicherheitskonzepte einzubeziehen und ihre Verantwortung für die Sicherheit des Gesamtsystems zu verdeutlichen. Neben den aus dem CN bzw. aus dem Internet auftretenden Gefährdungen sollten sie auch aufgeklärt werden über mögliche Folgen aus ihrem Fehlverhalten bei Sicherheitsverletzungen. Insbesondere mit der Nutzung des CN bzw. von Online-Aktivitäten im Internet muß eine klare Entscheidung zu Gunsten einer bedarfsgerechten Rechtevergabe erfolgen, die für die Mitarbeiter verständlich und transparent ist. Die Herausgabe von Benutzerrichtlinien stellt hierfür eine wertvolle Hilfe dar.
Das TIM als Betreiber des CN arbeitet an einem zentralen Sicherheitskonzept. Nach meinem Kenntnisstand soll entsprechend der getroffenen Aussagen des IMA-IT der Netzbetreiber die notwendigen Maßnahmen zur Absicherung des zentralen Internetzugangs, zur Absicherung der zentralen Intranetkomponenten und zur Absicherung der Schnittstellen zwischen dem CN und den ressortinternen Netzen treffen und die entsprechenden Komponenten administrativ verwalten. Die Schnittstellen zwischen den Ressortnetzen und dem CN werden demzufolge vom Netzbetreiber kontrolliert, wobei den Ressorts gesicherte LAN-Schnittstellen zur Verfügung gestellt werden. Für die Absicherung des Zugangs zum Internet ist entsprechend den Empfehlungen des BSI eine mehrstufige Firewallanordnung vorgesehen. Die sicherheitsrelevante Bewertung der ressortbezogenen Anwendungen liegt in der Verantwortung der am CN angeschlossenen Stellen. Aus datenschutzrechtlicher Sicht ist dieser konzeptionelle Sicherheitsansatz zu begrüßen.

15.3 IT-Richtlinien in der Thüringer Landesverwaltung

Vom IMA-IT wurde eine Überarbeitung der Richtlinien für den Einsatz der Informationstechnik mit dem Ziel angeregt, diese den aktuellen Entwicklungen anzupassen. Auch ich habe aus datenschutzrechtlicher Sicht entsprechende Empfehlungen zu Ergänzungen bzw. zu Änderungen für eine Überarbeitung der IT-Richtlinien vorgeschlagen. Damit soll den gesetzlichen Anforderungen des Datenschutzes besser entsprochen werden.
Mit Rundschreiben des TIM im Jahr 1993 (veröffentlicht im Staatsanzeiger Nr. 19/1993) sind verbindliche Richtlinien für den Einsatz von Informationstechnik (IT-Richtlinien) in den obersten Landesbehörden und ihren nachgeordneten Behörden und Dienststellen erlassen worden. Danach ist beim Einsatz von IT von Anfang an dafür Sorge zu tragen, daß die rechtlichen Rahmenbedingungen beachtet werden. Ausdrücklich wird in diesem Zusammenhang auch auf Datenschutzvorschriften verwiesen. Die Richtlinien verpflichten die obersten Landesbehörden einen IT-Ressortplan zu führen, der die IT-Vorhaben und -Verfahren beginnend mit dem jeweiligen Haushaltsjahr, für einen Zeitraum von drei Jahren enthält. Weiterhin ist festgelegt, daß

diese Ressortpläne für die ausgewiesenen IT-Vorhaben und -Verfahren auch Angaben zu Sicherungsmaßnahmen enthalten müssen.
Für den Aufbau der IT-Ressortpläne erließ das TIM im Jahre 1994 (veröffentlicht im Staatsanzeiger Nr. 30/1994) verbindliche Regelungen. Diese Regelungen enthalten auch grundlegende Ausführungen zu Konzepten und Maßnahmen zur Sicherheit beim Einsatz der IT, wobei auch datenschutzrechtliche Anforderungen hervorgehoben und berücksichtigt werden. So soll jede Behörde die Angemessenheit der getroffenen bzw. geplanten Sicherheitsmaßnahmen anhand eines IT-Sicherheitskonzeptes, welches auf einer Risikoanalyse aufbaut, nachweisen. Ausgehend von den Gefährdungen bei der Verarbeitung personenbezogener Daten, sind die technischen und organisatorischen Maßnahmen nach § 9 ThürDSG zu realisieren, die erforderlich sind, um den Datenschutz sicherzustellen. Das Datensicherungskonzept hat abgestufte Maßnahmen zu enthalten, die von der Klassifizierung der Daten nach schutzwürdigen Belangen abzuleiten sind. Für jedes IT-Verfahren und -Vorhaben sind entsprechende Maßnahmen zur IT-Sicherheit und zum Datenschutz vorzunehmen.
Sowohl für die Tätigkeit des behördeninternen Datenschutzbeauftragten als auch im Rahmen meiner Beratungs- und Kontrollfunktion sind diese Pläne eine wichtige Orientierungshilfe, indem sie notwendige Informationen aufzeigen, welche für eine datenschutzrechtliche Einschätzung insbesondere der IT-Vorhaben wichtig sind. Ich habe dem IMA-IT vorgeschlagen, daß die verantwortlichen Stellen den Ressortplänen zu jedem IT-Verfahren und -Vorhaben eine kurze Checkliste als Anlage beifügen. Diese Checkliste enthält kategorisierte Aussagen, die entsprechend den datenschutzrechtlichen Vorschriften für jedes IT-Verfahren und IT-Vorhaben vor der Inbetriebnahme geklärt sein müssen. Beispielsweise sind für jedes IT-Verfahren aus datenschutzrechtlicher Sicht u. a. Aussagen zu folgenden Aspekten relevant:

- Werden personenbezogene Daten verarbeitet?
- Ist der behördeninterne Datenschutzbeauftragte informiert?
- Ist das Verfahren nach § 34 Abs. 2 ThürDSG freigegeben?
- Ist das Verfahren gemäß § 10 ThürDSG in das Verfahrensverzeichnis aufgenommen?
- Liegt Auftragsdatenverarbeitung nach § 8 ThürDSG vor?
- Ist es ein Abrufverfahren nach § 7 ThürDSG?
- Ist die Meldung zum Datenschutzregister erfolgt?
- Liegt das IT-Sicherheitskonzept vor?

Die Checklisten sollen dem Leiter der verantwortlichen Stelle, dem bDSB, dem IT-Verantwortlichen als auch Mitarbeitern meiner Dienststelle bei Kontrollen als eine Art Richtschnur bezüglich der Einhaltung und Erfüllung wesentlicher datenschutzrechtlicher Erfordernisse dienen.
Auch zu den vom IMA-IT im Jahre 1993 verabschiedeten verbindlichen Regelungen zur Durchführung von Maßnahmen im Bereich der Informationstechnik (IT-Maßnahmenregelung, Staatsanzeiger Nr. 22/1993) habe ich dem IMA-IT aus datenschutzrechtlicher Sicht inhaltliche Empfehlungen für eine Überarbeitung vorgeschlagen. IT-Maßnahmen im Sinne dieser Regelung dienen der Erledigung von Aufgaben mit Hilfe der Informationstechnik, wie die Entwicklung und Einführung neuer Verfahren bzw. die Änderung bestehender oder Übernahme anderenorts laufender Verfahren, die einen Gesamtaufwand von mehr als 100.000,- DM erfordern.

In der IT-Maßnahmenregelung wird auf datenschutzrechtliche Erfordernisse nicht ausdrücklich Bezug genommen. So sind bei der Erläuterung zur Zuständigkeit der auftraggebenden Stelle die Einhaltung auch datenschutzrechtlicher Vorschriften nicht aufgeführt und in den Vorgaben für den Auftrag für eine IT-Maßnahme die datenschutzrechtlichen Erfordernisse nicht explizit erwähnt.
Meine Vorschläge zur Überarbeitung der IT-Maßnahmenregelung habe ich dem IMA-IT mitgeteilt. Diese sehen im wesentlichen vor, daß die datenver-

arbeitende Stelle bei der Erarbeitung einer Lösung, auch die datenschutzrechtlichen Vorgaben zu berücksichtigen hat.
Laut IT-Maßnahmenregelung soll die Durchführung eines Projektes in den Abschnitten Voruntersuchung, Hauptuntersuchung und Ausführung ausgeführt werden.
Gemäß der derzeitig vorliegenden Regelung ist der Zweck der Voruntersuchung, festzustellen, ob die Automatisierung der Aufgabe zweckmäßig und wirtschaftlich durchführbar ist. Hier fehlt meiner Auffassung nach ein Verweis darauf, in diesem Zusammenhang zu prüfen, ob die Automatisierung der Aufgabe unter Einhaltung der datenschutzrechtlichen Vorschriften durchführbar ist. Es ist wichtig, schon in diesem frühen Stadium datenschutzrechtliche Erfordernisse zu beachten, um im Ergebnis der Versuchsplanung Lösungsvorschläge zu präsentieren, welche auch den datenschutzrechtlichen Vorschriften Rechnung tragen. Zweck der Voruntersuchung muß es deshalb auch sein, festzustellen, ob die vorgesehene Maßnahme auf dem Gebiet der Informationstechnik auch unter Einhaltung datenschutzrechtlicher Vorschriften durchführbar ist. Darauf ist bei der Zweckbestimmung der Voruntersuchung hinzuweisen. Der in der Regelung geforderte Bericht über die Voruntersuchung muß demzufolge auch die Empfehlung einer bestimmten Lösungsalternative unter Beachtung datenschutzrechtlicher Aspekte beinhalten. Zu beachten ist insbesondere, daß nach § 34 Abs. 2 ThürDSG der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, hinsichtlich der Datenarten und der regelmäßigen Datenübermittlungen der vorherigen schriftlichen Freigabe durch die Stelle bedarf, die den Datenschutz sicherzustellen hat. Diese gesetzliche Regelung schon in die Voruntersuchung einzubeziehen, stellt auch unter wirtschaftlichen Gesichtspunkten eine elementare Voraussetzung dar, um die erforderliche datenschutzrechtliche Freigabe des Verfahrens vor seinem erstmaligen Einsatz zu gewährleisten. Somit können insbesondere zeitliche Verzögerungen durch z. T. mit erheblichen Aufwand verbundene Verfahrensänderungen vermieden werden. Liegen datenschutzrechtliche Bedenken zu Vorschlägen von Verfahrenslösungen vor, sind diese noch vor dem Stadium der Hauptuntersuchung auszuräumen bzw. wenn dies nicht möglich ist, hierfür neue Vorschläge zu erarbeiten.
Die in der IT-Maßnahmeregelung enthaltenen Ausführungen zur Hauptuntersuchung enthalten keine Aussagen zur IT-Sicherheit. Laut Regelung beschränkt sich der Zweck der Hauptuntersuchung darauf, die fachlichen Anforderungen an das IT-Verfahren im einzelnen festzulegen, ein zweckmäßiges Soll-Konzept auszuarbeiten und dessen Wirtschaftlichkeit eingehend darzulegen. Sicherheitsüberlegungen müssen jedoch parallel zur Verfahrensentwicklung ausgeführt werden und sind somit ein integraler und unverzichtbarer Bestandteil der Hauptuntersuchung. Zweck der Hauptuntersuchung muß somit auch sein, Anforderungen an die IT-Sicherheit zu definieren. Dies sollte ergänzend zum Ausdruck gebracht werden. Schutzbedarfsfeststellung, Risikoanalyse und eine Konzeption für notwendige technische und organisatorische Sicherheitsmaßnahmen sind hierzu in der Regel erforderlich. Die inhaltlichen Vorgaben zum Bericht über die Hauptuntersuchung sollten in diesem Sinne erweitert werden. Auch die in der Regelung enthaltenen inhaltlichen Vorgaben zur Dokumentation der Detailorganisation des Verfahrens sollten auf Festlegungen zum Datenschutz und zur Datensicherheit hinweisen.
Bezüglich der Verfahrensfreigabe ist zu beachten, daß bei einer Verarbeitung personenbezogener Daten die Freigabe des Verfahrens auch die datenschutzrechtliche Freigabe nach § 34 Abs. 2 ThürDSG einschließen muß. Ein entsprechender Hinweis ist hier einzufügen.
Inwieweit die laut vorliegender Regelung in der Verfahrensdokumentation aufzunehmenden Sicherheitsmaßnahmen den angestrebten Schutzeffekt gewährleisten, offenbart u. a. die Praxis beim Einsatz des Verfahrens. In angemessenen Zeitabständen ist somit unter Beachtung des Standes der

Technik abzuprüfen, ob mit den ergriffenen Sicherheitsmaßnahmen das o. g. Ziel erreicht wird. Eine solche periodische Überprüfung von Maßnahmen zur Datensicherheit sollte in der Verfahrensdokumentation zusätzlich aufgenommen werden.

15.4 Kontrolltätigkeit in öffentlichen Stellen

In dem vorliegenden Berichtszeitraum wurde schwerpunktmäßig der Einsatz von Einzelplatz-PC, lokalen Netzwerken, Großrechnern, Telefonanlagen und Zutrittskontrollsystemen in bezug auf die Einhaltung der nach § 9 ThürDSG vorgeschriebenen technischen und organisatorischen Maßnahmen kontrolliert. Grundsätzlich ist festzustellen, daß die öffentlichen Stellen bemüht sind, den Datenschutzbelangen Rechnung zu tragen und die Hinweise und Empfehlungen meinerseits entsprechend zu beachten und umzusetzen.

Wegen unzureichenden Datensicherheitsmaßnahmen wurde in drei Fällen eine Beanstandung gemäß § 9 ThürDSG ausgesprochen:
Das betraf in einer Stelle den Mangel, daß der Raum, in dem sich der zentrale Rechner befand, nicht ausreichend gegen unbefugten Zutritt von außen gesichert war.
In einem anderen Fall mußte ich in einer öffentlichen Stelle feststellen, daß den erforderlichen technischen und organisatorischen Maßnahmen gemäß § 9 ThürDSG nicht im ausreichenden Maß entsprochen wurde, was auf Grund der Anzahl der hier eingesetzten automatisierten Verfahren zu einer Beanstandung führte. Insbesondere fehlten verbindliche Regelungen sowohl für ein sicheres Betreiben der einzelnen Verfahren, als auch bereichsübergreifende Richtlinien in Form eines IT-Sicherheitskonzeptes.
Beim Einsatz eines automatisierten Zutrittskontrollsystems wurde bei einer anderen Stelle beanstandet, daß keine ausreichenden Sicherheitsmaßnahmen für den Betrieb des Systems vorhanden waren. U. a. war die Zutritts-, Zugangs- und Zugriffskontrolle mangelhaft (kein Boot-/Setup-Paßwörter, unzureichende LOGIN-Prozedur, und Paßworthandhabung, fehlende Protokollierung vergebener Zutrittsrechte etc.). Datensicherungen wurden nicht durchgeführt.

Nachfolgend möchte ich weiter auf wichtige Feststellungen, Hinweise und Empfehlungen meinerseits im Ergebnis der durchgeführten Kontrolltätigkeit eingehen:

Zugangs- und Zugriffskontrolle: Zur Gewährleistung, daß Unbefugte nicht auf gespeicherte personenbezogene Daten zugreifen können, ist unter anderem gemäß § 9 ThürDSG der unberechtigte Zugang zu Datenverarbeitungsanlagen und der Zugriff auf personenbezogene Daten zu verhindern. Vorhandene Sicherheitsmechanismen waren nicht immer aktiviert. So waren beispielsweise keine Boot-Paßwörter eingerichtet, die Anzahl fehlerhafter Login-Versuche nicht eingeschränkt, kein erzwungener Paßwortwechsel nach einer vorgegebenen Gültigkeitsdauer und keine Vergabe einer Mindestpaßwortlänge festgelegt.
In einer medizinischen Einrichtung und in einem Meldeamt mußte ich z. B. eingerichtete Zugriffsrechte bemängeln, die für die jeweilige Aufgabenerfüllung nicht erforderlich waren.
Zutrittskontrolle: Überprüfbare Regelungen für eine Zutrittskontrolle waren beispielsweise für den Vermieter, das Reinigungs-, das Wartungs- oder das Wachpersonal nicht vorhanden. Gerade für den Zutritt zu Gebäuden und Räumlichkeiten, in denen schutzwürdige Daten aufbewahrt werden, sehe ich solche Regelungen, wer, wann, wo und wie zutrittsberechtigt ist, als unerläßlich an. Diese organisatorischen Regelungen sind durch geeignete technische Maßnahmen zu ergänzen, um eine ausreichende Zutrittskontrolle zu erreichen.

Entsorgung von Datenträgern (DT): Nicht alle kontrollierten Behörden, die ihre DT-Entsorgung durch nicht-öffentliche Stellen ausführen lassen, beachten, daß es sich hierbei um eine Auftragsdatenverarbeitung im Sinne des § 8 ThürDSG handelt. So fehlten in den entsprechenden Verträgen Angaben über eingegangene Unterauftragsverhältnisse, sowie Vereinbarungen, daß sich der Auftragnehmer meiner Kontrolle unterwirft. Desweiteren wurde ich nicht immer gemäß § 8 Abs. 6 ThürDSG über die erfolgte Beauftragung unterrichtet.
Auch bei der Bereitstellung und beim Transport von Akten oder anderer Datenträger, die entsorgt werden sollen, ist das unbefugte Lesen und Kopieren der Daten gemäß § 9 Abs. 2 Ziffer 9 ThürDSG (Transportkontrolle) zu verhindern.
Die besten Sicherheitsvorkehrungen nützen jedoch nichts, wenn bei der Entsorgung leichtfertig mit den Daten umgegangen wird.
So habe ich bei einer Kontrolle in einer Behörde vor einer verschlossenen Tür einen Karton mit alten Lohnabrechnungen und Bescheiden vorgefunden die der Vernichtung zugeführt werden sollten. Eine Entnahme von Unterlagen war für jedermann ohne weiteres möglich. Dieser Verstoß gegen die Transportkontrolle führte deshalb nicht zur Beanstandung, weil der Karton sofort sichergestellt und mir die Auswertung des Vorfalls zugesichert wurde.
Anlagen- und Verfahrensverzeichnis: Das gemäß § 10 ThürDSG zu führende Verzeichnis der eingesetzten Datenverarbeitungsanlagen und automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, entsprach nicht immer dem aktuellen Stand. Es zeigte sich, daß sowohl Verfahren versehentlich nicht erfaßt wurden, aber auch, wie im Falle der Sprachkommunikation (Telefon), Zutrittskontrolle und Zeiterfassung, sich die Verantwortlichen nicht immer bewußt waren, daß auch diese automatisierten Verfahren, wie alle Verfahren, die personenbezogene Daten verarbeiten, dem § 10 ThürDSG unterfallen.
Das Anlagen- und Verfahrensverzeichnis ist in erster Linie ein wichtiges Instrument zur Eigenkontrolle der Behörde aber auch für meine Kontrolltätigkeit.
Hier zeigt sich wiederholt die Notwendigkeit, den bDSB in alle datenschutzrechtlichen Fragen mit einzubeziehen. So könnten auch fehlende datenschutzrechtliche Freigaben der Verfahren (§ 34 Abs. 2 ThürDSG) bzw. nicht erfolgte Datenschutzregistermeldungen an meine Behörde vermieden werden (1.2).
IT-Sicherheitskonzepte: Schwachstellen- bzw. Risikoanalysen und darauf aufbauende IT-Sicherheitskonzepte lagen mitunter nicht bzw. nicht in der erforderlichen Ausprägung vor. Meine entsprechenden Forderungen hierzu wurden von den betroffenen Stellen aufgenommen und werden derzeit realisiert.

15.5 Einsatz von Zutrittskontrollsystemen

15.5.1 Begriffsbestimmung

In den öffentlichen Stellen Thüringens werden Zutrittskontrollsysteme, welche teilweise mit einem Zeiterfassungssystem gekoppelt sind, zunehmend eingesetzt. Diese Zutrittskontrollsysteme sind in der Regel sehr komplexe Systeme und erfordern für ihre Installation und Betreuung besonders ausgebildetes Personal.
Die Praxis zeigt, daß es bei den Begriffen Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle immer wieder Unsicherheiten gibt. Hierbei geht es darum, insbesondere Maßnahmen zu treffen, die geeignet sind:

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**).
- Zu verhindern, daß Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**).
- Zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und daß personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**).

15.5.2 Funktionsweise eines Zutrittskontrollsystems

Mit einem Zutrittskontrollsystem wird der Zutritt zu einem Gelände oder zu einem Gebäude bzw. innerhalb des Gebäudes zu Diensträumen geregelt. Hierzu können entsprechend dem Schutzbedarf unterschiedliche Sicherheitszonen definiert werden.
Zunehmend kommen dabei rechnergestützte Zutrittskontrollsysteme zum Einsatz. Die Verwaltung der Zutrittsberechtigungen erfolgt dabei mit spezieller Software zentral auf einem Rechner. Für jede berechtigte Person kann eine räumliche und zeitlich eingeschränkte Zutrittsberechtigung je Sicherheitszone festgelegt werden.
Der Zutritt zu den jeweiligen Sicherheitszonen wird über sogenannte Terminals (bzw. Kartenleser) ermöglicht. Diese übernehmen in Zusammenarbeit mit dem PC die Kontrolle des Zutritts. Personen, die das Zutrittskontrollsystem passieren wollen, müssen sich gegenüber dem jeweiligen Terminal identifizieren. Dies kann z. B. mittels Magnet- oder Chipkarte erfolgen. Bei biometrischen Verfahren, die zunehmend in Hochsicherheitsbereichen eingesetzt werden, erfolgt die Identifizierung eines Zutrittswilligen anhand charakteristischer persönlicher Merkmale (z. B. Augenhintergrund, Gesicht oder Fingerabdruck).

15.5.3 Datenschutzrechtliche Anforderungen an Zutrittskontrollsysteme

Das ThürDSG schreibt keine konkreten Datensicherungsmaßnahmen zur Absicherung des Zutritts vor. Es überläßt somit der speichernden Stelle, die geeigneten technischen und organisatorischen Maßnahmen entsprechend den Gegebenheiten so auszuwählen und aufeinander abzustimmen, daß die gesetzlichen Forderungen erfüllt werden.
Eine Möglichkeit, diesen Forderungen nachzukommen, kann durch den Einsatz eines rechnergestützten Zutrittskontrollsystems gewährleistet werden.
Der Anschaffung solcher Systeme sollten aus datenschutzrechtlicher Sicht folgende grundlegenden Überlegungen vorausgehen:
- Welche Bereiche einer Einrichtung sollen wie abgesichert werden?
- Wie sind die Bereiche entsprechend dem Schutzbedarf zu klassifizieren und dementsprechend in welche Sicherheitszonen einzubeziehen?
- Sind zeitliche Zutritts-Einschränkungen erforderlich?
- Wer soll zu welcher Sicherheitszone wann Zutritt erhalten?
- In welcher Form soll das System auf unberechtigte Zutrittsversuche reagieren (akustische Meldung, Protokollierung)?
- Wie werden die Besucher in das Kontrollsystem einbezogen?
- Welche Daten sollen erfaßt und wie lange gespeichert werden?
- Welche Daten sollen von wem auswertbar sein?

Sollen mit dem Zutrittskontrollsystem personenbezogene Daten automatisiert erfaßt werden, so ist vor dem erstmaligen Einsatz die datenschutzrechtliche Freigabe gemäß § 34 Abs. 2 ThürDSG erforderlich.

Da Zutrittskontrollsysteme ermöglichen, das Verhalten oder die Leistungen der Beschäftigten zu überwachen, unterliegen sie der Mitbestimmung des Personalrates gemäß § 74 ThürPersVG.
Für die Speicherungsdauer der erfaßten Daten sind Fristen festzulegen (z. B. 3 Monate bzw. gemäß Regelung in der Dienstvereinbarung mit dem Personalrat).

Installierte Zutrittskontrollsysteme können ein hohes Maß an Zutrittssicherung gewährleisten, wenn sie ordnungsgemäß eingerichtet sind. Kontrollen vor Ort zeigten jedoch auch, daß mitunter vorhandener Zugangs- und Zugriffsschutz zum Schutz des Systems selbst unzureichend war (15.4). Bei der Planung des Einsatzes eines Zutrittskontrollsystems sind deshalb auch hierfür technische und organisatorische Maßnahmen vorzusehen. Unter anderem sollten hierbei folgende Anforderungen an die eingesetzte Hard- und Software beachtet werden:

- Zugangssicherung der Hardware
  (z. B. durch Boot-/Setup-Paßwort, Chipkarte)
- Zugangs- und Zutrittssicherung der Software durch:
  - Aufgabenbezogene Benutzerkennungen/Zugriffsberechtigungen
    (z. B. Systemverwaltung, Zutrittsverwaltung)
  - sichere Identifikation und Authentifikation der Zugriffsberechtigten (z. B. durch Paßwörter (1. TB, 15.6), Chipkarte)
  - Begrenzung und Protokollierung fehlerhafter Anmeldungen
  - Unterbindung unbefugter Zugriffe auf die Betriebssystemebene.

Das vorgesehene Zutrittskontrollsystem sollte neben einer übersichtlichen und sicheren Bedienerführung über Möglichkeiten der Protokollierung vergebener Zutrittsrechte und unbefugter Zutrittsversuche verfügen.

Gemäß § 9 Abs. 2 Ziff. 10 ThürDSG ist die innerbehördliche und innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle). Beispiele für organisatorische Maßnahmen beim Einsatz von Zutrittskontrollsystemen sind:

- Die Administration des Gesamtsystems muß von kompetenten Mitarbeitern der öffentlichen Stelle wahrgenommen werden. Externen Firmen sind die Rechte des Systemverwalters (Systemhauptbenutzer) zu entziehen bzw. nur bei erforderlichen Wartungsarbeiten zuzuweisen. Danach sind vom Systemverwalter der Behörde diese Paßwörter neu zu definieren.

- Um die ordnungsgemäße Einrichtung des Zutrittskontrollsystems und anderer damit in Verbindung stehender Systeme nicht zu gefährden, sollten nach Möglichkeit auf diesem Rechner keine weiteren Anwendungen zum Einsatz kommen. Nicht genutzte Dateien sind ggf. zu löschen.

- Der unbefugte Zutritt zum Rechner ist entsprechend § 9 ThürDSG zu verwehren.

- Die Datensicherung und die Protokollierung muß aktiviert werden. Die Protokolldatei ist regelmäßig auszuwerten.

- Die Schnittstellen der Hard- und Software müssen vor unbefugtem Zugang geschützt werden.

- Zum Einsatz des Zutrittskontrollsystems sind Regelungen in schriftlicher Form zu treffen.

Zutrittskontrollsysteme und Zeiterfassungssysteme
Zeiterfassungssysteme dienen in der Regel zur Ermittlung der Arbeitszeit der Mitarbeiter. Bei den kombinierten Zutrittskontroll- und Zeiterfassungssystemen wird bei der Anmeldung am Erfassungsterminal zusätzlich zur Prüfung der entsprechenden Zutrittsberechtigung eine Speicherung der Kommt- bzw. Geht-Zeit des Mitarbeiters durchgeführt.
Auch hier ist die o. g. datenschutzrechtliche Freigabe des Verfahrens und die Mitbestimmung des Personalrates erforderlich. Es ist darauf zu achten, daß jedes System über eine separate Zugangskontrolle verfügt und daß die Funktion des Zutrittskontrollsystems ausschließlich der Überprüfung unberechtigter Zutritte und die Funktion der Zeiterfassung ausschließlich der Erfassung der Arbeitszeit dient. Liegt die Auswertung der Daten in unterschiedlichen Zuständigkeitsbereichen (z. B. Zutrittskontrolle beim Sicherheitsbeauftragten der Behörde und Zeiterfassungskontrolle bei der Personalabteilung), so ist sicherzustellen, daß auch die erforderlichen Auswertungen voneinander getrennt erfolgen.

15.6 Datenschutzfreundliche Technologien

Immer mehr Bürger nutzen die moderne Informations- und Kommunikationstechnik. Die derzeit hier zum Einsatz kommenden Verfahren und Technologien berücksichtigen allerdings nicht immer in ausreichendem Maße datenschutzrechtliche Erfordernisse. Der Schutz persönlicher Daten erfolgt zumeist durch herkömmliche Sicherheitsfunktionen, wie Zugangs-, Zutritts- und Zugriffskontrolle, soweit überhaupt entsprechende Sicherheitsmechanismen für deren Realisierung vorgesehen sind. Der Schutz der Privatsphäre des einzelnen hängt somit lediglich von der Wirksamkeit der ergriffenen technischen und organisatorischen Maßnahmen und der Gewissenhaftigkeit ab, mit der diese durchgeführt werden. Andererseits werden beim Benutzen solcher Systeme eine Vielzahl persönlicher Daten des Nutzers elektronisch erfaßt und gespeichert, ohne daß dies für die Zweckerfüllung immer notwendig ist. So fallen beispielsweise beim Bezahlen mit Scheck- oder Kreditkarten und durch Teilnahme an Online-Diensten eine Vielzahl von Einzeldaten über den Benutzer an. Wer z. B. mit Kreditkarte beim Einkaufen bezahlt, hinterläßt personenbezogene Datenspuren insofern, als seine Kontonummer, eventuell der Name, Betrag, Geschäft etc. in digitaler Form erfaßt und der Bank übermittelt werden. Solche Daten ermöglichen der Bank tiefe Einblicke in das individuelle Kaufverhalten des Kunden. Auch beim Surfen im nicht auf nationale Grenzen beschränkten Internet hinterläßt der PC-Benutzer seine digitalen Spuren. Beim Aufruf von Web-Seiten (Informations- und Kaufangebote) wird häufig jeder Zugriff mit Rechneradresse, Datum, Zeitpunkt, Aktion und Zugriffsobjekt protokolliert. Vielfach hat der Benutzer über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der über ihn gespeicherten Daten weder Kenntnis noch Kontrolle. Ein Mißbrauch dieser teils auch sensiblen digitalen Datenspuren entgegen den Interessen des Benutzers ist unschwer möglich. Insbesondere die Vernetzung der Informationstechnik bietet qualitativ neue Möglichkeiten, die teilweise an unterschiedlichen Orten gespeicherten Daten mühelos zusammenzuführen, das Verhalten des Nutzers zu registrieren und zu kontrollieren und detaillierte Persönlichkeitsprofile zu erstellen.
Eine Arbeitsgruppe „Datenschutzfreundliche Technologien“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit diesen Gefährdungen auseinandergesetzt und nach Lösungsmöglichkeiten für einen verbesserten Datenschutz durch den Einsatz von datenschutzfreundlichen Technologien gesucht. Im Mittelpunkt dieser Bestrebungen steht der Ansatz, bei der Verarbeitung personenbezogener Daten Verfahren und Technologien einzusetzen, die durch Datensparsamkeit, vorzugsweise durch Datenvermeidung, einen verbesserten Datenschutz gewährleisten. Datensparsamkeit heißt,

daß so wenig wie möglich personenbezogene Daten mit dem eingesetzten Verfahren erhoben, gespeichert und verarbeitet werden müssen. Die anzustrebende Form der Datensparsamkeit ist die Datenvermeidung, d. h. die Nutzung der IuK mittels Verfahren, die zur Erfüllung ihres Zwecks auch ohne personenbezogene Daten auskommen. Allein mit den bisherigen datenschutzrechtlichen Restriktionen der Erforderlichkeit und der Zweckbindung personenbezogener Daten kann dies nicht erreicht werden. Insbesondere durch die Nutzung neuer Ergebnisse und Möglichkeiten von Wissenschaft und Technik ist es beim Einsatz von IuK möglich, den Umgang mit personenbezogenen Daten zu reduzieren oder vollständig zu vermeiden. Ein einfaches Beispiel für eine bekannte datenvermeidende und somit datenschutzfreundliche Technologie stellt die im voraus bezahlte Telefonkarte dar. Mit ihr kann der Benutzer anonym seine Telefongespräche bezahlen. Ein Erheben und Verarbeiten personenbezogener Daten selbst für Abrechnungszwekke ist hier nicht erforderlich. Neben Risiken bietet die Technik somit auch Möglichkeiten für einen effektiven Datenschutz.

Der Grundsatz der Datenvermeidung ist sowohl im IuKDG (4.3) als auch im MDStV (4.4) enthalten. Danach haben Anbieter von Tele- bzw. Mediendiensten den Nutzern die Inanspruchnahme und Zahlung einer Leistung entweder vollständig anonym oder unter Verwendung eines Pseudonyms zu ermöglichen, soweit es technisch möglich und zumutbar ist.

Die Anonymisierung sowie Pseudonymisierung personenbezogener Daten spielen bei der Durchsetzung des Prinzips der Datensparsamkeit eine wesentliche Rolle.

Anonymisieren ist eine Veränderung personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Ein Höchstmaß an Anonymität wird erreicht, wenn das eingesetzte Verfahren, z. B. die Abrechnung einer Leistung für einen Betroffenen keine personenbezogenen Daten erfordert, wie bei der erwähnten Telefonkarte oder bei Guthabenkarten. Das Ziel datenschutzfreundlicher Verfahren sollte u. a. sein, Daten ohne Personenbezug zu erheben oder erhobene personenbezogene Daten so bald wie möglich zu anonymisieren.

Pseudonyme werden anstelle personenbezogener Identifikationsdaten, wie beispielsweise Name, Anschrift, Geburtsdatum verwendet. Diese Daten werden mit einer Zuordnungsvorschrift so verändert, daß nur mit Kenntnis und Nutzung dieser Vorschrift der Personenbezug wieder möglich ist. Pseudonymisierung sollte insbesondere dort eingesetzt werden, wo eine Anonymisierung nicht möglich ist, beispielsweise in Fällen, wo ein Personenbezug unter bestimmten Voraussetzungen wieder erforderlich ist, wie bei der Bearbeitung von Reklamationen oder der Aufdeckung eines Mißbrauchs.

Bereits heute ist eine Reihe von Technologien und Hilfsmitteln zur Erreichung von verbessertem Datenschutz durch Technik verfügbar. An Industrie und Dienstleistungsanbieter wird deshalb appelliert, datenschutzfreundliche Technologien verstärkt in ihre Anwendungssysteme einzubauen und für den Benutzer mehr Transparenz bezüglich seiner Daten zu schaffen. Die Ergebnisse der o. g. Arbeitsgruppe sind in einem Arbeitspapier „Datenschutzfreundliche Technologien“ zusammengefaßt und können von meiner Behörde angefordert werden. Anhand konkreter Beispiele werden die derzeitigen Ansätze und Bemühungen zur Verwendung datenschutzfreundlicher Technologien in unterschiedlichen Bereichen aufgezeigt und Empfehlungen in allgemeiner Form gegeben.

Zu der Notwendigkeit von Datensparsamkeit durch moderne Informationstechnik haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer 52. Konferenz im Oktober 1996 in einem Kurzbericht hingewiesen (Anlage 19). In Anbetracht der hohen Relevanz dieser Thematik verabschiedeten die Datenschutzbeauftragten auf ihrer 54. Konferenz im Oktober 1997

eine Entschließung zur Erforderlichkeit datenschutzfreundlicher Technologien (Anlage 17).

15.7 Sicherheit mit -Kryptographischen Verfahren-

15.7.1 Einführung

Einen wirksamen Schutz für die Übertragung und Speicherung von Daten bieten kryptographische Verfahren. So stellt die Verschlüsselung der Daten eine wirksame Lösung dar, um die Vertraulichkeit der Informationen zu gewährleisten. Sie verhindert auch eine gezielte inhaltliche Manipulation der Daten. Mit der digitalen Signatur können zusätzlich die Integrität und Authentizität der Daten sichergestellt werden.
Sicherheit in offenen Netzen wird in Zukunft ohne die Verwendung kryptographischer Verfahren nicht zu gewährleisten sein. Das technologische Know how sowie hardware- und softwarebasierende Verfahren zum Schutz der Vertraulichkeit, der Integrität und der Zuordenbarkeit von über Netze zu übermittelnden Nachrichten und zu speichernden Daten ist vorhanden. In der Telekommunikation kann sowohl Verschlüsselungstechnik von den Betreibern der Dienste eingesetzt werden, wie beispielsweise im Mobilfunknetz, oder die Teilnehmer schützen ihre zu übermittelnden Informationen selbst, indem sie entsprechende Verschlüsselungs- und Signaturtechniken einsetzen.
Durch den Einsatz kryptographischer Verfahren können somit wesentliche datenschutzrechtliche Forderungen zum Schutz elektronisch gespeicherter oder zu übermittelnder personenbezogener Daten angemessen realisiert werden.
Der Einsatz kryptographischer Verfahren in den öffentlichen Stellen des Landes ist derzeit noch auf Ausnahmen beschränkt. Im Hinblick auf die zunehmende elektronische Datenkommunikation dieser Stellen untereinander sowie mit anderen Stellen ist einer datenschutzgerechten Übertragung personenbezogener Daten erhöhte Aufmerksamkeit zu widmen. Gemäß § 9 Abs. 2 Nr. 9 ThürDSG sind die öffentlichen Stellen verpflichtet zu verhindern, daß u. a. bei der Übertragung personenbezogener Daten diese unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle). Der große Stellenwert, der seitens des Datenschutzes einer sicheren Übertragung elektronisch gespeicherter personenbezogener Daten beigemessen wird, spiegelt sich auch darin wider, daß die Datenschutzbeauftragten des Bundes und der Länder hierzu eine Entschließung mit entsprechenden Forderungen (Anlage 4) verabschiedet haben. In dieser Entschließung wird ausdrücklich darauf hingewiesen, daß kryptographische Verfahren besonders geeignet sind, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Es wird weiterhin hervorgehoben, daß derartige Verfahren heute Stand der Technik sind und in vielen Anwendungsfällen mit vertretbaren Aufwand eingesetzt werden können. Die Datenschutzbeauftragten fordern deshalb, sichere kryptographische Verfahren beim Transport elektronisch gespeicherter Daten, unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.
Bezüglich des in meinem 1. TB (15.3) empfohlenen Schutzstufenkonzeptes sollten alle personenbezogenen Daten, die der Stufe 2 (hoher Schutzbedarf) zuordenbar sind, zum Schutz ihrer Vertraulichkeit verschlüsselt übertragen werden. Um Manipulationen und Übertragungsfehler nachweislich festzustellen, sollte auch das Verfahren der digitalen Signatur eingesetzt werden. Mit diesem kann auch der Urheber eines elektronischen Dokuments eindeutig authentifiziert werden.
Anfragen bei meiner Dienststelle und auch bisher vor Ort gesammelte Erfahrungen lassen die Schlußfolgerung zu, daß eine Vielzahl der Anwender keine oder nur geringe Kenntnisse über die Ziele und Möglichkeiten des Einsatzes kryptographischer Verfahren besitzen und vielfach nicht wissen, daß ihre Handhabung relativ einfach ist. In Anbetracht der Bedeutung solcher Verfah-

ren für die Realisierung und Gewährleistung grundlegender Sicherheitsfunktionen im Sinne von technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit sollen im folgenden hierzu einige wesentliche Aspekte und grundlegende Zusammenhänge dieser Technologien aufgezeigt werden. Ich wende mich dabei insbesondere an die Benutzer, welche schutzwürdige Daten verarbeiten. Sie sollten die mit einem Einsatz solcher Verfahren verbundenen Vorteile erkennen und davon überzeugt, diese auch nutzen, womit solche wichtigen Sicherheitsfunktionen wie Vertraulichkeit, Datenintegrität, Zuordenbarkeit des Datenurhebers, Authentisierung von Kommunikationspartnern sowie Zutritts- und Zugriffskontrollen effektiv und wirksam realisiert werden.

