THÜRINGER LANDTAG
2. Wahlperiode

Drucksache 2/871
13.02.1996

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

durch den Präsidenten des Landtags

Erster Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz für die Zeit vom 1. März 1994 bis 31. Dezember 1995

Der Thüringer Landesbeauftragte für den Datenschutz hat den nachstehend abgedruckten Bericht mit folgendem Schreiben vom 12. Februar 1996 zugeleitet:

"In der Anlage übersende ich gem. § 40 Abs. 1 des Thüringer Datenschutzgesetzes den ersten Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz für die Zeit vom 1. März 1994 bis 31. Dezember 1995.

Der Beirat hat den Entwurf des Berichtes in seiner Sitzung am 8. Februar 1996 vorberaten."

In Vertretung

Peter Friedrich
Vizepräsident des Landtags

Druck: Thüringer Landtag, 18. März 1996

1. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz

Berichtszeitraum
vom 1. März 1994 bis 31. Dezember 1995

Vorwort

Seit meinem Tätigwerden als Thüringer Landesbeauftragte für den Datenschutz im März 1994 war ich bestrebt, den gesetzlichen Auftrag dieser unabhängigen Kontrollbehörde zu praktizieren und mit den zur Verfügung stehenden Mitteln und Möglichkeiten das Recht auf informationelle Selbstbestimmung den Bürgern nahezubringen, öffentlichkeitswirksam zu werden sowie die öffentlichen Stellen und Behörden des Freistaats Thüringen im Umgang mit Regelungen zum Datenschutz zu beraten.
Insbesondere aus der Kontrolltätigkeit wurden erste Erfahrungen und Erkenntnisse gewonnen und Schwerpunkte für die weitere Tätigkeit abgeleitet.
Im nachfolgenden 1. Tätigkeitsbericht habe ich die Themenbereiche geschildert, mit denen sich der TLfD befaßt hat, und versucht, hierdurch einen Einblick zur praktischen Umsetzung des Datenschutzrechtes in Thüringen zu vermitteln.

Ich bedanke mich bei der Bayerischen Staatskanzlei und dem Bayerischen Landesbeauftragten für den Datenschutz für die personelle Unterstützung in den ersten Monaten des Aufbaus der Behörde. Der Dank gilt der Landtagsverwaltung für die Entlastung des TLfD durch Übernahme von Verwaltungsarbeit und den Beiratsmitgliedern für ihre unterstützende Tätigkeit.
Einen besonderen Dank möchte ich an dieser Stelle an alle Mitarbeiter des TLfD aussprechen, die durch ihr engagiertes Arbeiten maßgeblich dazu beigetragen haben, kurzfristig die volle Arbeitsfähigkeit und das Wirksamwerden der Behörde zu erreichen.

Erfurt, im Dezember 1995

Silvia Liebaug
Landesbeauftragte für den Datenschutz

1. Tätigkeitsbericht des TLfD
Berichtszeitraum vom 1. März 1994 bis 31. Dezember 1995

Inhaltsverzeichnis
Abkürzungsverzeichnis

Abkürzungsverzeichnis

Abkürz.	Bedeutung
Abs.	Absatz
ADMD	Administration Management Domains
AFIS	Automatisiertes Fingerabdruckidentifizierungssystem
AK	Arbeitskreis
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
ARoV	Amt zur Regelung offener Vermögensfragen
Art.	Artikel
AZR	Ausländerzentralregister
AZR-G	Ausländerzentralregistergesetz
AZRG-DV	Ausländerzentralregistergesetz-Durchführungsverordnung
BAföG	Berufsausbildungsförderungsgesetz
BAT	Bundesangestelltentarifvertrag
BBesG	Bundesbesoldungsgesetz
bDSB	behördeninterner Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMF	Bundesfinanzministerium
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz
BVS	Bundesanstalt für vereinigungsbedingte Sonderaufgaben
BZR	Bundeszentralregister
BZRÄndG	Bundeszentralregister-Änderungsgesetz
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
CCITT	Comité Consultatif International Télégraphie et Téléphonique (internationaler Ausschuß der Postverwaltungen)
CD-ROM	Compact-Disk-Read-Only-Memory
CN	Corporate Network
DDK	Datenschutz- und Datensicherheitskonzept
DES	Data Encrypting Standard System
DFÜ	Datenfernübertragung
DSB	Datenschutzbeauftragter/ Datenschutzbeauftragte
E-Mail	Elektronic-Mail (elektronische Post)
EC-Karte	Euroscheck-Karte
EDV	Elektronische Datenverarbeitung
EEPROM	Electrically Erasable Programmable Read Only Memory
EG	Europäische Gemeinschaft
EheG	Ehegesetz
EPROM	Erasable Programmable Read Only Memory
EStG	Einkommensteuergesetz
EU	Europäische Union
EUROPOL	Europäisches Polizeiamt
EvalO	Evaluationsordnung
FAGO	Geschäftsordnung für die Finanzämter
FTP	File Transfer Protocol
GBO	Grundbuchordnung
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
ggf.	gegebenenfalls
GVBl.	Gesetz- und Verordnungsblatt

GVG	Gerichtsverfassungsgesetz
GVO	Grundstücksverkehrsordnung
GwG	Geldwäschegesetz
ID	Identy bzw. Identifikation
IDEA	Blockchiffrieralgorithmus
IHK	Industrie- und Handelskammer
IHK-G	IHK-Gesetz
IMA-IT	Interministerieller Ausschuß für Informationstechnik
IP	Internet Protokoll
ISDN	Integrated Services Digital Network (dienstintegrierendes Digitalnetz)
ISO	International Standard Organisation
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
JMBl.	Justiz-Ministerialblatt
JVA	Justizvollzugsanstalt
KBA	Kraftfahrt-Bundesamt
KfZ	Kraftfahrzeug
KRG	Krebsregistergesetz
LAN	Local Area Network
LDN	Landesdatennetz
LfD	Landesbeauftragter für den Datenschutz
LHO	Landeshaushaltsordnung
LKA	Landeskriminalamt
LRA	Landratsamt
LVwA	Landesverwaltungsamt
MDK	Medizinischer Dienst der Krankenkasse
MDR	Mitteldeutscher Rundfunk
MfS/AfNS	Ministerium für Staatssicherheit/Amt für Nationale Sicherheit
MO	Magnetic-Optical (magnetooptischer Speicher)
MPU	Medizinisch-Psychologische Untersuchungsstellen
MRRG	Melderechtsrahmengesetz
MTA	Message Transfer Agent
MTL II	Manteltarifvertrag für Arbeiter des Landes
NIC	Network Information Centers
NSIS	Nationales Schengener Informationssystem
OFD	Oberfinanzdirektion
OSI	Open Systems Interconnection (Verbindung offener Systeme-Kommunikationsprotokoll)
OWiG	Ordnungswidrigkeitengesetz
PAG	Polizeiaufgabengesetz
PC	Personal Computer
PERSOS	Personalinformationssystem
PIN	Personen-Identifikations-Nummer
PRMD	Private Management Domains
PStG	Personenstandsgesetz
RAM	Random Access Memory
ROD	Rewritable Optical Disc
ROM	Read Only Memory (Nur-Lesespeicher)
RSA	Verschlüsselungsverfahren nach seinen Entwicklern benannt: Rivest, Shamir, Adlemann
SAD	Systemadministrator
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SIS	Schengener Informationssystem
Stasi	Staatssicherheitsdienst
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)

StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
TCP	Transmission Control Protokoll
TDSV	Telekom-Datenschutzverordnung
TFM	Thüringer Finanzministerium
ThLARoV	Thüringer Landesamt zur Regelung offener Vermögensfragen
ThürAPOgFD	Thüringer Verordnung über die Ausbildung und Prüfung für die Laufbahn des gehobenen Forstdienstes
ThürArchivG	Thüringer Archivgesetz
ThürBG	Thüringer Beamtengesetz
ThürBVVG	Thüringer Gesetz über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid
ThürDSG	Thüringer Datenschutzgesetz
ThürDSRegVO	Thüringer Datenschutzregisterverordnung
ThürHG	Thüringer Hochschulgesetz
ThürKAG	Thüringer Kommunalabgabengesetz
ThürKHG	Thüringer Krankenhausgesetz
ThürKO	Thüringer Kommunalordnung
ThürKWG	Thüringer Kommunalwahlgesetz
ThürLBStUG	Thüringer Landesbeauftragtengesetz
ThürMeldeG	Thüringer Meldegesetz
ThürPersVG	Thüringer Personalvertretungsgesetz
ThürRettG	Thüringer Rettungsdienstgesetz
ThürSchulG	Thüringer Schulgesetz
ThürStAnz	Thüringer Staatsanzeiger
ThürStatG	Thüringer Statistikgesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
TIDSV	Telekommunikations- und Informationsdienst-Unternehmen-Datenschutzverordnung
TIM	Thüringer Innenministerium
TK	Telekommunikationsanlage
TKM	Thüringer Kultusministerium
TKV	Telekommunikationsverordnung
TLfD	Thüringer Landesbeauftragter für den Datenschutz
TLfV	Thüringer Landesamt für Verfassungsschutz
TLRZ	Thüringer Landesrechenzentrum
TLS	Thüringer Landesamt für Statistik
TLStU	Thüringer Landesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
TMJE	Thüringer Ministerium für Justiz und Europaangelegenheiten
TMLNU	Thüringer Ministerium für Landwirtschaft, Naturschutz und Umwelt
TMSG	Thüringer Ministerium für Soziales und Gesundheit
TMWFK	Thüringer Ministerium für Wissenschaft, Forschung und Kultur
TMWI	Thüringer Ministerium für Wirtschaft und Infrastruktur
TMWK	Thüringer Ministerium für Wissenschaft und Kunst
UIG	Umweltinformationsgesetz
VerfThür	Verfassung des Freistaats Thüringen
VermG	Gesetz zur Regelung offener Vermögensfragen
VV	Verwaltungsvorschrift
VVThürDSG	Verwaltungsvorschriften zum Vollzug des Thüringer Datenschutzgesetzes
VWGO	Verwaltungsgerichtsordnung
WAIS	Wide Area Information Server
WAN	Wide Area Network
WoBindG	Wohnungsbindungsgesetz
WORM	Write Once, Read Many (einmalige Datenspeicherung, beliebig oft lesbar)
WRV	Weimarer Reichsverfassung
WWW	World Wide Web
ZGT	Zentrale Gehaltsstelle Thüringen
ZPO	Zivilprozeßordnung
ZSIS	Zentrales Schengener Informationssystem

1. Rechtliche Grundlagen für den Datenschutz in Thüringen

Die am 29. Oktober 1993 verkündete und durch Volksentscheid der Thüringer Bürger vom 16. Oktober 1994 endgültig in Kraft getretene Verfassung des Freistaats Thüringen vom 25. Oktober 1993 garantiert das Grundrecht auf Datenschutz. Nach Artikel 6 der Thüringer Verfassung hat jeder das Recht auf Achtung und Schutz seiner Persönlichkeit und seines privaten Lebensbereichs und den Anspruch auf Schutz seiner personenbezogenen Daten. Jeder ist berechtigt, über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst zu bestimmen. Dieses Grundrecht auf informationelle Selbstbestimmung darf nur auf Grund eines Gesetzes eingeschränkt werden. Nach Maßgabe der Gesetze hat auch jeder ein Auskunftsrecht darüber, welche Informationen über ihn in Akten und Dateien gespeichert sind und ein Recht, die ihn betreffenden Akten und Dateien einzusehen. Die Berufung eines Datenschutzbeauftragten beim Landtag zur Wahrung des Rechts auf Schutz der personenbezogenen Daten und zur Unterstützung bei der Ausübung der parlamentarischen Kontrolle ist in Artikel 69 der Thüringer Verfassung aufgenommen.

Das Thüringer Datenschutzgesetz (ThürDSG) vom 29. Oktober 1991 ist am 06.11.1991 in Kraft getreten. Zweck des ThürDSG ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten durch öffentliche Stellen in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 ThürDSG). Zu den öffentlichen Stellen, die das ThürDSG zu beachten haben, gehören gemäß § 2 ThürDSG die Behörden, die Gerichte und die sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform. Das ThürDSG ist als ein Auffanggesetz anzusehen, und gilt nur dort, wo keine speziellen Datenschutzvorschriften gelten.

Das Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 enthält die allgemeinen Datenschutzbestimmungen für den nicht-öffentlichen Bereich (d. h. für das Wirtschafts- und Geschäftsleben wie z. B. Firmen, Banken, Versicherungen u. a.). Ebenso wird im BDSG auch die Datenverarbeitung durch öffentliche Stellen des Bundes geregelt (z. B. Bundesversicherungsanstalt für Angestellte, Arbeitsämter, BKA u. a.). Das BDSG ist ebenfalls als generelles Auffanggesetz datenschutzrechtlicher Fragen zu sehen.

Vor allem im öffentlichen Bereich wurde die bereichsspezifische Datenschutzgesetzgebung vorangetrieben. Im Berichtszeitraum, der dem ersten Tätigkeitsbericht zugrunde liegt, sind wichtige gesetzgeberische Vorhaben auf Bundes- und Landesebene abgeschlossen worden, die das informationelle Selbstbestimmungsrecht tangieren. Auf die wichtigsten Regelungen wird nachstehend eingegangen.

1.1 Landesrechtliche Grundlagen

1.1.1 Thüringer Meldegesetz

Eines der wichtigsten Landesgesetze des bereichsspezifischen Datenschutzes ist das am 1. April 1994 in Kraft getretene Thüringer Meldegesetz (ThürMeldeG). Die wesentlichen Regelungen sind durch das Melderechtsrahmengesetz des Bundes vorgegeben. Alle sich aus der Novelle vom 20.03.1994 ergebenden Neuerungen wurden bereits aufgenommen (siehe Punkt 1.2.1). Durch die Aufnahme schon kraft Melderechtsrahmengesetz geltender Vorschriften ist ein benutzerfreundliches Gesetz entstanden. Materiell regelt es die Zurverfügungstellung personenbezogener Daten aus dem Melderegister zur Erledigung verschiedenster staatlicher und kommunaler Aufgaben.

Derzeit wird vom TIM eine Novelle des ThürMeldeG vorbereitet. Diese wurde u. a. erforderlich, weil im Thüringer Gesetz über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid (ThürBVVG) in § 4 Abs. 4 und 5 die Meldebehörden verpflichtet wurden, auf den eingereichten Unterschriftsbögen die Stimmberechtigung (Hauptwohnsitz seit mindestens 3 Monaten) unentgeltlich zu bestätigen. Um bei der Vielzahl der Unterstützungsunterschriften eine doppelte Unterschrift ausschließen zu können, soll im Meldegesetz eine Befugnis zur kurzzeitigen Speicherung nur der Tatsache, ob bereits eine Unterstützungsunterschrift geleistet wurde, die zudem einer strengen Zweckbindung unterliegt, geschaffen werden. Dies erscheint aus datenschutzrechtlicher Sicht vertretbar. Der TLfD, der Gelegenheit zur Stellungnahme zu dem Entwurf erhalten hat, hat darüber hinaus noch weitere Anregungen und Hinweise gegeben (siehe Punkt 5.2.4.7), über deren Berücksichtigung bei Berichtsabfassung noch keine Informationen vorlagen.

1.1.2 Thüringer Beamtengesetz

Mit dem Thüringer Beamtengesetz (ThürBG) vom 10.06.1994 hat der Landesgesetzgeber die Vorschriften des Beamtenrechtsrahmengesetzes übernommen und ist damit der Verpflichtung nach Anlage I Kapital IX Sachgebiet A Abschnitt III Nr. 2 des Einigungsvertrages zur Schaffung von Landesbeamtenrecht nachgekommen. In den §§ 97 bis 104 sind eindeutige Regelungen getroffen worden, die sowohl für den Betroffenen als auch für die personalverwaltenden Stellen Klarheit zum Umgang mit Personaldaten schaffen. Soweit sich in der Praxis Probleme ergeben haben, wird hierauf noch einzugehen sein.

1.1.3 Thüringer Personalvertretungsgesetz

Das Thüringer Personalvertretungsgesetz (ThürPersVG) vom 29.07.1993 enthält neben der allgemeinen Forderung in § 80, daß sich die Personalvertretungen für die Wahrung der Vorschriften über den Datenschutz einzusetzen haben, auch zahlreiche konkrete Regelungen, mit deren Hilfe sie als Interessenvertreter der Beschäftigten das Recht auf informationelle Selbstbestimmung im Rahmen ihrer Mitbestimmungsaufgaben durchsetzen sollen.
Dies betrifft insbesondere die Mitbestimmung über Regelungen zur "Ordnung in der Dienststelle und das Verhalten der Beschäftigten" (wie z. B. Festlegungen zum Postdurchlauf) gemäß § 74 Abs. 3 Nr. 15 ThürPersVG und über "Inhalt von Personalfragebogen für Angestellte und Arbeiter sowie für Beamte" gemäß § 74 Abs. 3 Nr. 8 bzw. § 75 Abs. 2 Nr. 2 ThürPersVG. Des weiteren wird gemäß § 74 Abs. 3 Nr. 18 und 19 ThürPersVG die volle Mitbestimmung des Personalrates bei der Einführung, Anwendung, wesentlichen Änderung oder Erweiterung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen oder zu erfassen (wie z. B. Arbeitszeiterfassungssysteme, Telefondatenerfassung) oder zur automatisierten Verarbeitung personenbezogener Daten der Beschäftigten (z. B. Programme zur Lohn- und Gehaltszahlung, zur Personalverwaltung, zur Beihilfebearbeitung) gefordert.
Bei der Kontrolltätigkeit des TLfD wird der Frage, ob der Personalrat beteiligt wurde, stets eine große Bedeutung beigemessen, da gemäß § 69 Abs. 10 ThürPersVG die Durchführung einer Maßnahme unzulässig ist, wenn sie ohne die gesetzlich vorgeschriebene Beteiligung der Personalvertretung erfolgte. Es zeigte sich mitunter bei Anfragen und Kontrollen in öffentlichen Stellen, daß Kritiken oder Beanstandungen (insbesondere hinsichtlich der Arbeitsweise der Personalverwaltungen) seitens des TLfD vermeidbar gewesen wären, wenn die Behördenleitungen immer ihre Informationspflicht den Personalvertretungen gegenüber und die Personalvertretungen selbst ihre vom Gesetzgeber zugewiesene Verantwortung zur Wahrung der Vorschriften des Datenschutzes gemäß § 80 ThürPersVG sowie ihre Rechte zur Mitbestimmung gemäß § 74 ThürPersVG wahrnehmen würden. Da nicht auszuschließen ist, daß gemäß § 80 ThürPersVG alle Prüfungsberichte des TLfD, soweit diese die Zuständigkeit der Personalvertretung betreffen, von der Behördenleitung zur Verfügung zu stellen sind, wird der TLfD künftig hierauf besonders hinweisen.