15.7.2 Verschlüsselung

Die Verschlüsselung von elektronisch gespeicherten und zu übermittelnden Daten stellt einen wirksamen Sicherheitsmechanismus dar, diese vor Einsichtnahme Unbefugter zu schützen.
Die wissenschaftliche Disziplin, die sich mit dem sicheren Übermitteln von Nachrichten beschäftigt, ist die Kryptologie, die sich in die Kryptographie, die Kryptoanalyse und in die Steganographie gliedert. Die Kryptographie beschäftigt sich mit der Absicherung von Nachrichten, welche ein Sender an einen Empfänger übermittelt. In der Regel haben sowohl der Sender als auch der Empfänger ein Interesse daran, daß die Nachricht sicher übermittelt wird (unverfälscht), von keinem Dritten gelesen werden kann (vertraulich) und daß die Nachricht von dem vorgegebenen Absender auch stammt (authentisch, verbindlich). Mittels Kryptographie wird eine Nachricht (Klartext) durch Verschlüsseln in ein Chiffrat (Kryptogramm) transformiert. Dabei wird die Nachricht mit einem bestimmten mathematischen Verfahren und einem Schlüssel in eine scheinbar sinnlose Zeichenfolge umgewandelt. Das befugte Umwandeln dieser Zeichenfolge in den ursprünglichen Klartext wird als Entschlüsseln bezeichnet. Die Kryptoanalyse wird für das (unbefugte) Brechen von verschlüsselten Texten und Verschlüsselungsalgorithmen eingesetzt. Sie wird aber auch zunehmend für eine systematische Qualitätsbeurteilung und Entwicklung von Kryptoalgorithmen verwendet.
Die mathematische Funktion, die zur Ver- oder Entschlüsselung eingesetzt wird, wird als kryptographischer Algorithmus bezeichnet. Im allgemeinen werden zwei verwandte Funktionen benutzt, eine zur Ver- und eine zur Entschlüsselung. Moderne Kryptoverfahren legen ihren Algorithmus offen. Ihre Sicherheit basiert ausschließlich auf dem Einsatz von Schlüsseln. Ohne Kenntnis der Schlüssel kann ein Dritter die Nachricht nicht lesen. Je nach Algorithmus können zur Ver- und Entschlüsselung der gleiche oder unterschiedliche Schlüssel verwendet werden. Ein Algorithmus einschließlich aller möglichen Klartexte, Chiffretexte und Schlüssel wird als Kryptosystem bezeichnet.
Die Steganographie beschäftigt sich mit dem Verbergen von Nachrichten, beispielsweise als Bitfolge in digitalen Signalen, versteckt in Audio- oder Bildschirminformationen. Es handelt sich um keine Verschlüsselung im Sinne der Kryptographie.
Insbesondere durch die rasante Entwicklung der Telekommunikationstechnik, der Integration von Nachrichtenübertragung und Datenverarbeitung, werden immer mehr Daten, auch vertrauliche und personenbezogene, über zumeist öffentliche Kommunikationsnetze transportiert. Über die hiermit verbundenen grundsätzlichen Bedrohungen für einen sicheren Datenverkehr habe ich schon ausführlich in meinem 1. TB (15.6) berichtet.
Nachrichten, die über Netze übermittelt werden, passieren auf ihrem Weg vom Sender zum Empfänger in der Regel eine Vielzahl von Vermittlungsrechnern (Netzknoten), auf deren Auswahl der Absender in der Regel keinen Einfluß besitzt. Es kann nicht ausgeschlossen werden, daß auf diesen (unbekannten) Netzknoten deren Verfügungsberechtigte (beispielsweise System-

verwalter) lesend auf die Nachrichten zugreifen und auch gezielt Inhalts- und Adreßmanipulationen vornehmen können. Der mögliche Einsatz von Programmen, die den Datenverkehr abhören und ihn nach bestimmten Textpassagen durchsuchen können, erhöhen das Sicherheitsrisiko.
Um der Gefahr des unbefugten Informationsgewinnes durch Dritte wirksam zu begegnen und somit einen Verlust der Vertraulichkeit von Informationen sowie deren gezielte Manipulation zu verhindern, bietet sich derzeit als effiziente Schutzmaßnahme nur eine Verschlüsselung der Daten an. Dies gilt auch für alle mittels Telefon oder Telefax (15.12) übertragenen vertraulichen Nachrichten. Mit der zunehmenden Datenkommunikation wird somit eine Verschlüsselung von Daten für eine sichere Übertragung immer wichtiger.
Eine Verschlüsselung von Daten zum Schutz ihrer Vertraulichkeit und zur Abwehr gezielter inhaltlicher Manipulationen bietet sich auch für die Speicherung schutzwürdiger Daten an. Somit können auch langfristig elektronisch archivierte Daten oder durch Verlust bzw. Diebstahl von Computern in den Besitz von Dritten geratene Daten wirksam vor unbefugter Kenntnisnahme geschützt werden.
Zentral oder lokal elektronisch gespeicherte Daten sind im herkömmlichen Sinne zumeist durch Paßworte in Verbindung mit logischen Zugriffsrechten gesichert. Diese Maßnahmen sind jedoch, wie die Praxis zeigt, nicht immer ausreichend, um schutzwürdige Daten wirksam abzusichern. In allen Fällen, in denen die Möglichkeit besteht, einen physikalischen Zugriff auf die Daten vorzunehmen, sind diese Sicherheitsmechanismen unzureichend. So ist z. B. ein Zugriffsschutz, der nur auf der Anwendungsebene implementiert ist, insofern lückenhaft, als über die Betriebssystemebene ein physikalischer Zugriff auf die Daten möglich ist. Selbst wenn unbefugten Benutzern dieser Zugriff verwehrt ist, besteht die Gefahr, daß der Inhalt externer Speicher (Magnetplatte, Magnetbänder, Disketten) zweckentfremdet, beispielsweise durch Diebstahl oder Wartung (15.10), auf anderen Rechnern gelesen werden kann. Aber auch Systemverwalter können auf Dateien zugreifen. Somit kann nur durch die Verschlüsselung der Daten deren Vertraulichkeit sichergestellt werden und zwar völlig unabhängig davon, ob auf diese Daten auch Unbefugte zugreifen können. Insbesondere bietet sich auch eine Verschlüsselung für schutzwürdige Daten an, die im Auftrag verarbeitet werden. Ebenso aber auch zur Sicherung von sensiblen Daten auf mobilen PC (1. TB, 15.8) oder Chipkarten (15.9 u. 1. TB, 15.10.3).
Daten können sowohl mittels Hard- als auch Software verschlüsselt werden. Verschlüsselungsgeräte für eine sichere Datenübertragung werden in zahlreichen Varianten angeboten. Problemlos ist beispielsweise die Verschlüsselung von Telefongesprächen, Fax- oder Datenübertragungen und Videokonferenzen heute technisch möglich. Ein besonders wirkungsvoller Schutz wird durch eine sogenannte Ende-zu-Ende-Verschlüsselung ermöglicht. Sie umfaßt den gesamten Übertragungsweg vom Absender zum Empfänger. Die Ver- und Entschlüsselung erfolgt hier unmittelbar am jeweiligen Endgerät (Arbeitsplatz-PC, Telefon, Faxgerät). Im Gegensatz dazu wird bei einer sogenannten Bündel-Verschlüsselung nur der Übertragungsweg zwischen den zentralen Kommunikationssystemen (Telekommunikationsanlage, Kommunikationsserver) abgesichert. Hier verläuft die Datenübertragung zwischen den zentralen lokalen Netzkomponenten und dem Endgerät unverschlüsselt. Letztendlich muß der Anwender entsprechend dem Schutzbedürfnis der zu übermittelnden Daten entscheiden, ob eine Ende-zu-Ende-Verschlüsselung, Bündel-Verschlüsselung oder eine Kombination beider Methoden erforderlich ist.
Man unterscheidet grundsätzlich zwei Arten von Verfahren zur Verschlüsselung, die symmetrischen und die asymmetrischen Verfahren. In der Praxis werden zur Verschlüsselung umfangreicher Nachrichten auch beide Verfahren vorteilhaft kombiniert eingesetzt. Die Nachrichten werden mit einem symmetrischen Verfahren und der hierfür eingesetzte Schlüssel mit einem asymmetrischen Verfahren verschlüsselt mitübertragen. Damit nutzt man das

vorteilhafte Schlüsselmanagement der asymmetrischen Verfahren als auch die hohe Verschlüsselungsrate der symmetrischen Verfahren.
Die Sicherheit kryptographischer Verfahren hängt zum einen von dem zugrundeliegenden mathematischen Verfahren ab, zum anderen von der Schlüssellänge. Ähnlich wie bei einem Tresor mit Nummernschloß kann ein Angreifer durch systematisches Ausprobieren aller Schlüsselvarianten (brute force attack) den Text entschlüsseln. Auf diese Weise wurde in den USA im Jahr 1997 der 56 Bit DES-Schlüssel, der ca. 72 Billiarden mögliche Schlüssel umfaßt, geknackt, allerdings mit der geballten Kraft von 14.000 über das Internet zusammengeschlossenen Computern, mit denen in jeder Sekunde 7 Milliarden Schlüssel ausprobiert werden konnten.

15.7.3 Symmetrische Verfahren

In der Regel wird zur Ver- und Entschlüsselung bei symmetrischen Verfahren ein geheimer Schlüssel verwendet, den Sender und Empfänger vorher vereinbaren müssen bzw. der Sender dem Empfänger auf einem sicheren Weg mitteilen muß. Die verschlüsselte Nachricht kann dann auf offenem Wege vom Sender zum Empfänger gelangen. Die Schlüsselabsprache kann auf unterschiedlichen Wegen und mit unterschiedlicher Sicherheit erfolgen. Ein Austausch des Schlüssels auf einem unsicheren Weg kann die Vertraulichkeit der gesamten Kommunikation gefährden.
Eine sichere Übermittlung des Schlüssels ist durch den zusätzlichen Einsatz eines asymmetrischen Verschlüsselungsverfahrens möglich, indem der vom Sender beliebig festgelegte symmetrische Schlüssel mit dem öffentlichen Schlüssel des Empfängers kryptiert und der Nachricht beigefügt wird. Der Empfänger dechiffriert wieder den Schlüssel mit seinem privaten Schlüssel.
Symmetrische Verfahren eignen sich besonders für die Verschlüsselung umfangreicher Nachrichten, da sie eine sehr schnelle Chiffrierung (hohe Verschlüsselungsrate) ermöglichen. Ein Nachteil der symmetrischen Verfahren kann in der großen Anzahl der zu vereinbarenden und zu verwaltenden Schlüssel bestehen, wenn ein Sender mit mehreren Teilnehmern kommuniziert. Für jedes Teilnehmerpaar wird genau ein Schlüssel benötigt. Kommuniziert ein Teilnehmer mit 100 Teilnehmern, so benötigt er hierfür 100 unterschiedliche Schlüssel. Kommunizieren alle Teilnehmer untereinander, erhöht sich diese Zahl schon auf 4950 Schlüssel. Ungünstig ist auch der vor einer erstmaligen Kommunikation notwendige Schlüsselaustausch. Weiterhin kann der Empfänger anhand der übermittelten Informationen nicht überprüfen, ob die Nachricht unversehrt übermittelt wurde und von dem ausgewiesenen Absender tatsächlich stammt.
Ein bekannter Vertreter der symmetrischen Verfahren ist der DES (Data Encryption Standard). DES stellt seit 20 Jahren einen weltweiten Standard dar. Die Daten werden in Blöcken von je 64 Bit Länge verschlüsselt. Der Algorithmus erhält als Eingabe einen Block von 64 Bit Klartext und liefert als Ausgabe 64 Bit Chiffretext. Sowohl bei der Ver- als auch bei Entschlüsselung kommt der gleiche Algorithmus zur Anwendung. Wegen der geringen Schlüssellänge von nur 56 Bit wird der DES von Experten als nicht sicher eingeschätzt. Bessere Sicherheit bietet der sogenannte Triple-DES mit einer Schlüssellänge von 112 Bit.
Ein weiterhin weit verbreitetes symmetrisches Verfahren ist IDEA (International Data Encryption Algorithm). Der 1990 veröffentlichte Algorithmus arbeitet mit Klartextblöcken in einer Länge von 64 Bit. Der Schlüssel ist 128 Bit lang. Auch hier dient der gleiche Algorithmus sowohl zur Ver- als auch zur Entschlüsselung. Er beruht auf einem sehr überzeugenden theoretischen Fundament und wird von den z. Z. öffentlich verfügbaren symmetrischen Verfahren als derzeit sicherster Algorithmus angesehen. Das Verfahren ist patentiert und muß für kommerzielle Anwendung lizensiert werden. Der Algorithmus ist in der öffentlich zugänglichen Verschlüsselungs-Software

PGP (Pretty Good Privacy) implementiert und kommt dadurch weltweit zum Einsatz.

15.7.4 Asymmetrische Verfahren

Bei asymmetrischen Verschlüsselungsverfahren (Public-Key-Verfahren) verfügt jeder Teilnehmer über genau ein Paar von zwei Schlüsseln. Der eine Schlüssel ist der geheimzuhaltende sogenannte private Schlüssel (Private Key) des Besitzers. Dieser darf nur von ihm verwendet und keiner weiteren Person mitgeteilt werden. Der zweite Schlüssel ist der sogenannte öffentliche Schlüssel (Public Key) des Besitzers, der für alle Kommunikationspartner analog einem Telefonbuch, öffentlich zur Verfügung gestellt werden kann. Der öffentliche und der private Schlüssel sind invers zueinander, d. h. wird mit einem Schlüssel die Nachricht kryptiert, so kann mit dem zugehörigen anderen Schlüssel diese Nachricht wieder entschlüsselt werden. Aus der Kenntnis nur eines Schlüssels kann der andere Schlüssel nach derzeitigem Erkenntnisstand praktisch nicht ermittelt werden. Eine solche Ermittlung beispielsweise des privaten Schlüssels aus dem verfügbaren öffentlichen Schlüssel hängt entscheidend von der gewählten Schlüssellänge ab. Bisher galt eine Schlüssellänge von 512 Bit (155 Dezimalstellen) als unüberwindbar. Die Entwicklung immer leistungsfähigerer Rechentechnik zwingt aber im Interesse der Sicherheit der asymmetrischen Verfahren, eine höhere Schlüssellänge zu fordern. Je länger der eingesetzte Schlüssel ist, um so größer ist der zu betreibende Aufwand, systematisch den Schlüssel zu bestimmen.
Der Nachrichtenaustausch mit einem asymmetrischen Verfahren erfolgt, indem der Absender seine Nachricht mit dem öffentlichen Schlüssel (Chiffrierschlüssel) des Empfängers verschlüsselt. Den zum Entschlüsseln notwendigen privaten Schlüssel (Dechiffrier-Schlüssel) besitzt nur der Empfänger. Ist dieser Schlüssel nicht offenbart worden, kann somit nur der Empfänger die Nachricht im Klartext zur Kenntnis nehmen. Damit ist selbst der Absender nicht in der Lage aus der chiffrierten Nachricht wieder den ursprünglichen Text herzustellen.
Asymmetrische Verschlüsselungsverfahren werden auch eingesetzt, um die Authentizität der Kommunikationspartner, die Datenintegrität und die Nicht-Abstreitbarkeit des Ursprungs der Nachricht sicherzustellen (Digitale Signatur).
Ein wesentlicher Vorteil asymmetrischer Verfahren gegenüber symmetrischer Verfahren besteht darin, daß kein Schlüsselaustausch zwischen den Teilnehmern erforderlich ist. Gesichert sein muß allerdings, daß der in einem allgemein zugänglichen Verzeichnis gespeicherte öffentliche Schlüssel auch wirklich zu dem ausgewiesenen Inhaber (Besitzer) gehört. Diese Zuordnung kann durch eine persönliche Überprüfung sichergestellt oder viel effektiver durch vertrauenswürdige Dritte (Zertifizierungsstellen) gewährleistet werden (15.8). Im Gegensatz zu den symmetrischen Verfahren weisen asymmetrische Verfahren eine vergleichsweise geringere Verschlüsselungsrate bedingt durch ihre große Komplexität auf. Das bekannteste asymmetrische Verfahren ist der nach seinen Erfindern Rivest, Schamier und Adleman benannte RSA-Algorithmus.

15.7.5 Digitale Signatur

Die verstärkte Nutzung auch öffentlicher Netze für die elektronische Kommunikation auch im Sinne der Rechtsverbindlichkeit fordert neben der Wahrung der Vertraulichkeit auch die Sicherung der Integrität der Daten und ihre Authentizität. Die Verschlüsselung gewährleistet „nur“ die Vertraulichkeit der Daten. Dies ist in vielen Fällen kein umfassender Schutz. Insbesondere muß auch die Unversehrtheit der Daten (Datenintegrität) gewährleistet wer-

den. Der Empfänger von Daten muß aber auch sicher sein, daß diese dem Absender eindeutig zuordenbar sind.
Die asymmetrische Verschlüsselung wird nicht nur zur Gewährleistung der Vertraulichkeit einer Nachricht eingesetzt. Auch die Authentizität des Senders und die Integrität der Nachricht kann damit abgesichert werden. Der erste vollständige asymmetrische Algorithmus, der sich sowohl für Verschlüsselung als auch für den Nachweis der Authentizität und der Integrität einer Nachricht eignet, ist RSA.
Will der Sender beweisen, daß die Nachricht von ihm stammt, verschlüsselt er die Nachricht mit seinem privaten Schlüssel und schickt die so verschlüsselte Nachricht mit dem Klartext zusammen an den Empfänger. Dieser entschlüsselt mit dem öffentlichen Schlüssel des vermutlichen Absenders die verschlüsselte Nachricht und vergleicht sie mit dem ebenfalls übermittelten offenen Text. Wird hierbei keine Abweichung festgestellt, ist sowohl von der Integrität der Nachricht, als auch der Authentizität des Absenders auszugehen. Um dieses Verfahren effektiver zu gestalten, wird mittels eines mathematischen Verfahrens (Hash-Verfahren) ein Komprimat (Hash-Wert) von der beliebig langen Nachricht erzeugt. Der Hash-Wert stellt eine Prüfsumme (häufig 128 Bit lang) dar, welche eindeutig die Nachricht identifiziert. Man spricht hier auch von einem digitalen Fingerabdruck, genannt MAC (Message Authentication Code). In der Regel werden hier sichere Hash-Funktionen eingesetzt, die verhindern, daß unterschiedliche Nachrichten den gleichen Hash-Wert ergeben und daß aus einem Hash-Wert die ursprüngliche Nachricht abgeleitet werden kann. Man bezeichnet solche Funktionen auch als Einwegfunktionen. Sie erlauben nur in einer Richtung, nämlich für eine vorgegebene Nachricht, einen eindeutigen Prüfwert zu ermitteln. Umgekehrt kann aus diesem Wert nicht wieder die ursprüngliche Nachricht erzeugt werden. Der Sender erzeugt also zuerst automatisiert aus seiner Nachricht einen Hash-Wert, der anschließend mit seinem privaten Schlüssel kryptiert wird. Dieser jetzt verschlüsselte komprimierte Hash-Wert wird als digitale Signatur bezeichnet. Die digitale Signatur wird zusammen mit der Nachricht übermittelt. Der Empfänger überprüft die Integrität der übermittelten Nachricht und die Authentizität des vermutlichen Absenders, indem er nach dem gleichen Verfahren des Senders aus der übermittelten Nachricht den Hash-Wert erzeugt sowie den vom Absender übermittelten Hash-Wert mit dessen öffentlichen Schlüssel dechiffriert und beide Hash-Werte auf Übereinstimmung prüft. Liegt diese vor, ist sowohl die Unversehrtheit der Nachricht als auch die Authentizität des vermutlichen Absenders bewiesen.
Bei der Bildung der digitalen Signatur wird, im Gegensatz zur herkömmlichen Signatur, in Form der manuellen Unterschrift des Absenders, jedes einzelne Zeichen des Textes einbezogen. Bei Abweichen auch nur eines Bits der übermittelten Nachricht stimmen somit der mitgelieferte Hash-Wert und der vom Empfänger erzeugte nicht überein.
Wird zusätzlich die Vertraulichkeit der übermittelten Nachricht gefordert, wird auf der Absenderseite die Nachricht zuerst mit dem eigenen geheimen Schlüssel signiert und anschließend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Auf der Empfängerseite wird die Nachricht mit dem privaten Schlüssel entschlüsselt und anschließend, wie beschrieben, die digitale Signatur auf Echtheit geprüft.

15.7.6 Kryptokontroverse

In der Vergangenheit war der Einsatz kryptographischer Verfahren zur Nachrichtenverschlüsselung vorwiegend auf den militärischen und geheimdienstlichen Bereich beschränkt. Der stark zunehmende Kommunikationsverkehr in allen gesellschaftlichen Bereichen bewirkt zunehmend nun auch folgerichtig im privaten und geschäftlichen Bereich den Einsatz dieser Verfahren. Entsprechende Verschlüsselungsverfahren (15.7.3, 15.7.4) stehen zur Verfügung und mit dem Signaturgesetz (15.8) werden die Voraussetzungen für

eine öffentliche Schlüsselverwaltung vorgegeben. Somit kann jeder Bürger das Recht auf informationelle Selbstbestimmung seiner Daten wahrnehmen, aber auch die Wirtschaft ihre Interessen auf Vertraulichkeit wahren. Der Einsatz von Verschlüsselungsverfahren erreicht somit eine neue Dimension. Daß sich auch kriminelle Täter, insbesondere das organisierte Verbrechen, solcher Verfahren bedienen wird, ist naheliegend. Entsprechende Überlegungen, inwieweit hierdurch ihre Aufgaben zur Bekämpfung von Straftaten beeinträchtigt werden, müssen zwangsläufig auch die Sicherheitsbehörden anstellen. Den berechtigten Schutzinteressen von Bürgern und der Wirtschaft nach absoluter Vertraulichkeit ihrer Daten steht die Notwendigkeit gegenüber, die Bürger vor Verbrechen und staatsgefährdenden Aktionen zu schützen. Dieser Interessenkonflikt wird in der Öffentlichkeit unter dem Thema Kryptokontroverse heftig diskutiert. Hiermit verbunden sind eine Reihe grundlegender Fragen. In Deutschland ist bisher der Einsatz von Verschlüsselungsverfahren ohne Einschränkungen möglich. Jeder Bürger kann somit wirksamen Datenschutz in eigener Regie betreiben. Für mögliche Regulierungen staatlicher Stellen beim Einsatz kryptographischer Verfahren, um unter bestimmten Voraussetzungen auch verschlüsselte Daten durch Einsatz bestimmter Verfahren wieder zu entschlüsseln, wären drei Arten von Krypto-Reglementierungen denkbar:

- Der Einsatz von Verschlüsselungsverfahren wird generell verboten oder einem Genehmigungsvorbehalt unterstellt.
- Es werden nur Algorithmen und Verfahren zur Verschlüsselung zugelassen, welche den Sicherheitsbehörden bekannte Schwachstellen aufweisen.
- Eine Verschlüsselung wird erlaubt, wenn die verwendeten Schlüssel oder Teile dieser an bestimmten Stellen hinterlegt werden, auf die im Falle einer Strafverfolgung die Sicherheitsbehörden Zugriff besitzen.

Jede der aufgezeigten Reglementierungen erfordert eine Überwachung durch eine entsprechende Kontrollinstanz. In Fachkreisen herrscht Übereinstimmung dahingehend, daß diese Überwachung jederzeit unterlaufen werden kann. So steht beispielsweise mit der Steganographie (15.7.2) eine Technik zur Verfügung, mit der Nachrichten zumeist unbemerkt für Ermittler oder Dritte versteckt übermittelt werden können. Entsprechende Programme stehen hierfür zur Verfügung. Aber auch mit zwischen den Kommunikationsteilnehmern vereinbarten sprachlichen Codes können die Reglementierungen ausgehebelt werden. Ein erlaubter Einsatz von Verschlüsselung mit o. g. Schwachstellen kann unterlaufen werden, indem die Nachricht vor einer Verschlüsselung in dem erlaubten Rahmen mit einem nicht reglementierten Verfahren chiffriert wird. Diese Doppelverschlüsselung festzustellen, erfordert eine gezielte Überwachung, im Ergebnis dessen die Nachricht weiterhin geheim bleibt.

Auch die zwangsweise Hinterlegung von Schlüsseln birgt insofern Risiken, als derzeit keine Technik bekannt ist, hinterlegte Schlüssel sicher aufzubewahren. Auswirkungen hätte dies unmittelbar auf eine dann zweifelhafte rechtsverbindliche Kommunikation mittels digitaler Signatur entsprechend dem Signaturgesetz (15.8). Denn die hier verwendeten Schlüsselpaare bieten sich optimal auch für eine Verschlüsselung an.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich in einer Entschließung (Anlage 8) nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird.

Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verankertes Recht. Eine Reglementierung der Verschlüsselung erscheint aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen - insbesondere im weltweiten Datenverkehr - ohnehin leicht zu umgehen und kaum kontrollierbar wären.

15.8 Das Signaturgesetz und die Signaturverordnung - ein wichtiger Schritt zum elektronischen Rechtsverkehr elektronischer Dokumente

Die weltweite Nutzung moderner Informations- und Kommunikationssysteme bewirkt auch eine zunehmende Erstellung, Verarbeitung, Kommunikation und Nutzung von Dokumenten auf der Basis digitaler Daten. Vermehrt werden beispielsweise E-Mail und Dokumentenmanagement (Workflow)-Systeme zur Übermittlung und Verwaltung solcher elektronischer Dokumente eingesetzt. Im Gegensatz zu Daten in Papierform sind elektronische Daten, die als Bitfolgen vorliegen, ohne sicherheitstechnische Vorkehrungen jederzeit ohne Nachweis von Spuren veränderbar und somit auch leicht fälschbar. Ihre Integrität ist somit nicht ausreichend sichergestellt. Auch die Authentizität des Urhebers elektronischer Daten kann nicht sicher nachgewiesen werden. Ohne den Nachweis der Integrität und Authentizität besitzen elektronische Dokumente keinen Beweiswert und damit auch keine rechtliche Verbindlichkeit.
Von einem Gericht anerkannte Dokumente (Verträge, Willenserklärungen, Briefe) waren somit bisher dem Datenträger Papier vorbehalten, deren handschriftliche Unterzeichnung eine ausschlaggebende Rolle spielt. Ungeachtet der technischen Möglichkeiten sind Medienbrüche somit zwangsläufig erforderlich, um zu Beweiszwecken Dokumente auf Papier auszudrucken und handschriftlich zu unterschreiben. Dies wirft insbesondere für den zunehmenden elektronischen Geschäftsverkehr (Bestellungen, Auftragsvergaben, Zahlungsanweisungen etc.) Probleme auf, zumal auch die technischen Möglichkeiten vorhanden sind, elektronische Dokumente auf Echtheit und Unversehrtheit zu prüfen.
Um die elektronische Kommunikation und Speicherung von Nachrichten beweissicher zu realisieren, ist Voraussetzung, daß digitale Dokumente bezüglich ihres Inhaltes und ihres Urhebers fälschungssicher sein müssen. Inhaltliche Manipulationen müssen eindeutig feststellbar sein und auch der Urheber eines Dokumentes muß eindeutig bestimmbar sein, so daß die Urheberschaft nicht mit Erfolg geleugnet werden kann. Kryptographische Verfahren ermöglichen solche Lösungen unter Einsatz von digitalen Signaturen (15.7.5), mit welchen diese Forderungen erfüllt werden. Bisher fehlte es jedoch an entsprechenden gesetzlichen Rahmenbedingungen, um die Verbindlichkeit von Willensäußerungen in digitaler Form auf breiter Ebene anzuerkennen. Als einen ersten und wesentlichen Schritt in dieser Richtung verabschiedete der Bundesgesetzgeber mit dem Signaturgesetz (SigG) als Art. 3 zum Informations- und Kommunikationsdienste-Gesetz (IuKDG) vom 22.07.1997 jetzt verbindliche Rahmenbedingungen für eine sichere digitale Signatur. Hiermit betrat der Gesetzgeber Neuland. Das Ziel ist, jedermann zu ermöglichen, den Inhaber eines Signaturschlüssels sowie die Unverfälschtheit von digitalen Daten festzustellen und auch gegenüber Dritten beweisen zu können. Regelungen darüber, wann digitale Signaturen nach dem SigG anzuwenden sind und welcher Beweiswert ihnen zukommt, bleiben allerdings den speziellen Rechtsvorschriften (z. B. Prozeßordnungen) vorbehalten, die hierzu angepaßt werden müssen. Eine digitale Signatur im Sinne des Gesetzes ist ein mit Hilfe eines privaten (geheimen) Signaturschlüssel erzeugtes Siegel zu digitalen Daten, welches unter Einbeziehung des zu signierenden Datenbestandes automatisiert erzeugt und diesen angehangen wird. In der Regel werden nicht die digitalen Daten selbst signiert, sondern ein aus diesen mit einer mathematischen Funktion (Hash-Algorithmus) ermittelter verdichteter Wert, der diese Daten unumkehrbar repräsentiert.
Für den Aufbau einer erforderlichen bundesweiten Sicherheitsinfrastruktur sowie für die Wahrung der berechtigten Interessen der Signaturschlüssel-Inhaber schafft das SigG grundlegende Bedingungen. Der Aufbau der Sicherheitsinfrastruktur und die Dienstleistung der Zertifizierung, d. h. Zuordnung von Signaturschlüsseln zu natürlichen Personen, soll durch die Wirt-

schaft im freien Wettbewerb erfolgen. Der staatliche Beitrag ist auf die Lizenzvergabe und die Kontrolle lizensierter vertrauenswürdiger Zertifizierungsstellen durch die am 01.01.1998 zu errichtende Regulierungsbehörde für Post und Telekommunikation (nach § 66 des Telekommunikationsgesetzes) begrenzt. Voraussetzung für die Erteilung einer Lizenz ist, daß die Zertifizierungsstelle u. a. über die erforderliche Zuverlässigkeit, Fachkunde und ein Sicherheitskonzept verfügen muß.

Das SigG verlangt eine hohe Fälschungssicherheit digitaler Signaturen. Es läßt hierfür Raum für unterschiedliche technische Lösungen, die allerdings durch von der Regulierungsbehörde anerkannte Stellen (z. B. TÜV) geprüft und bestätigt werden müssen. Auch die für das Verfahren eingesetzten technischen Komponenten müssen nach dem Stand der Technik hinreichend geprüft sein. Für die Erzeugung und Prüfung digitaler Signaturen wird ausschließlich die Verwendung eines Public-Key-Verfahrens (15.7.4) gefordert, d. h. Verschlüsselungsverfahren, die mit einem privaten (geheimen) und einem öffentlichen Schlüssel arbeiten. Spezielle Algorithmen zur Schlüsselgenerierung, zur Hash-Funktion und zum Signaturmechanismus werden nicht vorgeschrieben.

Die Signaturschlüssel (und damit digitale Signaturen) werden an natürliche Personen gebunden. Nach dem SigG benötigt jeder Benutzer des Verfahrens der digitalen Signatur ein Schlüsselpaar, bestehend aus einem privaten und öffentlichen Schlüssel sowie ein elektronisches Zertifikat, das die Zuordnung zum Signaturinhaber bestätigt. Ein solches Zertifikat, das auch digital erstellt werden kann, weist im einfachsten Fall die von einer Zertifizierungsstelle bestätigte Zuordnung zwischen öffentlichen Schlüssel und Namen des regulären Schlüsselinhabers aus. Es kann weitere Erkennungsmerkmale des Benutzers sowie die Gültigkeitsdauer des Zertifikats umfassen. Um die Authentizität des Urhebers einer digitalen Signatur sicherzustellen, setzt ein solches Zertifikat eine zuverlässige Identifikation des Signaturschlüssel-Inhabers, z. B. gegen Vorlage des Personalausweises, durch die Zertifizierungsstelle voraus. Ohne eine solche vertrauenswürdige Vergabe von Zertifikaten wäre die mit dem Verfahren der digitalen Signatur angestrebte Fälschungssicherheit von elektronischen Dokumenten nicht gewährleistet. Jeder Benutzer könnte sich sonst eine beliebige Anzahl von öffentlichen Schlüsseln und damit an digitalen Identitäten zulegen. Desweiteren wäre ein Signieren unter dem Namen eines anderen Benutzers möglich.

Die Zertifizierungsinstanz stellt nach Abschluß eines Dienstleistungsvertrages das Zertifikat und das Schlüsselpaar dem Antragsteller, z. B. auf einer Chipkarte bereit, wobei dessen privater Schlüssel weder der Zertifizierungsstelle noch dem Inhaber offenbart werden darf. Soweit der Antragsteller das Schlüsselpaar selbst generierte, muß die Zertifizierungsstelle sich davon überzeugen, daß hierfür ein Verfahren eingesetzt wurde, daß eine Offenbarung des privaten Schlüssels hinreichend ausschließt.

Die Zertifizierungsstelle muß weiterhin die Voraussetzungen dafür schaffen, daß vergebene Zertifikate auf ihre Echtheit und Gültigkeit überprüft werden können. Hierzu führt sie ein Verzeichnis über gültige und gesperrte Zertifikate. Mit Zustimmung des jeweiligen Inhabers werden die Zertifikate veröffentlicht und stehen online abrufbar zur Verfügung.

Liegt der öffentliche Signaturschlüssel des Absenders eines Dokumentes dem Empfänger nicht vor, so kann ersterer sein Zertifikat dem signierten Dokument anhängen, um somit letzterem die Prüfung seiner Signatur zu ermöglichen.

Jede Zertifizierungsstelle erhält wiederum ein von der Regulierungsbehörde, als oberste nationale Zertifizierungsstelle, ausgestelltes Signaturschlüssel-Zertifikat. Diese Zertifikate sind für den Anwender öffentlich zugänglich, damit dieser anhand des öffentlichen Schlüssels der Zertifizierungsinstanz deren erteilte Zertifikate auf ihre Echtheit überprüfen kann.

Ein Vor- oder Rückdatieren von digitalen Daten kann mittels einem Zeitstempel verhindert werden. Ein solcher Zeitstempel kann von der Zertifi-

zierungsstelle online abgerufen werden. Der Zeitstempel verkörpert eine digital signierte elektronische Bescheinigung, daß bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen haben.
Gemäß § 16 SigG wurde zur Durchführung der erforderlichen Rechtsvorschriften eine Verordnung zur digitalen Signatur (SigV) vom 22.10.1997 erlassen. Diese Verordnung enthält u. a. nähere Anforderungen an das Verfahren und die technischen Komponenten. Eine wesentliche Forderung ist unter anderem der notwendige Einsatz von Hardware zur sicheren Speicherung des privaten Schlüssels nach dem Prinzip Besitz (z. B. Chipkarte) und Wissen (PIN).
Die Sicherheit der eingesetzten kryptographischen Verfahren für digitale Signaturen wird regelmäßig durch einen Kreis führender Experten neu geprüft. Zeichnet sich ab, daß ein mathematisches Verfahren an Sicherheitswert verliert, so wird die Eignungsfeststellung nicht mehr verlängert. Die signierten Daten sind dann mit einer erneuten digitalen Signatur zu versehen, welche auf der Basis eines sicheren technischen Verfahrens erzeugt wurde. Die alte Signatur wird dabei mit eingeschlossen.
Der Benutzer, welcher das Verfahren der digitalen Signatur einsetzt, muß über einen PC verfügen, der eine Signaturkomponente und ein Chipkartenlesegerät besitzt. Auf der PIN-geschützten Chipkarte befindet sich die gesamte manipulationsgeschützte Signiertechnik, das Zertifikat sowie der private Schlüssel und die PIN. Nach Einstecken der Chipkarte und Eingabe der PIN zu seiner Authentifizierung kann der Benutzer per Mausklick Dokumente signieren bzw. signierte Dokumente auf Authentizität und Integrität prüfen lassen. Der Benutzer wählt dazu nur die Dokumente und einen von beiden Modi aus. Jedes mit dem privaten Schlüssel signierte Dokument enthält außer seinem Inhalt die digitale Signatur und wenn nötig, das Zertifikat des Signierenden. Der Empfänger kann aus diesem Zertifikat den öffentlichen Schlüssel des Absenders entnehmen, falls dieser ihm nicht bekannt ist, um damit die Signatur zu prüfen. Mittels einer Online-Abfrage im Zertifikatverzeichnis der betreffenden Zertifizierungsinstanz kann der Empfänger feststellen, ob das Zertifikat gültig ist. Von entscheidender Bedeutung für die Integrität eines elektronischen Dokumentes ist allerdings auch, daß der in digitalisierter Form gespeicherte Dokumenteninhalt dem Benutzer visuell korrekt auf seinem Bildschirm angezeigt wird. Hier erfolgte Manipulationen (z. B. durch spezielle Viren) führen dazu, daß der Benutzer ein Dokument im sicheren Glauben signiert, welches in Wirklichkeit vom gewollten und gezeichneten Inhalt wesentlich abweichen kann. Neben dem Signaturverfahren ergibt sich somit die Erforderlichkeit, daß ein solches Verfahren in einer gesicherten Infrastruktur (Hardwarebetriebssystem, Anwendungssoftware) nur zum Einsatz kommen darf bzw. eine solche voraussetzt. Die gesetzlichen Regelungen verlangen eine solche Beschaffenheit der eingesetzten technischen Komponenten, die eine Preisgabe von Identifikationsdaten oder eine Speicherung an anderer Stelle als auf den Datenträger des privaten Signaturschlüssels ausschließt. Entsprechend den gesetzlichen Vorgaben müssen die technischen Komponenten das räumliche Verändern von zum Signieren aufgerufenen Daten und das Signieren von anderen als auf dem Bildschirm angezeigten Daten verhindern.
Nach § 12 Abs. 1 SigG darf die Zertifizierungsstelle personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines Zertifikats erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Zwei wichtige Grundsätze des Datenschutzes, der Grundsatz der Erforderlichkeit und der Grundsatz der Zweckbindung werden damit verbindlich geregelt. Diese Regelungen existieren allerdings schon im allgemeinen Datenschutzrecht. Nach § 5 SigG hat die Zertifizierungsstelle auf Verlangen eines Antragstellers im Zertifikat anstelle seines Namens, ein Pseudonym aufzuführen. Damit wird einer datenschutzrechtlichen Forderung entsprochen. Der mögliche Einsatz

von Pseudonymen ist ein wichtiger Aspekt, der datenschutzfreundliche Technologien (15.6) kennzeichnet.
Nach § 12 Abs. 2 SigG hat die Zertifizierungsstelle die Daten über die Identität eines Signaturschlüsselinhabers auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des militärischen Abschirmdienstes oder des Zollkriminalamtes erforderlich ist. Die Auskünfte sind zu dokumentieren. Die ersuchende Behörde hat den Signaturschlüssel-Inhaber über die Aufdeckung des Pseudonyms zu unterrichten, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüssel-Inhabers an der Unterrichtung überwiegt.
Hervorzuheben ist, daß nach § 12 Abs. 3 SigG die Aufsichtsbehörde eine Überprüfung der Zertifizierungsstelle auch vornehmen kann, wenn keine Anhaltspunkte für eine Verletzung von Datenschutzvorschriften vorliegen.
Das Signaturgesetz ist ein wesentlicher Schritt im Hinblick darauf, eine mit einer digitalen Signatur verbundene elektronische Willenserklärung als beweiskräftig und rechtsverbindlich anzuerkennen. Elementaren datenschutzrechtlichen Forderungen nach Integrität und Authentizität von übermittelten und gespeicherten Daten wird damit entsprochen. Desweiteren wird die Basis für den breiten Einsatz von Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit schutzwürdiger Daten geschaffen. Die entsprechenden Gesetze, welche an eine bestimmte Form gebundene Willenserklärungen fordern, müßten, um der Beweiskraft eines mit einer digitalen Signatur unterzeichneten elektronischen Dokumentes Rechnung zu tragen, allerdings diesbezüglich angepaßt werden.