1.1.4 Thüringer Rettungsdienstgesetz

Das am 1. Januar 1993 in Kraft getretene Thüringer Rettungsdienstgesetz enthält in § 20 neben einer bereichsspezifischen Ausprägung des Erforderlichkeitsgrundsatzes und einer Verschwiegenheitsverpflichtung des Leistungserbringers und seiner Mitarbeiter eine Dokumentationspflicht zur Erfassung aller Einsätze in der Notfallrettung. Von letzterem ist den Aufgabenträgern in anonymisierter Form ein Abdruck für Zwecke der Qualitätssicherung zu überlassen. Diese Dokumentationspflichten zur Qualitätssicherung wurden im Landesrettungsdienstplan präzisiert, der am 27.06.1995 in Kraft getreten ist. Dieser Rahmenplan wird von den Aufgabenträgern des Rettungsdienstes (Kreise und kreisfreie Städte) durch Rettungsdienstbereichspläne nach § 6 ThürRettG konkretisiert. Aufgrund der erst kurzen Geltungsdauer dieser Vorschriften liegen dem TLfD bisher wenig praktische Erfahrungen im Umgang mit diesen Dokumentationspflichten vor (siehe Punkt 11.7*)*.

1.1.5 Thüringer Krankenhausgesetz

Das mit Wirkung vom 01.01.1994 in Kraft getretene Thüringer Krankenhausgesetz (ThürKHG) enthält in seinem § 27 ausführliche datenschutzrechtliche Regelungen, die insoweit als bereichsspezifische Vorschriften den Normen des ThürDSG vorgehen. So ist z. B. die Demonstration von Patienten zu Zwecken der Ausbildung und Lehre nur mit schriftlicher Einwilligung der Patienten erlaubt. Den Schwerpunkt der Regelung bildet der Umgang mit den Patientendaten. Dabei fallen unter diesen Begriff auch Daten von Angehörigen oder sonstigen Bezugspersonen, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden. Die Zweckbindung der Erhebung, Speicherung und Nutzung wird auf die dem Krankenhaus im Rahmen des Behandlungsvertrages obliegenden Aufgaben sowie die Aus- und Fortbildung beschränkt. Für krankenhausinterne Forschung dürfen die Patientendaten lediglich genutzt, nicht jedoch erhoben werden. Dabei sind die Daten jedoch so früh wie möglich zu anonymisieren. Im übrigen bedarf die Erhebung, Speicherung und Nutzung von Patientendaten der Einwilligung des Patienten. Hierzu ist die vorherige

schriftliche Einwilligung des Patienten einzuholen, wobei er zuvor in geeigneter Weise über die Bedeutung der Einwilligung sowie den Zweck der vorgesehenen Verarbeitung der Daten aufzuklären ist. Eine Übermittlung von Patientendaten ist nach § 27 Abs. 6 ThürKHG auch zulässig für die Durchführung qualitätssichernder Maßnahmen in der Krankenhausversorgung, die Abwehr besonderer Gefahren sowie für die Durchführung der mit der Behandlung in Zusammenhang stehenden gerichtlichen Verfahren. Die Patienten haben ein kostenfreies Auskunftsrecht (Absatz 8). Positiv hervorzuheben ist die Pflicht des Krankenhauses nach Absatz 10, einen Datenschutzbeauftragten zu bestellen.

1.1.6 Thüringer Datenschutzregisterverordnung

Der TLfD führt gemäß § 40 Abs. 7 i. V. m. § 12 ThürDSG ein Datenschutzregister, das die Angaben der öffentlichen Stellen, die personenbezogene Daten in automatisierten Verfahren verarbeiten, enthält sowie eine Darstellung des Dateiinhaltes und die Stellen, denen Daten regelmäßig übermittelt werden. Die Einzelheiten über Aufbau und Inhalt des Registers, die Art und Weise der Registerführung sowie die Form der Auskunftserteilung regelt die ThürDSRegVO vom 22.03.1994. Der ThürStAnz. Nr. 20/1994 enthält auf den Seiten 1367 bis 1370 die kopierfähig gestalteten Formblätter DSB 1 bis 3, die für die Meldung zum Datenschutzregister benutzt werden müssen, sowie ausführliche Erläuterungen zum Ausfüllen der Meldung. Die ausgefüllten Formblätter sind dann von der speichernden öffentlichen Stelle über die jeweils zuständige oberste Landesbehörde an den TLfD zu leiten. Sinn dieser Regelung ist es, daß die Aufsichtsbehörden Kenntnis von der jeweiligen Meldung erhalten und Hinweise sowie Unterstützung bei der ordnungsgemäßen Übergabe der Meldung leisten können. Die obersten Landesbehörden können in ihrem Bereich auch zulassen, daß bestimmte speichernde Stellen die Dateien unmittelbar an den TLfD melden. Kreisangehörige Städte und Gemeinden schicken die Meldung über das zuständige Landratsamt, kreisfreie Städte und Landkreise direkt an den TLfD. Alle zum Zeitpunkt des Inkrafttretens dieser Verordnung bereits bestehenden Dateien waren bis zum Ablauf des dritten, auf den Tag der Verkündung folgenden Kalendermonats abzugeben. Alle anderen sind unverzüglich nach deren Errichtung zu melden (siehe Punkt 2.3).

1.2 Bundesrechtliche Grundlagen

1.2.1 Novelle des Melderechtsrahmengesetzes

Das am 20. März 1994 in Kraft getretene Erste Gesetz zur Änderung des Melderechtsrahmengesetzes enthält Änderungen, die sich aus der praktischen Anwendung des Gesetzes seit 1980 ergeben haben. So darf die Meldebehörde gem. § 22 Abs. 1 Satz 1 MRRG nun auch Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Vorfeld von Wahlen Meldedaten über Gruppen von Wahlberechtigten übermitteln. Hierbei steht den Bürgern, ebenso wie bei Auskunftsbegehren über Alters- und Ehejubiläen, ein Widerspruchsrecht zu. Die Empfänger der Daten dürfen die Daten nur zum Zweck der Wahlwerbung verwenden und sind einen Monat nach der Wahl zu deren Löschung verpflichtet. Da das Thüringer Meldegesetz erst am 1. April 1994 in Kraft getreten ist, wurden darin schon alle rahmenrechtlichen Vorgaben erfüllt, so daß hierzu keine Novelle des Landesmeldegesetzes erforderlich ist (siehe Punkt 5.2.1).

Mit der am 9. November 1995 in Kraft getretenen Novelle der Zweiten Bundesmeldedatenübermittlungsverordnung wird der regelmäßige Datenabgleich insbesondere an die Sozialleistungsträger hinsichtlich der automatisierten Datenverarbeitung auf den Stand der Technik gebracht. Erfahrungen hierbei liegen wegen der Kürze der Geltungsdauer noch nicht vor.

1.2.2 Krebsregistergesetz

Nach langwierigen Beratungen zwischen Bund und Ländern ist am 01.01.1995 das Gesetz über Krebsregister (Krebsregistergesetz - KRG -) in Kraft getreten. Es schreibt vor, daß zur Krebserforschung flächendeckend in den Bundesländern Krebsregister einzurichten sind. Unter Beteiligung der DSB von Bund und Ländern ist ein - wenn auch verfahrenstechnisch aufwendiger - Kompromiß zwischen den Interessen der Forschung, möglichst viel und aussagekräftiges Datenmaterial zu bekommen, und den Interessen der Patienten auf Schutz ihres Rechts auf informationelle Selbstbestimmung gefunden worden. Das Gesetz ist bis 01.01.1999 befristet und soll durch Ländergesetze abgelöst werden. Die neuen Länder und Berlin sind derzeit dabei, die landesrechtlichen Grundlagen zu schaffen, um das zentrale Krebsregister der ehemaligen DDR als Gemeinsames Krebsregister in Berlin weiterzubetreiben (siehe Punkt 13.3.2).

1.2.3 Ausländerzentralregistergesetz

Mit dem Ausländerzentralregistergesetz (AZR-G), das am 01.10.1994 in Kraft getreten ist, findet ein regelungsbedürftiger Zustand seinen Abschluß, der schon seit Jahren Gegenstand der Erörterungen im Kreis der DSB ist. Zuletzt hat sich

die 47. Konferenz der DSB damit befaßt und noch einmal ihre Bedenken gegen den Informationsverbund für Aufgaben der Polizei, Strafverfolgung und Nachrichtendienste deutlich gemacht (siehe Anlage 1). Zwischenzeitlich ist aufgrund von § 40 Abs. 1 AZR-G die Verordnung zur Durchführung des Gesetzes für das Ausländerzentralregister (AZRG-DV) vom 17.05.1995 in Kraft getreten, vor deren Erlaß gegenüber dem TIM Stellung genommen wurde. Das TIM hat im Rahmen der Länderbeteiligung die Auffassung des TLfD geteilt. Die vorgetragenen Bedenken wurden in der Verordnung bedauerlicherweise nicht berücksichtigt.

1.2.4 Schuldnerverzeichnis

Mit dem Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis vom 15.07.1994 und der Verordnung über das Schuldnerverzeichnis vom 15.12.1994 sind Gesichtspunkte des Datenschutzes berücksichtigt worden, die im Gegensatz zu bisherigen Regelungen, wonach jedermann Auskunft aus dem Schuldnerverzeichnis zu erteilen war, vorsehen, daß Auskünfte nunmehr nur zweckgebunden erfolgen. Ob das Gesetz eine mißbräuchliche Verwendung von Daten verhindert (Bericht des Rechtsausschusses des Deutschen Bundestages, BT-Drucksache 12/6914, S. 1), scheint zumindest problematisch, da eine wirksame Überwachung nicht möglich ist, worauf Lappe in seinem Kurzbeitrag (NJW 1994, 3067 f. [3069]) zutreffend hinweist.

1.2.5 Verbrechensbekämpfungsgesetz

Am 01.12.1994 ist das "Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz)" vom 28.10.1994 in Kraft getreten. Durch das Verbrechensbekämpfungsgesetz sind eine Vielzahl von Bundesgesetzen verändert worden. Aus datenschutzrechtlicher Sicht besonders bedeutsam sind folgende mit dem Verbechensbekämpfungsgesetz eingeführte Änderungen:

- Nach § 100a Strafprozeßordnung (StPO) ist die Befugnis zur Überwachung des Fernmeldeverkehrs für Zwecke der Strafverfolgung auf die ebenfalls mit dem Verbrechensbekämpfungsgesetz eingeführten neuen Strafnormen im Ausländer- und Asylverfahrensgesetz erweitert worden.
- Nach §§ 474 ff. StPO wird bei dem BZR ein zentrales staatsanwaltschaftliches Verfahrensregister geführt. Die dort einzutragenden Daten dürfen nur für Strafverfahren gespeichert und verändert werden. Näheres wird in einer Errichtungsanordnung geregelt (siehe Punkt 10.5).
- Durch Änderung des Gesetzes zu Art. 10 GG erhält der Bundesnachrichtendienst erweiterte Befugnisse zur Überwachung der internationalen nicht leitungsgebundenen Fernmeldeverkehrsbeziehungen. Die klassische Zuständigkeit des Bundesnachrichtendienstes wird damit auch auf die Ermittlung von Sachverhalten, die zur Bekämpfung bestimmter gravierender Straftaten erforderlich sind, erweitert.

Hierzu haben die DSB in der 48. Konferenz (siehe Anlage 11) bereits zum Gesetzentwurf gefordert, das Trennungsgebot für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung strikt zu beachten und eine wirksame Kontrolle durch den DSB in diesem sensiblen Bereich sicherzustellen.

2. Der Thüringer Landesbeauftragte für den Datenschutz

2.1 Rechtliche Stellung, Aufgaben und Befugnisse

Im fünften Abschnitt des ThürDSG sind in den §§ 35 bis 40 die wesentlichen Aussagen zur Stellung, zu den Aufgaben und Befugnissen des TLfD zur Wahrnehmung seines Kontrollauftrages verankert. Der Landtag wählt, gemäß § 35 ThürDSG, auf Vorschlag der Landesregierung den Landesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Die Amtszeit des Landesbeauftragten für den Datenschutz beträgt sechs Jahre, wobei eine einmalige Wiederwahl zulässig ist. Bezüglich seiner Rechtsstellung ist in § 36 ThürDSG ausdrücklich festgeschrieben, daß der Landesbeauftragte in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen ist. Der Präsident des Landtags führt die Dienstaufsicht.

Auch im Rahmen der 50. Datenschutzkonferenz wurde ausführlich über die Beachtung der Unabhängigkeit der Datenschutzbeauftragten diskutiert. Es wurde festgehalten, daß Eingriffe in die Unabhängigkeit nicht hingenommen werden können.

Der TLfD kontrolliert gemäß § 37 ThürDSG bei allen öffentlichen Stellen die Einhaltung der Vorschriften des ThürDSG und anderer Rechtsvorschriften über den Datenschutz. Das Kontrollrecht des TLfD bezieht sich auch auf die öffentlichen Stellen, die am Wettbewerb teilnehmen. Die Gerichte und der Landtag unterliegen der Kontrolle nur, soweit sie in Verwaltungsangelegenheiten tätig werden. Für die öffentlichen Stellen besteht nach § 38 ThürDSG die Pflicht, den TLfD und seine Beauftragten in Erfüllung ihrer Aufgaben zu unterstützen. Das beinhaltet insbesondere, daß

Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme zu gewähren ist, die im Zusammenhang mit der Kontrolle stehen. Weiterhin ist jederzeit Zutritt in alle Diensträume zu gewähren.

Der TLfD beanstandet gemäß § 39 ThürDSG festgestellte Verletzungen von Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten und fordert ihre Behebung in angemessener Frist. Wird die Beanstandung nicht behoben, fordert der TLfD von der Aufsichtsbehörde binnen angemessener Frist geeignete Maßnahmen. Hat das nach Ablauf dieser Frist keinen Erfolg, verständigt der TLfD den Landtag und die Landesregierung.

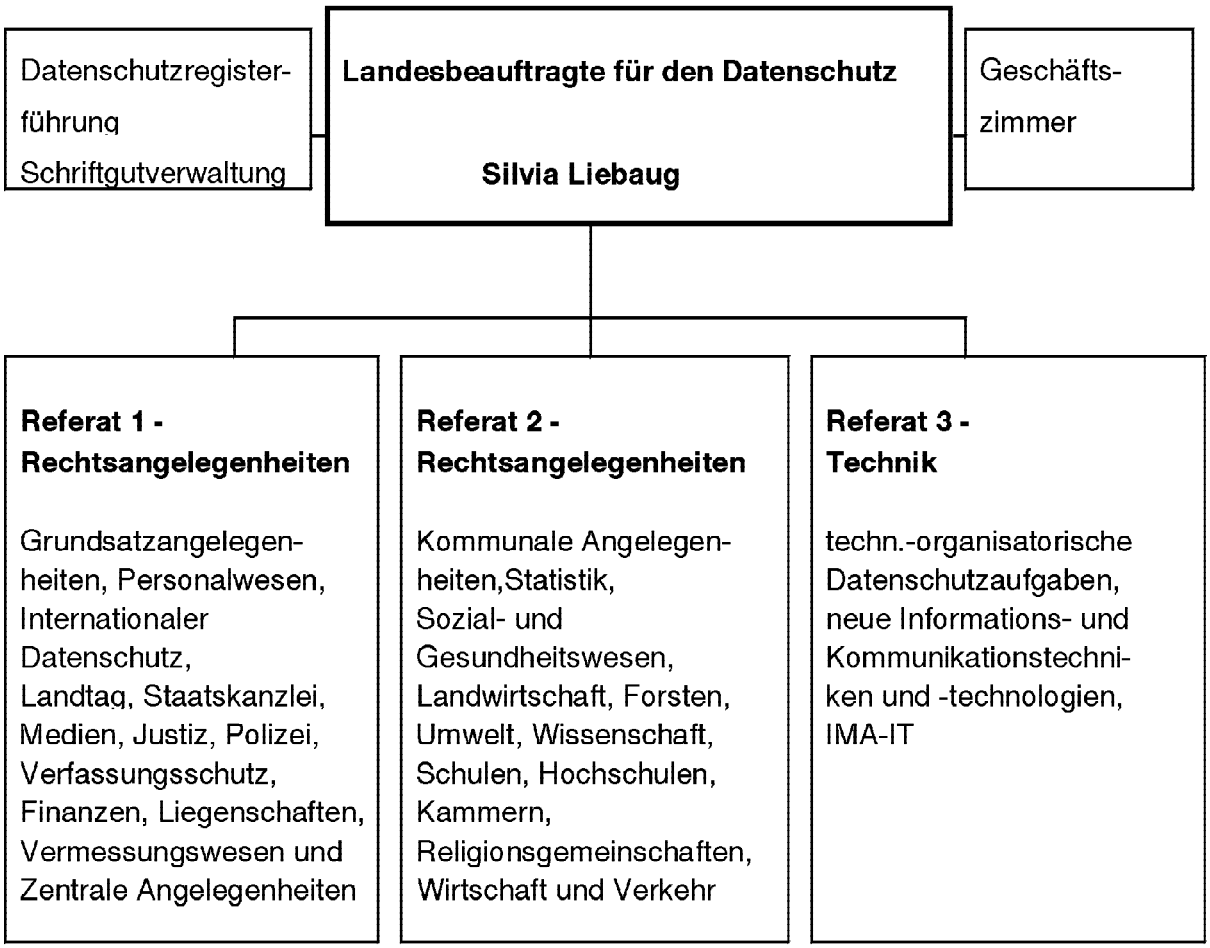
Der TLfD erstattet dem Landtag und der Landesregierung mindestens alle zwei Jahre Bericht über seine Tätigkeit. Dabei gibt er auch einen Überblick über die technischen und organisatorischen Maßnahmen und regt Verbesserungen des Datenschutzes an. Weiterhin ist in § 40 Abs. 3 ThürDSG enthalten, daß der TLfD den Landtag im Rahmen seiner Beratungsaufgabe bei seinen Entscheidungen unterstützt. Auf Anforderung des Landtags oder der Landesregierung hat der TLfD Gutachten zu erstellen und Berichte zu erstatten. Weiterhin können der Landtag oder die Landesregierung den Landesbeauftragten ersuchen, bestimmte Vorgänge aus seinem Aufgabenbereich zu überprüfen. Nach § 40 Abs. 5 ThürDSG beobachtet der TLfD die Entwicklung und Nutzung der Informations- und Kommunikationstechnik, insbesondere der automatisierten Datenverarbeitung, und ihre Auswirkungen auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen. Der TLfD kann sich jederzeit an den Landtag wenden.