15.9 Anforderungen zur informationstechnischen Sicherheit bei Chipkarten

Bereits in meinem 1. TB (15.10) habe ich, ausgehend von dem zunehmenden Einsatz von Chipkarten in vielen Bereichen, deren technische und datenschutzrechtliche Aspekte dargelegt. Tendenziell werden sich künftig neue Chipkarten-Anwendungen der Prozessorchipkartentechnologie bedienen. Das bedeutet, Chipkarten werden zunehmend durch den Einsatz von Prozessorchips zu kleinen miniaturisierten Computern.
Die wichtigsten Funktionalitäten der Chipkarten sind dabei:
- Chipkarten als Speicher von Daten,
- Chipkarten als Mittel zur Authentisierung ihres Trägers,
- Chipkarten als Mittel zur Signatur von Dokumenten,
- Chipkarten als Träger elektronischer Geldbörsen.

Aus datenschutzrechtlicher Sicht ist hier eine konsequente und überzeugende Sicherheitstechnologie erforderlich.
Die Arbeitsgruppe „Chipkarten“ des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb in einem Arbeitspapier die derzeitigen Anforderungen zur informationstechnischen Sicherheit bei Chipkarten (Anlage 21) zusammengefaßt.

Ausgehend von den Gefahren der:
- unbefugten Preisgabe von Informationen (Verlust der Vertraulichkeit),
- unbefugten Veränderung von Informationen (Verlust der Integrität),
- unbefugten Vorenthaltung von Informationen oder Betriebsmittel (Verlust der Verfügbarkeit),
- unbefugten Änderung identifizierender Angaben (Verlust der Authentität),

werden in dem Arbeitspapier Empfehlungen zum Einsatz von Chipkarten gegeben, ihre technischen Grundlagen dargestellt und auf daraus resultierende sicherheitstechnische Gestaltungsspielräume und Anforderungen eingegangen.
Danach sind folgende Grundschutzmaßnahmen beispielsweise erforderlich:
- Ausstattung des Kartenkörpers mit fälschungssicheren Authentisierungsmaßnahmen, wie z. B. durch Unterschrift, Foto, Hologramme,
- Steuerung der Zugriffs- und Nutzungsberechtigungen durch die Chipkarte selbst,
- Verhinderung unbefugter Einsichtnahme von Daten, die auf der Chipkarte gespeichert sind,
- Sicherung der Kommunikation zwischen der Chipkarte, dem Kartenterminal und den ggf. im Hintergrund wirkenden Systemen.

Darüber hinaus sollten u. a. folgende Maßnahmen berücksichtigt werden:
- Die Chipkartennutzung sollte möglichst anonym erfolgen.
- Der Chipkarteninhaber sollte die Möglichkeit erhalten, die Dateninhalte und die Funktionalitäten seiner Chipkarte zu überprüfen.

In der Regel befinden sich die Chipkarten und die Kartenterminals in unterschiedlicher Verfügungsgewalt. Wird die Chipkarte in ein Kartenterminal eingeführt, gibt der Inhaber der Karte die Verfügungsgewalt über die Software auf der Karte und die ihn betreffenden Datenbestände unter Umständen auf. Der Karteninhaber sollte daher nicht nur die Möglichkeit haben, sich den Inhalt der gespeicherten Daten anzeigen zu lassen, sondern auch die Möglichkeit besitzen, die tatsächlichen Funktionen, z. B. auf neutralen Kartenterminals, testen zu können.
Es sind daher auch Sicherheitsanforderungen an Kartenterminals zu stellen, z. B.:
- Die Kartenterminals müssen über mechanisch gesicherte Gehäuse verfügen, damit eine Hardware-Manipulation verhindert oder erschwert bzw. erkennbar wird.
- Die Sicherheitsmodule, die der vertraulichen Kommunikation zwischen der Chipkarte und dem Kartenterminal dienen, müssen gegen Angriffe besonders abgesichert sein.
- Hohen Anforderungen an die Schutzwürdigkeit der Kommunikation zwischen der Chipkarte und dem Kartenterminal kann man durch den Einsatz kryptographischer Verfahren gegen Abhören und Manipulationen oder durch mechanische Maßnahmen gerecht werden.

15.10 Wartung von Informations- und Kommunikationstechnik

Grundsätzliches

Eine fachmännische Wartung ist eine grundlegende Voraussetzung, um die Verfügbarkeit von IuK-Systemen zu gewährleisten. In den letzten Jahren ist ein zunehmender Trend zu verzeichnen, die Wartung von Informationstechnischen Systemen (IT-Systemen/Großrechneranlagen, Workstation, PC, TK-Anlagen, vernetzte Systeme) durch Fremdfirmen ausführen zu lassen. Auch öffentliche Stellen bedienen sich zunehmend eines solchen Services. Als wesentliche Gründe werden hierfür wirtschaftliche Erwägungen genannt. Nach DIN 31051 wird unter Wartung „die zur Betriebsbereitschaft notwendige Instandhaltung und Instandsetzung einer Anlage“ verstanden. Instandhaltung sind dabei alle vorbeugenden zur Aufrechterhaltung der Betriebsbereitschaft der Anlage erforderlichen Leistungen.
Seitens der Wartung erfolgt hier der Zugriff auf das (noch) normal funktionsfähige System, um seinen Zustand zu überprüfen, indem technische Zustandsdaten abgefragt und analysiert werden (Diagnose). Instandsetzung bedeutet die Beseitigung der Störung an der Anlage oder den Geräten durch Reparatur und Ersatz. Hier erfolgt der Zugriff nur im Falle eines Fehlers.

Im Kern zielt die o. g. Definition auf die eingesetzte Hardware. In der Praxis bezieht Wartung im erweiterten Sinne auch die installierte System- und Anwendungssoftware ein. Bezüglich der eingesetzten Software soll unter Wartung deren Pflege, die Analyse auftretender Fehler und deren Beseitigung sowie das Vorhalten einer optimalen Systemkonfiguration verstanden werden.
Der zunehmende Einsatz von gekaufter Software führt in der Regel dazu, daß der Anwender eine Programmpflege und Fehlerbehebungen nicht mehr selbst oder nur beschränkt ausführen kann und in Folge dessen, kompetenter externer Hilfe bedarf. Hiermit verbunden ist oftmals nicht nur eine Zugangsberechtigung für das externe Wartungspersonal, sondern auch eine Zugriffsberechtigung auf die visuell lesbaren Daten, um eine effektive Fehleranalyse und erfolgreiche Fehlerbehebung zu ermöglichen.
Die Wartung der Hard- und Software kann sowohl direkt vor Ort oder auch mittels sogenannter Fernwartung/Fernbetreuung ausgeführt werden. Der Trend zur Fernwartung ist unverkennbar. Für sie sprechen Kostenargumente als auch die zeitnahe Betreuung durch verfügbare Spezialisten. Jede Wartung ist aber mit datenschutzrechtlichen Risiken verbunden, wobei diese Risiken für die auf dem IT-System vorgehaltenen Daten bei einer Fernwartung erheblich größer sind. Unabhängig davon, ob die Wartung vor Ort oder mittels Datenfernübertragung vorgenommen wird, ob sie durch Fremdfirmen (Externe) oder durch eigenes Personal erfolgt, sind technische und organisatorische Sicherheitsmaßnahmen zum Schutz der auf dem IT-System gespeicherten Daten erforderlich. Für personenbezogene Daten sind hierfür die gemäß § 9 Abs. 2 ThürDSG geforderten Sicherheitsmaßnahmen zu beachten und entsprechend umzusetzen. Insbesondere die Beauftragung von Fremdfirmen zur Durchführung der Wartungsarbeiten unter Einbeziehung der Fernwartung erfordern umfangreiche Sicherheitsvorkehrungen.

Datenschutzrechtliche Einstufung

Grundsätzlich kann nicht ausgeschlossen werden, daß im Rahmen der Wartung auch auf personenbezogene oder schutzwürdige Daten zugegriffen werden muß. Ein solcher Zugriff kann in bestimmten Konstellationen zwingend erforderlich sein, um eine Wartung erfolgreich durchzuführen. So kann z. B. bei technischen Defekten externer Speichermedien (Magnetplatte) das Kopieren der hier gespeicherten Daten mittels spezieller Hard- und Softwarekomponenten unumgänglich sein, um einen Hardwarefehler zu beheben. Aber auch zur Behebung von Softwarefehlern können Aktionen mit echten Daten nicht zwingend ausgeschlossen werden. Ebenso zeigt die Praxis, daß die im konkreten Fall zu ergreifenden Wartungsmechanismen für eine erfolgreiche Fehlerbehebung sowohl bezüglich ihrer Auswahl als auch ihrer kombinierten Ablauffolge nicht detailliert vorhergesagt werden können. Ein grundsätzliches Verbot, bei Wartungsarbeiten auf Daten zuzugreifen, ist somit in dieser Abstraktheit nicht möglich. Sofern von vornherein nicht ausgeschlossen werden kann, daß Mitarbeiter von (externen) Wartungsfirmen Zugriff auf personenbezogene Daten erhalten, ist bei einer Vergabe der Wartungsarbeiten an Dritte von einer Auftragsdatenverarbeitung nach § 8 ThürDSG auszugehen. Die Regelungen gemäß § 8 ThürDSG sind somit bei einer Wartungsmaßnahme in einer öffentlichen Stelle zu beachten und in den Wartungsvertrag einzubeziehen. Zu beachten ist aber insoweit, daß eine Auftragsdatenverarbeitung, die in den allgemeinen Datenschutzgesetzen (ThürDSG/BDSG) geregelt ist, keine Befugnis zur Offenbarung von Daten, die unter den Schutzbereich des § 203 StGB (z. B. ärztliche Schweigepflicht) fallen, enthalten. Sofern eine Einwilligung der Betroffenen nicht vorliegt, sind die speziellen, für diese Amts- und Berufsgeheimnisse erlassenen Vorschriften über die Zulässigkeit der Auftragsdatenverarbeitung zu beachten (z. B. § 27 Abs. 10 ThürKHG für Krankenhausdaten; § 80 SGB X für Sozialdaten).

Datenschutzrechtliche Risiken

Ziel der Wartung ist es, die Funktionsweise des IT-Systems so zu gewährleisten, daß es die vorgegebenen Anforderungen auch hinsichtlich von Maßnahmen zur Datensicherheit erfüllt. Der Benutzer muß sich auf die Korrektheit und Verfügbarkeit der Funktionen des Systems und der mit Hilfe dieser Funktionen gewonnenen Ergebnisse verlassen können (Verläßlichkeit von IT-Systemen). Datenschutzrechtliche Risiken bestehen somit nicht nur in einem Verlust der Vertraulichkeit und der Integrität der auf dem System vorgehaltenen Daten, sondern auch in Folge einer nicht ordnungsgemäßen Wartung durch den Verlust der Verfügbarkeit des gesamten IT-Systems bzw. einzelner seiner Funktionen.
Eine Beeinträchtigung oder der totale Verlust der Verfügbarkeit kann durch eine bewußte unbefugte Veränderung der Funktionalität des Systems oder durch unzureichend qualifiziertes Wartungspersonal verursacht werden. Das Wartungspersonal besitzt im Hinblick auf die Gewährleistung der Verfügbarkeit des IT-Systems eine Schlüsselstellung.
Die Durchführung von Korrekturen zur Behebung der Störungen erfordert oftmals Befugnisse, die dem Status von System- und Netzwerkverwaltern entsprechen. Das Wartungspersonal ist insofern privilegiert, als es über geräte- und programmtechnische Mittel verfügt, welche Datenübertragungen aufzeichnen, Datenbestände nach unterschiedlichsten Kriterien durchsuchen sowie mittels Transfer Daten abziehen können.
Ein Fehlverhalten des Wartungspersonals kann gravierende Auswirkungen auf den gesamten IT-Betrieb haben. Wird technischen Funktionsstörungen nicht vorgebeugt oder werden aufgetretene Funktionsausfälle nicht rechtzeitig erkannt und behoben, besteht die Gefahr, daß die zu verarbeitenden Daten bezüglich ihrer Integrität (Unversehrtheit) gefährdet sind.
Eine wesentliche Schwachstelle aus datenschutzrechtlicher Sicht ergibt sich insbesondere bei der Betreuung von Anwendungssoftware, da hier häufig Zugriffsrechte vergeben werden müssen, die über die Autorisierung der Anwender-Nutzer hinausgeht. Dies kann einen unbefugten Informationsgewinn (Beeinträchtigung oder Verlust der Vertraulichkeit) seitens des Wartungspersonals zur Folge haben. Aber auch die Gefahr einer unbefugten Modifikation von Daten (Beeinträchtigung oder Verlust der Integrität) kann hiermit verbunden sein.
Eine ordnungsgemäße Datenverarbeitung, welche eine elementare Voraussetzung für die Sicherheit der Daten bildet, erfordert auch eine korrekte Generierung der Anwendungsprogramme ebenso wie der vorhandenen Systemsoftware. Hierbei ist von ausschlaggebender Bedeutung, daß nur die Funktionen implementiert werden, die für einen einwandfreien Ablauf der Datenverarbeitung notwendig sind. Bei der Generierung werden häufig auch die erforderlichen Sicherheitsmechanismen installiert. Wird nun in einer umfassenden Wartung des IT-Systems auch die Pflege dieser Software und in der Folge davon sogar ihre erneute Generierung oder Teile davon einbezogen, können sich im Zuge dieser Arbeiten unmittelbar Auswirkungen gravierend auf die Gesamtfunktionalität und die Sicherheit der IT-Anwendungen ergeben.
Betriebsstörungen können auch Sicherheitsfunktionen außer Kraft setzen oder zeitweise einschränken. Hier ergeben sich Schwachstellen bezüglich möglicher Manipulationen seitens der Wartung. Insbesondere wenn nicht nachvollziehbar ist, welche Aktionen von ihr ausgelöst werden.
Sowohl die Hardware- als auch Softwarediagnose erfordern Sonderschnittstellen. Nicht immer ist es möglich, daß diese Schnittstellen vom IT-System bewußt eingeschaltet und auch von diesen kontrolliert werden können. Insbesondere für die Hardwarediagnose gibt es, zusätzliche, nicht eingeschaltete Schnittstellen, die durch den physischen Zugang gegeben sind. Aber auch

Schnittstellen für die Softwarediagnose sind trotz einer bewußten Einschaltung durch das System nur schwer im Detail zu kontrollieren.
Zusätzliche Gefahren sind mit einer Fernwartung verbunden. Diese Form der Wartung erfolgt im allgemeinen unter Nutzung öffentlicher Netze. Hiermit verbundene Risiken sind im 1. TB (15.6) aufgezeigt. Der mit der Fernwartung existierende physische Zugang zum IT-System oder sogar auf vernetzte Systeme kann mit erheblichen Gefahren für die Sicherheit des gesamten IT-Systems verbunden sein, wenn es Unbefugten gelingt, in das zu wartende System einzudringen. Die übertragenen Daten und Kennwörter sind bezüglich ihrer Vertraulichkeit und Integrität durch mögliche Zugriffe auf die Netzknoten bzw. öffentlich zugänglichen Leitungswege gefährdet. Aber auch die technischen und organisatorischen Sicherheitsvorkehrungen seitens der fernwartenden externen Stelle können zusätzliche Sicherheitsprobleme aufwerfen.

Datenschutzrechtliche Forderungen

Aus datenschutzrechtlicher Sicht ergeben sich für eine Wartung vor Ort, die mit eigenem Personal durchgeführt wird, die geringsten Risiken. Werden auf dem IT-System personenbezogene Daten mit einem hohen Schutzbedarf verarbeitet (1. TB, 15.3) sollte diese Form der Wartung angestrebt werden. Für eine andere Form der Wartung ist deren Erforderlichkeit eingehend zu prüfen. Steht kein eigenes Fachpersonal zur Verfügung, ist der Auftragnehmer unter besonderer Berücksichtigung seiner Eignung für die technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Soweit möglich, ist eine Wartung vor Ort durchzuführen. Eine Fernwartung durch externe Stellen ist auf das unumgängliche Maß zu begrenzen.
Die mit einer Wartung verbundenen datenschutzrechtlichen Risiken müssen durch gezielte technische und organisatorische Maßnahmen weitestgehend vermieden werden.
Eine Wartung durch externe Stellen ist vertraglich zu vereinbaren. Hier sind Art und Umfang der Wartung sowie die Befugnisse des Wartungspersonals hinreichend festzulegen. Ein Zugriff auf personenbezogene Daten im Rahmen einer Wartung sollte generell nur im erforderlichen Fall und nur im notwendigen Rahmen erfolgen. Eine Verarbeitung oder Nutzung der personenbezogenen Daten für andere Zwecke ist vertraglich auszuschließen. Für das Wartungspersonal ist grundsätzlich das Datengeheimnis gemäß § 6 ThürDSG bzw. § 5 BDSG zu beachten. Für eine Fremdwartung sind insbesondere spezialgesetzliche Vorgaben zu beachten. Sind beispielsweise die personenbezogenen Daten durch ein Berufs- oder besonderen Amtsgeheimnis geschützt, wobei deren unbefugte Offenbarung nach § 203 StGB bestraft werden kann, ist die Wartung vor Ort durchzuführen. Sollte sich im konkreten Fall nach einer sorgfältigen Abwägung von datenschutzrechtlichen Erfordernissen mit dem berechtigten Interesse nach einer qualifizierten Wartung ergeben, daß eine erfolgreiche Wartung nur seitens der Fremdfirma möglich ist, sollte das externe Wartungspersonal zusätzlich nach dem Verpflichtungsgesetz vom 2. März 1974 (BGBl. I S. 469, 545) verpflichtet werden.
Auch für eine Wartung durch externe Stellen gilt, daß die speichernde Stelle („Herr der Daten“) als Auftraggeber für alle Daten und Verfahren verantwortlich ist.
Die speichernde Stelle hat die technischen und organisatorischen Maßnahmen zu veranlassen, die erforderlich sind, Datenschutz und Datensicherheit zu gewährleisten. Wartungs- bzw. Betreuungsfirmen dürfen nur auf konkrete Weisung der speichernden Stellen tätig werden. Wird die Wartung durch nicht-öffentliche Stellen ausgeführt, ist der öffentliche Auftraggeber verpflichtet, vertraglich sicherzustellen, daß der Auftragnehmer die Bestimmungen des ThürDSG befolgt und sich der Kontrolle durch den TLfD unterwirft.

Der Auftraggeber hat den Landesbeauftragten für den Datenschutz über die Beauftragung zu unterrichten.
Ein Fernwartungszugang ist besonders abzusichern und zu überwachen. Hierfür werden intelligente Technologien auf dem Markt angeboten. Erst nach Durchlaufen eines sicheren Authentifikationsverfahrens und dessen positives Ergebnis sollte der angewählte Wartungsport durchgeschaltet werden. In der Regel muß der Aufbau einer Fernwartungsverbindung von der speichernden Stellen ausgehen. Es werden Verfahren angeboten, die nach dem derzeitigen Kenntnisstand eine sichere und auch gegenseitige Authentifikation realisieren (Challenge-Response-Prinzip).

Technische und organisatorische Sicherheitsmaßnahmen

Für eine Wartung/Fernwartung sind gemäß § 9 Abs. 2 ThürDSG Maßnahmen insbesondere zur Zugangs-, Speicher-, Datenträger-, Zugriffs-, Transport- und Organisationskontrolle festzulegen.
Die speichernde Stelle sollte bei einer Wartung sicherstellen, daß:
- diese nur mit ihrem Einverständnis und im Einzelfall erfolgen kann,
- sie kontrollieren kann, was bei ihrer Durchführung im einzelnen geschieht,
- der Kreis des autorisierten Wartungspersonals festgelegt ist,
- eine Fernwartungsverbindung nur von der zu wartenden Stelle aufgebaut wird, welche diese jederzeit abbrechen kann,
- das Wartungspersonal nur Zugriff nach einer positiven Identifikation und Authentifikation gegenüber dem System erhält,
- der Zeitpunkt und die Zeitdauer der Wartungsarbeit und alle wesentlichen Wartungsaktivitäten protokolliert werden,
- ein Zugriff auf personenbezogene Daten nur nach einer Einzelfallprüfung erfolgen kann,
- keine Datenträger den Bereich der speichernden Stelle unkontrolliert verlassen können,
- kein unzulässiger Datentransfer erfolgen kann,
- alle offenbarten Paßworte nach der Wartung unverzüglich geändert werden,
- auf dem IT-System gespeicherte Test- und Wartungsprogramme mit einer gesonderten Kennung vor unbefugtem Zugriff abzusichern sind,
- geprüft wird, inwieweit diese Daten vor einem unumgänglichen Zugriff ausgelagert werden können,
- das Wartungspersonal auf das Datengeheimnis verpflichtet ist und ausdrücklich eine Nutzung evtl. offenbarter personenbezogener Daten für anderweitige Zwecke strikt verboten ist.

Im Wartungsvertrag sind diese grundlegenden Forderungen entsprechend den konkreten Anforderungen und Erfordernissen vor Ort spezifiziert festzulegen sowie gegebenenfalls um weitere Sicherheitsmaßnahmen zu ergänzen, die sich beispielsweise aufgrund betriebsspezifischer Gegebenheiten ergeben können. Dieser Vertrag muß klare Regelungen zur Art und zum Umfang der Wartung sowie zur Abgrenzung der Kompetenzen und Pflichten zwischen Wartungspersonal und Personal der speichernden Stelle enthalten.

15.11 Virenschutz

Ein Computervirus ist eine Programmroutine, die sich selbst reproduziert und absichtliche Manipulationen an Programmen und Daten verursachen kann. Der Begriff Virus ist entsprechend seiner Reproduzierbarkeit dem biologischen Abbild entliehen. Eine Übertragung von Viren kann beispielsweise von einer Diskette oder CD-ROM, aus dem Internet oder über E-Mail erfolgen.
Veröffentlichte Untersuchungen zeigen, daß mit der zunehmenden Vernetzung der Informations- und Kommunikationstechnik, trotz ergriffener

Schutzmaßnahmen, die Infizierung mit einem Computer-Virus nicht immer vermeidbar ist. Unter Umständen ist deshalb der Einsatz von mehreren Anti-Viren-Programmen sinnvoll. Im Februar 1997 wurde die Zahl der bekannten Computerviren vom Virentestcenter der Universität Hamburg auf rund 13.000 beziffert und jeden Tag kommen neue Viren dazu. Viren bedrohen nicht nur die Verfügbarkeit von IT-Systemen und Programmen, sondern auch die zu verarbeitenden Daten.

Wichtig ist, das man das Virus erkennt, sein Vorhandensein nicht vertuscht und sofortige Maßnahmen zu seiner Bekämpfung ergreift. Nur so läßt sich seine Verbreitung einschränken und das Virus wirksam bekämpfen. Ein wirksamer Schutz ist nur möglich, wenn die Benutzer hierüber hinreichend informiert werden.

Meine Kontrollen zeigten, daß viele öffentliche Stellen Anti-Viren-Programme im Einsatz haben, aber nicht in jedem Fall auch entsprechende Richtlinien zur Verhaltensweise beim Auftreten von Computer-Viren zur Verfügung stehen.

Zum aktiven Schutz gegen Computerviren gibt es diverse Anti-Viren-Programme. Die Vielzahl auftretender Viren erfordert, solche Programme einzusetzen, die mit hoher Wahrscheinlichkeit erkennen, daß ein Virus als solches vorliegt, dieses konkret identifizieren und verlustarm auf Wunsch auch beseitigen können. Zahlreiche Anti-Viren-Programme setzen deshalb nicht nur normale **Scanner-Verfahren** ein, die im herkömmlichen Sinne die Dateien abtesten und mit bereits bekannten Viren vergleichen, sondern auch sogenannte heuristische- und Prüfsummenverfahren.

Heuristische Verfahren werden für die Suche nach bisher noch nicht bekannten Viren, die oft durch charakteristische Befehlsfolgen erkennbar sind, eingesetzt.

Mit Hilfe von **Prüfsummenverfahren** wird, um zusätzlich ein hohes Maß an Sicherheit zu gewährleisten, mittels eines Integritätstests geprüft, ob an bestimmten Programmen Änderungen seit deren Installation auf dem Computer vorgenommen wurden, also z. B. nichts überschrieben oder angehangen wurde.

Es gibt typische Arten von Computerviren, die teilweise auch unterschiedliche Prüfverfahren erfordern.

Programm-Viren kopieren sich an das Ende von Programmdateien und manipulieren diese, so daß der Virus vor dem infizierten Programm ausgeführt wird.

Beim Laden des Betriebssystems (Booten) werden z. B. Programmteile ausgeführt, die in nicht sichtbaren Sektoren des jeweiligen Datenträgers gespeichert sind.

Boot-Viren verlagern diesen Inhalt an eine andere Stelle und nisten sich selbst in diese Sektoren ein. Beim erneuten Hochfahren des PC gelangt dann der Boot-Virus vor dem Laden des Betriebssystems unbemerkt in den Arbeitsspeicher und kann so beispielsweise auch nicht schreibgeschützte Datenträger infizieren. Boot-Viren lassen sich durch Prüfprogramme aufspüren.

Stealth-Viren sind intelligentere Programm-Viren, die auf alle Lesezugriffe auf infizierte Dateien den Originaltext (einschließlich Originallänge) zurückgibt. Dadurch wird der vom Virus erzeugte Dateiunterschied nicht erkennbar. Anti-Viren-Programme können diese intelligenten Programm-Viren mittels heuristischer Verfahren an ihrer charakteristischen Befehlfolge erkennen.

Polymorphe Viren verändern ihre Befehlsabfolge oder verschlüsseln diese, um das Entdecken ihrer charakteristischen Befehlsfolgen zu verhindern.

Zusätzlich zu heuristischen Verfahren, die nach virentypischen Merkmalen und Verfahren suchen, ist hier der Einsatz von Prüfsummen-Verfahren zu empfehlen.

Makro-Viren werden in Dokumenten verborgen, bei denen eine Makro-Sprache zum Einsatz kommt, wie z. B. bei den Anwendungen Word für Windows oder Excel. So kann z. B. durch das Verknüpfen einer Winword-Dokumentenvorlage mit einer entsprechenden Folge von Befehlen (Makro-

Befehle) der Ablauf des Programms in vielfältigster Weise beeinflußt werden. Dieser in den letzten Jahren verbreitete Virus, von dem z. Z. ca. 50 verschiedene bekannt sind, unterscheidet sich maßgeblich von den bisherigen Virenarten, welche nur Programmdateien und keine Datendateien infizieren. Durch die Möglichkeit, auch in Datendateien umfangreiche Steuerinformationen für Layout, Ton oder Programmteile (sogenannte Makros) einzubetten, besteht nunmehr die Gefahr, daß keine saubere Trennung zwischen Datendateien und Programmdateien mehr möglich ist. Somit kann z. B. jede übermittelte Nachricht oder ihre angehängte Mitteilung mit Viren infiziert sein. Die Tatsache, daß Makroviren häufig auf unterschiedlichen Rechner-Plattformen lauffähig sind, erhöht die Gefahr der Virenübertragung zwischen verschiedenen Systemplattformen.
Die Verbreitung von Makro-Viren kann eingeschränkt werden, indem z. B. die elektronischen Dokumente und Tabellenkalkulationsdateien, die keine gewollten Makros enthalten, in Formate, die keine Makros abspeichern (z. B. RTF und DIF), abgelegt werden.

Durch die Vielzahl der im Handel erhältlichen Anti-Viren-Programme ist es unumgänglich, vorher zu spezifizieren, welche Systeme zu schützen sind (Server, Workstations, Stand-alone-PCs usw.) und über welche eingesetzten Medien Viren auf die zu sichernden Systeme gelangen können (per Datenträger oder über das Internet, per E-Mail usw.).
Dementsprechend sollten Anti-Viren-Programme ausgewählt werden, die u. a. folgende Anforderungen erfüllen:
- Das Anti-Viren-Programm sollte nicht nur in der Lage sein, viele Viren zu finden, sondern es muß sie auch identifizieren und beseitigen können.
- Um die neusten Viren bekämpfen zu können, müssen ständig aktuelle Programmversionen vom Hersteller zur Verfügung gestellt werden.
- Bei der Wahl der Anti-Viren-Programme sollte nach Möglichkeit auf das Vorhandensein eines Hintergrundscanners geachtet werden, der automatisch für alle Laufwerke einen permanenten Virenschutz bietet.
- Bei einem Einsatz im Netzwerk sollte der Hintergrundscanner sowohl auf dem Server als auch auf angeschlossenen Rechnern installierbar sein.
- Anti-Viren-Programme für E-Mails sollten alle ankommenden und auch ausgehenden Mails und deren Anlagen auf Viren überprüfen.

Eine Orientierungshilfe über die Qualität gängiger Anti-Viren-Programme stellen die in zahlreichen Fachzeitschriften regelmäßig veröffentlichten Testergebnisse dar.
Um Computer-Viren wirksam begegnen zu können sind, neben einer sorgfältigen Auswahl der geeigneten Anti-Viren-Programme, zusätzliche organisatorische Maßnahmen zu treffen, wie:
- Durchführen regelmäßiger Datensicherungen als eine wichtige Maßnahme zum ordnungsgemäßen Erhalt von Daten.
- Einsetzen der aktuellen Version der Anti-Viren-Programme, um auch neue Viren zu erkennen.
- Erstellen einer Notfall-Diskette, um ein virenfreies Hochfahren des Rechners (Booten), trotz eingetretenem Virenbefall, zu ermöglichen.
- Grundsätzlich überprüfen, inwieweit die Übernahme fremder Dateien erforderlich ist.

15.12 Datenschutz beim Telefaxen

Der Telefaxdienst wird heute routinemäßig eingesetzt, um Nachrichten an einen Empfänger zu senden. Dokumente jeglicher Art (Texte, Zeichnungen, Grafiken, Urkunden etc.) lassen sich innerhalb von Minuten als Kopie des auf der Absenderseite verbleibenden Originals übermitteln. Der ursprünglich nur als ein Sonderdienst im Rahmen der Bürokommunikation im Jahre 1979 in Deutschland eingeführte Telefaxdienst hat sich neben dem Telefondienst

zum wichtigsten Kommunikationsmittel etabliert. Telefax gehört nicht nur zur selbstverständlichen Ausstattung von Firmen, auch viele private Haushalte verfügen heute über Faxgeräte. Meine Kontrollen und auch zahlreiche Anfragen ergaben, daß viele Benutzer des Telefaxdienstes sich nicht der Risiken und Gefahren bewußt sind, welche mit einer Übermittlung personenbezogener Daten mittels Fax verbunden sein können. Die Datenschutzbeauftragten des Bundes und der Länder haben zur Thematik -Datenschutz und Telefax- eine Empfehlung veröffentlicht, die vom Arbeitskreis für technische und organisatorische Fragen der Datenschutzbeauftragten erarbeitet wurde (Anlage 20). Die Entschließung weist auf datenschutzrechtliche Risiken hin, die bei der Übermittlung schutzwürdiger Daten mittels Telefax bestehen und enthält entsprechende Hinweise, diese Risiken auszuschalten bzw. zu vermeiden. Meine nachfolgenden Ausführungen enthalten hierzu noch einige grundlegende und zusammenhängende Erläuterungen sowie Ergänzungen zum Telefaxdienst und sind insbesondere für die zahlreichen Nutzer gedacht, welche mit den Details dieser Technik nicht so vertraut sind.

Ein Telefax kann sowohl mit konventionellen Faxgeräten als auch mit speziell hierfür ausgerüsteten PCs versendet oder empfangen werden. Notwendig hierfür ist eine entsprechende Fax-Software sowie ein sogenanntes Faxmodem. Der PC-gestützte Faxversand bietet einige Vorteile gegenüber herkömmlichen Faxgeräten. Da Dokumente fast ausschließlich nur noch mittels PC erstellt werden, kann der zu versendende Text ohne Medienbruch (Ausdruck auf Papier) direkt aus der laufenden Anwendung auf dem PC an den Empfänger abgesandt werden. Dokumente müssen nicht mehr ausgedruckt werden, um anschließend ins Faxgerät wieder eingescannt und verschickt zu werden. Zeit- und Arbeitsaufwand können hierdurch eingespart werden. Beachtet werden muß aber, daß in Papierform vorliegende Dokumente zuvor gescannt werden müssen. Der Empfang von Telefaxen am PC hat ebenfalls Vorteile. Empfangene Telefaxe können auf beliebigen Drucker und somit auf normalem Papier ausgegeben werden. Die Qualität des Ausdrucks ist gegenüber herkömmlichen Faxgeräten qualitativ besser. Desweiteren kann eine so übermittelte Nachricht auch auf dem Bildschirm dargestellt werden und muß somit nur noch bei Erforderlichkeit ausgedruckt werden.

Telefonanschlüsse, an denen ein PC über ein Faxmodem angeschlossen ist, werden jetzt auch in das amtliche Telefaxverzeichnis der Telekom aufgenommen.

Auch moderne herkömmliche Telefaxgeräte sind nichts anderes als spezielle Computer, deren Funktionen über eine sogenannte „Firmware“ (Mikroprogramm) gesteuert wird. Über optische Verfahren wird der Inhalt der eingelegten Vorlage zeilenweise gescannt. Dabei wird der vorliegende Text bzw. Grafik durch einzelne Punkte, denen Graucodierungen zugewiesen sind, zerlegt. Diese digitalen Werte werden komprimiert und mittels Modem als analoge Signale über die Telefonleitung zum Faxgerät des Empfängers übertragen und hier mit Modem wieder digitalisiert und ausgedruckt.

Der Telefaxdienst hat bisher mehrere Entwicklungsstufen (Gruppen) durchlaufen. Die Einteilung in Gruppen erfolgt im wesentlichen nach der Bildauflösung und der Übertragungsgeschwindigkeit. Standard sind derzeit Faxgeräte der Gruppe 3. Es handelt sich um analoge Faxgeräte. Diese lassen sich mit sogenannten a/b-Terminal-Adaptern allerdings auch an digitalen Anschlüssen (ISDN) betreiben. Diese Adapter dienen als Dolmetscher zwischen der analogen und der digitalen ISDN-Welt. Sie übernehmen die Umwandlung der verschiedenen Protokolle sowie die Anpassung der im Vergleich langsamen analogen Übertragungsgeschwindigkeiten an die wesentlich höhere ISDN-Geschwindigkeit.

Faxgeräte der Gruppe 4 verfügen über Leistungsmerkmale, die sich nur im digitalen Netz (z. B. ISDN) realisieren lassen. Kennzeichnend ist hier eine wesentlich höhere Übertragungsgeschwindigkeit und Bildauflösung, welche die Qualität von Laserdruckern erreicht. Faxgeräte dieser Gruppe sind nicht immer kompatibel zu den weltweit verbreiteten Faxgeräten der Gruppe 3.

Im Gegensatz zur normalen Datenübertragung findet der Faxversand im Halbduplex-Betrieb statt. Zu einem bestimmten Zeitpunkt können Daten nur in einer Richtung übertragen werden, was allerdings für die einseitige Form der Kommunikation mittels Fax ausreichend ist.
Ohne zusätzliche Sicherheitsmaßnahmen ist beim Telefax die Vertraulichkeit und die Integrität der Daten und die Authentizität des Absenders nicht gewährleistet. Die Datenübermittlung erfolgt über das öffentliche Telefonnetz, so daß Telefaxen ebenso wie Telefonieren abhörbar ist. Darüber hinaus kann ein Verlust der Vertraulichkeit einerseits durch fehlerhafte Adressierungen, andererseits durch organisatorische Schwächen beim Faxempfänger verursacht werden. Die tägliche Praxis zeigt, daß falsch adressierte Faxe keine Einzelfälle sind. Fehladressierungen können darauf beruhen, daß der Absender nach Eingabe einer Empfängernummer oder nach Auswahl einer Nummer aus den Nummernspeichern diese vor Absenden des Fax nicht noch einmal einer Kontrolle unterzieht. Auslöser hierfür sind nicht selten kurzfristig umprogrammierte Zielwahltasten des Faxgerätes, welche für häufig gewählte Empfänger eingesetzt werden. Mit der erheblichen Zunahme von Telefaxanschlüssen in allen gesellschaftlichen Bereichen, insbesondere auch in den privaten Haushalten, hat sich auch die Wahrscheinlichkeit erhöht, bei einer versehentlich falsch eingegebenen Fax-Nummer unter dieser Nummer statt einem Fernsprechanschluß, wo eine Anzeige einer Fehlmeldung und keine Fax-Übertragung erfolgt, einen anderen Fax-Teilnehmer zu erreichen, welcher dann auch die zu übermittelnden Nachrichten empfängt. Vertrauliche Informationen können somit sowohl seitens des Sendenden als auch des eigentlichen Empfängers, ungewollt in unbefugte Hände geraten. Deshalb sollte die Eingabe der Fax-Nummer mit größter Sorgfalt erfolgen.
Fax-Irrläufer treten aber auch auf, wenn der Empfänger seinen Fax-Anschluß aus beliebigen Gründen gekündigt hat und den Absender hierüber nicht informierte. Um diesem Risiko zu begegnen, sollte sich der Absender im Zweifelsfall vor dem Versand durch einen Anruf vergewissern, daß der richtige Adressat unter der gewählten Nummer auch erreicht werden kann.
Die Vertraulichkeit beim Faxempfänger ist in der Regel dadurch gefährdet, daß Faxgeräte möglicherweise nicht vor unbefugtem Zugriff geschützt sind und somit die Möglichkeit besteht, eingegangene Faxe zu lesen, zu kopieren bzw. zu entwenden. Da Faxgeräte rund um die Uhr betriebsbereit sind, sind damit entstehende Gefährdungen zu berücksichtigen. Bei Thermotransfer-Faxgeräten ist die Vertraulichkeit insofern gefährdet, daß hier aufgrund des Druckverfahrens die Faxinhalte zunächst auf ein wachsbeschichtetes Farbband geschrieben werden, dessen Inhalt mittels Hitze anschließend auf Papier übertragen wird. Das Farbband, welches das negative Abbild der Faxausdrücke enthält, kann mehrere hundert Faxseiten umfassen und stellt somit bezüglich der Vertraulichkeit eine Gefährdung dar.
Zum Schutz der Vertraulichkeit, der mittels eines Faxgerätes über das Telefonnetz übermittelten Nachrichten, werden Verschlüsselungssysteme angeboten. In der Regel wird zum Ver- und Entschlüsseln der DES-Algorithmus (15.7.3) eingesetzt. Zu Beginn der Kommunikation erfolgt der Schlüsseltransfer zwischen den Kommunikationspartnern mit Hilfe des RSA-Verfahrens (15.7.4). Die hierfür notwendigen Sicherheitseinrichtungen werden zumeist zwischen der Telefondose und dem Endgerät plaziert. Diese Sicherheitseinrichtung kann mittels Chipkarte durch eine authentisierte Person aktiviert werden. Die Chipkarte enthält die Chiffrierprogramme und führt online die Ver- bzw. Entschlüsselung durch. Mit Hilfe der Chipkarten können auch Benutzergruppen festgelegt werden und Berechtigungsebenen analysiert werden. Somit kann sichergestellt werden, daß am Faxgerät ein berechtigter Empfänger die Nachricht entgegennimmt.
Beim Einsatz eines Fax-PC müssen, wie auch bei jedem anderen PC, auf dem schutzwürdige Daten gespeichert werden, ausgehend von der Sensibilität der zu sendenden bzw. empfangenen personenbezogenen Daten, technische Sicherheitsmaßnahmen ergriffen werden. Erfolgt der Einsatz von Fax-

PCs in einem Rechnernetz, so sind die hiermit zusätzlich verbundenen Sicherheitsrisiken abzuschätzen, um den Gefährdungen vorzubeugen. Insbesondere die Zugriffsrechte für eingesetzte Faxserver sind befugnisorientiert festzulegen und nachvollziehbar zu verwalten. Je nach eingesetzter Betriebs- und Netzsoftware muß entschieden werden, inwieweit zusätzliche Datenschutzsoftware zum Einsatz kommt. Mögliche technische Sicherheitsmaßnahmen, die auch für den Einsatz von Fax-PCs in Netzen zutreffen, habe ich in meinem 1. TB (15.6) aufgeführt.
PC-Faxe werden oft mit gescannten Unterschriften gekennzeichnet, wodurch sie persönlicher und verbindlicher wirken. Hier ist zu beachten, daß solche eingescannten handschriftlichen Unterschriften, Siegel- oder Stempelabdrükke nicht die Authentizität des Absenders beweisen. Jedermann kann solche Signaturen aus Dokumenten mit einem Scanner einlesen und in ein Faxdokument einfügen. Hier ist Mißbrauch jederzeit seitens des Absenders möglich, aber auch der Empfänger kann eine echte Unterschrift des Absenders zu dessen Schaden weiter verwenden. Wo es darum geht, nachweislich die Authentizität des Absenders und inhaltliche Integrität von PC-Faxen sicherzustellen, sollte deshalb die digitale Signatur (15.7.5) eingesetzt werden.

15.13 Datenspuren beim Zugriff auf Web-Server

Mit der Einführung des World Wide Web (WWW) trat das Internet seinen Siegeszug als Massenmedium an. Dieser Dienst ermöglicht mittels der Seitenbeschreibungssprache HTML (Hypertext Markup Language), Datenbestände im Internet in strukturierter und präsentativer Form auf Web-Servern bereitzustellen. Die so präsentierten Informationen werden als Hypertextdokumente bezeichnet, da sie neben Text, Grafiken und Audioabschnitte auch Referenzen enthalten können, die auf weitere HTML-Dokumente verweisen, so daß zwischen den Informationsquellen hin- und hergesprungen werden kann. Der Internet-Nutzer kommuniziert über HTML mit Hilfe eines auf seinem Rechner (Client) ablaufenden Dienstprogrammes, genannt Browser, mit dem jeweiligen Web-Server. Ein solcher Web-Browser ermöglicht die Navigation durch das WWW und stellt die vom Benutzer ausgewählten Web-Seiten auf dessen Client zur Verfügung. Für den jeweiligen Benutzer nicht immer erkennbar, werden in der Regel beim Zugriff auf Web-Seiten Daten des Benutzers aufgezeichnet, beispielsweise die Internet-Adresse des Abrufers, der verwendete Browser und die aufgerufene Web-Seite. Insbesondere sind Online-Anbieter von Waren oder elektronischen Dienstleistungen an Benutzerdaten interessiert, welche das Kaufverhalten, Interessen und Neigungen von Kunden offenbaren. Die Anbieter wollen im Regelfall aber auch wissen, auf welche Angebote bzw. Web-Seiten ihres jeweiligen Gesamtangebotes der Benutzer schon zugegriffen hat. Um solche benutzerbezogenen Aktionen u. a. nachvollziehbar aufzuzeichnen, werden von vielen Anbietern sogenannte „Cookies“ hierzu eingesetzt.
Ein Cookie ist eine kleine Textdatei, in welcher der Online-Anbieter automatisiert persönliche Daten des Benutzers sammelt. So kann der Text beispielsweise Informationen über vom Benutzer abgerufene Web-Seiten, seine hier durchgeführten Aktivitäten, dessen E-Mail-Adresse aber auch von diesem in Online-Formularen des Anbieters eingegebene Paßwörter und Kreditkartennummern beinhalten. Beim erstmaligen Zugriff auf ein Web-Angebot wird an den Browser des Client das Cookie übermittelt. Der Browser registriert die Herkunft dieser Daten und speichert sie auf der lokalen Festplatte des Benutzers ab. Bei einem erneuten Zugriff des Client auf das Web-Angebot übermittelt der Browser automatisch diesen gespeicherten Text an den Server zurück. Auf diese Daten greift der Online-Anbieter zu, um u. a. Rückschlüsse über das Kundenverhalten zu erhalten und um neue Informationen einzutragen.
Wie eine Vielzahl anderer Technologien bieten auch Cookies nützliche Funktionen für den Benutzer. Cookies werden z. B. eingesetzt, damit ein

Kunde sich einen Warenkorb über alle Web-Seiten des Anbieters zusammenstellen kann, um diese abschließend nur in einem Vorgang zu verrechnen. Desweiteren werden Cookies zunehmend genutzt, um Interessenten gezielt Angebote anzuzeigen.
Das Nutzen dieser Technologien entgegen datenschutzrechtlicher Vorschriften (§§ 4 ff. TDDSG) kann jedoch nicht ausgeschlossen werden. Eine Information der Benutzer über die o. g. Zusammenhänge sowie welche Daten und in welchem Umfang automatisch erhoben werden, ist noch die Ausnahme. Gefahren können sich für den Schutz der personenbezogenen Daten des Benutzers ergeben, so daß dieser in seinem Persönlichkeitsrecht beeinträchtigt werden kann. Ein Mißbrauch dieser Daten im weltweiten Internet ist nicht ausgeschlossen.
Das Erstellen von Cookies wird erst durch die Dienstleistung von Web-Browsern ermöglicht. Aktuelle Browser ermöglichen allerdings durch gezielte Einstellungen ihrer Optionen, den Einsatz von Cookies zu verhindern bzw. den Benutzer vor der Annahme von Cookies zu warnen. Um sich vor Cookies zu schützen, müssen diese Optionen vom Nutzer erst aktiviert werden, denn standardmäßig werden Cookies vom Browser übernommen. Es wird empfohlen, zumindestens die Warnmeldung zu aktivieren. Wem diese Meldungen zu hinderlich sind und wer Cookies grundsätzlich verhindern möchte, sollte in dem entsprechenden Konfigurationsverzeichnis des Browsers eventuell schon gespeicherte Cookie-Eintragungen löschen, eine leere Cookie-Datei anlegen und diese mit einem Schreibschutz versehen. Nach dem derzeitigen Erkenntnisstand ist somit das Speichern von Cookies nicht möglich.
Jeder Benutzer, der netzweite Dienste nutzt, sollte sich der aufgezeigten Risiken beim Zugriff auf Web-Seiten insbesondere im Internet bewußt sein, zumal die nicht mehr überschaubare Anzahl solcher Angebote auch von unseriösen Quellen stammen können.
Grundsätzlich sollten in öffentlichen Stellen Sicherheitsmaßnahmen zur Nutzung der neuen Technologien festgelegt werden.

Anlage 1

Entschließung
der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 14./15. März 1996 in Hamburg

zum

Transplantationsgesetz

Bei der anstehenden gesetzlichen Regelung, unter welchen Voraussetzungen die Entnahme von Organen zur Transplantation zulässig sein soll, werden untrennbar mit der Ausformung des Rechts auf Selbstbestimmung auch Bedingungen des Rechts auf informationelle Selbstbestimmung festgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont hierzu, daß von den im Gesetzgebungsverfahren diskutierten Modellen die „enge Zustimmungslösung“ - also eine ausdrückliche Zustimmung des Organspenders - den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet. Sie zwingt niemanden, eine Ablehnung zu dokumentieren. Sie setzt auch kein Organspenderegister voraus.

Mit einer engen Zustimmungslösung ist auch vereinbar, daß der Organspender seine Entscheidung z. B. einem nahen Angehörigen überträgt.

Anlage 2

Entschließung
der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 14./15. März 1996 in Hamburg

zu

Grundsätze für die Öffentliche Fahndung im Strafverfahren

Bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und Zeugen) wird stets das Recht des Betroffenen auf informationelle Selbstbestimmung eingeschränkt. Es bedarf daher nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15.12.1983 für alle Maßnahmen der öffentlichen Fahndung nach Personen einer normenklaren und dem Grundsatz der Verhältnismäßigkeit entsprechenden gesetzlichen Regelung, die bisher fehlt.

1. Der Gesetzgeber hat zunächst die Voraussetzungen der öffentlichen Fahndung zu regeln und dabei einen sachgerechten Ausgleich zwischen dem öffentlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen.

   Die öffentliche Fahndung sollte nur bei Verfahren wegen Verletzung bestimmter vom Gesetzgeber zu bezeichnender Straftatbestände und bei Straftaten, die aufgrund der Art der Begehung oder des verursachten Schadens ein vergleichbares Gewicht haben, zugelassen werden.

   Sie soll nur stattfinden, wenn weniger intensive Fahndungsmaßnahmen keinen hinreichenden Erfolg versprechen.

   Der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets ist auch bei der Auswahl des Mediums zu berücksichtigen.

2. Bei der öffentlichen Fahndung nach unbekannten Tatverdächtigen, Beschuldigten, Angeschuldigten, Angeklagten einerseits und Zeugen andererseits erscheint es geboten, die Entscheidung, ob und in welcher Weise gefahndet werden darf, grundsätzlich dem Richter vorzubehalten; dies gilt nicht bei der öffentlichen Fahndung zum Zwecke der Straf- oder Maßregelvollstreckung gegenüber Erwachsenen.

   Bei Gefahr in Verzug kann eine Eilkompetenz der Staatsanwaltschaft vorgesehen werden, dies gilt nicht bei der öffentlichen Fahndung nach Zeugen. In diesem Falle ist unverzüglich die richterliche Bestätigung der Maßnahme einzuholen.

   Die öffentliche Fahndung nach Beschuldigten setzt voraus, daß ein Haftbefehl oder Unterbringungsbefehl vorliegt, bzw. dessen Erlaß nicht ohne Gefährdung des Fahndungserfolges abgewartet werden kann.

3. Eine besonders eingehende Prüfung der Verhältnismäßigkeit hat bei der Fahndung nach Zeugen stattzufinden.

   Eine öffentliche Fahndung nach Zeugen darf nach Art und Umfang nicht außer Verhältnis zur Bedeutung der Zeugenaussage für die Aufklärung der Straftat stehen. Hat ein Zeuge bei früherer Vernehmung bereits von seinem gesetzlichen Zeugnis- oder Auskunftsverweigerungsrecht Ge-

brauch gemacht, so soll von Maßnahmen der öffentlichen Fahndung abgesehen werden.

4. In Unterbringungssachen darf eine öffentliche Fahndung mit Rücksicht auf den Grundsatz der Verhältnismäßigkeit nur unter angemessener Berücksichtigung des gesetzlichen Zwecks der freiheitsentziehenden Maßregel, insbesondere der Therapieaussichten und des Schutzes der Allgemeinheit angeordnet werden.

5. Die öffentliche Fahndung zur Sicherung der Strafvollstreckung sollte zur Voraussetzung haben, daß

   – eine Verurteilung wegen einer Straftat von erheblicher Bedeutung vorliegt und

   – der Verurteilte, der sich der Strafvollstreckung entzieht, (noch) eine Restfreiheitsstrafe von in der Regel mindestens einem Jahr zu verbüßen hat, oder ein besonderes öffentliches Interesse, etwa tatsächliche Anhaltspunkte für die Begehung weiterer Straftaten von erheblicher Bedeutung, an der alsbaldigen Ergreifung des Verurteilten besteht.

6. Besondere Zurückhaltung ist bei internationaler öffentlicher Fahndung geboten. Dies gilt sowohl für Ersuchen deutscher Stellen um Fahndung im Ausland als auch für Fahndung auf Ersuchen ausländischer Stellen im Inland.

7. Öffentliche Fahndung unter Beteiligung der Medien sollte in den Katalog anderer entschädigungspflichtiger Strafverfolgungsmaßnahmen des § 2 Abs. 2 StrEG aufgenommen werden.

   Durch Ergänzung des § 7 StrEG sollte in solchen Fällen auch der immaterielle Schaden als entschädigungspflichtig anerkannt werden.

   Der Gesetzgeber sollte vorsehen, daß auf Antrag des Betroffenen die Entscheidung über die Entschädigungspflicht öffentlich bekanntzumachen ist.

Anlage 3

Entschließung
der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 14./15. März 1996 in Hamburg

zur

Modernisierung und europäische Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: „Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten
2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung
3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz
4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität
5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen
6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung
8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist
9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren

10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten
11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen
12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung
13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing
14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau

Anlage 4

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 09. Mai 1996

zu

Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

Der Schutz personenbezogener Daten ist während der Übertragung oder anderer Formen des Transportes nicht immer gewährleistet. Elektronisch gespeicherte, personenbezogene Daten können sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen als auch auf maschinell lesbaren Datenträgern weitergegeben werden. Oft sind die Eigenschaften des Transportweges dem Absender und dem Empfänger weder bekannt noch durch sie beeinflußbar. Vor allem die Vertraulichkeit, die Integrität (Unversehrtheit) und die Zurechenbarkeit der Daten (Authentizität) sind nicht sichergestellt, solange Manipulationen, unbefugte Kenntnisnahme und Fehler während des Transportes nicht ausgeschlossen werden können. Die Verletzung der Vertraulichkeit ist möglich, ohne daß Spuren hinterlassen werden.

Zahlreiche Rechtsvorschriften gebieten, das Grundrecht des Bürgers auf informationelle Selbstbestimmung auch während der automatisierten Verarbeitung personenbezogener Daten zu sichern (z. B. § 78a SGB X mit Anlage, § 10 Abs. 8 Btx-Staatsvertrag, § 9 BDSG nebst Anlage und entsprechende landesgesetzliche Regelungen).

Kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können in vielen Anwendungsfällen mit vertretbarem Aufwand eingesetzt werden.

Angesichts der beschriebenen Situation und der vorhandenen technischen Möglichkeiten fordern die Datenschutzbeauftragten des Bundes und der Länder, geeignete, sichere kryptographische Verfahren beim Transport elektronisch gespeicherter personenbezogener Daten unter Berücksichtigung ihrer Schutzwürdigkeit anzuwenden.

Anlage 5

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 29. April 1996

zu

Eckpunkte für die datenschutzrechtliche Regelung von Mediendiensten

In letzter Zeit finden Online-Dienste und Multimedia-Anwendungen zunehmend Verbreitung. Mit den - häufig multimedialen - Angeboten, auf die interaktiv über Telekommunikationsnetze zugegriffen werden kann, sind besondere Risiken für das Recht auf informationelle Selbstbestimmung der Teilnehmer verbunden; hinzuweisen ist insbesondere auf die Gefahr, daß das Nutzerverhalten unbemerkt registriert und zu Verhaltensprofilen zusammengeführt wird. Das allgemeine Datenschutzrecht reicht nicht aus, die mit den neuen technischen Möglichkeiten und Nutzungsformen verbundenen Risiken wirkungsvoll zu beherrschen.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, durch bereichsspezifische Regelungen technische und rechtliche Gestaltungsanforderungen für die elektronischen Dienste zu formulieren, die den Datenschutz sicherstellen. Leitlinie sollte hierbei der Grundsatz der Datenvermeidung bzw. -minimierung sein. Die Datenschutzbeauftragten haben dazu in einer Entschließung vom 14./15. März 1996 zur Modernisierung und zur europäischen Harmonisierung des Datenschutzrechts vorgeschlagen, daß die informationelle Selbstbestimmung bei Multimediadiensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsverfahren anzubieten, durch den Schutz vor übereilter Einwilligung, z. B. durch ein Widerspruchsrecht, und durch strenge Zweckbindung für die bei der Verbindung, Nutzung und Abrechnung anfallenden Daten sichergestellt wird.

Die Datenschutzbeauftragten weisen darauf hin, daß auch mit Inhalten, die durch Mediendienste verbreitet werden, datenschutzrechtliche Probleme verbunden sein können. Auf diese Probleme wird im folgenden jedoch - ebenso wie auf die Datenschutzaspekte der Telekommunikation - nicht näher eingegangen. Bei den datenschutzrechtlichen Eckpunkten wird ferner bewußt darauf verzichtet, den Regelungsort - etwa einen Länder-Staatsvertrag oder ein Bundesgesetz - anzugeben. Die Datenschutzbeauftragten appellieren an die Gesetzgeber in Bund und Ländern, eine angemessene datenschutzgerechte Regulierung der neuen Dienste nicht an Kompetenzstreitigkeiten scheitern zu lassen.

1. Anonyme bzw. datensparsame Nutzung: Die Dienste und Multimedia-Einrichtungen sollten so gestaltet werden, daß keine oder möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden; deshalb sind auch anonyme Nutzungs- und Zahlungsformen anzubieten. Auch zur Aufrechterhaltung und zu bedarfsgerechten Gestaltung von Diensten und Dienstleistungen (Systempflege) sind soweit wie möglich anonymisierte Daten zu verwenden. Soweit eine vollständig anonyme Nutzung nicht realisiert werden kann, muß jeweils geprüft werden, ob durch andere Verfahren, z. B. die Verwendung von Pseudonymen, ein unmittelbarer Personenbezug vermieden werden kann. Die Herstellung des Personenbezugs sollte bei diesen Nutzungsformen nur dann erfolgen, wenn hieran ein begründetes rechtliches Interesse besteht.

2. Bestandsdaten: Bestandsdaten dürfen nur in dem Maße erhoben, verarbeitet und genutzt werden, soweit sie für die Begründung und Abwicklung eines Vertragsverhältnisses sowie für die Systempflege erforderlich sind. Die Bestandsdaten dürfen nur zur bedarfsgerechten Gestaltung von Diensten und Dienstleistungen sowie zur Werbung und Marktforschung genutzt werden, soweit der Betroffene dem nicht widersprochen hat. Für die Werbung und Marktforschung durch Dritte dürfen Bestandsdaten nur mit der ausdrücklichen Einwilligung des Betroffenen verarbeitet werden.

3. Verbindungs- und Abrechnungsdaten: Verbindungs- und Abrechnungsdaten dürfen nur für Zwecke der Vermittlung von Abgeboten und für Abrechnungszwecke erhoben, gespeichert und genutzt werden. Sie sind zu löschen, wenn sie für die Erbringung der Dienstleistung oder für Abrechnungszwecke nicht mehr erforderlich sind. Soweit Verbindungsdaten ausschließlich zur Vermittlung einer Dienstleistung gespeichert werden, sind sie spätestens nach Beendigung der Verbindung zu löschen. Die Speicherung der Abrechnungsdaten darf den Zeitpunkt, die Dauer, die Art, den Inhalt und die Häufigkeit bestimmter von den einzelnen Teilnehmern in Anspruch genommener Angebote nicht erkennen lassen, es sei denn, der Teilnehmer beantragt eine dahingehende Speicherung. Verbindungs- und Abrechnungsdaten sind einer strikten Zweckbindung zu unterwerfen. Sie dürfen über den hier genannten Umfang hinaus nur mit der ausdrücklichen Einwilligung des Betroffenen erhoben, verarbeitet und genutzt werden. Unberührt hiervon bleibt die Speicherung von Daten von Verantwortlichen für Angebote im Zusammenhang mit Impressumspflichten.

4. Interaktionsdaten: Werden im Rahmen von interaktiven Dienstleistungen darüber hinaus personenbezogene Daten erhoben, die nachweisen, welche Eingaben der Teilnehmer während der Nutzung des Angebots zur Beeinflussung des Ablaufs vorgenommen hat (Interaktionsdaten; hierzu gehören z. B. Daten, die bei lexikalischen Abfragen, in interaktive Suchsysteme - etwa elektronische Fahrpläne und Telefonverzeichnisse - und bei Online-Spielen eingegeben werden), darf dies nur in Kenntnis und mit ausdrücklicher Einwilligung des Betroffenen geschehen. Interaktionsdaten dürfen nur unter Beachtung einer strikten Zweckbindung verarbeitet und genutzt werden. Sie sind grundsätzlich zu löschen, wenn der Zweck, zu dem sie erhoben wurden, erreicht wurde (so müssen Daten über die interaktive Suche von Angeboten unmittelbar nach Beendigung des Suchprozesses gelöscht werden). Eine weitergehende Verarbeitung dieser Daten ist nur auf Grundlage einer ausdrücklichen Einwilligung des Betroffenen zulässig.

5. Einwilligung: Der Abschluß oder die Erfüllung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene in die Verarbeitung oder Nutzung seiner Daten außerhalb der zulässigen Zweckbestimmung eingewilligt hat. Soweit Daten auf Grund einer Einwilligung erhoben werden, muß diese jederzeit widerrufen werden können. Für die Form und Dokumentation elektronisch abgegebener Einwilligungen und sonstiger Willenserklärungen ist ein Mindeststandard zu definieren, der einen fälschungssicheren Nachweis über die Tatsache, den Zeitpunkt und den Gegenstand gewährleistet. Dabei ist sicherzustellen, daß der Teilnehmer bereits vor der Einwilligung soweit wie möglich über den Inhalt und die Folgen seiner Einwilligung und über sein Widerrufsrecht informiert ist. Deshalb müssen die Betroffenen sowohl vor als auch nach Eingabe der Erklärung die Möglichkeit haben, auf Einwilligungen, Verträge und sonstige Informationen über die Bedingungen der Nutzung von Diensten, Multimedia-Einrichtungen und Dienstleistungen zuzugreifen und diese auch in schriftlicher Form zu erhalten. Da Verträge oder andere rechtswirksame Erklärungen, die in einer Fremdsprache verfaßt sind, unter Umständen juristische Fachbegriffe enthalten, die nur vor dem Hintergrund der jeweiligen Rechtsordnung zu verste-

hen sind, sollten zumindest diejenigen Dienste, die eine deutschsprachige Benutzeroberfläche anbieten, derartige Unterlagen auch in deutscher Sprache bereitstellen.

6. Transparenz der Dienst und Steuerung der Datenübertragung durch die Teilnehmer: Die automatischer Übermittlung von Daten durch die beim Betroffenen eingesetzte Datenverarbeitungsanlage ist auf das technisch für die Vertragsabwicklung notwendige Maß zu beschränken. Eine darüber hinausgehende Übermittlung ist nur auf Grund einer besonderen Einwilligung zulässig. Im Hinblick darauf, daß die Teilnehmer bei der eingesetzten Technik nicht erkennen können, in welchen Dienst sie sich befinden und welche Daten bei der Nutzung von elektronischen Diensten bzw. bei der Erbringung von Dienstleistungen automatisiert übertragen und gespeichert werden, ist sicherzustellen, daß die Teilnehmer vor Beginn der Datenübertragung hierüber informiert werden und die Möglichkeit haben, den Prozeß jederzeit abzubrechen. Die zur Nutzung vom Anbieter oder Netzbetreiber bereitgestellte Software muß eine vom Nutzer aktivierbare Möglichkeit enthalten, den gesamten Strom der ein- und ausgehenden Daten vollständig zu protokollieren. Bei einer Durchschaltung zu einem anderen Dienst bzw. zu einer anderen Multimedia-Einrichtung müssen die Teilnehmer über die Durchschaltung und damit mögliche Datenübertragungen informiert werden. Diensteanbieter haben zu gewährleisten, daß sie keine erkennbar unsicheren Netze für die Übertragung personenbezogener Daten nutzen bzw. den Schutz dieser Daten durch angemessene Maßnahmen sicherstellen. Entsprechend dem Stand der Technik sind geeignete (z. B. kryptographische) Verfahren anzuwenden, um die Vertraulichkeit und Integrität der übertragenen Daten sowie eine sichere Identifizierung und Authentifikation zwischen Teilnehmern und Anbieten zu gewährleisten.

7. Rechte von Betroffenen: Die Rechte von Betroffenen auf Auskunft, Sperrung, Berichtigung und Löschung sind auch bei multimedialen und sonstigen elektronischen Diensten zu gewährleisten. Soweit personenbezogene Daten im Rahmen eines elektronischen Dienstes veröffentlicht wurden, der dem Medienprivileg unterliegt, ist das Gegendarstellungsrecht der von der Veröffentlichung Betroffenen sicherzustellen.

8. Datenschutzkontrolle: Eine effektive, unabhängige und nicht anlaßgebundene Datenschutzaufsicht ist zu gewährleisten. Den für die Kontrolle des Datenschutzes zuständigen Behörden ist ein jederzeitiger kostenfreier elektronischer Zugriff auf die Dienste und Dienstleistungen und der Zugang zu den eingesetzten technischen Einrichtungen zu ermöglichen. Bei elektronischen Diensten, für das Medienprivileg gilt, ist die externe Datenschutzkontrolle entsprechend zu beschränken.

9. Geltungsbereich: Der Geltungsbereich der jeweiligen Regelungen ist eindeutig festzulegen. Es ist sicherzustellen, daß die Datenschutzbestimmungen auch gelten, sofern personenbezogene Daten nicht in Dateien verarbeitet werden.

10. Internationale Datenschutzregelung: Im Hinblick auf die zunehmende Bedeutung grenzüberschreitender elektronischer Dienste und Dienstleistungen ist eine Fortentwicklung der europäischen und internationalen Rechtsordnung dringend erforderlich, die auch bei ausländischen Diensten, Dienstleistungen und Multimedia-Angeboten ein angemessenes Datenschutzniveau gewährleistet. Die Verabschiedung der sog. ISDN-Datenschutzrichtlinie mit einem europaweiten hohen Schutzstandard ist überfällig. Kurzfristig ist es notwendig, den Betroffenen angemessene Mittel zur Durchsetzung ihrer Datenschutzrechte gegenüber ausländischen Betreibern und Dienstleistern in die Hand zu geben. Die in Deutschland aktiven Dienste aus Nicht-EG-

Staaten haben im Sinne der EG-Datenschutzrichtlinie (95/46/EG) vom 24.10.1995 einen verantwortlichen inländischen Vertreter zu benennen.

Anlage 6

Entschließung
der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 22./23. Oktober 1996 in Hamburg

zur

Automatisierte Übermittlung von Abrechnungsdaten durch Kassenzahnärztliche Vereinigungen an gesetzliche Krankenkassen

Der in dem Schiedsspruch vom 20. Februar 1995 für die Abrechnung festgelegte Umfang der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen erfüllt nicht die Anforderungen des Sozialgesetzbuches an diesen Datenaustausch. § 295 SGB V fordert, daß Daten nur **im erforderlichen Umfang** und **nicht versichertenbezogen** übermittelt werden dürfen.

Die Datenschutzbeauftragten begrüßen es deshalb, daß der größte Teil der gesetzlichen Krankenkassen in „Protokollnotizen“ - Stand 22. März 1996 - den Umfang der zu übermittelnden Daten reduziert hat. Das Risiko der Identifizierbarkeit des Versicherten wurde dadurch deutlich verringert. Zum letztlich erforderlichen Umfang haben die Spitzenverbände der gesetzlichen Krankenkassen erklärt, daß genauere Begründungen für die Erforderlichkeit der Daten erst gegeben werden könnten, wenn das DV-Projekt für das Abrechnungsverfahren auf Kassenseite weit genug entwickelt sei.

Der Verband der Angestellten-Ersatzkassen (VDAK) hat bisher als einziger Spitzenverband der gesetzlichen Krankenkassen diese Datenreduzierungen nicht mitgetragen. Die Datenschutzbeauftragten fordern den VDAK auf, sich für die Frage der Datenübermittlung zwischen Kassenzahnärztlichen Vereinigungen und gesetzlichen Krankenkassen der einheitlichen Linie anzuschließen. Dies liegt im gesetzlich geschützten Interesse der Versicherten.

Die besonderen Vorgaben des Sozialgesetzbuches für die Prüfung der Wirtschaftlichkeit der ärztlichen Abrechnung werden dadurch nicht berührt.

Anlage 7

Entschließung
der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 22./23. Oktober 1996 in Hamburg

zum

Datenschutz bei der Vermittlung und Abrechnung digitaler Fernsehsendungen

Mit der Markteinführung des digitalen Fernsehens eröffnen sich für die Anbieter - neben einem deutlich ausgeweiteten Programmvolumen - neue Möglichkeiten für die Vermittlung und Abrechnung von Sendungen. Hinzuweisen ist in erster Linie auf Systeme, bei denen die Kunden für die einzelnen empfangenen Sendungen bezahlen müssen. Dort entsteht die Gefahr, daß die individuellen Vorlieben, Interessen und Sehgewohnheiten registriert und damit Mediennutzungsprofile einzelner Zuschauer erstellt werden. Die zur Vermittlung und zur Abrechnung verfügbaren technischen Verfahren können die Privatsphäre des Zuschauers in unterschiedlicher Weise beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter und Programmlieferanten auf, den Nutzern zumindest alternativ auch solche Lösungen anzubieten, bei denen die Nutzung der einzelnen Programmangebote nicht personenbezogen registriert werden kann wie es der Entwurf des Mediendienste-Staatsvertrages bereits vorsieht. Die technischen Voraussetzungen für derartige Lösungen sind gegeben.

Die technischen Verfahren sind so zu gestalten, daß möglichst keine personenbezogenen Daten erhoben, gespeichert und verarbeitet werden (Prinzip der Datensparsamkeit). Verfahren, die im voraus bezahlte Wertkarten - Chipkarten - nutzen, um die mit entsprechenden Entgeltinformationen ausgestrahlten Sendungen zu empfangen und zu entschlüsseln, entsprechen weitgehend dieser Forderung. Allerdings setzt eine anonyme Nutzung voraus, daß beim Zuschauer gespeicherte Informationen über die gesehenen Sendungen nicht durch den Anbieter abgerufen werden können.

Die Datenschutzbeauftragten sprechen sich außerdem dafür aus, daß für die Verfahren auf europäischer Ebene Vorgaben für eine einheitliche Architektur mit gleichwertigen Datenschutzvorkehrungen entwickelt werden.

Anlage 8

Entschließung
der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 22./23. Oktober 1996 in Hamburg

zu

Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

Die Entwicklung moderner Informations- und Telekommunikationstechniken führt zu einem grundlegend veränderten Kommunikationsverhalten der Bürger.

Die Privatisierung der Netze und die weite Verbreitung des Mobilfunks geht einher mit einer weitreichenden Digitalisierung der Kommunikation. Mailboxen und das Internet prägen die Informationsgewinnung und -verbreitung von Privatleuten, von Unternehmen und öffentlichen Institutionen gleichermaßen.

Neue Dienste wie Tele-Working, Tele-Banking, Tele-Shopping, digitale Videodienste und Rundfunk im Internet sind einfach überwachbar, weil personenbezogene Daten der Nutzer in digitaler Form vorliegen. Die herkömmlichen Befugnisse zur Überwachung des Fermneldeverkehrs erhalten eine neue Dimension, weil immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden, können sie mit geringem Aufwand kontrolliert und ausgewertet werden. Demgegenüber stehen jedoch auch Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken. Die Datenschutzbeauftragten erkennen an, daß die Strafverfolgungsbehörden in die Lage versetzt werden müssen, solchen mißbräuchlichen Nutzungen der neuen Techniken zu kriminellen Zwecken wirksam zu begegnen.

Sie betonen jedoch, daß die herkömmlichen weitreichenden Eingriffsbefugnisse auch unter wesentlich veränderten Bedingungen nicht einfach auf die neuen Formen der Individual- und Massenkommunikation übertragen werden können. Die zum Schutz der Persönlichkeitsrechte des einzelnen gezogenen Grenzen müssen auch unter den geänderten tatsächlichen Bedingungen der Verwendung der modernen Informationstechnologien aufrechterhalten und gewährleistet werden. Eine Wahrheitsfindung um jeden Preis darf es auch insoweit nicht geben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher Thesen zur Bewältigung dieses Spannungsverhältnisses entwickelt.

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunikationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen. Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die In-

formationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z. B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

Die Datenschutzbeauftragten wenden sich nachhaltig dagegen, daß den Nutzern die Verschlüsselung des Inhalts ihrer Nachrichten verboten wird. Die Möglichkeit für den Bürger, seine Kommunikation durch geeignete Maßnahmen vor unberechtigten Zugriffen zu schützen, ist ein traditionelles verfassungsrechtlich verbürgtes Recht.

Aus Sicht des Datenschutzes besteht andererseits durchaus Verständnis für das Interesse der Sicherheits- und Strafverfolgungsbehörden, sich rechtlich zulässige Zugriffsmöglichkeiten nicht dadurch versperren zu lassen, daß Verschlüsselungen verwandt werden, zu denen sie keinen Zugriff haben. Eine Reglementierung der Verschlüsselung, z. B. durch Schlüsselhinterlegung, erscheint aber aus derzeitiger technischer Sicht kaum durchsetzbar, da entsprechende staatliche Maßnahmen - insbesondere im weltweiten Datenverkehr - ohnehin leicht zu umgehen und kaum kontrollierbar wären.

Anlage 9

Forderungen der Datenschutzbeauftragten des Bundes und der Länder
anläßlich der 52. Konferenz am 22./23. 10.1996 in Hamburg

zu

Maßnahmen zur Sicherung der Privatsphäre für den Fall der Einführung der akustischen Raumüberwachung

1. Im Grundgesetz selbst ist festzulegen,

   - daß der Einsatz technischer Mittel zur Wohnraumüberwachung nur zur Verfolgung schwerster Straftaten, die im Hinblick auf ihre Begehungsform oder Folgen die Rechtsordnung nachhaltig gefährden und die im Gesetz einzeln bestimmt sind

   - und nur auf Anordnung eines Kollegialgerichts

   erfolgen darf.

2. Die Maßnahme darf sich nur gegen den Beschuldigten richten. Erfolgt ein Lauschangriff in der Wohnung eines Dritten, müssen konkrete Anhaltspunkte die Annahme rechtfertigen, daß sich der Beschuldigte in der Wohnung aufhält. In allen Fällen muß die durch Tatsachen begründete Erwartung vorliegen, daß in der überwachten Wohnung zur Strafverfolgung relevante Gespräche geführt werden.

3. Das Mittel der Wohnungsüberwachung darf nur dann angewandt werden, wenn andere Methoden zur Erforschung des Sachverhalts erschöpft oder untauglich sind. Bei einem Lauschangriff in Wohnungen dritter Personen bedeutet dies auch, daß die Maßnahme nur durchgeführt werden darf, wenn aufgrund bestimmter Tatsachen anzunehmen ist, daß ihre Durchführung in der Wohnung des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts des Täters führen wird.

4. Das Zeugnisverweigerungsrecht von Berufsgeheimnisträgern und Personen, die aus persönlichen Gründen zur Verweigerung des Zeugnisses berechtigt sind, muß gewahrt werden.

5. Die Dauer der Maßnahme wird zeitlich eng begrenzt. Auch die Möglichkeit der Verlängerung der Maßnahme ist zu befristen.

6. Eine anderweitige Verwendung der erhobenen Daten (Zweckänderung) ist weder zu Beweiszwecken noch als Ermittlungsansatz für andere als Katalogtaten zulässig.
   Personenbezogene Erkenntnisse aus einem Lauschangriff dürfen zur Abwehr von konkreten Gefahren für gewichtige Rechtsgüter verwendet werden.

7. Wenn sich der ursprüngliche Verdacht nicht bestätigt, sind die durch den Lauschangriff erhobenen Daten unverzüglich zu löschen.

8. Die Betroffenen müssen unverzüglich und vollständig über die Durchführung der Maßnahme informiert werden, sobald dies ohne Gefährdung des Ermittlungsverfahrens möglich ist.

9. Eine Verfahrenssicherung durch den Zwang zur eingehenden Begründung und durch detaillierte jährliche Berichtspflichten der Staatsanwaltschaft für die Öffentlichkeit ähnlich den gerichtlichen Wire-Tap-Reports in den USA einschließlich einer Erfolgskontrolle ist vorzusehen. Anhand der Berichte ist jeweils - wegen der Schwere des Eingriffs - in entsprechenden Fristen zu überprüfen, ob die gesetzliche Regelung weiterhin erforderlich ist.