Der TLfD führt das Datenschutzregister nach § 12 ThürDSG, in welches jedermann kostenlos Einsicht nehmen kann und sich bei glaubhaft vorgebrachtem berechtigten Interesse Auszüge aus dem Datenschutzregister anfertigen lassen kann. An dieser Stelle sei auf ein wichtiges Schutzrecht der Bürgerinnen und Bürger des Freistaats Thüringen verwiesen. Gemäß § 11 ThürDSG kann sich jedermann - unbeschadet des allgemeinen Petitionsrechtes oder anderer Rechte - an den TLfD mit Vorbringen wenden, daß bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen seine schutzwürdigen Belange beeinträchtigt werden. Niemand darf benachteiligt oder gemaßregelt werden, weil er von seinem diesbezüglichen Recht Gebrauch gemacht hat.

2.2 Die Dienststelle des TLfD (Organigramm)

Mit Wirkung vom 01.03.1994 ist der Thüringer Landesbeauftragte für den Datenschutz im Amt. Seit diesem Zeitpunkt lag ein Aufgabenschwerpunkt im Aufbau der Behörde. Im Jahr 1994 waren im Haushaltstitel des Landtags für den TLfD 6 Personalstellen vorgesehen, was zur Bewältigung aller Aufgabenbereiche nicht ausreichend war. Der vom TLfD beantragten Aufstockung um weitere 6 Stellen wurde für 1995 von seiten des Landtags zugestimmt. Seit dem 01.07.1995 sind alle Stellen beim TLfD besetzt. Gemäß § 36 Abs. 5 ThürDSG ist dem TLfD die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Sie ist im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen. Diesbezüglich sieht der TLfD auch seine volle Entscheidungs- und Verfügungsfreiheit über alle im Einzelplan für den TLfD ausgewiesenen Mittel.
Die gesetzlich garantierte unabhängige Amtsausübung des TLfD ist im Rahmen der Anbindung an den Landtag praktisch zu beachten und sicherzustellen. Zwischen dem TLfD und dem Präsidenten des Thüringer Landtags fand diesbezüglich ein umfangreicher Austausch der Positionen zur Art und Weise und zum Umfang der möglichen und effektiven Zusammenarbeit des TLfD mit der Landtagsverwaltung statt. Im Ergebnis scheint gegenwärtig eine akzeptable Grundlage erreicht worden zu sein. Für routinemäßige nicht behördenspezifische Verwaltungsarbeiten eines DSB, wie z. B. Reisekostenabrechnung und Postbeförderung, ist die Unterstützung durch die Landtagsverwaltung sinnvoll. Wenn alle diese anfallenden Verwaltungsarbeiten von der Dienststelle des TLfD übernommen werden müßten, wäre eine Personalaufstockung in diesem Bereich notwendig, was aber im Sinne einer effektiven Verwaltungsführung nicht geboten erscheint.

Thüringer Landesbeauftragter für den Datenschutz (TLfD)



Anschrift
Am Hügel 10a
99084 Erfurt

Postanschrift
PF 941
99019 Erfurt

Tel. 0361/590 26-0
Fax 0361/590 2620

2.3 Aufgabenschwerpunkte im Berichtszeitraum

Ein wichtiger Schwerpunkt im Berichtszeitraum lag im Aufbau der Behörde des TLfD. Ausgehend von der Einstellung geeigneten und fachlich kompetenten Personals nach erfolgter Stellenausschreibung war möglichst rasch eine effektive Organisationsstruktur und Geschäftsverteilung festzulegen, die auch für eine kleine Behörde mit den ihr eigenen umfangreichen Aufgabenstellungen eine optimale Arbeitsgrundlage bietet. In diesem Zusammenhang spielt auch die entsprechende technische Ausstattung eine grundlegende Rolle. Die Umsetzung des IT-Konzeptes beim TLfD erfolgt wie vorgesehen.

Der TLfD war stets bemüht, die vorgebrachten Bürgeranfragen oder -beschwerden kurzfristig zu bearbeiten und zu beantworten.

Im Rahmen der Kontrolltätigkeit, als einem wesentlichen Aufgabenschwerpunkt des TLfD, fanden im Berichtszeitraum insgesamt 35 Kontrollen bei öffentlichen Stellen im Freistaat Thüringen statt. Im Ergebnis der Kontrollen wurden 11 öffentliche Stellen beanstandet. Darüber hinaus wurden aufgrund von Hinweisen und vorliegender Stellungnahmen drei weitere Beanstandungen ausgesprochen. Die Feststellungen und Ergebnisse sind im 1. Tätigkeitsbericht jeweils unter den konkreten sachbezogenen Gliederungspunkten festgehalten.

Ein Hauptanliegen des TLfD ist es, ein kompetenter Ansprechpartner auf dem Gebiet des Datenschutzes und der Datensicherheit zu sein. Die beratende und Informationstätigkeit war ein weiterer Schwerpunkt der Arbeit des TLfD. Gerade hier kann im Vorfeld einiges getan werden, Datenschutzforderungen nahezubringen, um Datenschutzverstöße weitestgehend vermeiden zu helfen.

Trotz hoher Arbeitsbelastung und der Aufbauphase der Behörde wurden Anfragen hinsichtlich der Teilnahme des Datenschutzbeauftragten an Beratungen in Behörden mit datenschutzrelevanten Themen im Rahmen der Möglichkeiten wahrgenommen. Auch fanden Beratungen beim TLfD mit den jeweilig zuständigen bDSB zu Einzelfragen statt.

Um den Bürgern und Behörden den Zugang zu den einschlägigen Bestimmungen des Datenschutzes in der Verwaltungspraxis zu erleichtern, wurden vom TLfD ein Informationsfaltblatt "Datenschutz im öffentlichen Bereich des Freistaates Thüringen" und zwei Informationsbroschüren - "Der TLfD informiert" - Teil 1 und Teil 2, veröffentlicht.
Teil 1 enthält dabei neben dem Thüringer Datenschutzgesetz und dem Bundesdatenschutzgesetz die Verwaltungsvorschriften zum Vollzug des Thüringer Datenschutzgesetzes und die Thüringer Datenschutzregisterverordnung; Teil 2 beinhaltet Auszüge wichtiger spezialgesetzlicher Regelungen zur Gewährleistung des Datenschutzes.
Darüber hinaus hat der TLfD mehrere Rundschreiben (siehe Anlage 33 bis 36) herausgegeben, die jeweils den obersten Landesbehörden mit der Bitte um Beachtung und Weiterleitung im Zuständigkeitsbereich zur Kenntnis gegeben wurden.

Durch Vorträge in Fortbildungseinrichtungen sowie in Landesbehörden konnten einer Vielzahl von Beschäftigten im öffentlichen Dienst Kenntnisse auf dem Gebiet des Datenschutzes vermittelt und Erfahrungen ausgetauscht werden. Daneben wurden auch Prüfungen, insbesondere im kommunalen Bereich, dazu genutzt, dort die Mitarbeiter für Probleme des Datenschutzes zu sensibilisieren.
Dieses reicht selbstverständlich bei weitem nicht aus, weshalb alle Verantwortlichen aufgefordert sind, bei Fortbildungsmaßnahmen den Datenschutz stärker einzubeziehen. Der TLfD wird sich auf Wunsch auch künftig dieser Aufgabe widmen. Entsprechende Vorschläge wurden hierzu gegeben. Auch im Gespräch mit dem Landkreistag hat der TLfD seine diesbezügliche Bereitschaft, besondere Themenschwerpunkte in Fortbildungsseminaren zu behandeln, erklärt.

Ein weiteres Tätigkeitsfeld des TLfD bestand in der Beteiligung und Mitarbeit bei der Erarbeitung von Rechtsvorschriften mit datenschutzrelevanten Regelungen und deren Umsetzung. Durch die rechtzeitige Einbeziehung des TLfD können auftretende Fragen bereits im Vorfeld geklärt werden.

Bei den Sachthemen, mit denen sich der TLfD im Berichtszeitraum zu beschäftigen hatte, spielten die Altdatenproblematik, die Diskussion der Chip-Karte im Gesundheitswesen, zahlreiche Fragen aus dem Meldewesen und die Kontrolle der Einhaltung der technischen organisatorischen Maßnahmen zur Gewährleistung der Vorschriften auf dem Gebiet des Datenschutzes und der Datensicherheit eine wichtige Rolle.