10. Die effektive Kontrolle der Abhörmaßnahme und der Verarbeitung und Nutzung der durch sie gewonnenen Erkenntnisse durch Gerichte und Datenschutzbeauftragte ist sicherzustellen

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 17./18. April 1997 in München

zu

Beratungen zum StVÄG 1996

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Entwicklung, im Gesetzgebungsverfahren zu einem Strafverfahrensänderungsgesetz 1996, die Gewährleistung der informationellen Selbstbestimmung im Strafverfahren nicht nur nicht zu verbessern, sondern vielmehr bestehende Rechte sogar noch zu beschränken. Dies gilt insbesondere für den Beschluß des Bundesrates, der gravierende datenschutzrechtliche Verschlechterungen vorsieht.

Bereits der Gesetzentwurf der Bundesregierung wird in Teilbereichen den Vorgaben des Bundesverfassungsgerichts nicht gerecht und fällt teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.

Kritik erheben die Datenschutzbeauftragten des Bundes und der Länder insbesondere an folgenden Punkten:

- Die Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sind nicht hinreichend bestimmt. So wird z. B. nicht angemessen zwischen Beschuldigten und Zeugen differenziert.

- Für Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind, wird als Voraussetzung zur Auskunfts- und Akteneinsicht lediglich ein vages „berechtigtes“ statt eines rechtlichen Interesses gefordert.

  Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, daß nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z. B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

Die Bedenken und Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder fanden in den ersten Beratungen des Bundesrates zum Gesetzentwurf nahezu keinen Niederschlag.

Darüber hinaus hat der Bundesrat in seiner Stellungnahme weitergehende datenschutzrechtliche Verschlechterungen beschlossen, die vor allem die Entfernung mehrerer im Gesetzentwurf noch vorhandener Beschränkungen und verfahrensrechtlicher Sicherungen zum Schutz des Persönlichkeitsrechts und des Rechtes auf informationelle Selbstbestimmung der Betroffenen zum Inhalt haben.

Beispiele hierfür sind:

- Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.

- Die Verwendungsbeschränkungen bei Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht gewonnen wurden, sollen herausgenommen werden.

- Das Auskunfts- und Akteneinsichtsrecht auch für öffentliche Stellen soll erheblich erweitert werden.

- Detaillierte Regelungen für Fälle, in denen personenbezogene Daten von Amts wegen durch Strafverfolgungs- und Strafjustizbehörden an andere Stellen übermittelt werden dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben, sollen gestrichen werden.

- Das Verbot soll gestrichen werden, über die Grunddaten hinausgehende weitere Angaben nach Freispruch, endgültiger Verfahrenseinstellung oder unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens Daten in Dateien zu speichern.

- Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.

- Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Deutschen Bundestag auf, bei den anstehenden weiteren Beratungen des Gesetzentwurfes die vom Bundesrat empfohlenen datenschutzrechtlichen Verschlechterungen nicht zu übernehmen und die noch bestehenden datenschutzrechtlichen Mängel zu beseitigen.

Hingegen sollten Vorschläge des Bundesrates für Regelungen für den Einsatz von Lichtbildvorlagen und für die Datenverarbeitung zur Durchführung des Täter-Opfer-Ausgleichs aufgegriffen werden.

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 17./18. April 1997 in München

zu

Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

Immer häufiger wird bei der Verfolgung von Straftaten am Tatort oder beim Opfer festgestelltes, sog. biologisches Material als Spurenmaterial durch die Polizei sichergestellt, mittels DNA-Analyse untersucht und mit anderen DNA-Materialien verglichen. Die DNA-Analyse ist zur Standardmethode geworden, um die Herkunft von Spurenmaterial von bestimmten bekannten Personen (Verdächtigen, Opfern, unbeteiligten Dritten) oder die Identität mit anderem Spurenmaterial unbekannter Personen feststellen zu können.

Der Gesetzgeber hat zwar vor kurzem im Strafverfahrensänderungsgesetz - DNA-Analyse („Genetischer Fingerabdruck“) - die Voraussetzungen und Grenzen genetischer Untersuchungen im Strafverfahren geregelt. Eine Festlegung, ob und in welchen Grenzen die Speicherung und Nutzung der durch eine DNA-Analyse gewonnenen Untersuchungsergebnisse in Datenbanken der Polizei zu erkennungsdienstlichen Zwecken zulässig ist, enthält dieses Gesetz jedoch nicht.

Bezüglich des Aussagegehalts der gespeicherten Daten der Analyseergebnisse ist ein grundsätzlich neuer Aspekt zu berücksichtigen:

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht codierenden persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, daß künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen konkrete Aussagen über genetische Dispositionen der betroffenen Personen mit inhaltlichem Informationswert getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten menschlichen Genoms vorangetrieben wird.

Dieser Gefährdung kann dadurch begegnet werden, daß bei Bekanntwerden von Überschußinformationen durch die bisherigen Untersuchungsmethoden andere Untersuchungsmethoden (Analyse eines anderen Genomabschnitts) verwendet werden, die keine Informationen über die genetische Disposition liefern. Derartige Ausweichstrategien können jedoch zur Folge haben, daß die mit anderen Methoden erlangten Untersuchungsergebnisse nicht mit bereits vorliegenden vergleichbar sind. Datenspeicherungen über verformelte Untersuchungsergebnisse könnten daher dazu führen, daß einmal verwendete Untersuchungsformen im Interesse der Vergleichbarkeit beibehalten werden, obwohl sie sich als problematisch herausgestellt haben und unproblematische Alternativen zur Verfügung stehen, z. B. durch Verschlüsselung problematischer Informationen.

In Anbetracht dieser Situation und angesichts der Tendenz, mittels der DNA-Analyse gewonnene Daten nicht nur in einem bestimmten Strafverfahren zu verwenden, sondern diese Daten in abrufbaren Datenbanken auch für andere Strafverfahren zugänglich zu machen, fordern die Datenschutzbeauftragten des Bundes und der Länder ergänzend zu §§ 81 e und f StPO für die automatisierte Speicherung und Nutzung von DNA-Identitätsdaten eine spezielle gesetzliche Regelung in der Strafprozeßordnung, um das Persönlichkeitsrecht der Betroffenen zu schützen:

1. Es muß ein grundsätzliches Verbot der Verformelung und Speicherung solcher Analyseergebnisse statuiert werden, die inhaltliche Aussagen über Erbanlagen ermöglichen.

   Im Hinblick auf die nicht auszuschließende Möglichkeit künftiger Rückschlüsse auf genetische Dispositionen ist bereits jetzt ein striktes Nutzungsverbot für persönlichkeitsrelevante Erkenntnisse zu statuieren, die aus den gespeicherten Verformelungen der DNA resultieren.

2. Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwecken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:

   – Nicht jede DNA-Analyse, die zum Zweck der Aufklärung einer konkreten Straftat erfolgt ist, darf in diese Datei aufgenommen werden. Die Speicherung von Verformelungen der DNA-Struktur in eine Datenbank darf nur dann erfolgen, wenn tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte künftig strafrechtlich in Erscheinung treten wird und daß die Speicherung aufgrund einer Prognose unter Zugrundelegung des bisherigen Täterverhaltens die künftige Strafverfolgung fördern kann.

   – Eine Speicherung kommt insbesondere dann nicht in Betracht, wenn der Tatverdacht gegen den Beschuldigten ausgeräumt wurde. Bereits erfolgte Speicherungen sind zu löschen. Gleiches gilt für den Fall, daß die Anordnung der DNA-Untersuchung oder die Art und Weise ihrer Durchführung unzulässig war.

   – Die Aufbewahrungsdauer von Verformelungen der DNA-Struktur ist konkret festzulegen (z. B. gestaffelt nach der Schwere des Tatvorwurfs).

3. Voraussetzung für Gen-Analysen muß in jedem Fall mindestens die richterliche Anordnung sein, unabhängig davon, ob die Daten in einem anhängigen Strafverfahren zum Zweck der Straftatenaufklärung, wie in § 81 f Absatz 1 Satz 1 StPO normiert, oder ob sie zum Zweck der künftigen Strafverfolgung (also zu Zwecken des Erkennungsdienstes) benötigt werden.

4. Ein DNA-Screening von Personengruppen, deren Zusammensetzung nach abstrakt festgelegten Kriterien ohne konkreten Tatverdacht gegenüber einzelnen erfolgt, führt im Regelfall zur Erhebung von DNA-Daten zahlreicher, völlig unbeteiligter und unschuldiger Bürger. Die Daten dieser Personen sind unmittelbar dann zu löschen, wenn sie für das Anlaßstrafverfahren nicht mehr erforderlich sind. Sie dürfen nicht in verfahrensübergreifenden DNA-Dateien gespeichert werden und auch nicht mit solchen Datenbeständen abgeglichen werden.

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 17./18. April 1997 in München

zu

Geplante Verpflichtung von Teledienstеanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln

Der Entwurf der Bundesregierung für ein Teledienstedatenschutzgesetz (Artikel 2 (§ 5 Absatz 3) des Informations- und Kommunikationsdienste-Gesetzes vom 20.12.1996 - BR-Drs. 966/96) sieht vor, daß die Anbieter von Telediensten (z. B. Home-Banking, Home-Shopping) dazu verpflichtet werden sollen, insbesondere der Polizei und den Nachrichtendiensten Auskunft über Daten zur Begründung, inhaltlichen Ausgestaltung oder Änderung der Vertragsverhältnisse mit ihren Kunden (sog. Bestandsdaten) zu erteilen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Aufnahme einer solchen Übermittlungsvorschrift in das Teledienstedatenschutzgesetz des Bundes. Eine Folge dieser Vorschrift wäre, daß Anbieter von elektronischen Informationsdiensten (z. B. Diskussionsforen) offenlegen müßten, welche ihrer Kunden welche Dienste z. B. mit einer bestimmten politischen Tendenz in Anspruch nehmen. Darin läge ein massiver Eingriff nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Informations- und Meinungsfreiheit des Einzelnen. Das geltende Recht, insbesondere die Strafprozeßordnung und das Polizeirecht enthalten hinreichende Möglichkeiten, um strafbaren und gefährlichen Handlungen auch im Bereich der Teledienste zu begegnen. Über die bisherige Rechtslage hinaus würde bei Verabschiedung der geplanten Regelung zudem den Nachrichtendiensten ein nichtöffentlicher Datenbestand offenstehen. In keinem anderen Wirtschaftsbereich sind vergleichbare Übermittlungspflichten der Anbieter von Gütern und Dienstleistungen hinsichtlich ihrer Kunden bekannt.

Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Dienstanbieter schwierige Fragen der Abgrenzung zwischen den Geltungsbereichen des Mediendienste-Staatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Absatz 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

Anlage 13

Entschließung
der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 17./18. April 1997 in München

zu

Achtung der Menschenrechte in der Europäischen Union

Die DSB-Konferenz ist gemeinsam der Überzeugung, daß hinsichtlich nicht Verdächtiger und hinsichtlich nicht kriminalitätsbezogener Daten die Forderung des Europäischen Parlaments vom 17.09.1996 zu den Dateien von Europol unterstützt werden soll.

Das Europäische Parlament hat in seiner Entschließung zur Achtung der Menschenrechte gefordert, „alle Informationen persönlichen Charakters, wie Angaben zur Religionszugehörigkeit, zu philosophischen oder religiösen Überzeugungen, Rasse, Gesundheit und sexuellen Gewohnheiten, von der Erfassung in Datenbanken von EUROPOL auszuschließen.“

Entschließung
der Datenschutzbeauftragten des Bundes und der Länder
vom 20.10.1997
zu den Vorschlägen der
Arbeitsgruppe der ASMK

Verbesserter Datenaustausch bei Sozialleistungen

Mit dem von der ASMK-Arbeitsgruppe vorgeschlagenen erweiterten Datenaustausch bei Sozialleistungen wird die Bekämpfung von Leistungsmißbräuchen angestrebt. Soweit dieses Ziel der Arbeitsgruppe mit einer Veränderung der Strukturen der Verarbeitung personenbezogener Daten im Sozialleistungsbereich - insbesondere mit veränderten Verfahren der Datenerhebung - erreicht werden soll, muß der verfassungsrechtlich gewährleistete Grundsatz der Verhältnismäßigkeit beachtet werden.

Die gegenwärtigen Regelungen der Datenerhebung im Sozialleistungsbereich sehen unterschiedliche Verfahren der Datenerhebung vor, vor allem

- Datenerhebungen beim Betroffenen selbst
- Datenerhebungen bei Dritten mit Mitwirkung des Betroffenen
- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen aus konkretem Anlaß
- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen ohne konkreten Anlaß (Stichproben/Datenabgleich)

Diese Verfahren der Datenerhebung sind mit jeweils unterschiedlich schwerwiegenden Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden. So weiß z. B. bei einer Datenerhebung beim Betroffenen dieser, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritte erhalten keine Kenntnis von diesen Datenerhebungen.
Im Gegensatz dazu wird bei einer Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen dieser darüber im unklaren gelassen, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritten werden Daten über den Betroffenen zur Kenntnis gegeben (z. B. der Bank die Tatsache, daß der Betroffene Sozialhilfeempfänger ist).

Dieses System der Differenzierung des Verfahrens der Datenerhebung entspricht dem Grundsatz der Verhältnismäßigkeit. Ferner ist zu differenzieren, ob Daten aus dem Bereich der Sozialleistungsträger oder Daten außerhalb dieses Bereichs erhoben werden.

In dem Bericht der Arbeitsgruppe wird dieses System zum Teil aufgegeben. Es werden Verfahren der Datenerhebung vorgesehen, die schwerwiegend in die Rechte der Betroffenen eingreifen, ohne daß hinreichend geprüft und dargelegt wird, ob minder schwere Eingriffe in das Persönlichkeitsrecht zum Erfolg führen können. Die Datenschutzbeauftragten wenden sich nicht um jeden Preis gegen Erweiterungen des Datenaustauschs, gehen aber davon aus, daß pauschale und undifferenzierte Änderungen des gegenwärtigen Systems unterbleiben.

Datenabgleichsverfahren sollen nur in Frage kommen bei Anhaltspunkten für Mißbrauchsfälle in nennenswertem Umfang. Deshalb müssen etwaige neue Datenabgleichsverfahren hinsichtlich ihrer Wirkungen bewertet werden.

Daher ist parallel zu ihrer Einführung die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfaßt. Dies ermöglicht, Aufwand und Nutzen zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen.

Soweit unter Beachtung dieser Prinzipien neue Kontrollinstrumente gegen den Leistungsmißbrauch tatsächlich erforderlich sind, muß für den Bürger die Transparenz der Datenflüsse sichergestellt werden. Diese Transparenz soll gewährleisten, daß der Bürger nicht zum bloßen Objekt von Datenerhebungen wird.

Bezugnehmend auf die bisherigen Äußerungen des BfD und von LfD bestehen gegen folgende Vorschläge im Bericht gravierende Bedenken:

1. **Mitwirkung bei der Ahndung des Mißbrauchs (für alle Leistungsträger) und Verbesserungen für die Leistungsempfänger (zu D.II.10.1 und B.I)**

   Die vorgeschlagenen Möglichkeiten von anlaßunabhängigen Mißbrauchskontrollen beinhalten keine Klarstellung der gegebenen Rechtslage, sondern stellen erhebliche Änderungen des bisherigen abgestuften Systems der Datenerhebung dar.

   Die mit der Datenerhebung verbundene Offenlegung des Kontaktes bzw. einer Leistungsbeziehung zu einem Sozialleistungsträger stellt einen erheblichen Eingriff für den Betroffenen dar, u. a. da sie geeignet ist, seine Stellung in der Öffentlichkeit, z. B. seine Kreditwürdigkeit, wesentlich zu beeinträchtigen. Anfragen bei Dritten ohne Kenntnis des Betroffenen lassen diesen im unklaren, welche Daten wann an wen übermittelt wurden.

   Derartige Datenerhebungen werden vom geltenden Recht deshalb mit Rücksicht auf das verfassungsrechtliche Verhältnismäßigkeitsprinzip nur in begrenzten und konkretisierten Ausnahmefällen zugelassen. Von dieser verfassungsrechtlich gebotenen Systematik würde die Neuregelung grundlegend abweichen. Die Datenschutzbeauftragten betonen bei dieser Gelegenheit den allgemeinen Grundsatz, daß Datenerhebungen, die sowohl pauschal und undifferenziert sind, als auch ohne Anlaß erfolgen, abzulehnen sind.

   Die Datenschutzbeauftragten weisen schließlich darauf hin, daß gegen eine Ausnutzung der technischen Datenverarbeitungsmöglichkeiten zugunsten des Betroffenen (B.I des Berichts) nichts spricht, solange die Betroffenen davon informiert sind und soweit sie dem Verfahren zugestimmt haben.

2. **Nachfrage beim Wohnsitzfinanzamt des Hilfesuchenden zu Schenkungen und Erbschaften (zu D.I.1.1)**

   Die Datenschutzbeauftragten teilen nicht die Auffassung, daß Stichproben nach der geltenden Rechtslage zu § 21 Abs. 4 SGB X möglich sind. § 21 Abs. 4 SGB X ist eine Auskunftsvorschrift für die Finanzbehörden, die über die Datenerhebungsbefugnis der Sozialleistungsträger nichts aussagt. Die Leistungsträger dürfen diese Auskünfte bei den Finanzbehörden als Dritten nur nach Maßgabe des § 67a SGB X einholen, soweit das erforderlich ist: Diese Erforderlichkeit setzt Anhaltspunkte für Leistungsmißbrauch im Einzelfall voraus.

3. **Auskunftspflicht der Banken und Lebensversicherungen (zu D.II.1.6)**

   Die Datenerhebung im Sozialbereich ist von einer möglichst weitgehenden Einbeziehung des Betroffenen gekennzeichnet. Der Vorschlag zur Einführung einer Auskunftspflicht geht auf dieses undifferenzierte System der Datenerhebungen im Sozialbereich überhaupt nicht ein.

   Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünfte gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben.

   Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, daß dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, daß der Betroffene desavouiert wird.

   Die Datenschutzbeauftragten halten deshalb eine Klarstellung für dringend erforderlich, daß derartige unmittelbare Anfragen und Auskünfte erst in Betracht kommen, wenn die Ermittlungen unter Mitwirkung des Betroffenen zu keinem ausreichenden Ergebnis führen und Anhaltspunkte dafür bestehen, daß bei der fraglichen Bank/Lebensversicherung nicht angegebenes Vermögen vorhanden ist.

4. **Akzeptanz des Datenaustausches (zu E.IV)**

   Datenabgleiche beinhalten eine Verarbeitung personenbezogener Daten, die nicht beliebig durchgeführt werden darf und anerkanntermaßen einer gesetzlichen Grundlage bedarf. Die im Papier der Arbeitsgruppe unter E.IV vertretene These, daß anlaßunabhängige Datenabgleiche keiner speziellen Grundlage bedürften, trifft deshalb nicht zu.

Die Datenschutzbeauftragten wenden sich nicht gegen einzelne Veränderungen der Datenverarbeitung im Sozialleistungsbereich, soweit sie tatsächlich erforderlich und verhältnismäßig sind und die zuvor aufgezeigten Grundsätze beachtet werden. Die Datenschutzbeauftragten sind dazu gesprächsbereit.

Anlage 15

Entschließung
der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 23./24. Oktober 1997 in Bamberg

zur

Novellierung des Bundesdatenschutzgesetzes
und Modernisierung des Datenschutzrechts

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschluß; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

- Verbesserungen des Datenschutzes der Bürger, z. B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;

- dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

- weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;

- Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;

- Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z. B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;

- Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen;

– Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

– Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;

– mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;

– Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Video-Überwachung;

– Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;

– Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;

– Regelungen für Chipkarten-Anwendungen;

– Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;

– Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß vor Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;

– Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereichs verwenden darf;

– möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;

– Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

Entschließung
der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 23./24. Oktober 1997 in Bamberg

zu

Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, daß Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wider. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozeß entscheidet. Erkennbar und nachvollziehbar sollte sein, daß der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, daß Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzentwürfe des Bundesrates (BT-Drs. 13/4983 vom 19.06.1996) sowie der Fraktionen der CDU/CSU und F.D.P. (BT-Drs. 13/7165 vom 11.03.1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten („Vermeidung kognitiver Dissonanzen“). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

Für Videoaufzeichnungen des Betroffenen, die zu seinem Schutz gefertigt werden sollen, ist dessen Einwilligung unverzichtbare Voraussetzung für die Zulässigkeit einer Bild-Ton-Aufzeichnung im Strafverfahren. Sofern der Betroffene nicht in der Lage ist, die Bedeutung und Tragweite einer Bild-Ton-Aufzeichnung und ihrer Verwendungsmöglichkeiten hinreichend zu beurteilen, hat der Gesetzgeber festzulegen, wer anstelle des Betroffenen die Einwilligung erteilen darf. Vor Abgabe der Einwilligungserklärung ist der Betroffene umfassend aufzuklären, insbesondere auch über alle zulässigen Arten der weiteren Verwertung und über die Möglichkeit des Widerrufs der

Einwilligung für die Zukunft. Die Aufklärung ist zuverlässig zu dokumentieren. Entsprechendes gilt für die Herausgabe von Videoaufzeichnungen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Verwendung von Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage, welche Zielsetzung mit Bild-Ton-Aufzeichnungen im Strafverfahren verfolgt werden soll, sind hierbei insbesondere folgende Gesichtspunkte von Bedeutung:

1. Es ist sicherzustellen, daß der Eindruck des Aussagegeschehens z. B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild und Zoom nicht gezielt verfremdet oder verzerrt wird.

2. Einsatz und Verwertung von Bild-Ton-Aufzeichnungen sind so zu regeln, daß gesetzliche Zeugnisverweigerungsrechte gewahrt bleiben. Insbesondere ist eine weitere Nutzung der Aufnahme, auch zum Zwecke des Vorhalts, ausgeschlossen, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.

3. Vorbehaltlich des o. g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen erlaubt sein, da nur so ein wirksamer Schutz vor Mißbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fairen, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zuläßt, müssen jedenfalls wirksame Vorkehrungen gegen Mißbrauch gewährleistet sein, z. B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.

4. Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die Zwecke dieses anderen Verfahrens hätten angefertigt werden dürfen.

5. Soweit eine Verwertung in einem anderen gerichtlichen Verfahren - etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht - zugelassen werden sollte, sind in entsprechenden Ausnahmeregelungen präzise Voraussetzungen hierfür abschließend zu bestimmen und enge Verwendungsregelungen zu treffen.

6. Spätestens mit dem rechtskräftigen Abschluß des Strafverfahrens sind grundsätzlich die Aufzeichnungen unter Aufsicht der Staatsanwaltschaft zu vernichten. Der Betroffene ist davon zu benachrichtigen. Soweit der Gesetzgeber ausnahmsweise zur Wahrung vorrangiger Rechtsgüter eine längere Aufbewahrung der Aufzeichnungen zuläßt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.

Entschließung
der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 23./24. Oktober 1997 in Bamberg

zur

Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne daß die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff „Privacy enhancing technology (PET)“ eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm „Forschung und Entwicklung“ aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

Datenschutzrechtliche Forderungen zum Einsatz von automatisierten staatsanwaltschaftlichen Informationssystemen

(Vorschlag des AK Justiz, zustimmende Kenntnisnahme der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18. April 1997 in München)

In strafrechtlichen Ermittlungsverfahren werden eine Vielzahl höchst sensibler personenbezogener Daten nicht nur von Beschuldigten, sondern auch von Zeugen, Opfern, Hinweisgebern, Anzeigeerstattern und Dritten verarbeitet. Diese Daten bedürfen eines besonderen Schutzes. Sie wurden früher nur in Akten und Karteien bei der jeweils zuständigen Staatsanwaltschaft gespeichert. Ende der siebziger Jahre wurde damit begonnen, Grunddaten aus den Strafverfahren (z. B.: Name des Täters, Aktenzeichen, Straftat und Ausgang des Verfahrens) bei den einzelnen Staatsanwaltschaften in automatisierten Systemen zentral zu speichern.

Heute gestaltet sich die Anwendung von Informationstechnik bei der Staatsanwaltschaft anders. Durch den Einsatz von Netzwerken und leistungsfähigen Computern ist bereits jetzt bei vielen Staatsanwaltschaften die Menge der jeweils zu einem Strafverfahren automatisiert gespeicherten Daten um ein Vielfaches gestiegen. Zudem sind auch die technischen Zugriffsmöglichkeiten der bei den Staatsanwaltschaften Beschäftigten vermehrt worden. Für die Zukunft ist auch nicht auszuschließen, daß darüber hinaus in staatsanwaltschaftlichen Informationssystemen gespeicherte Daten nicht nur verschiedenen Staatsanwaltschaften, Polizei und Gerichten, sondern beispielsweise auch Bewährungshelfern und der Gerichtshilfe online abrufbar zur Verfügung gestellt werden. Durch die Speicherung von Ermittlungsdaten in modernen automatisierten staatsanwaltschaftlichen Informationssystemen für die Bearbeitung von Strafverfahren und für die Vorgangsverwaltung sind somit die Zweckbindung und die Wahrung der Vertraulichkeit der Daten durch eine Vielzahl von Zugriffs- und Nutzungsmöglichkeiten in besonderem Maße gefährdet.

Der Einsatz staatsanwaltschaftlicher automatisierter Informationssysteme begegnet zwar keinen grundsätzlichen datenschutzrechtlichen Bedenken, es sind aber neben den in den meisten Ländern immer noch fehlenden bereichsspezifischen gesetzlichen Grundlagen geeignete und angemessene Maßnahmen und Beschränkungen der Datenverarbeitung erforderlich, die sicherstellen, daß das Grundrecht auf informationelle Selbstbestimmung in erforderlichem Maße geschützt wird.

Im Hinblick auf die Sensibilität der verarbeiteten Daten sind bereits zum Zeitpunkt der Planung aber auch während des Betriebes geeignete Schutzmaßnahmen zu treffen. Diese beinhalten die Erstellung und Fortschreibung eines auf das jeweilige Verfahren und dessen Umfeld ausgerichtetes Datenschutz- und IT-Sicherheitskonzeptes. Nur auf der Basis solcher Konzepte kann beurteilt werden, ob die ausgewählten Maßnahmen geeignet und angemessen sind. Hierbei ist auch eine funktionsfähige interne Kontrolle mit entsprechendem Berichtswesen vorzusehen.

Die Konferenz der Datenschutzbeauftragten sieht es daher - jedenfalls unter der gegenwärtig geltenden Rechtslage - für notwendig an, daß beim Betrieb staatsanwaltschaftlicher Informationssysteme insbesondere die im folgenden aufgezählten Datenschutzvorkehrungen getroffen werden. Sie stellen gleichzeitig eine geeignete Beratungs- und Beurteilungsgrundlage der gegenwärtig in den Ländern eingesetzten Informationssysteme der Staatsanwaltschaften dar.

1. **Speicherungsumfang:**

   In staatsanwaltschaftlichen Informationssystemen dürfen nur Daten gespeichert werden, die für die jeweilige Aufgabenerfüllung der Staatsanwaltschaft erforderlich sind. Die Datenfelder sind festzulegen. Darüber hinaus sollte der jeweils gespeicherte Datenbestand stets entsprechend dem Verfahrensstand aktualisiert bzw. reduziert werden. Soweit Freitextfelder überhaupt erforderlich sind, sind die darin zulässigen Einträge abschließend festzulegen. Soweit Freitextfelder der Aufnahme von Bemerkungen, Notizen und ähnlichem dienen, sind diese nicht recherchierbar auszugestalten.

2. **Löschungsfristen:**

   Konkrete Löschungsfristen müssen vorgesehen werden. Diese haben sich am jeweiligen Zweck der Speicherung zu orientieren (laufende Strafverfahren, Strafvollstreckung, künftige Strafverfahren, Vorgangsverwaltung). Für Zwecke der Vorgangsverwaltung dürfen die Löschungsfristen keinesfalls länger sein, als die entsprechenden Aufbewahrungsfristen für die zugehörigen Akten bzw. Aktenteile.

   Die Daten von Nebenbeteiligten (z. B. Zeugen, Geschädigten und Anzeigeerstattern) in Js-Verfahren sind spätestens bei Weglegung der Akte zu löschen. Sobald die Daten von Hauptbeteiligten (z. B. Mitbeschuldigten) für das Strafverfahren nicht mehr benötigt werden, ist eine Teillöschung der Daten vorzunehmen. Dabei ist der Zeitpunkt der Teillöschung für jeden Hauptbeteiligten individuell zu bestimmen.

   Die automatisierten staatsanwaltschaftlichen Informationssysteme sind zur Kontrolle der Löschfristen und Aktenvernichtung einzusetzen.

3. **Zugriffsbeschränkungen und Datensperren:**

   Werden Daten eines Ermittlungsverfahrens in automatisierten staatsanwaltschaftlichen Informationssystemen für andere Stellen abrufbar bei der bearbeitenden Staatsanwaltschaft gespeichert, ist der Zugriff auf diese Daten auf das für die jeweilige Aufgabenerfüllung der abrufenden Stelle erforderliche Maß zu beschränken.

   Eine geeignete Maßnahme zur Beschränkung des Zugriffs ist die Vergabe differenzierter Zugriffsrechte. Sie muß systemseitig ermöglicht werden. Zur besseren Handhabbarkeit können, soweit die jeweiligen Arbeitsabläufe dies zulassen, verschiedene Benutzergruppen mit jeweils gleichen Rechten eingerichtet werden. Über die genaue Vergabe von Zugriffsrechten kann keine allgemeingültige Aussage getroffen werden, da die jeweiligen Organisationsformen der Staatsanwaltschaften berücksichtigt werden müssen. Zugriffsbeschränkungen können z. B. einsetzen beim datenverändernden Zugriff, beim lesenden Zugriff sowie beim Kreis der Zugriffsberechtigten in Abhängigkeit vom Verfahrensstand und von der Art der Daten. Vor allem der Zugriff auf die Daten der Nebenbeteiligten (wie Zeugen und Opfer) ist eng zu begrenzen. Der Kreis der zugriffsberechtigten Personen sollte darüber hinaus entsprechend dem Zweck der Speicherung (z. B. Sachberarbeitung, Vorgangsverwaltung) eingeschränkt werden.

Eine weitere Möglichkeit der Zugriffsbeschränkung liegt in der Sperrung von Daten. Eine Sperrung von Daten kommt aus datenschutzrechtlicher Sicht, insbesondere in folgenden Fällen in Betracht:

- bei Eintragungen von Vorgängen gegen Strafunmündige,
- bei Verfahrenseinstellungen, bei denen der Betroffene eine Mitteilung gemäß Nr. 88 Satz 2 RiStBV erhalten hat,
- wenn der Angeklagte rechtskräftig freigesprochen oder die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt wurde oder der Tatverdacht entfallen ist,
- bei Opferdaten von Sexualstraftaten,
- bei gefährdeten Personen gemäß § 68 StPO,
- bei Suizid oder Suizidversuch.

4. **Vergabe und Dokumentation von Zugriffsrechten:**

   Die Vergabe von Zugriffs- und Bearbeitungsrechten sowie deren Änderung, Sperrung oder Löschung ist revisionsfähig zu dokumentieren. Im Datenschutzkonzept der Anwender ist festzulegen, auf welche Art und Weise und durch wen die Vergabe und die Dokumentation dieser Rechte erfolgt. Als softwaretechnische Hilfsmittel haben sich Rechteverwaltungstabellen oder Verfahren der objektorientierten Rechtevergabe bewährt.

5. **Protokollierung:**

   Das Ändern, Sperren und Löschen der Daten ist in jedem Fall zu protokollieren. Auch der lesende Zugriff sollte regelmäßig protokolliert werden. Dies um so wichtiger, je weniger detailliert und eng Zugriffsbeschränkungen innerhalb der datenverarbeitenden Stelle (Staatsanwaltschaften) realisiert worden sind. Eine Protokollierung der Abfrage muß im Interesse einer effektiven Datenschutzkontrolle den Abfragegrund wie z. B. die Eingabe des Aktenzeichens des staatsanwaltschaftlichen Vorgangs, für dessen Bearbeitung die Abfrage erfolgt, umfassen.

   Die Aufbewahrung der Protokolldaten sollte über einen angemessenen Zeitraum hinweg erfolgen. Nicht ausreichend ist die Protokollierung lediglich des jeweils letzten Zugriffs auf einen Datensatz. Die Nutzung der Protokolldaten z. B. für Zwecke der Datenschutzkontrolle oder zur Sicherung eines ordnungsgemäßen Betriebes der DV-Anlage ist vorher festzulegen. Dabei ist eine enge Zweckbindung sicherzustellen. Um eine verbotswidrige Auswertung der Protokolldaten zu vermeiden, ist das „Vier-Augen-Prinzip„ zu gewährleisten.

   Alle Aktivitäten, die der Systemverwaltung dienen, müssen revisionssicher aufgezeichnet werden.

6. **Datenaustausch mit anderen Stellen:**

   Bei der Einführung landesweiter staatsanwaltschaftlicher Informationssysteme ist zu prüfen, ob überhaupt, ggf. welche zusätzlichen Daten, die nicht im ZStV abgerufen werden können, zur Aufgabenerfüllung bei den einzelnen Staatsanwaltschaften benötigt werden. Der Datenaustausch (Übermittlung und Abruf) mit ZStV, BZR und anderen speichernden

Stellen wie z. B. Gerichten, Strafvollzug und Polizei sollte grundsätzlich nur im Rahmen von Verfahren eingesetzt und abgewickelt werden, die durch Einsatz geeigneter kryptographischer Verfahren (z. B. Verschlüsselung, digitale Signatur) die Vertraulichkeit, Integrität und Zurechenbarkeit der Daten sicherstellen. Kommen Abrufverfahren zum Einsatz, so sind sowohl auf den Übertragungswegen als auch bei den abrufenden Stellen Vorkehrungen zu treffen, die das interne Sicherheitsniveau der staatsanwaltschaftlichen Systeme nicht senken.

Die staatsanwaltschaftlichen Informationssysteme sollten darüber hinaus gewährleisten, daß die Polizei sowohl über die Berichtigung des Tatvorwurfs wie auch über den Ausgang des Verfahrens möglichst umgehend informiert wird, soweit sie mit der Angelegenheit befaßt waren.

7. **Weitere technische Datenschutzvorkehrungen:**

Der Zugang zu den staatsanwaltschaftlichen Informationssystemen ist durch geeignete technische und organisatorische Maßnahmen wie beispielsweise Zugangskontrolle mittels Chipkartensystem oder Sicherheitssoftware mit Paßwort zu schützen. Darüber hinaus kann nach mehrmaligen fehlerhaften Anmeldeversuchen in ununterbrochener Reihenfolge eine Sperrung des Endgerätes oder der Benutzerkennung (oder Setzen eines Timeout-Parameters) erfolgen. Die Entsperrung darf nur durch die Systemverwaltung bzw. durch eine dazu bestimmte Person vorgenommen werden.

Ein ausreichender Schutz vor dem unbefugten Einsatz fremder Programme sowie von Manipulationen der eingesetzten Software oder vor Eigenprogrammierungen ist vorzusehen. Die Betriebssystemebene (Shell-Ebene) sollte für den Anwender gesperrt sein. Die Datenbankabfragesprache (SQL) sollte nicht nutzbar sein.

Der Einsatz von PC stellt eine besondere Gefährdung in staatsanwaltschaftlichen Informationssystemen dar. Es sind daher Maßnahmen zu treffen, die einen Im- und Export von Daten über ungesicherte Schnittstellen und Laufwerke, eine unerlaubte Weiterverarbeitung mittels Standardsoftware, z. B. Office-Produkte und einen wirkungsvollen Schutz vor dem Zugriff auf die Systemebene beinhalten. Soweit bei den PC die Diskettenlaufwerke nicht gesperrt werden können, sind besondere Sicherheitsmaßnahmen wie z. B. die verschlüsselte Speicherung vorzusehen. Sonstige nicht benötigte Schnittstellen sind zu sperren.

Die Konferenz der Datenschutzbeauftragten macht im übrigen darauf aufmerksam, daß sie sich bereits mehrfach in Entschließungen zu den Bedingungen geäußert hat, unter denen ein datenschutzgerechter Einsatz staatsanwaltschaftlicher Informationssysteme erfolgen kann. In diesem Zusammenhang ist auf die folgenden Entschließungen der Konferenz hinzuweisen:

- „Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren“ vom 24./25. 11.1986,

- Stellungnahme zum StVÄG 88 vom 05./06.04.1989,

- Rückmeldung über den Ausgang des Verfahrens an die Polizei vom 04./05.05.1987,

- Zur Informationsverarbeitung im Strafverfahren vom 09./10.03.1994,

- Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich vom 09./10.03.1995,

- Datenschutz bei elektronischen Mitteilungssystemen vom 09./10.03.1995 und

- Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten vom 09.05.1996.

Die Konferenz der Datenschutzbeauftragten nimmt die Vorlage des AK Justiz grundsätzlich zustimmend zur Kenntnis.

Datensparsamkeit durch moderne Informationstechnik
- Datenvermeidung, Anonymisierung und Pseudonymisierung -
(Kurzbericht der AK Technik, zustimmende Kenntnisnahme
der 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 22./23. Oktober 1996 in Hamburg)

Die zunehmende Verbreitung, Nutzung und Verknüpfbarkeit von Informations- und Kommunikationstechnik bringt mit sich, daß jeder Benutzer immer mehr elektronische Spuren hinterläßt. Das wird dazu führen, daß er über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der vielen über ihn gespeicherten Daten keine Kontrolle mehr hat, so daß die Gefahr des Mißbrauchs und der Zusammenführung zu komplexen Persönlichkeitsprofilen ständig zunimmt.

Dieser Gefahr kann dann begegnet werden, wenn in Zukunft die Frage nach der Erforderlichkeit personenbezogener Daten im Vordergrund steht, wobei Datensparsamkeit bis hin zur Datenvermeidung angestrebt werden muß. Durch die Nutzung neuer Möglichkeiten der modernen Informations- und Kommunikationstechnik (IuK-Technik) ist es in vielen Anwendungsfällen möglich, den Umgang mit personenbezogenen Daten zu reduzieren bis hin zur vollständigen Vermeidung. Auf diese Weise kann das Prinzip **„Datenschutz durch Technik“** umgesetzt werden. Datensparsamkeit und Datenvermeidung werden sich dabei auch zunehmend als Wettbewerbsvorteil erweisen.