Ein weiterer Schwerpunkt im Berichtszeitraum war die Einrichtung des Datenschutzregisters (siehe Punkt 1.1.6). Die Meldungen hierzu waren schleppend eingegangen und größtenteils mit Fehlern behaftet. In einem Rundschreiben des TLfD vom 23.08.1994 wurden alle Ministerien und Landkreise auf die in Kraft getretene ThürDSRegVO hingewiesen. Da weiterhin eine große Anzahl der Meldungen zum Datenschutzregister fehlerhaft waren und es einen erheblichen Aufwand für den TLfD darstellt, diese Meldungen mit Korrekturhinweisen zu versehen und zurückzuschicken oder in Telefongesprächen mit den behördlichen Datenschutzbeauftragten auftretende Probleme beim Ausfüllen des Formulars zu klären, wurden Anfang Dezember 1994 alle behördlichen Datenschutzbeauftragten der Ministerien und der Landkreise eingeladen, um alle auftretenden Fragen im Zusammenhang mit den Datenschutzregistermeldungen zu besprechen.

Die Fehlerquote in den Meldungen ist seitdem zurückgegangen. Weiterhin auftretende Mängel stellen aber noch immer eine zusätzliche Arbeitsbelastung für den TLfD dar. Insbesondere werden mitunter weiterhin die in der ThürDSRegVO festgelegten Formvorschriften nicht beachtet. Einheitliche Formvorschriften dienen jedoch dazu, dem Bürger die übersichtliche Einsichtnahme in das Register gemäß § 12 ThürDSG zu ermöglichen.

Ungeachtet des vorhandenen Verwaltungsaufwandes ist die Führung des Registers gesetzlich vorgeschrieben. Indem jeder Bürger Einsicht in das Datenschutzregister nehmen kann und bei berechtigtem Interesse einen Anspruch auf Anfertigung eines Auszugs hat, wird ihm eine wertvolle Hilfestellung geleistet, wenn er sein Auskunftsrecht bei der entsprechenden Stelle wahrnehmen will. Außerdem kann der einzelne aus dem Datenschutzregister Hinweise zur Ausübung seines Auskunftsanspruches gegenüber der speichernden Stelle erhalten. Aus dem Datenschutzregister lassen sich auch für die Tätigkeit des TLfD, etwa für die Vorbereitung von Kontrollen, wertvolle Erkenntnisse gewinnen. Nicht zuletzt wird der datenverarbeitenden Stelle selbst die Gelegenheit zur Prüfung geboten, ob der gesamte gespeicherte Dateieninhalt benötigt wird und ob für die Speicherung auch eine Rechtsgrundlage besteht. Bei der Durchsicht der Formblätter fällt besonders auf, daß verschiedene öffentliche Stellen oftmals die spezialgesetzliche Regelung, die eine Verarbeitung der personenbezogenen Daten erlauben, gar nicht kennen. Dieses ist besonders gut bei einigen Meldebehörden zu erkennen, da das Thüringer Meldegesetz abschließend aufzählt, welche Daten hier zur Aufgabenerfüllung überhaupt gespeichert werden dürfen. Ohne die Führung eines Datenschutzregisters könnten unzulässige Speicherungen nur in weitaus geringerer Anzahl festgestellt werden.
In manchen Bereichen fehlen auch gesetzliche spezifische Regelungen, wie z. B. bei den Notaren, so daß auf die Erforderlichkeit zur Aufgabenerfüllung abgestellt werden muß, denn auch in diesen Bereichen soll der Vorteil der Einfachheit und Schnelligkeit durch automatisierte Datenverarbeitung genutzt werden.

Der Datenschutz steht infolge der immer schneller voranschreitenden technischen Entwicklung sicherlich gerade auch in der Zukunft vor großen Herausforderungen bezüglich der neuen technischen Möglichkeiten und deren Vereinbarkeit mit dem Recht auf informationelle Selbstbestimmung jedes Bürgers. Moderne Informationstechnologien in einer Informationsgesellschaft und Begriffe wie Multi-Media und Datenautobahn sind im Gespräch. Aus der Sicht des TLfD geht es dabei nicht darum, die technische Entwicklung einschränken zu wollen. Es muß jedoch ein Anliegen aller Beteiligten in der sich entwickelnden Informationsgesellschaft sein, datenschutzrechtliche Anforderungen an die neuen Technologien umzusetzen, um somit den Bürger vor Mißbrauch seiner personenbezogenen Daten zu schützen.

2.4 Der Beirat beim TLfD

Der gemäß § 41 ThürDSG beim TLfD gebildete Beirat besteht aus neun Mitgliedern. Für den Beirat bestellen sechs Mitglieder der Landtag, ein Mitglied die Landesregierung, ein Mitglied die kommunalen Spitzenverbände und ein Mitglied das Ministerium für Soziales und Gesundheit aus dem Bereich der gesetzlichen Sozialversicherungsträger. Für jedes Beiratsmitglied ist zugleich ein Stellvertreter bestellt. Die konstituierende Sitzung des Beirates fand am 12. April 1994 statt. Als Vorsitzender des Beirates wurde der Abgeordnete Bernd Wolf gewählt. Der Beirat arbeitet nach einer Geschäftsordnung. Die Mitglieder des Beirates sind in ihrer Tätigkeit an Aufträge und Weisungen nicht gebunden. Durch den Beirat wird der Landesbeauftragte in seiner Arbeit unterstützt. Vorrangige Unterstützung erfolgt durch die Beratung des Landesbeauftragten, aber auch dadurch, daß sich die Mitglieder des Beirates in ihren Organen für die Tätigkeit des Landesbeauftragten einsetzen. Der Landesbeauftragte hat den Beirat von wesentlichen Entscheidungen unterrichtet. In der Anfangszeit betraf dies insbesondere den Aufbau der Behörde des TLfD. Ausdrücklich im ThürDSG ist die Pflicht zur Verständigung des Beirates enthalten, wenn der Landesbeauftragte festgestellte Verletzungen von Vorschriften über den Datenschutz nach § 39 Abs. 1 ThürDSG beanstandet und deren Behebung fordert. In der Geschäftsordnung des Beirates wurde beschlossen, daß der TLfD vor Maßnahmen nach § 39 Abs. 2 Satz 2 ThürDSG, das betrifft die Verständigung des Landtags und der Landesregierung, dem Beirat Gelegenheit zur Stellungnahme gibt. Nach der Landtagswahl am 16.10.1994 wurden die aus dem Landtag zu bestellenden Beiratsmitglieder und stellvertretenden Mitglieder erneut vom Landtag gewählt. In der darauffolgenden Beiratssitzung wurde der Abgeordnete Bernd Wolf erneut zum Vorsitzenden des Beirates beim TLfD gewählt.
Im Berichtszeitraum fanden insgesamt 5 Beiratssitzungen statt.
Der vorliegende Bericht ist gemäß § 40 Abs. 4 ThürDSG im Beirat vorberaten worden.

2.5 Behördeninterner Datenschutzbeauftragter

Einige Kontrollbesuche haben gezeigt, daß behördeninterne Datenschutzbeauftragte (bDSB) nicht bei all jenen öffentlichen Stellen bestellt worden sind, bei denen dies vorgeschrieben bzw. empfohlen wird. Die öffentlichen Stellen des Landes sind nach Ziffer 34.2 der Verwaltungsvorschrift zum Vollzug des Thüringer Datenschutzgesetzes (VVThürDSG) verpflichtet, einen bDSB zu bestellen, wenn in der Regel mindestens 5 Beschäftigte in automatisierten und mindestens 20 Beschäftigte in nichtautomatisierten Verfahren personenbezogene Daten verarbeiten. Dasselbe gilt für Krankenhäuser mit mehr als 100 Betten sowie bei Auftragsdatenverarbeitung. Den Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Landes unterliegenden Personen des öffentlichen Rechts und deren Vereinigungen wird in der Verwaltungsvorschrift die entsprechende Verfahrensweise empfohlen. Da bei Kontrollen solcher Stellen mangels eines Sachwalters für den Datenschutz erhebliche Unsicherheiten im Umgang mit personenbezogenen Daten

festgestellt wurden, ist die Befolgung dieser Empfehlung anzuraten. Der bDSB sollte die notwendigen Fachkenntnisse in Fragen des Datenschutzes haben. Wichtiger ist jedoch, daß der bDSB nicht in Interessenkonflikte gerät. Insbesondere sollte eine gleichzeitige Wahrnehmung von Aufgaben in den Bereichen Personal, automatisierte Datenverarbeitung/ Informationstechnik sowie in Organisationseinheiten mit besonders umfangreicher oder sensitiver Verarbeitung von personenbezogenen Daten vermieden werden. Dies kommt auch in Ziffer 34.4 VVThürDSG zum Ausdruck, die vorsieht, nach Möglichkeit nicht den Leiter der Datenverarbeitung zum bDSB zu bestellen. Vielerorts bestellen daher die Behörden kurzerhand dessen Stellvertreter zum bDSB. Dies ist jedoch keine Lösung, da hier grundsätzlich derselbe Interessenkonflikt besteht.