Ausgehend von einer Untersuchung des niederländischen Datenschutzbeauftragten und des Datenschutzbeauftragten von Ontario/Kanada zum sogenannten **Identity Protector** beschäftigen sich derzeit die Datenschutzbeauftragten des Bundes und der Länder intensiv mit der Formulierung von Anforderungen zur datenschutzfreundlichen Ausgestaltung von IuK-Technik. Schon die Sommerakademie in Kiel zeigte unter dem Motto „Datenschutz durch Technik - Technik im Dienste der Grundrechte“ Wege zur Wahrung der Persönlichkeitsrechte der Bürger auf. Einige datenvermeidende Technologien wie die anonyme, vorausbezahlte Telefonkarte, sind bereits seit längerer Zeit allgemein akzeptiert. Erste Ansätze der Datenvermeidung auf gesetzgeberischer Ebene sind im Entwurf zum Teledienstegesetz und zum Mediendienstestaatsvertrag enthalten.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ erarbeitet im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Bericht mit Vorschlägen und Empfehlungen, wie unter Nutzung der modernen Datenschutztechnik das Prinzip der Datenvermeidung umgesetzt werden kann. Neben der Entwicklung entsprechender Hard- und Software werden Anonymisierung und Pseudonymisierung eine zentrale Rolle spielen. Bei der Erarbeitung des Berichtes werden Experten aus Wissenschaft und Forschung hinzugezogen, um die technische Entwicklung berücksichtigen zu können. Auch Vertreter der Wirtschaft als Entwickler und Anwender werden einbezogen, damit die Umsetzung der Vorschläge der Datenschutzbeauftragten als zukünftiger Wettbewerbsvorteil erkannt wird.

Datenschutz und Telefax
(Empfehlungen des AK Technik, zustimmende Kenntnisnahme durch die Datenschutzbeauftragten des Bundes und der Länder im Dezember 1996)

I. Konventionelle Telefaxgeräte

Telefaxgeräte sind datenverarbeitende Geräte, mit denen auch personenbezogene Daten automatisiert übertragen werden können. Sie werden eingesetzt, um bei einfacher Handhabung schnell Informationen zu übermitteln. Das Telefax ist nach dem Telefon inzwischen zum wichtigsten Kommunikationsverfahren geworden. Nicht alle Nutzer von Telefaxgeräten sind sich darüber im klaren, welche Risiken für die Vertraulichkeit der per Telefax übermittelten Informationen bestehen.

Die besonderen Gefahren sind:

- Die Informationen werden grundsätzlich „offen“ (unverschlüsselt) übertragen, und der Empfänger erhält sie - vergleichbar mit einer Postkarte - in unverschlossener Form.

- Der Telefaxverkehr ist wie ein Telefongespräch abhörbar.

- Die Adressierung erfolgt durch eine Zahlenfolge (Telefaxnummer) und nicht durch eine mehrgliedrige Anschrift. Dadurch sind Adressierungsfehler wahrscheinlicher, und Übertragungen an den falschen Adressaten werden nicht oder erst nachträglich bemerkt.

- Bei Telefaxgeräten neueren Typs kann der Hersteller Fernwartungen durchführen, ohne daß der Besitzer diesen Zugriff wahrnimmt. Unter bestimmten Umständen kann er dabei auf die im Telefaxgerät gespeicherten Daten zugreifen (z. B. Lesen der Seitenspeicher sowie Lesen und Beschreiben der Rufnummern- und Parameterspeicher).

Diese Gefahren werden von Anbietern der Telekommunikationsnetze und -dienste nicht abgefangen. Deshalb ist insbesondere die absendende Stelle für die ordnungsgemäße Übertragung und die richtige Einstellung der technischen Parameter am Telefaxgerät verantwortlich.

Die Datenschutzbeauftragten des Bundes und der Länder habe sich mit den Risiken vertraulicher Kommunikation beim Einsatz von Telefaxgeräten befaßt. Sie geben die folgenden Empfehlungen, um den datenschutzgerechten Umgang mit Telefaxgeräten weitgehend zu gewährleisten:

1. Aufgrund der gegebenen Gefährdungen darf die Übertragung sensibler personenbezogener Daten per Telefax nicht zum Regelfall werden, sondern darf nur im Ausnahmefall unter Einhaltung zusätzlicher Sicherheitsvorkehrungen erfolgen.

2. Was am Telefon aus Gründen der Geheimhaltung nicht gesagt wird, darf auch nicht ohne besondere Sicherheitsvorkehrungen (z. B. Verschlüsselungsgeräte) gefaxt werden. Das gilt insbesondere für sensible personenbezogene Daten, beispielsweise solche, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (Sozial-, Steuer-, Personal- und medizinische Daten).

3. Bei der Übertragung sensibler personenbezogener Daten ist zusätzlich zu hier genannten Maßnahmen mit dem Empfänger ein Sendezeitpunkt abzustimmen, damit Unbefugte keinen Einblick nehmen können. So kann auch eine Fehlleitung durch z. B. veraltete Anschlußnummern oder beim Empfänger aktivierte Anrufumleitungen bzw. -weiterleitungen vermieden werden.

4. Telefaxgeräte sollten nur auf der Grundlage schriftlicher Dienstanweisungen eingesetzt werden. Die Bedienung darf nur durch eingewiesenes Personal erfolgen.

5. Das Telefaxgerät ist so aufzustellen, daß Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Schreiben erhalten können.

6. Alle vom Gerät angebotenen Sicherheitsmaßnahmen (z. B. Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Paßwort, Fernwartungsmöglichkeit sperren) sollten genutzt werden.

7. Die vom Gerät auf Gegenseite vor dem eigentlichen Sendevorgang abgegebene Kennung ist sofort zu überprüfen, damit bei eventuellen Wählfehlern die Übertragung unverzüglich abgebrochen werden kann.

8. Bei Telefaxgeräten, die an Nebenstellenanlagen angeschlossen sind, ist das Risiko einer Fehladressierung besonders groß, da vor der Nummer des Teilnehmers zusätzlich Zeichen zur Steuerung der Anlage eingegeben werden müssen. Beim Umgang mit derartigen Geräten ist deshalb besondere Sorgfalt geboten.

9. Die Dokumentationspflichten müssen eingehalten werden (z. B. Vorblatt oder entsprechend aussagekräftige Aufkleber verwenden, Zahl der Seiten angeben, Protokolle aufbewahren). Sende- und Empfangsprotokolle sind vertraulich abzulegen, da sie dem Fernmeldegeheimnis unterliegen.

10. Vor Verkauf, Weitergabe oder Aussortieren von Telefaxgeräten ist zu beachten, daß alle im Gerät gespeicherten Daten (Textinhalte, Verbindungsdaten, Kurzwahlziele usw.) gelöscht werden.

11. Die am Telefaxgerät eingestellten technischen Parameter und Speicherinhalte sind regelmäßig zu überprüfen, damit beispielsweise Manipulationsversuche frühzeitig erkannt und verhindert werden können.

12. Verfügt das Telefaxgerät über eine Fernwartungsfunktion, sollte sie grundsätzlich durch den Nutzer aktiviert werden. Nur für notwendige Wartungsarbeiten ist diese Funktionen freizugeben. Nach Abschluß der Wartungsarbeiten sollten die eingestellten Parameter und Speicherinhalte kontrolliert werden.

II. Telefax in Bürokommunikationslösungen

Rechner mit Standard- oder Bürokommunikationssoftware können um Hard- und Softwarekomponenten erweitert werden, mit deren Hilfe Telefaxe gesendet und empfangen werden können (integrierte Telefaxlösungen). Lösungen für den Faxbetrieb werden sowohl für Einplatzrechner als auch für Rechnernetze angeboten.

Der Betrieb (Installation, Konfiguration, Bedienung und Wartung) integrierter Telefaxlösungen birgt gegenüber dem konventionellen Telefaxgerät zusätzliche Gefahren, da beispielsweise die verwendeten Faxmodems bzw. - karten oft nicht nur für Telefaxsendung und -empfang geeignet sind, son-

dern auch andere Formen der Datenübertragung und des Zugriffes ermöglichen.

Daher sollten die folgenden Empfehlungen beim Umgang mit integrierten Telefaxlösungen zusätzlich zu den bereits genannten beachtet werden.

1. Das verwendete Rechnersystem muß sorgfältig konfiguriert und gesichert sein. Die IT-Sicherheit des verwendeten Rechners bzw. Netzes ist Voraussetzung für einen datenschutzgerechten Betrieb der Faxlösung. Dazu gehört unter anderem, daß kein Unbefugter Zugang oder Zugriff zu den benutzten Rechnern und Netzwerken hat.

2. Beim Absenden ist auf die korrekte Angabe der Empfänger zu achten. Dazu sind die durch die Faxsoftware bereitgestellten Hilfsmittel wie Faxanschlußlisten, in denen Empfänger und Verteiler mit aussagekräftigen Bezeichnungen versehen werden können, zu benutzen.

3. Die vielfältigen Nutzungsmöglichkeiten integrierter Faxlösungen erfordern die regelmäßige und besonders sorgfältige Überprüfung der in der Faxsoftware gespeicherten technischen Parameter, Anschlußlisten und Protokolle.

4. Der Einsatz kryptographischer Verfahren ist bei integrierten Faxlösungen unkompliziert und kostengünstig möglich, sofern beide Seiten kompatible Produkte einsetzen. Deshalb sollten personenbezogene Daten immer verschlüsselt und digital signiert übertragen werden, um das Abhören zu verhindern und um den Absender sicher ermitteln und Manipulationen erkennen zu können.

5. Schon bei der Beschaffung integrierter Telefaxlösungen sollte darauf geachtet werden, daß ausreichende Konfigurationsmöglichkeiten vorhanden sind, um die dringend notwendige Anpassung an die datenschutzrechtlichen Erfordernisse des Nutzers zu gewährleisten.

Anforderungen zur informationstechnischen Sicherheit bei Chipkarten[1]

(Arbeitspapier des AK Technik, Stand: 02.12.1996)

I. Einleitung

Chipkarten sind miniaturisierte IT-Komponenten, meist in der genormten Größe einer Kreditkarte. Sie haben Eingang ins tägliche Leben gefunden, gewinnen zunehmend an gesellschaftlicher Bedeutung und bedürfen aus der Sicht des Datenschutzes zur Wahrung der informationellen Selbstbestimmung und der informationstechnischen Sicherheit größter Aufmerksamkeit.

Die derzeit bekannteste Chipkarten-Anwendung ist die Telefonkarte, die ein Guthaben enthält, das beim Gebrauch der Chipkarte in einem Kartentelefon reduziert wird, bis das Konto erschöpft ist und die Chipkarte unbrauchbar wird. Ebenfalls allgemein bekannt ist die Krankenversicherungskarte (KVK), die lediglich einen gesetzlich vorgegebenen Inhalt hat und zur Identifizierung des Patienten sowie zur Abrechnung ärztlicher Leistungen verwendet wird. Sie ist ein Beispiel für eine Chipkarte, die lediglich die dem Versicherten erkennbare Oberfläche einer umfassenden IT-Infrastruktur ist. Was unterhalb dieser Oberfläche geschieht, ist für die Betroffenen nicht transparent.

Weitere neue Anwendungsbereiche von Chipkarten sind derzeit in der Diskussion bzw. in der Erprobung, z. B.:

- die Chipkarte im bargeldlosen Zahlungsverkehr
- Gesundheits- oder Patientenchipkarten zur Speicherung und Übermittlung medizinischer Daten.

Von der Technik her sind reine Speicherchipkarten zur Aufnahme von Daten (meist in Halbleiter-Technologie oder optischer Speichertechnik) von solchen Karten zu unterscheiden, in die Mikroprozessoren und speichernde Bauteile integriert sind. Solche Prozessorchipkarten sind als Kleinstcomputer ohne Mensch-Maschine-Schnittstelle anzusehen. Ihre Verwendung bedarf also zusätzlicher technischer Systeme zum Lesen der gespeicherten Daten, zum Aktivieren der Funktionen der Mikroprozessoren und zum Beschreiben der Speicher.

Systeme zur Erschließung der Funktionen von Chipkarten werden im folgenden Chipkartenbasierte Dienstleistungssysteme (CDLS) genannt. Beispiele für solche Systeme sind:

- Öffentliches Telefon-Kartenterminal
- Funktelefon (Handy)
- PC mit externem Kartenterminal oder integriertem Kartenleser
- Laptop mit PCMCIA-Kartenleser
- Geldausgabeautomat

[1] Die hiermit vorgelegte Ausarbeitung ist in der Version vom 02. Dezember 1996. Der schnelle Fortschritt bei der Entwicklung der Chipkartentechnologien macht im Prinzip eine ständige Anpassung oder Fortschreibung erforderlich. Die Arbeitskreisgruppe hat jedoch beschlossen, zunächst ein fertiges Papier mit festgelegtem Aktualitätsstand vorzulegen, da sonst die Gefahr besteht, nie zu einem Abschluß zu kommen. Jedoch ist es geeignet, in weiteren Arbeitsschritten fortgeschrieben zu werden.

- Point-of-Sale-Kartenterminal (POS-Kartenterminal)
- Versicherten-Kartenterminal in seiner Stand-alone-Ausführung (ohne PC-Anschluß)
- Kontoauszugsdrucker
- Airline-Checkin-Terminal
- Customer-Service-Terminal
- Fahrschein-/Parkticket-Terminal

Sicherheitsbetrachtungen zum Einsatz von Chipkarten müssen deshalb auch die Sicherheit dieser Infrastrukturen einbeziehen.

Wichtige Funktionalitäten der Chipkarten sind:

- Chipkarten als Speicher von Daten, die hinsichtlich ihrer Vertraulichkeit und/oder Integrität hohen Schutzbedarf aufweisen (z. B. Kontodaten, medizinische lndividualdaten, Personalausweisdaten, Führerscheindaten);
- Chipkarten als Mittel zur Authentisierung ihres Trägers für die Gewährung des Zugriffs auf sicherheitsrelevante Daten und Funktionen (Kontoverfügungen, Änderung medizinischer lndividualdaten);
- Chipkarten als Mittel zur Signatur von Dokumenten (Verträge, Willenserklärungen, Befunde etc.);
- Chipkarten als Träger elektronischer Geldbörsen.

Die weiteren Ausführungen dieses Papiers beschränken sich auf die für die Sicherheit der Informationstechnik relevanten Merkmale und Anforderungen an Chipkarten, sowohl in ihrer Funktion als Instrumente zur Herstellung von Sicherheit als auch als sicherheitsbedürftige IT-Komponenten.

Obwohl - wie die Krankenversicherungskarte zeigt - auch Speicherchipkarten datenschutzrechtlich relevant sind, beschränken sich die weiteren Ausführungen auf Prozessorchipkarten. Diese haben in Zukunft sowohl hinsichtlich ihrer Verbreitung und Anwendungen als auch in Hinblick auf datenschutzrechtliche Chancen und Risiken eine größere datenschutzrechtliche Bedeutung.

II. Empfehlungen zum Einsatz von Chipkarten

Für den datenschutzgerechten Einsatz von Chipkarten ist eine konsequente und überzeugende Sicherungstechnologie erforderlich. Datensicherungsmaßnahmen müssen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Mißbrauch gewährleisten. Dabei ist von folgenden Gefahren auszugehen:

- unbefugte Preisgabe von Informationen (Verlust der **Vertraulichkeit);**
- unbefugte Veränderung von Informationen (Verlust der **Integrität);**
- unbefugte Vorenthaltung von Informationen oder Betriebsmittel (Verlust der **Verfügbarkeit);**
- unbefugte Änderung identifizierender Angaben (Verlust der **Authentität).**

Diese Gefahren sind sowohl dann zu betrachten, wenn die Daten auf der Chipkarte gespeichert werden, als auch dann, wenn sie in einer externen Datenbank gespeichert werden, die durch Chipkarten erschlossen wird.

Vor der Entscheidung über den sicherheitsrelevanten Einsatz von Chipkarten-Anwendungen sollte eine projektbezogene Technikfolgenabschätzung durchgeführt werden, so wie dies Art. 20 der EU-Datenschutzrichtlinie als Vorabkontrolle fordert. Zur Auswahl geeigneter und angemessener Sicherungsmaßnahmen ist eine systematische Einschätzung der Gefahren für das informationelle Selbstbestimmungsrecht und das Recht auf kommunikative

Selbstbestimmung vorzunehmen und sind Lösungsvorschläge für eine Sicherungstechnologie zu erarbeiten.

Die Auseinandersetzung mit dem Phänomen „Chipkarte“ zwingt zur Differenzierung zwischen den technischen Systemen und den Applikationen, die sich dieser Systeme bedienen, und der Chipkarte selbst. Genausowenig wie es „die“ Chipkarte gibt, genausowenig kann man von „der“ Chipkartenanwendung sprechen. Würde man datenschutzrechtliche und sicherheitstechnische Schlußfolgerungen ausschließlich aus einer der vielen Kombinationsmöglichkeiten ziehen, wäre eine Allgemeinverbindlichkeit der Aussagen bzw. Anforderungen nicht zu erreichen. Konkrete Rechtsprobleme und Risiken lassen sich nur mit einem Bezug zu bestimmten inhaltlichen und technischen Rahmenbedingungen aufzeigen. Die geplanten Gesundheits- und Patientenchipkartensysteme sind insoweit geeignete Beispiele.

Notwendig erscheint auch eine dauernde Bereitschaft, die schnell fortschreitende technologische Weiterentwicklung aufmerksam zu begleiten und bei Bedarf steuernd einzugreifen, denn die datenschutztechnischen Fragestellungen werden umso komplexer, je weiter sich die Chipkartentechnologie entwickelt.

Künftige neue Anwendungen werden sich tendenziell der Prozessorchipkartentechnologie bedienen. Prozessorchipkarten sind miniaturisierte Computer, die allerdings nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Diese werden über CDLS realisiert. Datenschutzrechtliche Anforderungen erstrecken sich hier neben den CDLS auch auf die Rahmenbedingungen bei der Herstellung, bei der Initialisierung, beim Versand und bei der Ersatzbeschaffung von Chipkarten in Fällen des Verlustes oder der Zerstörung einschließlich des „Ungültigkeitsmanagements“. Die Hersteller bieten Chipkarten an, deren Leistungsfähigkeit und Funktionsweise diesbezüglich zum Teil sehr unterschiedlich ist. Eine Standardisierung wäre auch aus datenschutzrechtlicher Sicht in diesem Bereich dringend zu empfehlen.

Das Sicherungskonzept für Chipkarten sollte folgende Mindestanforderungen erfüllen, wenn Schutzbedarf besteht:

1 . Grundschutzmaßnahmen
- Ausstattung des Kartenkörpers mit fälschungssicheren Authentifizierungsmerkmalen wie z. B. Unterschrift, Foto, Hologramme.
- Steuerung der Zugriffs- und Nutzungsberechtigungen durch die Chipkarte selbst.
- Realisierung aktiver und passiver Sicherheitsmechanismen gegen eine unbefugte Analyse der Chip-Inhalte sowie der chipintegrierten Sicherheitsfunktionen.
- Benutzung allgemein anerkannter, veröffentlichter Algorithmen für Verschlüsselungs- und Signaturfunktionen sowie zur Generierung von Zufallszahlen.
- Sicherung der Kommunikation zwischen der Chipkarte, dem Kartenterminal CDLS und dem ggf. im Hintergrund wirkenden System durch kryptographische Maßnahmen.
- Sicherung unterschiedlicher Chipkartenanwendungen auf einer Chipkarte durch gegenseitige Abschottung.
- Durchführung einer gegenseitigen Authentisierung von Chipkarte und CDLS mit dem Challenge-Response-Verfahren.

2. Erweiterte Sicherungsmaßnahmen
- Realisierung weiterer „aktiver“ Sicherheitsfunktionen des Betriebssystems wie „Secure Messaging“, I/O-Kontrolle aller Schnittstellen, lnterferenzfreiheit der einzelnen Anwendungen,

Verzicht auf Trace- und Debug-Funktionen und dergleichen. Zur Sicherung von Transaktionen oder zur Rekonstruktion nicht korrekt abgelaufener Transaktionen kann ein Logging vorhanden sein.
- Auslagerung von Teilen der Sicherheitsfunktionen des Betriebssystems in dynamisch bei der Initialisierung bzw. Personalisierung zuladbare Tabellen, damit der Chipkartenhersteller nicht über ein „Gesamtwissen“ verfügt.

3. Grundsätzlich sollte zunächst die Möglichkeit in Betracht gezogen werden, daß bei der Chipkartenbenutzung Anonymität gewahrt bleiben kann. Ist dies nicht möglich, sollten Wahlmöglichkeiten anonymer Alternativen geschaffen werden.

4. Der Chipkarteninhaber bzw. die Betroffenen sollten die Möglichkeit, erhalten, auf neutralen, zertifizierten Systemumgebungen die Dateninhalte und Funktionalitäten ihrer Chipkarten einzusehen (Gebot der Transparenz).

5. Die gesamte Infrastruktur ist zu dokumentieren und die Produktion, die Initialisierung und der Versand der Chipkarten zu überwachen.

6. Für die gesamte Infrastruktur ist ein Mindestschutzniveau vorzuschreiben, das bei unbefugten Handlungen das Strafrecht anwendbar macht.

7. Alle Systemkomponenten datenschutzrelevanter Chipkartenanwendungen sind auf der Basis der Grundsätze ordnungsgemäßer Datenverarbeitung zu evaluieren.

8. Für die Informationsstrukturen sind zu Echtheits- und Gültigkeitsüberprüfungen (z. B. Abgleich gegen Sperr- und Gültigkeitsdateien) Kontrollmöglichkeiten zu schaffen.

9. Sicherheitsrelevante Karten (z. B. Bankkarten) sollten über den gesamten Lebenszyklus der Karte kryptographisch gesichert sein.

III. Technische Grundlagen

III.1 Hardware der Chipkarten

Chipkarten gibt es in vielfältigen Bauformen, Funktionsweisen und Funktionsspektren.
Man unterscheidet Chipkarten hinsichtlich der

- Art der Datenübertragung bei der Interaktion mit der Außenwelt:
  => kontaktbehaftet oder
  => kontaktlos über elektromagnetische Felder (bestimmte kontaktlose Karten können auch über eine Entfernung von mehreren Metern von einem CDLS gelesen werden);

- Art der in der Karte bereitgestellten IT-Ressourcen:
  => reine Speicherchipkarten mit nicht flüchtigem Speicher (z. B. Identifikationskarten),
  => intelligente Speicherchipkarten mit EPROM (z. B. Telefonkarte) oder EEPROM (z. B. Krankenversichertenkarten),
  => Prozessorchipkarten mit EEPROM, RAM, ROM und CPU
  => Prozessorchipkarten mit Coprozessoren für die Abwicklung kryptografischer Verfahren (Krypto-Coprozessor).

– Art der Anwendung:
  => elektronischer Zahlungsverkehr (Elektronische Geldbörse),
  => Wegwerfkarten (Telefonkarte),
  => wiederaufladbare Karten (z. B. Chipkarten im öffentlichen Personennahverkehr),
  => multifunktionale wiederaufladbare Chipkarten (z. B. unterschiedliche Geldbörsen auf einer Chipkarte)
  => Berechtigungskarten (z. B. Mobiltelefone, Betriebsausweise)

Der Mikroprozessor einer Chipkarte leistet derzeit ca. 1 Million Befehle pro Sekunde. Direktzugriffsspeicher (RAM) erreichen eine Kapazität von 512 Byte, Festwertspeicher (ROM) für das Betriebssystem erreichen derzeit eine Kapazität von 16 KB, der elektrisch löschbare, programmierbare Festwertspeicher (EEPROM) mit der Kapazität von 16 KB erlaubt die Installation einer kleinen Datenbank. Im Vergleich dazu leisten Mikroprozessoren heute üblicherweise eingesetzter PCs ca. 100 - 150 Millionen Befehle pro Sekunde und arbeiten mit RAM-Speichern von 8 - 32 MB.

III.2 Chipkarten-Betriebssysteme

Prozessorchipkarten verfügen über einen nicht überschreibbaren Speicherbereich, der keine Änderungen und somit auch keine Manipulationen ermöglicht.

In diesem „Read-Only-Memory“ (ROM) befindet sich das Betriebssystem einer Chipkarte. Für Chipkarten-Betriebssysteme existiert u. a. die Normen aus der Serie ISO/IEC 7816-4, in der die Befehle solcher Systeme beschrieben werden. Die Chipkarten-Betriebssysteme nutzen diese Befehle in unterschiedlicher Weise, d. h. nicht jedes Betriebssystem unterstützt jedes Kommando oder jede Option eines Kommandos. Auch weisen fast alle Chipkarten-Betriebssysteme zusätzliche herstellerspezifische Kommandos auf. Die Chipkarten-Betriebssysteme ermöglichen die multifunktionale Nutzung von Chipkarten, können also mehrere unterschiedliche Anwendungen unterstützen.

Die folgende Darstellung wird an den internationalen Standard angelehnt:

III.2.1 Filesystem

Die Dateien des Betriebssystems sind hierarchisch organisiert. Den Ursprung des Dateisystems bildet das Master File (MF). Auf der MF-Ebene können Daten vorhanden sein, die von allen Anwendungen der Chipkarte gemeinsam genutzt werden (z. B. Daten über den Karteninhaber, Seriennummer, Schlüssel). Sie sind in der Regel in Elementary Files (EF) abgelegt.

Daneben gibt es auch sog. Dedicated Files (DF), die mit ihren untergeordneten EFs und ihren Funktionen die Anwendungen einer Karte repräsentieren. Für jedes DF können separate Sicherheitsfunktionen definiert werden. Die DFs einer Chipkarte sind physikalisch und logisch voneinander getrennt, können aber auf die Daten auf der MF-Ebene zugreifen.

EFs können dem Betriebssystem zugeordnet sein und damit Daten enthalten, die das Betriebssystem nutzt, z. B. anwendungsbezogene Paßwörter, Schlüssel und andere Zugriffsattribute zu Nutzdaten. Ein direkter Zugriff mittels des CDLS ist nicht möglich.

Sie können aber auch die Nutzdaten einer Anwendung enthalten, die ggf. erst nach einer Authentisierung unter Berücksichtigung von Sicherheitsattributen gelesen und/oder verändert werden. Es gibt unterschiedliche Dateistrukturen

für EFs: Sie können Records mit fester (linear fixed) oder variabler (linear variable) Länge enthalten, können eine Ringstruktur mit fester Länge (cyclic) haben, können jedoch auch eine amorphe, d.h. vom Benutzer frei wählbare Struktur (transparent) aufweisen, auf denen auf Daten byte- oder blockweise zugegriffen werden kann.

III.2.2 Authentisierung

Die Authentisierungstechniken zwischen Chipkarte und einer externen Einheit werden in der Norm ISO/IEC 9798-2 beschrieben. Es wird dabei zwischen interner Authentisierung, bei der sich die Chipkarte gegenüber der externen Einheit authentisiert und externer Authentisierung, bei der sich die externe Einheit gegenüber der Chipkarte authentisiert unterschieden. Die gegenseitige Authentisierung ist in Vorbereitung.

Neben diversen Befehlen zum Lesen, Schreiben und Löschen (jeweils nach der Authentisierung) von Files sowie zur Auswahl von zu bearbeitenden Files definiert ISO 7816-4 einige Kommandos, die für die lmplementation von Sicherheitsfunktionalitäten bedeutsam sind:

- VERIFY zur Benutzerauthentisierung mit einer PIN. Dies kann eine auf MF-Ebene gespeicherte globale PIN oder eine DF-spezifische anwendungsbezogene PIN sein. Der Befehl überträgt die vom Nutzer eingegebene PIN und - falls erforderlich - die Nummer der zu überprüfenden PIN an die Karte. Diese vergleicht die eingegebene PIN mit dem gespeicherten Referenzwert. Ein Erfolg wird durch Senden des Status „OK“ angezeigt, ansonsten ein interner Fehlversuchszähler dekrementiert und als Status „nicht OK“ übertragen. Bei Zählerstand 0 wird die Anwendung der Applikation, die die PIN benutzt, blockiert. Bei einigen Betriebssystemen kann die Blockierung durch Eingabe eines Personal Unblocking Key (PUK) aufgehoben werden, der ebenfalls durch einen Fehlerzähler geschützt ist.
- INTERNAL AUTHENTICATE löst eine interne Authentisierung aus. Dazu erhält die Chipkarte den Schlüsselbezeichner des ausgewählten EF und Authentisierungsdaten (Zufallszahl). Die Chipkarte verschlüsselt dann die Zufallszahlen mit dem Schlüssel des ausgewählten EF und sendet das Chiffrat zurück. Die prüfende Einheit (z. B. das CDLS oder eine Patientenkarte) entschlüsselt und prüft die Übereinstimmung der Zufallszahlen.
- EXTERNAL AUTHENTICATE löst die externe Authentisierung aus. Dazu wird mit dem Befehl GET CHALLENGE eine Zufallszahl von der Chipkarte gefordert, die an die zu authentisierende Instanz übergeben wird. Diese verschlüsselt sie und sendet das Ergebnis zusammen mit der Nummer des zu verwendenden Schlüssels an die Karte zurück. Dann entschlüsselt die Karte die Zufallszahl mit dem Schlüssel der angegebenen Schlüsselnummer. Bei Übereinstimmung wird die zu authentisierende Instanz als authentisch anerkannt.

Weitere Sicherheitsfunktionen sind derzeit in ISO 7816-8 spezifiziert. Von besonderer Bedeutung ist hierbei das Kommando PERFORM SECURITY OPERATION, mit dem folgende Sicherheitsoperationen ausgeführt werden können:

- COMPUTE DIGITAL SIGNATURE
- VERIFY DIGITAL SIGNATURE
- VERIFY CERTIFICATE
- HASH
- COMPUTE CRYPTOGRAPHIC CHECKSUM
- VERIFY CRYPTOGRAPHIC CHECKSUM

– ENCIPHER
– DECIPHER.

In ISO 7816-7 sind außerdem spezielle Sicherheitsfunktionen beschrieben, die sich auf Chipkarten mit einer sog. SCQL-Datenbank (Structured Card Query Language) beziehen.

III.3 Chipkartenbasierte Dienstleistungssysteme (CDLS)

Wie in der Einleitung kurz dargestellt, sind Chipkarten nicht als isolierte Träger von Risiken zu betrachten, wenn es um Fragen ihrer IT-Sicherheit geht. Aufwendige sicherheitstechnische Maßnahmen an und in der Chipkarte können durch unsichere Systemumgebungen bei der weiteren Verwendung der Daten konterkariert werden.

Wenn zum Beispiel das System eines zugriffsberechtigten Arztes nicht den erforderlichen Schutz bietet, können die Schutzmaßnahmen der Karte umgangen werden. Der Schutz der Chipkarte gegen unbefugte Manipulationen ist weitgehend wertlos, wenn beim elektronischen Zahlungsverkehr das POS-Terminal leicht manipuliert werden kann. Jedoch sieht ISO/IEC 7816 Schutzmechanismen vor, die bei richtiger Anwendung mit vertretbarem Aufwand nicht umgangen werden können.

Hier sollen jedoch nur für solche Komponenten Sicherheitsbetrachtungen angestellt werden, die chipkartenspezifisch sind. Solange die Chipkarten keine eigenen Mensch-Maschine-Schnittstellen enthalten, sind für die Erschließung der Chipkarteninhalte und -funktionen Systeme notwendig, mit denen die Chipkarten gelesen und beschrieben werden können. Auch wenn es einmal möglich sein wird, direkt mit der Chipkarte zu kommunizieren, z. B. über Sensorfelder, werden CDLS kaum entbehrlich sein, denn sie stellen zumindest die Schnittstelle zu jenen Nutzern dar, die mit dem Inhaber der Karte nicht identisch sind. CDLS können eigene Verarbeitungskapazitäten bieten und auch die Verbindung zu anderen Systemteilen herstellen.

Bisher sind für alle Chipkarten-Anwendungen (Telefonkarten, Krankenversicherungskarten, Sicherungskarten für Mobiltelefone usw.) spezielle CDLS entwickelt und eingesetzt worden. Soweit erkennbar werden universell einsetzbare CDLS bisher nicht auf dem Markt angeboten. Im Gesundheitswesen werden derzeit CDLS eingesetzt, deren Verwendung auf die Kommunikation mit der Krankenversichertenkarte eingeschränkt wurde. Da sich weitergehende Anwendungen abzeichnen, wurde eine Spezifikation für multifunktionale CDLS angefertigt, die von einem Arbeitskreis der Arbeitsgemeinschaft „Karten im Gesundheitswesen“ und der Gesellschaft für Mathematik und Datenverarbeitung (GMD) herausgegeben worden ist.

Dieser Spezifikation liegt folgende Konzeption zugrunde:

– Die CDLS sind transparent für jeden Dialog zwischen einem Anwendungsprogramm und einer Chipkarte, sofern dieser Dialog über eine genormte Schnittstelle geführt wird. Damit ist ihre Anwendung außerhalb des Gesundheitswesens *möglich.*
– Allerdings ist die Option, ein universell einsetzbares CDLS zu schaffen, aus pragmatischen Erwägungen heraus relativiert worden. Von den nach ISO 7816-3 zulässigen Optionen für die Übertragungsparameter wird nur ein Teil als obligatorisch gefordert. Dies entspricht der Politik des Kreditkartensektors, die zulässigen Lösungen enger zu fassen als das Spektrum der Optionen. Der Spezifikation entsprechende CDLS können sowohl mit synchronen Chipkarten wie die Krankenversicherungskarte als

auch mit Prozessorchipkarten kommunizieren, die ein standardisiertes Übertragungsprotokoll unterstützen.
- Es können anwendungsspezifische Funktionen im CDLS realisiert werden, die dann nicht dem Anwendungsprogramm überlassen werden, solange nicht andere Vorkehrungen zum Schutz der Karte vor unbefugten oder durch Fehlfunktionen ausgelösten schreibenden Zugriffen getroffen sind. So ist z. B. ein Modul zur Verarbeitung der Versichertenkarte gem. § 291 SGB V für Gesundheitskarten-Terminal spezifiziert worden.
- Es können je nach Anwendung weitere anwendungsspezifische Module definiert werden, die periphere Geräte steuern. So wurde für die Gesundheitschipkarten ein Modul definiert, das einen Drucker steuert, damit Ärzte ohne IT-Einsatz die Kartensysteme zumindest für die Übertragung des Inhalts der Versichertenkarte auf die Belege der vertragsärztlichen Versorgung nutzen können. Das Druckmodul mit der parallelen Schnittstelle ist optional zu realisieren.
- Eine Download-Funktion erlaubt die Behebung von Softwarefehlern und ggf. im gewissen Umfang eine Upgrade von Leistungen.
- Die Spezifikation gilt für kontaktbehaftete Chipkarten nach ISO 7816 in 5-Volt-Technologie. Kontaktlose Chipkarten und kontaktbehaftete Chipkarten in 3-Volt-Technologie sollen einbezogen werden, wenn die Normung Klarheit geschaffen hat. Das gleiche gilt für eine Erweiterung von Standards für die Nutzung der Kontakte und für höhere als derzeit spezifizierte Übertragungsraten.
- Das Anwendungssystem in einem PC wird auf eine anwendungsunabhängige Schnittstelle für die Integration der Chipkartentechnik aufgesetzt.
- CDLS als separate Endgeräte können zusätzlich mit folgenden Optionen ausgestattet sein:
  * Display und/oder Tastatur,
  * mehrere Kontaktiereinheiten für eine Chipkarte im Normalformat gem. ISO-IEC 7816-2 oder im Plug-in-Format.

IV. Sicherheitstechnische Gestaltungsspielräume

Für die Entwicklung sicherer Chipkartenanwendungen gibt es eine Vielzahl von Ansatzpunkten, die je nach den in einer anwendungsspezifischen Sicherheitspolitik definierten Anforderungen zur Verbesserung der Sicherheit mit gewissen Spielräumen ausgenutzt werden können. In diesem abschließenden Kapitel geht es einerseits darum, diese sicherheitstechnischen Gestaltungsspielräume darzustellen und andererseits die Empfehlungen der Datenschutzbeauftragten zur Ausschöpfung dieser Spielräume hervorzuheben.

IV.l. Allgemeine Anforderungen

Wie bereits einleitend dargestellt sind Chipkarten als miniaturisierte Computer anzusehen, die (noch) nicht über eigene Mensch-Maschine-Schnittstellen verfügen. Daraus ergeben sich folgende Konsequenzen:

- Chipkarten sind leicht transportable Rechner. Die besonderen Bedrohungen der IT-Sicherheit, die z. B. bei anderen transportablen Rechnern (Laptops, Notebooks,...) berücksichtigten werden müssen, existieren in ähnlicher Weise auch für Chipkarten.
- Die Interaktion zwischen Mensch und Chipkarte bedarf zwischengeschalteter technischer Systeme (CDLS), die ebenfalls besonders zu sichern sind. Eine Chipkarte bildet zusammen mit dem CDLS ein vollständiges Rechnersystem mit Ein- und Ausgabekomponente. Die Evaluation der richtigen Funktionsweise setzt voraus, daß dabei alle Systemkomponenten einbezogen sind.

– Speicher- und Prozessorkapazitäten bilden Schranken für Sicherheitsfunktionen. Die technische Entwicklung dürfte diese Engpässe bald beseitigen. Heutige Betrachtungen müssen sie jedoch noch berücksichtigen.

Allgemein sind an die Sicherheitsfunktionen folgende Anforderungen zu stellen:

– Zugriffs- und Nutzungsberechtigungen sollten soweit möglich von der Chipkarte selbst geprüft und gesteuert werden.
– In Anwendungen sollten sich alle beteiligten Rechner (incl. Chipkarten) gegenseitig authentifizieren. Die Authentifizierung des Benutzers hat gegenüber der Chipkarte zu erfolgen, wobei für die Zukunft angestrebt werden sollte, daß dies in sicherer Umgebung oder ohne zwischengeschaltete Systeme erfolgen kann. Dies würde eine autonome Stromversorgung der Chipkarte und geeignete Mensch-Maschine-Schnittstellen voraussetzen (z. B. Sensorfelder für biometrische Merkmale).
– Es muß grundsätzlich ein Mindestschutz vorhanden sein, mit dem die in § 202a Abs. 1 StGB geforderte „besondere Sicherung gegen unberechtigten Zugang“ realisiert wird, um bei unbefugter Nutzung einer Chipkarte das Strafrecht anwendbar zu machen.

IV.2. Hardwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.2.1 Herstellung, Initialisierung und Versand von Chipkarten

Sicherheitserwägungen greifen bereits bei der Herstellung, Initialisierung und dem Versand von Chipkarten. Dabei müssen

– die Produktion der Prozessoren und Chipkarten,
– die Produktion und das Laden von Software,
– das Erzeugen der Schlüssel,
– das Laden der Schlüssel in die Sicherheitsmodule (Internal Elemetary Files),
– das Laden von Hersteller- und Transportschlüssel für die spätere Initialisierung und
– der Versand der Chipkarten und Transportschlüssel an den Empfänger

durch entsprechende technische und organisatorische Maßnahmen abgesichert werden.

IV.2.2 Sicherheitsmerkmale des Kartenkörpers

Zur Unterstützung der Authentifizierung des Karteninhabers gegenüber der Chipkarte und damit des Nachweises, daß die Chipkarte

– zur jeweiligen Anwendung gehört und
– die die Karte vorlegende Person die Karte rechtmäßig nutzt,

sollte der Kartenkörper mit Sicherheitsmerkmalen ausgestattet sein**,** die der Sensibilität angemessen sind:

– Aufdruck
– Hologramm
– Unterschrift des Besitzers (nur bei nicht anonymen Anwendungen)
– Foto des Besitzers (nur bei nicht anonymen Anwendungen)
– aufgebrachtes Echtheitsmerkmal
– Multiple Laser Image (durch Lasergravur auf der Chipkarte aufgebrachte hologrammähnliches Kippbild mit kartenindividuellen Informationen).

Dabei ist allerdings zu berücksichtigen, daß es Sicherheitsmerkmale gibt, die z. B. bei anonymen Chipkartenanwendungen (z. B. anonyme Zahlungsverfahren) die Anonymität aufheben würden und daher dabei nicht verwendet werden können

IV.2.3 Sicherheitsmechanismen der Chip-Hardware

Sicherheitsmechanismen der Chip-Hardware richten sich vor allem gegen die Analyse der Chip-Inhalte und -Sicherheitssysteme mit Hilfe von Spezialgeräten, z. B. durch Abtragen dünner Chipschichten. Dabei kann unterschieden werden zwischen passiven Mechanismen, bei denen eine bestimmte Bauweise des Chips die Schutzfunktionen ergibt, und aktiven Mechanismen, die auf äußere Eingriffe passend reagieren und ggf. den Chip zerstören.

Passive Mechanismen:

- Es gibt von außen keine direkte Verbindung zu den Funktionseinheiten. Ein Testmodus, der eventuell später nicht mehr erlaubte Zugriffe auf den Speicher ermöglicht, muß irreversibel auf den Benutzermodus geschaltet werden können.
- Interne Busse werden nicht nach außen geführt.
- Der Datenfluß auf den Bussen wird mit Scrambling geschützt.
- Der ROM befindet sich in den unteren Halbleiterschichten, um eine optische Analyse zu verhindern.
- Gegen das Abtasten von Ladungspotentialen erfolgt eine Metallisierung des gesamten Chips.
- Die Chipnummern werden eindeutig vergeben (werden u. U. von den Anwendungen benötigt).

Aktive Mechanismen:

- Es wird eine Passivierungsschicht aufgebracht, deren Entfernen einen Interrupt auslöst, der die Ausführung der Software unterbindet, sowie Schlüssel und andere sicherheitsrelevante Daten löscht.
- Es erfolgt eine Spannungsüberwachung. Wenn der Spannungswert den zulässigen Bereich über- oder unterschreitet, wird die weitere Ausführung von Prozessorbefehlen unterbunden.
- Den gleichen Zweck verfolgt die Taktüberwachung. Es werden damit Angriffe erschwert, mit denen die Abarbeitung einzelner Befehle analysiert werden soll.
- Es erfolgt eine Power-On-Erkennung, um bei Reset einen definierten Zustand herzustellen.

IV.3. Softwarebezogene Maßnahmen zur IT-Sicherheit bei Chipkarten

IV.3.1 Basisalgorithmen für Schutzfunktionen der Software

Die Schutzfunktionen der Chipkarten-Software basieren auf den bekannten und teilweise standardisierten Algorithmen zur Verschlüsselung, Signatur und Generierung von Zufallszahlen.

Dazu gehören symmetrische Verschlüsselungsalgorithmen wie DES, Triple-DES, IDEA und SC85 und asymmetrische Verfahren wie RSA, Signieralgorithmen wie DSS und RSA mit MD160, Einwegfunktionen zur Berechnung des MAC und für das Hashing wie SHA und MD16+0 sowie Zufallszahlengeneratoren.

IV.3.2 Schutzfunktionalitäten und -mechanismen des Betriebssystems

Zunächst sollte sichergestellt sein, daß sich nicht alle Teile des Betriebssystems im ROM befinden, damit der Chiphersteller nicht über das ganze Wissen über die Sicherung der Chipkarte verfügt. Wesentliche Teile des Betriebssystems können bei der späteren Initialisierung über entsprechend authentisierte CDLS dynamisch aus Tabellen geladen werden.

Darüber hinaus sollte das Betriebssystem in folgender Weise Sicherheit „erzeugen“:

a) Die Identifizierung und Authentifizierung des Benutzers erfolgt mittels PIN oder mit biometrischen Verfahren.
   Üblicherweise erfolgt die Prüfung einer PIN. Zwar können die normale Forderungen zur Paßwortverwaltung bei Rechnern nicht voll auf Chipkarten übertragen werden, jedoch sollte die PIN-Länge je nach Sensibilität mindestens 4 oder mehr Stellen betragen, die Anzahl der Fehlversuche begrenzt sein, die Möglichkeit bestehen, die PIN zu ändern und eine Freischaltung der Karte auch mittels Personal Unblocking Key (PUK) in Abhängigkeit von der Anwendung ermöglicht werden.
   Biometrische Verfahren erfassen Fingerabdrücke, Augenhintergründe, Handgeometrien, Sprachmerkmale oder Unterschriftsdynamiken, verformeln sie und übertragen das Ergebnis zur Überprüfung auf die Chipkarte.
b) Es erfolgt eine Zugriffskontrolle mit einer Rechteverwaltung, wobei die Zugriffsrechte an die einzelnen Dateien geknüpft werden. Den Dateien sind Sicherheitsattribute zugeordnet, mit denen festgelegt wird, ob die Dateien (Daten) gelesen, kopiert, beschrieben, gelöscht, gesperrt oder freigegeben werden dürfen.
c) Wenn anderen Personen als dem Karteninhaber Zugriffsmöglichkeiten auf die Chipkarte gewährt werden sollen, erfolgt dies im Rahmen einer Programm-Programm-Kommunikation mit einem anderen Rechner oder einer anderen Karte (z. B. mit einer Professional Card). Der Rechner bzw. die andere Karte muß authentifiziert werden.
   Die Rechnerauthentifizierung wird meist nach einem auf DES basierenden Challenge-Response-Verfahren vorgenommen.
   Nach dem gleichen Schema verläuft die gegenseitige Authentifizierung von Chipkarte und Professional Card. Beide Benutzer müssen ihre Chipkarte aktivieren. Dann erfolgt die Authentifizierung zwischen den beiden Karten, wobei das KT die Daten transparent weiterleitet.
d) Zum Schutz gegen Ausforschung und Manipulation erfolgt eine sichere Datenübertragung zwischen Chipkarte und CDLS („Secure Messaging“).
e) Auf Opto-Hybridkarten können die Daten auf der optischen Fläche verschlüsselt abgelegt werden. Die Entschlüsselung kann mit Hilfe des Prozessors erfolgen, der die Schlüssel verwaltet.
f) Das Betriebssystem führt eine I/O-Kontrolle aller Schnittstellen gegen unerlaubte Zugriffe durch.
g) Die Interferenzfreiheit der einzelnen Anwendungen wird gewährleistet, d.h. eine gegenseitige unerwünschte Beeinflussung der Anwendungen wird ausgeschlossen.
h) Trace- und Debugfunktionen sind nicht verfügbar.
i) Beim Initialisieren des Betriebssystems werden RAM und EEPROM geprüft.
i) Fehleingaben werden abgefangen.
k) Der Befehlsumfang wird auf die notwendigen Befehle reduziert. Funktionalitäten, die nicht zugelassen werden sollen, werden vom Betriebssystem unterbunden.

l) Die Dateiorganisation, Header und Speicherbereiche im EEPROM werden durch Prüfsummen abgesichert.
m) Das Betriebssystem sieht die Möglichkeit vor, die Chipkarte durch Löschung zu deaktivieren (etwa nach Ablauf einer Gültigkeitsdauer), jedoch verhindert es die mißbräuchliche Deaktivierung.

IV.3.3 Die Sicherheit der Anwendung

Die Betrachtung der Sicherheit bei der Anwendung von Chipkarten setzt die ganzheitliche Betrachtung der Kommunikation zwischen Chipkarten, CDLS und im Hintergrund wirkenden Systemen voraus. Die Kommunikation zwischen den einzelnen Systemen und Systembestandteilen ist ebenfalls mit kryptographischen Methoden zu sichern:

- Zur Unterstützung der Sicherheit der Kommunikation dienen Funktionen des Chipkarten-Betriebssystems zur gegenseitigem Authentifizierung von Chipkarten und Rechnern, zur sicheren Datenübertragung und zum Signieren und Verschlüsseln (siehe IV.3.2. c), d)).
- Gegen die unberechtigte Nutzung der Daten auf der Chipkarte muß eine Zugriffskontrolle erfolgen, die auf einer sicheren Identifikation und Authentifizierung der Benutzer beruht (siehe IV.3.2 a), b)).

Darüber hinaus sind die folgenden für die Sicherheit der Anwendung bedeutsamen Maßnahmen zu berücksichtigen:

- Den Dateien auf der Chipkarte sind Befehle zuzuordnen, die mit ihnen ausgeführt werden können. Die Ausführung anderer Befehle ist zu unterbinden.
- Zugriffe auf geschützte Datenbereiche und Veränderungen der Daten sollten protokolliert werden - vorzugsweise auf der Chipkarte. Die Anwendung muß die Auswertung der Protokolldaten unterstützen.
- Bedarfsweise sollten Überprüfungen durch Abgleich mit Hintergrundsystemen erfolgen, z. B. die Erkennung gesperrter Karten durch Abgleich mit Sperrdateien, Feststellung von Betragslimits im chipkartengestützten Zahlungsverkehr.
- Die eindeutige Nummer des Chips schützt vor der Erstellung von Dubletten.

Bei den letzten beiden Spiegelstrichen muß allerdings berücksichtigt werden, daß mit solchen Maßnahmen bei anonymen Systemen unter Umständen die Anonymität gefährdet sein kann. Es kann nicht immer ausgeschlossen werden, daß anonyme Chipkarten einzelnen Nutzern zugeordnet werden, wenn die Identifizierung der Karte möglich ist.

IV.4. Risiken und Anforderungen bei Chipkartenbasierten Dienstleistungssystemen (CDLS)

Zwar bilden - wie oben festgestellt - Chipkarten und CDLS erst zusammen ein vollwertiges, Rechensystem, jedoch befinden sich beide Komponenten in der Regel in unterschiedlicher Verfügungsgewalt, die Karte in der des Inhabers und das CDLS in der von Anwendern. Denkbar ist auch, daß bei Inhabern und Anwendern unterschiedliche Vorstellungen und Interessen mit der Nutzung verbunden werden. Wesentliche Teile der unabdingbaren Sicherheitsmechanismen der Karte können daher konterkariert werden, indem die Steuerungssoftware des CDLS verändert oder die Hardware des CDLS manipuliert wird. Eine Zertifizierung von CDLS kann sich daher nur auf unveränderliche Teile beziehen.

Wenn eine Chipkarte in ein CDLS eingeführt wird, gibt der Inhaber die Verfügungsgewalt über die Software auf der Karte und die ihn betreffenden Datenbestände auf. Eine unbefugte Veränderung der Software muß daher technisch verhindert werden.

Allerdings sind die Datenbestände grundsätzlich variabel. Sie können daher benutzt werden, über das CDLS Daten abzulegen, die für den Karteninhaber verdeckt sind und nur mit bestimmten Codes gelesen werden können (verdeckte Kanäle). Dies eröffnet Möglichkeiten für unbefugtes oder gar kriminelles Handeln.

Der Karteninhaber sollte daher nicht nur die Möglichkeit haben, sich den Inhalt der gespeicherten Daten anzeigen zu lassen, sondern die tatsächlichen Funktionen z. B. auf neutralen CDLS testen zu können. Wegen der u. U. unterschiedlichen Interessenlagen (z. B. in wirtschaftlichen Beziehungen) ist die Prüfung der korrekten Funktion der Software sowie umgekehrt des Ausschlusses ungewollter Funktionen im realisierbaren Rahmen zu ermöglichen.

Manipulationen an der Hardware und der Eingabesteuerungssoftware der CDLS können auch dazu führen, daß die geheimen oder unverfälschbaren Authentifizierungsmerkmale (PIN, biometrische Merkmale), die bei der Authentifizierung des Kartenbesitzers in das CDLS übertragen werden und so Dritten bekannt werden.

Es sind daher folgende Sicherheitsanforderungen an CDLS zu stellen:

- Die CDLS müssen über mechanisch gesicherte Gehäuse verfügen, damit eine Hardware-Manipulation verhindert oder erschwert bzw. erkennbar wird.
- Sicherheitsmodule, die die für die vertrauliche Kommunikation mit Chipkarten und die gegenseitigen Authentifizierungen erforderlichen Hauptschlüssel enthalten, sind mechanisch (zum Beispiel durch Vergießung in Epoxidharz) und elektrisch gegen vielfältige Angriffsformen besonders abzusichern. Jeder Angriff auf das Sicherheitsmodul muß zum Löschen aller Schlüssel im Sicherheitsmodul führen. Dies setzt auch voraus, daß das Sicherheitsmodul weitgehend von der Stromversorgung des CDLS autark sein muß.
- Die CDLS müssen alle automatisch prüfbaren Sicherheitsmerkmale des Kartenkörpers prüfen können, müssen demzufolge also über die entsprechenden Sensoren verfügen (siehe IV.2.2).
- Sofern die Kommunikation zwischen Chipkarte und CDLS nicht durch kryptographische Verfahren gegen Abhören und Manipulation gesichert wird, ist das Abhören der Kommunikation durch mechanische Maßnahmen (sog. Shutter zum Abschneiden aller manipulativ mit der Karte in das CDLS eingebrachten Drähte) zu verhindern.

Als besonders angriffsgefährdet sind CDLS vom Typ „PC mit Kartenterminal“ anzusehen, sofern sie nicht in manipulationsgeschützten Umgebungen eingesetzt werden. Erhöhte Schutzfunktionen werden hier als notwendig angesehen. Die bisherigen Spezifikationen für die CDLS lassen nicht erkennen, daß Maßnahmen gegen Penetrationsversuche aus der IT-Umgebung der Chipkartenanwendung im CDLS ergriffen werden können. Es fehlt daher an einem schlüssigen Sicherheitskonzept für das Zusammenspiel zwischen dem Betriebssystem und den Applikationen der (übergeordneten) IT-Umgebung und dem Betriebssystem und den Applikationen des Systems Chipkarte/CDLS.

Anlage 22

Entschließung
der Europäischen Konferenz der Datenschutzbeauftragten

zum

Entwurf einer Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen
vom 19.09.1997
- Übersetzung -

Die Europäischen Datenschutzbeauftragten haben bei ihrer Konferenz in Brüssel am 19. September 1997 den gegenwärtigen Stand des Vermittlungsverfahrens zum Entwurf einer Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen erörtert.

Die Datenschutzbeauftragten stellen mit Besorgnis fest, daß das Vermittlungsverfahren aufgrund von Kontroversen hinsichtlich gewisser Detailfragen (z. B. Fernmeldegeheimnis; Schutz juristischer Personen; kostenloser Nichteintrag in öffentlichen Teilnehmerverzeichnissen) noch immer nicht abgeschlossen worden ist.

Die Europäischen Datenschutzbeauftragten vertreten mit Nachdruck die Auffassung, daß die Annahme des Richtlinienentwurfs eine notwendige bereichsspezifische Maßnahme für den Datenschutz im Binnenmarkt ist. Mit der vollen Liberalisierung des Telekommunikationsmarktes im Januar 1998 ist ein spezieller Mindeststandard des Datenschutzes in diesem Bereich von entscheidender Bedeutung.

Nach Auffassung der Datenschutzbeauftragten ist die Vertraulichkeit von Daten, die aus der Kommunikation stammen, für den Schutz der Privatsphäre wesentlich, wie dies im Gemeinsamen Standpunkt mit den Änderungen des Europäischen Parlaments zum Ausdruck gekommen ist.

Es ist in höchstem Maße wünschenswert, daß die Richtlinie unter Berücksichtigung dieser Gesichtspunkte in naher Zukunft verabschiedet wird, da die Umsetzungsfrist im Oktober 1998 abläuft. Jede weitere Verzögerung würde die Möglichkeiten einer rechtzeitigen Umsetzung in das Recht der Mitgliedstaaten reduzieren.

Erklärung der Europäischen Konferenz gegenüber dem Vorsitzenden des Ministerrats für Justiz und Innere Angelegenheiten

zu

EUROPOL

Die Europäische Datenschutzkonferenz in Manchester am 24./25. April 1996 erörterte die EUROPOL-Konvention.

Bei verschiedenen Gelegenheiten in vergangenen Jahren haben die Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union die Notwendigkeit betont, ein zusammenhängendes System von Datenschutzregelungen in die EUROPOL-Konvention einzufügen. In einer gemeinsamen Erklärung vom April 1995 haben die Datenschutzbeauftragten ihre Auffassung zum Konventionsentwurf dargelegt, insbesondere hinsichtlich der Rechte des Betroffenen.

Die Datenschutzbeauftragten haben mit Befriedigung festgestellt, daß die Konvention dem Datenschutz erhebliche Bedeutung beimißt. Sie haben auch festgestellt, daß Artikel 24 eine gemeinsame Kontrollinstanz vorsieht, die aus Vertretern der nationalen Kontrollinstanzen bestehen soll.

Vertreter der Datenschutzbeauftragten haben auf der Basis des Ministerübereinkommens von Kopenhagen, erweitert durch die Mitgliedstaaten im März 1995, die EUROPOL-Drogeneinheit (EDU) mehrfach aufgesucht, um sich über die Aktivitäten ihrer nationalen Verbindungsbeamten bei EDU/EUROPOL zu informieren.

Die Datenschutzbeauftragten sind überzeugt, daß der Zeitraum zwischen der gegenwärtigen EUROPOL-Drogeneinheit auf der Grundlage des Ministerübereinkommens von Kopenhagen in der erweiterten Fassung und EUROPOL auf der Grundlage der Konvention von erheblicher Bedeutung für die praktische Umsetzung des Datenschutzstandards der EUROPOL-Konvention sein wird.

In diesem Zeitraum - bevor die Konvention in Kraft tritt - wird ein EUROPOL-Informationssystem entwickelt werden, und Entscheidungen übe die Informationsarchitektur von EUROPOL und die Regeln für die Verarbeitung von Analysedateien werden getroffen. Diese Entscheidungen werden von wesentlicher Bedeutung für die praktische Anwendung der Konvention sein. Deshalb betonen die Datenschutzbeauftragten die Notwendigkeit, die gemeinsame Kontrollinstanz nach Artikel 24 der Konvention möglichst frühzeitig einzurichten. Es sollte dringend geprüft werden, ob eine vorläufige gemeinsame Kontrollinstanz eingerichtet werden kann, die das Inkrafttreten der Konvention vorbereiten sollte und zur Entwicklung des EUROPOL-Informationssystems beitragen könnte.

In der Zwischenzeit würden die Datenschutzbeauftragten eine rechtzeitige Information über die Entwicklung des EUROPOL-Informationssystems begrüßen, insbesondere über die Erfordernisse und funktionalen Spezifikationen des zu entwickelnden Systems, so daß sie bereits vorab feststellen können, ob Datenschutzgrundsätze in bezug auf die EUROPOL-Konvention angemessen berücksichtigt werden.

Sie würden es außerdem begrüßen, wenn sie bei der Beratung von Fragen der praktischen Umsetzung der Datenschutzprinzipien im Zusammenhang mit

der Entwicklung des EUROPOL-Informationssystems beteiligt würden. Zu diesem Zweck steht die Arbeitsgruppe Polizei der Datenschutzbeauftragten zur Verfügung und ist bereit, Vertreter zu Diskussionen mit dem Projektausschuß und dem Projektteam zu entsenden.

Anlage 24

Erklärung der Europäischen Konferenz vom 24./25. April 1996

zum

Geänderten Vorschlag für eine ISDN-Richtlinie

Die Europäische Konferenz der Datenschutzbeauftragten in Manchester am 24./25. April 1996 stellt mit Befriedigung fest, daß die Ratsarbeitsgruppe ihre Beratung des geänderten Vorschlags für eine ISDN-Richtlinie (KOM (94) 128 endg.-COD 288) abgeschlossen hat. Die Europäischen Datenschutzbeauftragten stellen außerdem fest, daß die gegenwärtige Fassung des Entwurfs den Datenschutz berücksichtigt. Dennoch sind einige grundlegende Datenschutzbestimmungen, die die europäischen Datenschutzbeauftragten in ihren beiden gemeinsamen Stellungnahmen vom Dezember 1994 und 1995 vorgeschlagen hatten, nicht angenommen worden. In der weiteren Beratung sollten auch andere Verbesserungen geprüft werden, insbesondere sollte der Zweckbindungsgrundsatz ausdrücklich in der Richtlinie erwähnt werden.

Stellungnahme der Europäischen Datenschutzbeauftragten vom Dezember 1996

zum

Grünbuch der Europäischen Kommission „Leben und Arbeiten in der Informationsgesellschaft - Im Vordergrund der Mensch“ (KOM (96) 389)

- Übersetzung -

Es besteht ein rechtlicher Rahmen hinsichtlich des Datenschutzes, der die Grundrechte der Einzelnen schützen soll. Dieser Rahmen ist insbesondere in der Europäischen Datenschutzrichtlinie (95/46/EG), dem Gemeinsamen Standpunkt zum Entwurf der Richtlinie zum Datenschutz im Telekommunikationsbereich und in der Datenschutzkonvention des Europarats Nr. 108 von 1981 zu sehen. In diesem Zusammenhang bekunden die Europäischen Datenschutzbeauftragten ein besonderes Interesse an diesem Grünbuch, das auf der Tatsache beruht, daß die entstehende Informationsgesellschaft neue Herausforderungen für Datenschutzbeauftragte mit sich bringt. Auch im Bangemann-Bericht wurde festgestellt, daß „die Anforderungen an den Datenschutz in dem Maße zunehmen werden, wie das Potential der neuen Technologien, detaillierte Informationen über Privatpersonen aus Daten, Sprache und Bildquellen zu gewinnen und zu manipulieren, genutzt wird.“ Wenngleich wir die Entwicklung neuer Technologien, die das Sammeln und Übermitteln von Informationen erleichtern, in vollem Umfang unterstützen, wollen wir auf die Konsequenzen für den Datenschutz aufmerksam machen, die der Einsatz dieser Technologien in der Informationsgesellschaft haben wird.

Da sich das Grünbuch auf eine Verbesserung des Lebensstandards der Bürger konzentriert, hätten wir Hinweise auf die Risiken erwartet, die die Informationsgesellschaft bezüglich des Datenschutzes und des Umgangs mit personenbezogenen Daten mit sich bringt. Das Dokument erwähnt zu Recht das Problem der Gewährleistung gleichen Zugangs zu Online-Diensten. Die Verbreitung rassistischen und pornographischen Materials im Internet wird ebenso als negative Aspekte der Informationsgesellschaft erörtert. Es gibt andere Risiken, die bekannt werden sollten, damit Grundrechte und - freiheiten der Bürger wie auch die Rechte der Nutzer und Verbraucher in der Informationsgesellschaft geschützt werden können.

Elektronische Verwaltung

Die Initiative für eine elektronische Verwaltung (Electronic Government) hat einige wirkliche Vorteile für den Einzelnen. Wir begrüßen die Tatsache, daß öffentliche Dienstleistungen 24 Stunden am Tag zur Verfügung stehen und daß es eine Möglichkeit gibt, um sich anonym an die Verwaltung zu wenden. Zugang zu Informationen ohne Identifizierung kann durch den Einsatz datenschutzfreundlicher Technologien wie Verschlüsselung, Pseudonyme oder digitale Unterschriften erreicht werden.

Datenschutzprobleme entstehen, wenn die Inanspruchnahme der elektronischen Verwaltung durch den Einzelnen registriert und gespeichert werden soll. Die Person, die Daten über sich offenbart, sollte über die Zwecke informiert werden, zu denen ihre Daten erhoben und weiterverwendet werden sollen.

Internet

Es wäre hilfreich, die in hohem Maße unsichere Struktur des Internet zu berücksichtigen. Bürger sollten über die Risiken informiert werden, die bei der Offenbarung persönlicher oder vertraulicher Daten entstehen, und über die Tatsache, daß Details des Nutzungsverhaltens von Diensteanbietern gespeichert werden können. Wir hätten einige Anmerkungen zu der Notwendigkeit erwartet, das Bewußtsein für Datenschutzüberlegungen in diesem Bereich zu erhöhen.

Arbeit

Wir halten eine Erwähnung der Datenschutzprobleme bei der Telearbeit (Heimarbeit) für wünschenswert. Es sollte betont werden, daß Daten aus dem persönlichen Bereich und Daten, die sich auf das Arbeitsverhältnis beziehen, getrennt gespeichert werden müssen und daß weder der Arbeitgeber Zugang zu den persönlichen Daten des Arbeitnehmers noch dessen Familie Zugang zu Daten aus dem Beschäftigungsverhältnis haben dürfen.

Neue Technologien haben Auswirkungen am Arbeitsplatz. Die Entwicklung der Anwendung von Multimedia-Arbeitsräumen nimmt einen Kulturwandel vorweg. Sind die Bürger der Europäischen Union innerlich auf einen solchen Wandel vorbereitet, oder sind sie sich überhaupt der Entwicklungen bewußt? Können Techniken entwickelt werden, um sicherzustellen, daß Systeme in einer Weise eingesetzt werden, die die natürlichen sozialen Verhaltensregeln widerspiegeln, durch die die Privatsphäre am Arbeitsplatz gegenwärtig geschützt wird?

Neue Technologien im Einzelhandel

Neue Technologien im Einzelhandel wie Supermarkt-Kundenkartensysteme ermöglichen die Erhebung von personenbezogenen Daten, die Erzeugung von Profilen des Einzelnen und die Nutzung dieser Daten für Zwecke der Direktwerbung. Der Einsatz dieser neuen Technologien darf nicht zu einer Situation führen, in der der Kunde die Zwecke nicht kennt, zu denen seine personenbezogenen Daten erhoben und weiterverwendet werden.

Zusätzlich zu diesen Anmerkungen ist es vielleicht nützlich, den Umstand zur Kenntnis zu nehmen, daß eine große Anzahl von Unionsbürgern nicht auf die Informationsgesellschaft vorbereitet oder über sie informiert sind und deshalb möglicherweise nicht erkennen, wie ihre personenbezogenen Daten in Zukunft behandelt werden können. Es sollte deshalb betont werden, daß alle Erziehungsprogramme oder Aktionspläne, die die Europäische Kommission bezüglich der Informationsgesellschaft beschließt, Informationen über die jeweiligen Datenschutzprobleme enthalten sollte.

Bericht und Empfehlungen der Internationalen Arbeitsgruppe vom 19. November 1996

zu

Datenschutz und Privatsphäre im Internet (Budapest-Berlin Memorandum)

- Übersetzung -

Zusammenfassung

Es steht außer Zweifel, daß der gesetzliche und technische Datenschutz von Benutzern des Internet gegenwärtig unzureichend ist.

In diesem Dokument werden zehn Prinzipien zur Verbesserung des Datenschutzes im Internet beschrieben:

1. Die Diensteanbieter sollten jeden Benutzer des Internet unaufgefordert über die Risiken für seine Privatsphäre informieren. Der Benutzer wird dann diese Risiken gegen die erwarteten Vorteile abwägen müssen.

2. In vielen Fällen ist die Entscheidung, am Internet teilzunehmen und wie es zu benutzen ist, durch nationales Datenschutzrecht geregelt. Dies bedeutet z. B. daß personenbezogene Daten nur auf eine nachvollziehbare Art und Weise gespeichert werden dürfen. Medizinische und besonders sensible personenbezogene Daten sollten nur in verschlüsselter Form über das Internet übertragen oder auf den an das Internet angeschlossenen Computern gespeichert werden. Polizeiliche Steckbriefe und Fahndungsaufrufe sollten nicht im Internet veröffentlicht werden.

3. Initiativen für eine engere internationale Zusammenarbeit, ja sogar für eine internationale Konvention, die den Datenschutz im Zusammenhang mit grenzüberschreitenden Computernetzen und Diensten regelt, sollten unterstützt werden.

4. Es sollte ein internationaler Kontrollmechanismus geschaffen werden, der auf bereits existierenden Strukturen wie der Internet Society und anderer Einrichtungen aufbauen könnte. Die Verantwortung für den Schutz personenbezogener Daten muß in einem gewissen Ausmaß institutionalisiert werden.

5. Nationale und internationale Gesetze sollten unmißverständlich regeln, daß auch der Vorgang der Übermittlung (z. B. durch elektronische Post) vom Post- und Fernmeldegeheimnis geschützt wird.

6. Darüber hinaus ist es notwendig, technische Mittel zur Verbesserung des Datenschutzes der Benutzer auf dem Netz zu entwickeln. Es ist zwingend, Entwurfskriterien für Informations- und Kommunikationstechnologie und Multimedia-Hard- und Software zu entwickeln, den Benutzer befähigen, die Verwendung seiner personenbezogenen Daten selbst zu kontrollieren. Generell sollten die Benutzer jedenfalls in den Fällen die Möglichkeit haben, auf das Internet ohne Offenlegung ihrer Identität zuzugreifen, in denen personenbezogene Daten nicht erforderlich sind, um eine bestimmte Dienstleistung zu erbringen.

7. Auch für den Schutz der Vertraulichkeit sollten technische Mittel entwikkelt werden. Insbesondere die Nutzung sicherer Verschlüsselungsmethoden muß eine rechtmäßige Möglichkeit für jeden Benutzer des Internet werden und bleiben.

8. Die Arbeitsgruppe würde eine Studie über die Machbarkeit eines neuen Zertifizierungsverfahrens durch die Ausgabe von „Qualitätsstempeln" für Dienstanbieter und Produkte im Hinblick auf ihre Datenschutzfreundlichkeit unterstützen. Diese könnten zu einer verbesserten Transparenz für die Benutzer der Datenautobahn führen.

9. Anonymität ist ein wichtiges zusätzliches Gut für den Datenschutz im Internet. Einschränkungen des Prinzips der Anonymität sollten strikt auf das begrenzt werden, was in einer demokratischen Gesellschaft notwendig ist, ohne jedoch das Prinzip als solches in Frage zu stellen.

10. Schließlich wird es entscheidend sein, herauszufinden, wie Selbstregulierungen im Wege einer erweiterten „Netiquette" und datenschutzfreundliche Technologie die Implementierung nationaler und internationaler Regelung über den Datenschutz ergänzen und verbessern können. Es wird nicht ausreichen, sich auf eine dieser Handlungsmöglichkeiten zu beschränken: Sie müssen effektiv kombiniert werden, um zu einer globalen Informations-Infrastruktur zu gelangen, die das Menschenrecht auf Datenschutz und unbeobachtete Kommunikation respektiert.

Bericht

Das Internet ist gegenwärtig das größte internationale Computernetz der Welt. In mehr als 140 Ländern gibt es „Auffahrten" zu dieser „Datenautobahn". Das Internet besteht aus mehr als vier Millionen angeschlossenen Rechnern („hosts"); mehr als 40 Millionen Benutzer aus aller Welt können wenigstens einen der verschiedenen Internet-Dienste nutzen und haben die Möglichkeit, miteinander durch elektronische Post zu kommunizieren. Die Benutzer haben Zugriff auf einen immensen Informationsbestand, der an verschiedene Orten in aller Welt gespeichert wird. Das Internet kann als erste Stufe der sich entwickelnden Globalen Informations-Infrastruktur (GII) bezeichnet werden. Das World Wide Web bildet als die modernste Benutzeroberfläche im Internet eine Basis für neue interaktive Multimedia-Dienste. Die Internet-Protokolle werden zunehmend auch für die Kommunikation innerhalb großer Unternehmen genutzt („Intranet").

Die Teilnehmer am Internet haben unterschiedliche Aufgaben, Interessen und Möglichkeiten:

- Die Software-, Computer- und Telekommunikationsindustrien erstellen die Kommunikationsnetze und die angebotenen Dienste.
- Telekommunikationsorganisationen wie die nationalen Telekommunikationsunternehmen stellen die Basisnetze für die Datenübertragung zur Verfügung (Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Verbindungen).
- Dienstleistungsunternehmen stellen Basisdienste für die Speicherung, Übertragung und Darstellung von Daten zur Verfügung. Sie sind für den Datentransport im Internet verantwortlich (routing, delivery) und verarbeiten Verbindungsdaten.
- Informationsanbieter stellen den Benutzern in Dateien und Datenbanken gespeicherte Informationen zur Verfügung.
- Die Benutzer greifen auf die verschiedenen Internet-Dienste (elektronische Post, news, Informationsdienste) zu und nutzen das Netz sowohl zur Unterhaltung als auch für Teleshopping, Telearbeit, Fernunterricht und Telemedizin.

I. Probleme und Risiken

Anders als bei der traditionellen Verarbeitung personenbezogener Daten, bei der normalerweise eine einzelne Behörde oder ein Unternehmen für den Schutz der personenbezogenen Daten ihrer Kunden verantwortlich ist, ist im Internet eine solche Gesamtverantwortung keiner bestimmten Einrichtung zugewiesen. Darüber hinaus gibt es keinen internationalen Kontrollmechanismus zur Erzwingung der Einhaltung gesetzlicher Verpflichtungen, soweit diese existieren. Der Benutzer muß daher Vertrauen in die Sicherheit des gesamten Netzes, unabhängig davon, wo dieser angesiedelt ist oder von wem er verwaltet wird. Die Vertrauenswürdigkeit des Netzes wird durch die Einführung neuer Software, bei deren Nutzung Programme aus dem Netz geladen werden und die mit einer Verschlechterung der Kontrolle der auf dem Rechner des Benutzers gespeicherten personenbezogenen Daten verbunden ist, sogar noch wichtiger werden.

Die schnelle Ausbreitung des Internet und seine zunehmende Nutzung für kommerzielle und private Zwecke führen zur Entstehung schwerwiegender Datenschutzprobleme:

- Das Internet ermöglicht die schnelle Übertragung großer Informationsmengen auf beliebige andere an das Netzwerk angeschlossene Computersysteme. Sensible personenbezogene Daten können in Länder übertragen werden, die nicht über ein angemessenes Datenschutzniveau verfügen.
  Informationsanbieter könnten personenbezogene Daten auf Rechnern in Ländern ohne jegliche Datenschutzgesetzgebung anbieten, auf die aus aller Welt durch einen einfachen Mausklick zugegriffen werden kann.
- Personenbezogene Daten können über Länder ohne jegliche oder ohne hinreichende Datenschutzgesetzgebung geleitet werden. Im Internet, das ursprünglich für akademische Zwecke eingerichtet wurde, ist die Vertraulichkeit der Kommunikation nicht sichergestellt.
  Es gibt keine zentrale Vermittlungsstelle oder sonstige verantwortliche Einrichtung, die das gesamte Netz kontrolliert. Damit ist die Verantwortung für Datenschutz und Datensicherheit auf Millionen von Anbietern verteilt. Eine übertragene Nachricht könnte an jedem Computersystem, das sie passiert, abgehört und zurückverfolgt, verändert, gefälscht, unterdrückt oder verzögert werden. Trotzdem nimmt die Nutzung des Internet für Geschäftszwecke exponentiell zu, und personenbezogene und andere sensible Daten (Kreditkarten-Informationen und Gesundheitsdaten) werden über das Internet übertragen.
- Bei der Nutzung von Internet-Diensten wird weder eine angemessene Anonymität noch eine angemessene Authentifizierung sichergestellt. Computernetzwerk-Protokolle und viele Internet-Dienste arbeiten in der Regel mit dedizierten (Punkt-zu-Punkt-)Verbindungen. Zusätzlich zu den Inhaltsdaten wird dabei die Identität von Sender und Empfänger übertragen. Jeder elektronische Brief enthält einen „header“ mit Informationen über Sender und Empfänger (Name und Internet-Protocol-Nummer, Name des Rechners, Zeitpunkt der Übertragung). Der „header“ enthält weitere Informationen über den Übertragungsweg und den Inhalt der Nachricht. Er kann auch Hinweise auf Publikationen anderer Autoren enthalten. Die Benutzer sind gezwungen, eine elektronische Spur zu hinterlassen, die zur Erstellung eines Benutzerprofils über persönliche Interessen und Vorlieben verwendet werden kann. Obwohl es keinen zentralen Abrechnungsmechanismus für Zugriffe auf news oder das World Wide Web gibt, kann das Informationsgebaren von Sendern und Empfängern zumindest von dem Dienstleistungsunternehmen, an das der Benutzer angeschlossen ist, verfolgt und überwacht werden.
- Andererseits sind die unzureichenden Identifizierungs- und Authentifizierungsprozeduren im Internet bereits dazu benutzt worden, in unzurei-

chend geschützte Computersysteme einzudringen, auf dort gespeicherte Informationen zuzugreifen und diese zu verändern oder zu löschen. Das Fehlen einer sicheren Authentifikation könnte auch genutzt werden, um auf kommerzielle Dienste auf Kosten eines anderen Benutzers zuzugreifen.

- Es gibt im Internet Tausende von speziellen news-groups, von denen die meisten jedem Nutzer offenstehen. Die Artikel können personenbezogene Daten von Dritten enthalten, die gleichzeitig auf vielen tausend Computersystemen gespeichert werden, ohne daß der Einzelne die Möglichkeit hat, dagegen vorzugehen.

Die Teilnehmer am Internet haben ein gemeinsames Interesse an der Integrität und Vertraulichkeit der übertragenen Information: Die Benutzer sind an verläßlichen Diensten interessiert und erwarten, daß ihre personenbezogenen Daten geschützt werden. In bestimmten Fällen können sie ein Interesse daran haben, Dienste ohne Identifizierung benutzen zu können. Den Benutzern ist es normalerweise nicht bewußt, daß sie beim „Surfen" im Netz einen globalen Marktplatz betreten und daß jeder einzelne Schritt dort überwacht werden kann.

Andererseits sind viele Diensteanbieter an der Identifizierung und Authentifizierung von Benutzern interessiert: Sie benötigen personenbezogene Daten für die Abrechnung, könnten diese Daten aber auch für andere Zwecke nutzen. Je mehr das Internet für kommerzielle Zwecke genutzt wird, desto interessanter wird es für Diensteanbieter und andere Einrichtungen sein, so viele Verbindungsdaten über das Nutzerverhalten im Netz wie möglich zu speichern und damit das Risiko für den Datenschutz der Kunden zu verstärken. Unternehmen bieten in zunehmendem Maße freien Zugang zum Internet an, um sicherzustellen, daß die Kunden ihre Werbeanzeigen lesen, die zu einer der hauptsächlichen Finanzierungsquellen des gesamten Internets werden. Die Unternehmen wollen nachvollziehen können, in welchem Ausmaß, von wem und wie oft ihre Werbeanzeigen gelesen werden.