Mit zunehmender Tendenz werden auch in den Gemeinden und Verwaltungsgemeinschaften entsprechend der Empfehlung der Landesregierung bDSB bestellt. Aufgrund des geringen Personalbestandes stellt sich dann häufig die Frage nach der Zulässigkeit, für mehrere Gemeinden und Verwaltungsgemeinschaften einen gemeinsamen oder auch einen Externen als Datenschutzbeauftragten zu bestellen. Der bDSB sollte neben organisatorischen und EDV-Kenntnissen insbesondere mit den Aufgaben und der Arbeitsweise der Behörde aus eigener - möglichst mehrjähriger - Erfahrung gut vertraut sein. Gleichzeitig muß er die dort geltenden gesetzlichen Regelungen kennen und sicher anwenden können. Dies ist erforderlich, um den Behördenleiter bei der Ausführung von Vorschriften zum Datenschutz zu unterstützen und zu beraten. Eine einseitige Orientierung auf Kenntnisse der Informationstechnik bzw. Datensicherungsmaßnahmen bei datenverarbeitenden Prozessen wird diesen Forderungen nicht in allen Fällen gerecht werden können.
Unbedingt zu beachten ist, daß beim bDSB eine Interessenkollision mit seiner sonstigen Tätigkeit ausgeschlossen werden muß. Aus datenschutzrechtlicher Sicht bestehen keine Bedenken, für mehrere (gleichartige) öffentliche Stellen einen gemeinsamen bDSB zu bestellen. Demgegenüber ist es zwar zulässig aber regelmäßig nicht empfehlenswert, Externe als bDSB zu bestellen. Eine entsprechende Bestellung sollte erst nach eingehender Prüfung unter Einbeziehung von Alternativen vorgenommen werden. Im Interesse einer späteren vertrauensvollen Zusammenarbeit ist es angeraten, den Personalrat hieran zu beteiligen.
Soweit im Ausnahmefall Externe als bDSB bestellt werden, ist zu sichern, daß diese Personen verpflichtet werden, alle im Rahmen ihrer Beratungs- und Kontrolltätigkeit zur Kenntnis gelangten Tatsachen und personenbezogene Daten geheimzuhalten.

3. Konferenzen und Arbeitskreise der DSB des Bundes und der Länder im Berichtszeitraum

Im Berichtszeitraum fanden vier Konferenzen der DSB des Bundes und der Länder statt. Dabei wurden die 47. und 48. unter der Leitung des Landesbeauftragten für den Datenschutz Brandenburg in Potsdam, die 49. und 50. unter Leitung des Bremer Datenschutzbeauftragten in Bremen bzw. Bremerhaven durchgeführt.
Die Entschließungen, die auf den Konferenzen unter Beteiligung und mit Zustimmung des TLfD verabschiedet wurden, beinhalten folgende Themen:
Entschließungen der 47. Konferenz vom 09./10.03.1994
- Ausländerzentralregistergesetz (Anlage 1)
- Informationsverarbeitung im Strafverfahren (Anlage 2)
- Abbau des Sozialdatenschutzes (Anlage 3)
- Chipkarten im Gesundheitswesen (Anlage 4)
- Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation (Anlage 5)

Entschließungen der 48. Konferenz vom 26./27.09.1994
- Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13.06.1994 (Anlage 6)
- Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (Anlage 7)
- Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedsstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL) (Anlage 8)
- Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen (Anlage 9)
- Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz (Anlage 10)
- Artikel 12 Verbrechensbekämpfungsgesetz (Anlage 11)

Entschließungen der 49. Konferenz vom 09./10.03.1995
- Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz) (Anlage 14)
- Maßhalten beim vorbeugenden personellen Sabotageschutz (Anlage 15)

- Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich (Anlage 16)
- Anforderungen an den Persönlichkeitsschutz im Medienbereich (Anlage 17)
- Sozialgesetzbuch VII - Verfassungsgemäßer Datenschutz für Unfallversicherte (Anlage 18)
- Eingeschränkter Zugriff auf Versicherungsdaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen (Anlage 19)
- Datenschutz bei Wahlen (Anlage 20)
- Automatische Erhebung von Straßennutzungsgebühren (Anlage 21)
- Datenschutz bei elektronischen Mitteilungssystemen (Anlage 22)

Entschließungen der 50. Konferenz vom 09./10.11.1995
- Weiterentwicklung des Datenschutzes in der Europäischen Union (Anlage 23)
- Planungen für ein Korruptionsbekämpfungsgesetz (Anlage 24)
- Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden) (Anlage 25)
- Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen (Anlage 26)
- Datenschutz bei der Neuordnung der Telekommunikation (Postreform III) (Anlage 27)

Im Berichtszeitraum wurden weiterhin folgende Entschließungen im Umlaufverfahren beschlossen:
- Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen (Anlage 28)
- Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) des Bundesministeriums für Post und Telekommunikation (Anlage 29)

Zwischen den Konferenzen der DSB des Bundes und der Länder sind entsprechende, nachfolgend aufgeführte Arbeitskreise tätig und befassen sich mit aktuellen datenschutzrechtlichen Themen:
- AK Personalwesen
- AK Medien
- AK Sicherheit
- AK Justiz
- AK Gesundheits- und Sozialwesen
- AK Statistik
- AK Wissenschaft
- AK Technik
- AK Umwelt/ Landwirtschaft
- AK Steuerverwaltung
- AK Europa

Diese Arbeitskreisberatungen fanden in der Regel ein- bis zweimal jährlich statt und haben neben der fachlichen Begleitung und Vorbereitung der Entschließungsentwürfe für die Konferenz der DSB folgende Aufgaben wahrzunehmen:
- Analyse der nationalen und internationalen Entwicklungen unter Einbeziehung von Fachexperten
- Erarbeitung von Orientierungshilfen und Richtlinien
- Erfahrungsaustausch zwischen den Vertretern der einzelnen Bundesländer

Wegen anstehender Fragen zum Ausländerrecht wurde im Zeitraum des Berichtes des weiteren die Ad-hoc-Arbeitsgruppe “Ausländerrecht” einberufen.

Darüber hinaus wurde für den Erfahrungsaustausch beim Aufbau des Datenschutzes in den neuen Ländern 1991 eine Arbeitsgruppe “Neue Länder” gegründet, an deren Sitzungen sich der TLfD im Berichtszeitraum ebenfalls beteiligte. Die Beratungen befaßten sich hauptsächlich mit speziellen Themen der neuen Bundesländer. Der Vorsitz für die 13. Beratung der Arbeitsgruppe “Neue Länder” am 20.09.1994 in Erfurt wurde vom TLfD übernommen. Die 15. Sitzung der Arbeitsgruppe “Neue Länder” war die letzte regelmäßige Sitzung der Arbeitsgruppe. In Zukunft werden jedoch bei Bedarf weiterhin Sitzungen zu konkreten Problemen stattfinden.

4. Datenschutzrelevante Regelungen in der EU

4.1 EG-Datenschutzrichtlinie

1990 legte die EG-Kommission einen Entwurf für ein EG-Datenschutzpaket vor. Nach intensiven Diskussionen und verschiedenen Änderungen hat das Europäische Parlament und der Rat der Europäischen Union nach dem gemeinsamen

Standpunkt des Rates vom 20. Februar 1995 und Beschluß des Europäischen Parlaments vom 15. Juni 1995 die 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 beschlossen. Diese EG-Datenschutzrichtlinie ist im Amtsblatt der Europäischen Gemeinschaft am 23. November 1995 veröffentlicht worden.
In der 50. Konferenz haben die DSB mit der Entschließung zur Weiterentwicklung des Datenschutzes in der Europäischen Union (Anlage 23) festgestellt, daß mit der EG-Datenschutzrichtlinie ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht wurde. Im materiellen Bereich wurde aber darauf hingewiesen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen.
Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26.05.1994, 08.09.1995) und die 48. Konferenz der DSB haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt worden zu sein.
Gemäß Artikel 32 der Richtlinie erlassen die Mitgliedstaaten die erforderlichen Rechts- und Verwaltungsvorschriften, um der Richtlinie binnen drei Jahren nach ihrer Annahme nachzukommen. Zur Umsetzung der EG-Datenschutzrichtlinie werden im Kreise der DSB mögliche notwendige Gesetzesänderungen des BDSG hinsichtlich des Anwendungsbereichs, der Zulässigkeit des Umgangs mit Daten, der Rechte der Betroffenen, der Durchführung technischer und organisatorischer Maßnahmen, der externen Kontrolle, des grenzüberschreitenden Datenumgangs, der Strafen und Haftung, des anwendbaren Rechts und der Datenschutzgruppe diskutiert. Die DSB werden eine entsprechende Novellierung aus datenschutzrechtlicher Sicht begleiten. Die DSB sind sich darüber einig, daß die Chancen, die sich aus der EG-Datenschutzrichtlinie über den unmittelbaren Anpassungsbedarf hinaus für eine Weiterentwicklung und Modernisierung des Datenschutzrechts ergeben, ausgeschöpft werden sollen. Zur Vorbereitung einer Entschließung zur Novellierung ist ein Ad-hoc-Arbeitskreis unter Vorsitz des BfD einberufen worden. Auch die Landesdatenschutzgesetze sind auf die erforderliche Anpassung zur Umsetzung der EG-Datenschutzrichtlinie zu überprüfen.
Nach Artikel 29 der EG-Datenschutzrichtlinie wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt. Die Gruppe besteht aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen und einem Vertreter der Stelle bzw. der Stellen, die für die Institutionen und Organe der Gemeinschaft eingerichtet sind, sowie einem Vertreter der Kommission. Die Gruppe ist unabhängig und hat beratende Funktion. Sie prüft alle Fragen im Zusammenhang mit der Umsetzung dieser Richtlinie und nimmt Stellung gegenüber der Kommission.