Im Hinblick auf die erwähnten Risiken kommt den Einrichtungen, die das Netz auf internationaler, regionaler und nationaler Ebene verwalten, insbesondere bei der Entwicklung der Protokolle und Standards für das Internet, bei der Festlegung der Regeln für die Identifikation der angeschlossenen Server und schließlich bei der Identifikation der Benutzer, eine wichtige Funktion zu.

II. Vorhandene Regelungen und Empfehlungen

Obwohl verschiedene nationale Regierungen und internationale Organisationen (z. B. die Europäische Union) Programme gestartet haben, um die Entwicklung von Computernetzen und -diensten zu erleichtern und zu intensivieren, sind dabei nur sehr geringe Anstrengungen unternommen worden, um für ausreichende Datenschutz- und Datensicherheitsregelungen zu sorgen. Einige nationale Datenschutzbehörden haben bereits Empfehlungen für die technische Sicherheit von an das Internet angeschlossenen Computernetzen und über Datenschutzrisiken für die einzelnen Benutzer von Internet-Diensten herauszugeben. Solche Empfehlungen sind z. B. in Frankreich, Großbritannien (vgl. den 11. Jahresbericht des Data Protection Registrar, Anhang 6) und in Deutschland erarbeitet worden. Die wesentlichen Punkte können wie folgt zusammengefaßt werden:

- Das Anbieten von Informationen auf dem Internet fällt in den Regelungsbereich der nationalen Datenschutzgesetze und -regelungen. In dieser Hinsicht ist das Internet nicht so ungeregelt, wie oft behauptet wird. Es ist, um nur ein Beispiel zu nennen, einem deutschen Anbieter eines

WorldWideWebServers verboten, ohne Wissen des Benutzers die vollständigen Angaben über den auf ihr Angebot zugreifenden Rechner, die abgerufenen Seiten und heruntergeladene Dateien zu speichern (wie es im Netz allgemein praktiziert wird). Nationale Regelungen können eine Verpflichtung für Informationsanbieter enthalten, sich bei einer nationalen Datenschutzbehörde anzumelden. Nationale Gesetze enthalten darüber hinaus spezielle Regelungen im Hinblick auf internationales Straf-, Privat- und Verwaltungsrecht (Kollisionsrecht), die unter bestimmten Umständen Lösungen bereitstellen können.

- Bevor ein lokales Computernetz - z. B. das einer Behörde - an das Internet angeschlossen wird, müssen die Risiken für das lokale Netzwerk und die darauf gespeicherten Daten im Einklang mit dem nationalen Recht abgeschätzt werden. Dazu kann die Erarbeitung eines Sicherheitskonzepts und einer Abschätzung, ob es erforderlich ist, das gesamte Netz oder nur Teile davon an das Internet anzuschließen, gehören. Abhängig von dem verfolgten Zweck kann es sogar ausreichend sein, nur ein Einzelplatzsystem an das Netz anzuschließen. Es sollten technische Maßnahmen getroffen werden, um sicherzustellen, daß auf dem Internet nur auf Daten, die veröffentlicht werden könnten, zugegriffen werden kann, z. B. durch Einrichtung eines Firewall-Systems, das das lokale Netzwerk vom Internet trennt. Es muß jedoch festgestellt werden, daß der Anschluß eines Computernetzwerks an das Internet eine Erhöhung des Sicherheitsrisikos auch dann bedeutet, wenn solche technischen Maßnahmen getroffen worden sind.
- Falls personenbezogene Daten von Nutzern eines bestimmten Dienstes gespeichert werden, muß für die Benutzer klar sein, wer diese Daten nutzen wird und zu welchen Zwecken die Daten genutzt oder übermittelt werden sollen. Dies bedeutet eine Information am Bildschirm vor der Übermittlung und die Schaffung einer Möglichkeit, die Übermittlung zu unterbinden. Der Benutzer sollte in der Lage sein, diese Unterrichtung und aller übrigen Bedingungen, die durch den Diensteanbieter gestellt werden, auszudrucken.
- Wenn der Zugang zu personenbezogenen Daten auf einem Computersystem bereitgestellt wird - z. B. durch die Veröffentlichung biographischer Angaben über Mitarbeiter in einem Verzeichnis - muß der Informationsanbieter sicherstellen, daß diese Personen sich der globalen Natur des Zugriffs bewußt sind. Am sichersten ist es, die Daten nur mit der informierten Einwilligung der betroffenen Person zu veröffentlichen.

Darüber hinaus gibt es eine Reihe von internationalen gesetzlichen Bestimmungen und Konventionen, die u. a. auch auf das Internet anwendbar sind:

- Empfehlungen des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten, verabschiedet vom Rat der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) am 23. September 1980
- Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981
- Richtlinien betreffend personenbezogene Daten in automatisierten Dateien, von der Generalversammlung der Vereinten Nationen verabschiedet am 4. Dezember 1990
- Richtlinie des Rates der Europäischen Gemeinschaften 90/387/EWG vom 28. Juni 1990 zur Verwirklichung des Binnenmarktes für Telekommunikationsdienste durch Einführung eines offenen Netzzugangs (Open Network Provision - ONP) (in der Datenschutz als „grundlegende Anforderung“ definiert wird)
- 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 (EU-Datenschutzrichtlinie)

– Allgemeines Abkommen über Handel und Dienstleistungen (GATS) (das in Artikel XIV regelt, daß die Mitgliedstaaten durch das weltweite Abkommen nicht daran gehindert werden, Regelungen über den Datenschutz von Einzelpersonen im Zusammenhang mit der Verarbeitung und Verbreitung von personenbezogenen Daten und dem Schutz der Vertraulichkeit von Akten und Aufzeichnungen über Einzelpersonen zu erlassen oder durchzusetzen).

Die Richtlinie der Europäischen Union enthält als erstes suprationales Gesetzeswerk eine wichtige Neudefinition des Begriffs „für die Verarbeitung Verantwortlicher“, die im Zusammenhang mit dem Internet von Bedeutung ist. Artikel 2 Buchstabe c) definiert den „für die Verarbeitung Verantwortlichen“ als 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. Wenn man diese Definition auf die Nutzung des Internet für die Zwecke der Übermittlung elektronischer Post anwendet, muß der Absender einer elektronischen Nachricht als „für die Verarbeitung Verantwortlicher“ dieser Nachricht angesehen werden, wenn er eine Datei mit personenbezogenen Daten absendet, da er die Zwecke und Mittel der Verarbeitung und Übermittlung dieser Daten bestimmt. Andererseits bestimmt der Anbieter eines Mailbox-Dienstes selbst die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Betrieb des Mailbox-Dienstes und hat damit wenigstens eine Mitverantwortung für die Einhaltung der anwendbaren Regelungen über den Datenschutz.

Kürzlich hat die Europäische Kommission zwei Dokumente veröffentlicht, die zu einer europäischen Gesetzgebung führen könnten und in diesem Fall beträchtliche Auswirkungen auf den Datenschutz im Internet haben werden:

– Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen über illegale und schädigende Inhalte im Internet (KOM (96) 487)

und

– Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audiovisuellen und Informationsdiensten (KOM (96) 483).

Obwohl auch diese nicht rechtlich bindend und eher auf einer nationalen denn auf einer internationalen Ebene verabschiedet worden sind, sollten die

– Grundsätze für die Bereitstellung und Nutzung personenbezogener Daten
„Privacy und die nationale Informations-Infrastruktur“
verabschiedet von der Privacy Working Group
des Information Policy Committee
innerhalb der Information Infrastructure Task Force (IITF) am 6. Juni 1995

genannt werden, da sie einen Einfluß auf die internationalen Datenflüsse haben werden. Sie sind intensiv und fruchtbar mit der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation bei einem gemeinsamen Treffen in Washington D. C. am 28. April 1995 diskutiert worden.

In der Praxis werden einige wichtige und effektive Regeln zur Selbstregulierung von der Netzgemeinde selbst aufgestellt (z. B. „Netiquette“). Solche Maßnahmen dürfen im Hinblick auf die Rolle, die sie gegenwärtig und zukünftig für den Datenschutz des einzelnen Benutzers spielen können, nicht unterschätzt werden. Sie tragen mindestens dazu bei, die nötige Aufmerk-

samkeit unter den Benutzers dafür zu schaffen, daß Vertraulichkeit als eine Grundanforderung auf dem Netz nicht existiert („Sende oder speichere niemals etwas in Deiner Mailbox, das Du nicht in den Abendnachrichten sehen möchtest"). Die EU-Datenschutzrichtlinie wiederum fordert Verhaltensregeln (Artikel 27), die von den Mitgliedstaaten und der Kommission gefördert werden sollen.

III. Empfehlungen

Es steht außer Zweifel, daß der gesetzliche und technische Datenschutz im Internet im Augenblick unzureichend ist.

Das Recht des Einzelnen, die Datenautobahn zu benutzen, ohne überwacht und identifiziert zu werden, sollte garantiert werden. Andererseits muß es im Hinblick auf die Nutzung personenbezogener Daten auf der Datenautobahn (z. B. von Dritten) Grenzen geben („Leitplanken").

Eine Lösung für dieses Grunddilemma muß auf folgenden Ebenen gefunden werden:

1. Die Diensteanbieter sollten jeden potentiellen Nutzer des Internet unaufgefordert über die Risiken für seine Privatsphäre informieren. Der Benutzer wird dann diese Risiken gegen die erwarteten Vorteile abwägen müssen.

2. Da „sowohl die einzelnen Teile der Netzwerk-Infrastruktur als auch die Benutzer jeder einen physikalischen Standort haben, können Staaten einen bestimmten Grad von Verläßlichkeit in bezug auf die Netze und ihre Teilnehmer verhängen und durchsetzen" (Joel Reidenberg). In vielen Fällen ist die Entscheidung, am Internet teilzunehmen und wie es zu benutzen ist, durch nationale Datenschutzgesetze geregelt.

   Personenbezogene Daten dürfen nur in einer nachvollziehbaren Art und Weise gespeichert werden. Medizinische und andere sensible personenbezogene Daten sollten nur in verschlüsselter Form über das Internet übertragen oder auf den am Internet angeschlossenen Computern gespeichert werden.

   Es spricht viel dafür, die Nutzung des Internet für die Veröffentlichung von Steckbriefen und Fahndungsaufrufen durch die Polizei zu verbieten (das amerikanische Federal Bureau of Investigations veröffentlicht seit einiger Zeit eine Liste von gesuchten Verdächtigen im Internet). Die beschriebenen Defizite der Authentifizierungsprozeduren und die Manipulierbarkeit von Bildern im Cyberspace scheinen die Nutzung des Internet für diesen Zweck auszuschließen.

3. Verschiedene nationale Regierungen haben internationale Übereinkommen über die globale Informations-Infrastruktur angeregt. Initiativen für eine engere internationale Zusammenarbeit, ja sogar eine internationale Konvention, die den Datenschutz im Hinblick auf grenzüberschreitende Netze und Dienste regelt, sollten unterstützt werden.

4. Es sollte ein internationaler Kontrollmechanismus geschaffen werden, der auf bereits existierenden Strukturen wie der Internet Society und anderer Einrichtungen aufbauen könnte. Die Verantwortung für den Schutz personenbezogener Daten muß in einem gewissen Ausmaß institutionalisiert werden.

5. Nationale und internationale Gesetze sollten unmißverständlich regeln, daß auch der Vorgang der Übermittlung (z. B. durch elektronische Post) vom Post- und Fernmeldegeheimnis geschützt wird.

6. Darüber hinaus ist es notwendig, technische Mittel zur Verbesserung des Datenschutzes der Benutzer auf dem Netz zu entwickeln. Es ist zwingend, Entwurfskriterien für Informations- und Kommunikationstechnologie und Multimedia-Hard- und Software zu entwickeln, die den Benutzer befähigen, die Verwendung seiner personenbezogenen Daten selbst zu kontrollieren. Generell sollten die Benutzer jedenfalls in den Fällen die Möglichkeit haben, auf das Internet ohne Offenlegung ihrer Identität zuzugreifen, in denen personenbezogene Daten nicht erforderlich sind, um eine bestimmte Dienstleistung zu erbringen. Konzepte für solche Maßnahmen sind bereits entwickelt und veröffentlicht worden. Beispiele sind das „Identity-Protector"-Konzept, das in „Privacy-enhancing technologies: The path to anonymity" von der niederländischen Registratiekammer und dem Datenschutzbeauftragten von Ontario/Kanada enthalten ist (vorgestellt auf der 17. Internationalen Konferenz der Datenschutzbeauftragten in Kopenhagen (1995)) und das „User Agent-Konzept", das auf der gemeinsamen Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation und der Privacy Working Group der Information Infrastructure Task Force vorgestellt wurde (April 1995).

7. Auch für den Schutz der Vertraulichkeit sollten technische Mittel entwikkelt werden.

   Die Möglichkeit sicherer Verschlüsselungsmethoden muß eine rechtmäßige Möglichkeit für jeden Benutzer des Internet werden und bleiben.

   Die Arbeitsgruppe unterstützt neue Entwicklungen im Internet-Protokoll (z. B. IP v6), die die Vertraulichkeit durch Verschlüsselung, Klassifizierung von Nachrichten und bessere Authentifizierungsprozeduren verbessern. Die Hersteller von Software sollten den Sicherheitsstandard des neuen Internet-Protokolls in ihre Produkte aufnehmen, und Diensteanbieter sollten die Nutzung dieser Produkte so schnell wie möglich unterstützen.

8. Die Arbeitsgruppe würde eine Studie über die Machbarkeit eines neuen Zertifizierungsverfahrens durch die Ausgabe von „Qualitätsstempeln" für Diensteanbieter und Produkte im Hinblick auf ihre Datenschutzfreundlichkeit unterstützen. Diese könnten zu einer verbesserten Transparenz für die Benutzer der Datenautobahn führen.

9. Anonymität ist ein wichtiges zusätzliches Gut für den Datenschutz im Internet. Einschränkungen des Prinzips der Anonymität sollten strikt auf das begrenzt werden, was in einer demokratischen Gesellschaft notwendig ist, ohne jedoch das Prinzip als solches in Frage zu stellen.

10. Schließlich wird es entscheidend sein, herauszufinden, wie Selbstregulierung im Wege einer erweiterten „Netiquette" und datenschutzfreundliche Technologie die Implementierung nationaler und internationaler Regelung über den Datenschutz ergänzen und verbessern können. Es wird nicht ausreichen, sich auf eine dieser Handlungsmöglichkeiten zu beschränken: Sie müssen effektiv kombiniert werden, um zu einer globalen Informations-Infrastruktur zu gelangen, die das Menschenrecht auf Datenschutz und unbeobachtete Kommunikation respektiert.

    Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die weitere Entwicklung in diesem Bereich genau beobachten, Anregungen aus der Netzgemeinde berücksichtigen und weitere, detailliertere Vorschläge entwickeln.

Rundschreiben

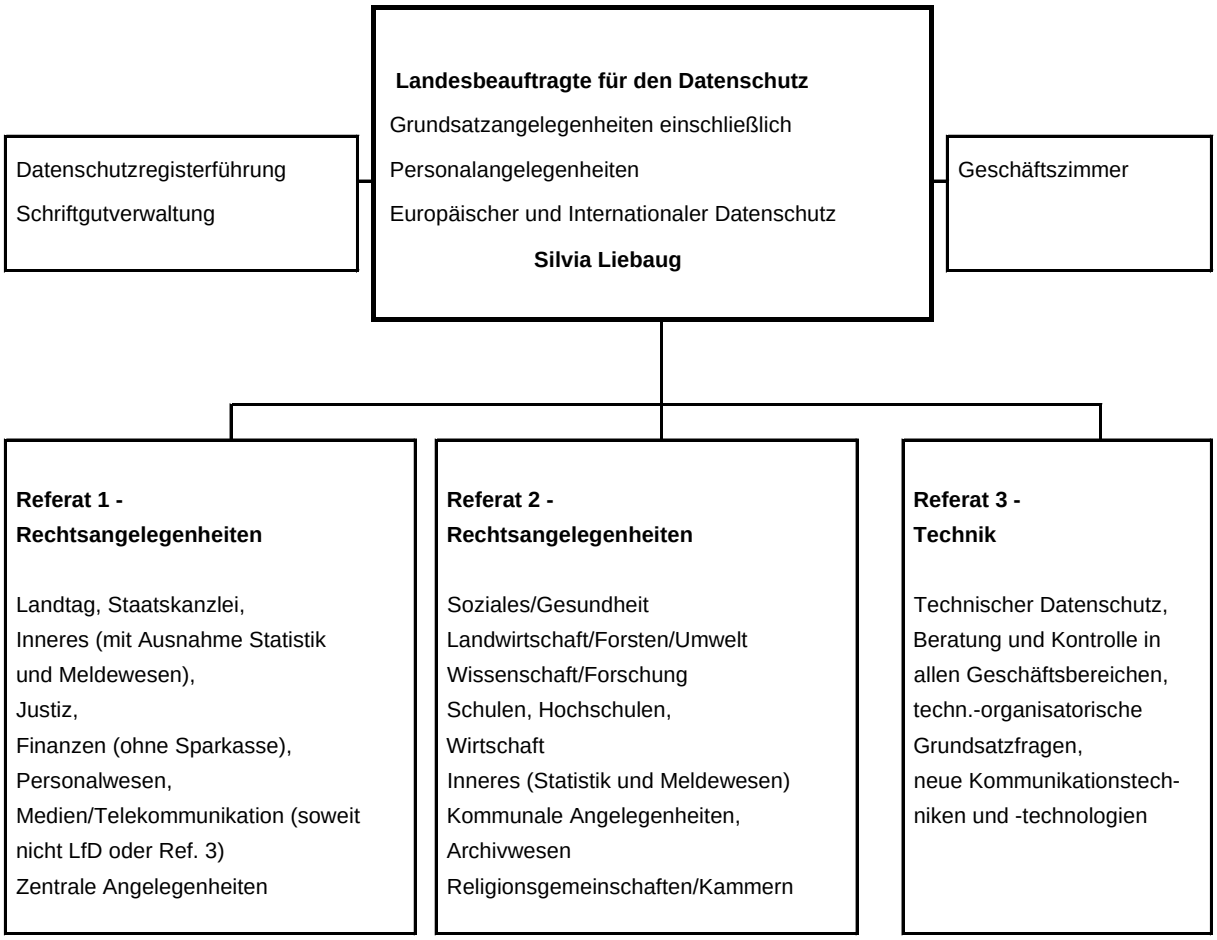
Meldungen zum Thüringer Datenschutzregister (DSR)
gemäß § 2 ThürDSRegVO

Beigefügt übersende ich Ihnen ein in meinem Auftrag vom TLRZ erstelltes Programm, welches die rechnergestützte Erfassung und den Druck der Formblätter für die Meldung zum Datenschutzregister gemäß § 40 Abs. 7 i. V. m. § 12 ThürDSG ermöglicht. Ich empfehle, soweit die technischen Möglichkeiten vorhanden sind, dieses Programm für zukünftige Meldungen an meine Dienststelle einzusetzen. Das Programm eröffnet auch die Möglichkeit, die Registermeldung für das nach § 10 ThürDSG von der öffentlichen Stelle zu führende Verzeichnis der eingesetzten Datenverarbeitungsanlagen und automatisierten Verfahren zu verwenden, indem es auf Wunsch hierfür ein zusätzliches Ergänzungsblatt erstellt.
Bei dem Ausfüllen der elektronischen Formulare werden umfangreiche Hilfestellungen angeboten. Das Programm ist lediglich eine Hilfe zur Erstellung von papiergebundenen Datenschutzregistermeldungen. Es ersetzt diese nicht!

Das DSR-Programm ist lauffähig unter Winword 2.0 bzw. Winword 6.0. Empfohlen wird aufgrund der umfangreicheren Funktionalität ein Einsatz unter Winword 6.0.
Auf der Diskette befinden sich die Verzeichnisse Winword2 und Winword6. Ich empfehle vor der Installation des Programmes die Datei ***liesmich.doc*** aus dem entsprechenden Verzeichnis zu lesen. In dieser Datei sind alle notwendigen Hinweise zur Installation und zur Handhabung des Programms beschrieben.

Sollte es Probleme oder Fragen beim praktischen Einsatz geben, wäre ich für eine Rückinformation dankbar.
Einer entsprechenden Weiterleitung des DSR-Programms im Geschäfts- und Verantwortungsbereich steht nichts entgegen.

Thüringer Landesbeauftragter für den Datenschutz (TLfD)



Anschrift	**Postanschrift**
Am Hügel 10a	PF 941
99084 Erfurt	99019 Erfurt
Tel. 0361/590 26-0	
Fax 0361/590 2620	
E-Mail:DSB-THUERINGEN@t-online.de	

Sachregister

Abgabenordnung	**1**/9.1.8; **2**/9.1, 9.8
Abgeordneter	**2**/3.3
Abgleich von Fingerabdrücken	**2**/7.6
Abrufdienst	**2**/4.4
Abrufverfahren	**1**/5.2.3, 5.3.1, 10.5, 11.1.1; **2**/4.1, 5.2.2, 11.29
Adreßbücher	**1**/5.2.4.7, 15.3; **2**/5.2.4
Adreßdaten	**2**/11.19
Adressenfeststellungsverfahren	**2**/9.5
Akteneinsicht	**1**/8.1,10.4; **2**/9.2
Aktenzeichen	**2**/7.9
Akustische Wohnraumüberwachung	**2**/10.8
Altdaten	**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
Amtsarzt	**1**/11.3.3; **2**/5.2.11
Analyse	**2**/7.3
Anhörungsbogen	**1**/7.5.1; **2**/7.10, 14.9
Anlagen- und Verfahrensverzeichnis	**2**/15.4
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
Antragsformular	**1**/11.9.3, 14.1.2, 14.3.2, 14.3.5; **2**/5.2.6
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
Asylbewerber	**2**/5.1.6
Asylcard	**1**/5.3.2; **2**/5.1.1
Asymmetrische Verschlüsselung	**2**/15.7
Aufbewahrungsfrist	**1**/6.1.9, 11.3.1, 11.3.2; **2**/5.1.8, 5.2.9, 10.17, 11.9
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
Ausbildungsverkehr	**2**/14.11
Auskunftserteilung	**1**/1.1.6, 6.3.2, 9.1.6, 9.2.3; **2**/5.1.8
Auskunftspflicht	**2**/11.3
Ausländer	**2**/5.1.2
Ausländerbehörde	**1**/5.3.1; **2**/5.1.6, 5.2.7
Ausländergesetz	**2**/5.1.2, 5.1.7
Ausländerzentralregister	**1**/1.2.3, 5.3.1; **2**/5.1.2, 7.6
automatisierte Verfahren	**2**/9.4, 10.11, 10.11.3, 10.12

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
Bedrohungs- und Risikoanalyse **2**/10.5
behördeninterner Datenschutzbeauftragter **2**/5.1.9
Bekenntnisfreiheit **1**/11.3.4; **2**/11.7
belegungsgebundener Wohnraum **2**/14.14
Beschlagnahmeschutz **2**/5.2.9
Besucherdaten **2**/10.17
Betretungsverbot **2**/7.8
Bild-Ton-Aufzeichnung **2**/7.12, 10.7
Biotopkartierung **2**/14.20
Bodenbewertungsverfahren **2**/9.4
Browser **2**/15.13
Bundeskriminalamt, -Gesetz **1**/1.2.3, 7.6; **2**/7.3, 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
Bürgerkriegsflüchtlinge **2**/5.1.3

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
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

Datenaustausch **2**/11.2, 15.4
Datenerhebung **1**/6.1.2, 11.5, 11.9.3, 12.5, 12.6, **2**/8.2
Datennetze **2**/11.13
Datenschutz-Audit **2**/4.4, 4.5
Datenschutzfreundliche Technologien **2**/15.6
Datenschutzklausel **2**/11.25
Datenschutzregistermeldung **1**/1.1.6, 2.1, 2.3, 10.16, 15.2; **2**/1.2, 9.3, 9.4, 13.10
Datensicherheit **1**/7.7, 10.5, 15.2, 15.3; **2**/4.4
Datensparsamkeit **2**/4.3, 15.6
Datenspeicher Wohnungspolitik **2**/14.14
Datenträgeraustauschvereinbarung **2**/11.18
Datenträgerentsorgung **2**/15.4
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
Datenvermeidung **2**/15.6
Diensteanbieter **2**/4.3
Digitale Signatur **2**/15.7, 15.8, 15.12
DNA-Analyse **2**/10.4

EG-Datenschutzrichtlinie **1**/4.1; **2**/2.
EG-Führerscheinrichtlinie **1**/14.2.1; **2**/14.7
Ehescheidungsverbundurteile **1**/10.12; **2**/10.11
Eingliederungshilfe **2**/11.28
Einkommensnachweis **2**/5.2.14
Einmessungsverfahren **2**/14.16
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
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
Einzelangaben **2**/12.2
Emissionskataster **2**/14.19
Erhebungsbogen **2**/5.2.12, 13.3, 14.17
Errichtungsanordnung **1**/1.2.5, 7.1, 7.4, 7.6, 10.5; **2**/7.6, 10.5
Europäische Datenbank über gerichtliche Verfahren **2**/10.9
Europäischer Datenschutz **2**/2.
Europol **1**/7.9; **2**/7.3

Fahndung **1**/4.3; **2**/7.6, 10.3
Fahrerfoto **2**/7.10
Fahrtenbuch **2**/9.6
Fax-PC **2**/15.12
Fehlbelegung in Krankenhäusern **2**/11.23
Fernmeldegeheimnis **2**/4.1
Fernwartung **2**/15.10
Finddateien **2**/13.10
Fingerabdruck **2**/7.5
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, 13.9
Freigabe automatisierter Verfahren **1**/6.1.11, 7.7, 15.7.3; **2**/1.2, 9.3, 9.4, 10.18
Führerscheinstelle **1**/14.2.4; **2**/14.8, 14.9
Führungszeugnis **2**/11.14

Gebäuderegister **2**/12.2
Gebrauchtwarenhandel **2**/14.2
Geburtsurkunde **2**/5.2.5
Gefahrenabwehr **2**/7.1, 7.12
Gefahrstoffdatenbank **2**/13.9
Geldauflagen **2**/10.15
Gemeinderat **2**/5.2.16, 5.2.17
Gemeinsame Kontrollinstanz **2**/7.4
Generierung **2**/15.10
Genetischer Fingerabdruck **2**/10.4
Gesundheitsamt **2**/5.2.11
Gewerbeanzeige **2**/14.6
Gewerbebehörde **2**/14.3
Großer Lauschangriff **2**/10.8
Grundbuchamt **1**/10.13; **2**/10.12

Grundstücksdaten **2**/5.2.17
GSM-Netze **2**/15.1
Gutachten **2**/11.22

Handelsregisterdaten **2**/14.5
Hausordnungen **2**/14.13
Health Professional Card **2**/11.13
Hochschule **2**/7.12, 13.4, 13.5, 13.6

ICD-10-Code **2**/11.18
Immunität **2**/3.3
Industrie- und Handelskammer **1**/14.1.2, 14.1.3, 14.1.4; **2**/14.5
Informations- und Kommunikationsdienste-Gesetz **2**/4.3, 15.8
Informationsanspruch des Abgeordneten **2**/3.2
Informationssystem der Thüringer Polizei **2**/7.6
Ingenieurliste **2**/14.1
INPOL **2**/7.6, 7.7
Integrationsverfahren Thüringen-Grundstufe **2**/7.6
Integriertes Automatisches Besteuerungsverfahren **2**/9.4
International Data Encryption Algorithm **2**/15.7
Internationaler Datenschutz **2**/2.
Internet **1**/15.1, 15.13, **2**/14.5
Intranet **2**/15.2
IT-Maßnahmenregelung **2**/15.3
IT-Ressortplan **1**/15.4; **2**/15.3
IT-Richtlinien **2**/15.3
IT-Sicherheitskonzept **2**/5.1.9, 7.6, 15.3, 15.4

Jugendamt **2**/5.2.12, 5.2.13
Jugendgerichtshilfe **2**/13.7
Jugendgesundheitsdienst **2**/5.2.10
Justizmitteilungsgesetz **1**/10.1; **2**/10.1
Justizvollzugsanstalt **1**/6.1.12, 10.11, 11.3.2; **2**/10.11.3, 10.17

Kartierung **2**/14.20
Kassenärztliche Bundesvereinigung **2**/11.18
Kassenärztliche Vereinigung **2**/11.14, 11.15
Kassenarztverzeichnis **2**/11.15
Katasteramt **2**/14.16
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
Kontrollkompetenz **1**/5.1.2, 5.4.1, 7.9, 9.3, 11.1.1; **2**/10.12
Kontrollstellen, private **2**/14.21
Kostenübernahme **2**/5.1.7
Krankenakte **2**/11.10, 11.11, 11.12
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

Krankenkasse **1**/11.2, 11.2.4, 11.2.5, **2**/5.2.12, 11.17, 11.20, 11.22, 11.24, 14.6
Krebsregistergesetz **1**/1.2.2, 13.3.2; **2**/13.8
Kriminalaktennachweis **2**/7.6
Kriminalpolizeiliche Angelegenheiten **2**/7.1
Kriminalstatistik **2**/7.6
Kryptographie **2**/15.7, 15.8
Kurbeitrag **2**/5.2.1

Landesaufnahmestelle für Aussiedler (LAST) **2**/5.1.8
Landesbank Hessen-Thüringen **1**/5.4.1; **2**/5.3
Landeshaushaltsordnung **2**/9.9
Landestierärztekammer **2**/11.16
Landwirtschaft, ökologische **2**/14.21
Lebenslauf **2**/13.5
Leistungsmißbrauch **2**/11.2
Lichtbilddatei **2**/7.11
Liegenschaftskataster **2**/14.17
Lohnsteuerkarte **1**/9.1.1, 9.1.2, **2**/9.7
Löschung **1**/14.2.3, 15.2, 15.9, 15.11, 15.14.2; **2**/7.7, 11.18

Machbarkeitsstudie **2**/5.1.1
Mediendienste **2**/4.4, 4.6
Medienforschung **2**/4.5
Medizinischer Dienst **1**/11.2.4, 11.2.6; **2**/11.22, 11.23
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
Meldekarteien **1**/5.2.2; **2**/5.2.3
Mietschuldner **2**/14.12
Mietspiegel **2**/14.15
Mikroverfilmung **2**/11.10
Mitgliederwerbung **1**/11.2.1; **2**/11.20
Mitgliedstaat **2**/7.3
Mitnutzer **2**/4.5
Mitteilungen:
- in Strafsachen **2**/10.1, 10.16
- in Zivilsachen **2**/10.1
- zum Wählerverzeichnis **2**/10.16

Mitteilungsverordnung **2**/9.8
MPU-Gutachten **1**/14.2.5, **2**/14.9
Müllgebühren **2**/14.18

Namenslisten **2**/5.2.15
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
Notarielle Urkunde **2**/10.20

Notarzteinsatzprotokoll **1**/11.7, **2**/11.21
Nutzungsprofil **2**/4.3

Öffentlichkeitsarbeit **2**/1.1
Online-Zugriff **2**/5.2.2
Ordnungswidrigkeitsverfahren **1**/7.5, 14.2.2; **2**/14.9
Organisierte Kriminalität **2**/10.8
Orientierungshilfen **2**/1.3

Parlament **2**/3., 3.1, 3.3
Paßwort **1**/15.14, **2**/9.4, 10.18
Patientendaten **1**/1.1.5, 11.2.4, 11.2.5, 11.3, 11.10, **2**/9.6, 11.8
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
Personalnebenakten **1**/6.1.10, 6.1.11, 6.1.12, 6.1.16, 9.1.7, **2**/9.4
Personenbeförderung **2**/14.11
Petitionsausschuß **2**/3.1
Pfändung **2**/14.10
Pflegedienst **2**/11.3
Pflegekassen **2**/11.24
Pflegeplanung **2**/11.3
Pflegeversicherung **1**/11.2.6, **2**/11.3, 11.24
Pflichtuntersuchungen **1**/13.1.3; **2**/5.2.10
Planungsaufgaben **2**/14.19
Poliklinikakten **1**/11.3.1; **2**/5.2.9
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
Prozessor **2**/15.9
Pseudonym **2**/4.3
Pseudonymität **2**/15.6
Public-Key-Verfahren **2**/15.7

Rechenzentrum **2**/11.17
Rechnungshof **1**/6.1.4, 9.3; **2**/9.9
Rechnungsprüfung **2**/11.3
Referenzperson **2**/8.1
Regulierungsbehörde **2**/15.8
Religionsunterricht **2**/13.3
Rentenversicherungsträger **2**/11.29
Rettungsdienst **1**/1.1.4, 11.7; **2**/11.21
Risikoanalyse **1**/15.3; **2**/15.3
RSA **2**/15.7, 15.12
ruhender Verkehr **1**/14.2.2, **2**/14.9
Rundfunkgebühren **1**/11.9.1, **2**/4.7

Scheinehe **2**/5.1.5
Schengener Durchführungsübereinkommen **2**/7.4
Schengener Informationssystem **1**/4.3, **2**/7.4

Schuldnerkralle **2**/14.10
Schuldunfähigkeit **2**/10.6
Schulgesundheitspflege **1**/13.1.3; **2**/5.2.10, 13.1
Schulpflichtüberwachung **2**/13.2
Schuluntersuchungen **2**/13.1
Schweigepflicht, ärztliche **1**/11.3, 11.10.2, 13.3.3, **2**/11.12, 11.21, 11.24, 11.25, 11.26
Sekundärstatistik **1**/12.4, 13.1.1; **2**/12.1
Sicherheitskonzept **1**/15.3; **2**/9.4
Sicherheitsüberprüfung **1**/6.3.2, 8.1, 8.2, 8.4; **2**/8.1, 8.2
Signaturgesetz **2**/4.3, 15.8
Signaturschlüssel **2**/15.8
Signaturverordnung **2**/15.8
Sozialamt **1**/9.2.2, 11.9.1, 12.4, 14.3.6, **2**/4.7, 5.2.6, 5.2.7
Sozialdaten **1**/11.; **2**/3.1, 5.2.7, 5.2.8, 14.13
Sozialhilfe **1**/14.3.6; **2**/11.2, 11.28
- datenabgleich **2**/11.2
- empfänger **2**/14.13
- statistik **1**/12.4; **2**/5.2.6
- träger **2**/11.2

Staatsanwaltschaft **2**/10.11, 10.14, 10.18
Staatsanwaltschaftliche Register **2**/10.11
Standesamt **1**/5.1.6, 5.1.7; **2**/5.2.5
Statistik **1**/4.2, 11.3.5, 12., 13.1.1,
- geheimnis **2**/5.2.6, 12.1, 14.15 **1**/4.2, 12.5, 14.1.1; **2**/13.3

Steganographie **2**/15.7
Steuererhebung **2**/9.4
Steuergeheimnis **1**/9.1.3, 9.1.8; **2**/9.1
Stichtagserhebungen **2**/11.23
Strafprozeßordnung **2**/5.1.2
Strafverfahrensänderungsgesetz (StVÄG) **1**/10.4; **2**/10.2, 10.4, 10.14
Strafverfolgung **2**/7.1
Strafverfolgungsstatistik **2**/12.1
Strafvollzugsänderungsgesetz **1**/ 10.1, 10.11; **2**/10.17
Straßenverkehrsgesetz **1**/14.2.1, 14.2.4; **2**/14.7
Symmetrische Verschlüsselung **2**/15.7

Täter-Opfer-Ausgleich **2**/10.14
technisch-organisatorische Leitlinien **2**/10.5
technisch-organisatorische Mängel **2**/10.18,
technisch-organisatorische Maßnahmen **1**/6.3.1, 14.4.2, 15.2; **2**/7.6, 9.4, 10.12, 10.19, 11.8, 11.18, 11.29, 14.8
Teledienste **2**/4.3, 4.4
Telefax **2**/15.12
Telefon
- gebührenabrechnung **2**/11.25
- gespräch **1**/15.7, **2**/5.3
- gesprächslisten **2**/10.18
- überwachung **2**/10.13
- verzeichnis **2**/4.1

Telekommunikation **1**/15.7, 15.14.4, **2**/4.1, 4.2, 4.3

Tierschutzkommission **2**/3.2
Tilgungsfristen **1**/10.8, **2**/10.6
Transplantation **2**/11.1

Übergangsbonus **1**/10.1; **2**/12.1
Unterhaltsfestsetzung **1**/9.1.6, **2**/5.2.13
Unterstützungspflicht **2**/5.2.18
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
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
Versorgungsamt **2**/11.25, 11.26, 11.27
Video **2**/7.12, 10.7, 13.5
Viren **2**/15.11
Vollstreckung **2**/14.10
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
Warndatei **2**/5.1.2
Wartung **2**/15.10
Wasser-/Abwasserzweckverbände **1**/14.4.2; **2**/14.17
Werbung **2**/5.2.1
Wettbewerbsunternehmen **2**/11.6
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
Wohnungsdateien **1**/14.3.1, **2**/14.14
Wohnungsgesellschaft **1**/14.3.3, 14.3.6; **2**/14.12, 14.15

X.400 **1**/15.5.2, 15.14.2; **2**/15.2

Zentrale Anlaufstelle für Asylbewerber (ZAST) **2**/5.1.8
Zentrale TK-Anlage **2**/15.2
Zentrales Fahrerlaubnisregister **1**/14.2.1; **2**/14.7
Zentrales Staatsanwaltschaftliches Verfahrensregister **1**/1.2.5, 10.5; **2**/10.5
Zertifizierungsstellen **2**/15.8
Zeugenschutz **2**/10.7
Zeugenvernehmung **2**/10.7
Zeugnisverweigerungsrecht **2**/4.1, 10.8
Zugangskontrolle **2**/15.4, 15.5
Zugriff, externer **2**/15.4
Zugriffe **2**/9.4
Zugriffsbeschränkung **2**/10.11.3, 11.5, 11.29
Zugriffskontrolle **1**/15.14; **2**/15.5
Zugriffsrechte **1**/15.14; **2**/11.5

Zugriffsschutz **2**/15.4
Zulassungsausschuß für Vertragsärzte **1**/11.11.2, **2**/11.14
Zutrittskontrolle **2**/5.1.9, 15.5
Zutrittskontrollsystem **2**/15.4, 15.5
zweckfremde Nutzung **2**/11.20