4.2 EG-Statistik-Verordnung

Im Zuge der Harmonisierung von Statistiken innerhalb der Europäischen Union streben die Mitgliedstaaten gemeinschaftsrechtliche Regelungen an, die sich auch auf die nationalen statistikrechtlichen Vorschriften, insbesondere die Gewährleistung des Statistikgeheimnisses, auswirken werden. Dazu liegt ein Vorschlag der Kommission der Europäischen Union für eine Verordnung des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistik-Verordnung) vor. Grundsätzlich kann man diese allgemeinen Regelungen auch aus Sicht der DSB begrüßen, dennoch bestehen im einzelnen teilweise erhebliche datenschutzrechtliche Bedenken, die auf der 48. Konferenz der DSB des Bundes und der Länder in ihrem Beschluß (siehe Anlage 7) ihren Niederschlag gefunden haben. So sieht der Vorschlag der Kommission insbesondere keine Trennung von Erhebungs- und Hilfsmerkmalen sowie keine Löschung personenbezogener Hilfsmerkmale vor. Solche Regelungen gehören in der Bundesrepublik Deutschland aber zum Kernbereich des Statistikrechts und wurden vom Bundesverfassungsgericht im Volkszählungsurteil aufgrund ihrer grundrechtssichernden Bedeutung gefordert.
Da in dieser Sache noch keine abschließenden Entscheidungen getroffen wurden, bleibt zu hoffen, daß sich die Bundesregierung im Rahmen der weiteren Verhandlungen mit der Europäischen Union für eine Berücksichtigung der von den DSB vorgelegten Änderungsvorschlägen und Hinweisen einsetzen wird.

4.3 Schengener Informationssystem - Durchführungsübereinkommen

Aufgrund des “Schengener Abkommens” vom 14.06.1985 wurde am 19.06.1990 zwischen den beteiligten Staaten Benelux, Frankreich und der Bundesrepublik Deutschland durch einen Staatsvertrag das “Schengener Durchführungsübereinkommen (SDÜ)” geschlossen, das am 26.03.1995 in Kraft getreten ist. In der Zwischenzeit sind auch Italien, Portugal, Spanien und Griechenland beigetreten, wobei das SDÜ in Italien und Griechenland nicht in Kraft gesetzt ist.
Das Schengener Durchführungsübereinkommen hat zum Wegfall der Kontrollen an den gemeinsamen Binnengrenzen geführt.

In datenschutzrechtlicher Hinsicht haben sich die Vertragsparteien verpflichtet, ihr nationales Datenschutzrecht bezüglich der nach dem Übereinkommen übermittelten Daten zumindest dem Standard anzupassen, der sich aus den Grundsätzen des Übereinkommens des Europarates über den Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28.01.1991 ergibt.
Wesentliche datenschutzrechtliche Bestandteile sind:
- die Zweckbindung übermittelter Daten,
- die Verpflichtung, auf die Richtigkeit der Daten zu achten und sie erforderlichenfalls zu berichtigen,
- die Möglichkeit der Geltendmachung von Schadensersatzansprüchen,
- die Protokollierung der Übermittlungsvorgänge,
- die Einrichtung einer unabhängigen Kontrollinstanz bei jeder Vertragspartei, die den nationalen Datenbestand zu überwachen hat,
- der Auskunftsanspruch der Betroffenen.

Mit der Übermittlung personenbezogener Daten darf erst begonnen werden, wenn die im Übereinkommen vorgesehenen datenschutzrechtlichen Regelungen in dem Hoheitsgebiet der an der Datenübermittlung beteiligten Vertragsparteien in Kraft getreten sind.

Mit Inkrafttreten des SDÜ ist auch das Schengener Informationssystem (SIS) in Betrieb genommen worden. Es besteht aus einem Zentralen System (ZSIS) mit Sitz in Straßburg und den nationalen Teilsystemen (NSIS) der angeschlossenen Vertragsstaaten, für die Bundesrepublik Deutschland beim BKA. Alle Informationen müssen über das ZSIS laufen, eine direkte Verbindung von nationalen Stellen untereinander besteht nicht. Es handelt sich um ein polizeiliches Fahndungssystem, mit dem Personen oder Sachen durch Ausschreibung in allen Vertragsstaaten gesucht werden können. Die Ausschreibung zur Suche erfolgt nach dem Recht des ausschreibenden Vertragsstaates. Es sollen Personen ausgeschrieben werden, um deren Festnahme mit dem Ziel der Auslieferung ersucht wird, deren Aufenthalt ermittelt und deren Einreise in einen Vertragsstaat verweigert werden soll. Der Betrieb und die Nutzung des SIS wird aus datenschutzrechtlicher Sicht weiter begleitet. In der gemeinsamen Kontrollinstanz nach Artikel 115 SDÜ wird die deutsche Delegation durch den BfD und den Hessischen Datenschutzbeauftragten vertreten.

5. Kommunale Angelegenheiten, Meldewesen, Ausländer, Sparkassen

5.1 Kommunales

5.1.1 Kommunalgesetze 1994

Die neuen Kommunalgesetze, bestehend aus der Thüringer Kommunalordnung, dem Thüringer Kommunalwahlgesetz sowie dem Thüringer Gesetz über kommunale Wahlbeamte, wurden bereits im Sommer 1993 zusammen mit der Kreisgebietsreform beschlossen, sind jedoch erst nach den Kommunalwahlen am 1. Juli 1994 in Kraft getreten. Doch schon vor den Kommunalwahlen hat der Thüringer Landtag am 25.03.1994 eine Änderung im Kommunalwahlgesetz beschlossen, die das Persönlichkeitsrecht der Bewerber berührt. Die bisherige Fassung sah in § 12 Abs. 2 bzw. § 24 Abs. 3 Satz 3 vor, daß nicht wählbar ist, wer gegenüber dem Gemeindewahlleiter die Abgabe einer schriftlichen Erklärung zu der Frage verweigert, ob er wissentlich als hauptamtlicher oder inoffizieller Mitarbeiter mit dem Ministerium für Staatssicherheit, dem Amt für Nationale Sicherheit oder Beauftragten dieser Einrichtungen zusammengearbeitet hat. Wird diese Frage wahrheitswidrig verneint, so verlieren die Gemeinderats- und Kreistagsmitglieder ihr Amt gemäß § 30 Abs. 1 Satz 2 ThürKWG.
Anknüpfungspunkt für die Nichtwählbarkeit bzw. den Verlust des Amtes ist also die Verweigerung der Antwort bzw. die wahrheitswidrige Verneinung der Frage nach einer Zusammenarbeit mit der Stasi, nicht jedoch die Zusammenarbeit als solche. Es soll der Wähler entscheiden, ob er einem Bewerber seine Stimme gibt, der solche Kontakte eingeräumt hat.

Bei der Vorbereitung der Kommunalwahlen war festgestellt worden, daß diese Intention nicht erreicht werden kann, wenn diese Erklärung des Bewerbers lediglich dem Gemeindewahlleiter gegenüber abgegeben werden kann, dieser jedoch mangels Rechtsgrundlage solche sensiblen personenbezogenen Daten nicht den Wählern bekanntgeben darf. Deshalb wurde in § 12 Abs. 2 und in § 24 Abs. 3 jeweils ein Satz hinzugefügt, der die Veröffentlichung dieser schriftlichen Erklärung zusammen mit dem Wahlvorschlag vorschreibt.

5.1.2 Behinderung des Kontrollrechtes des TLfD

Im Rahmen der Bearbeitung einer Beschwerde eines Bürgers war es erforderlich, eine Kontrolle in einer Stadtverwaltung durchzuführen. Der Bürgermeister war vom Landrat vom Dienst suspendiert worden. Deshalb mußte sich der TLfD an den stellvertretenden ehrenamtlichen Bürgermeister wenden, dem die Dienstgeschäfte übertragen worden waren. Aufgrund anhängiger gerichtlicher Auseinandersetzungen war trotz der Aufgabenübertragung an den ehrenamtlichen Bürgermeister nicht dafür gesorgt worden, daß diesem der Zugang zu allen Räumen und Unterlagen in der Stadtverwaltung ermöglicht wurde. Obwohl die Kontrolle angekündigt worden war, konnte dadurch der TLfD sein im ThürDSG garantiertes Recht auf uneingeschränkten Zutritt zu allen Diensträumen sowie Kontrolle und Einsichtnahme in alle vorhandenen Unterlagen und Akten mit personenbezogenen Daten nicht wahrnehmen.
Dies stellte eine Verletzung der Vorschriften über den Datenschutz gemäß § 38 ThürDSG dar und wurde gemäß § 39 ThürDSG beanstandet. Gleichzeitig wurde das Landratsamt darüber in Kenntnis gesetzt und aufgefordert, umgehend Maßnahmen zu treffen, die dem TLfD die erforderlichen Einsichts- und Zugangsrechte gewährleisten.

5.1.3 Wie umfassend darf der Bürgermeister informieren?

5.1.3.1 Was nicht durch den Bürgermeister veröffentlicht werden darf

Mit einer Eingabe, die von der örtlichen Landtagsabgeordneten unterstützt wurde, baten die Mitglieder einer unabhängigen Wählergruppe einer Thüringer Gemeinde den TLfD um Hilfe. Sie sahen in verschiedenen Handlungsweisen des Bürgermeisters und des Gemeinderats Pflichtverletzungen, die sie in einem Gespräch mit dem zuständigen Landrat benannt hatten. Dieser forderte die Petenten auf, ihm ihre Vorwürfe in schriftlicher Form zukommen zu lassen. Nachdem der Landrat die Unterlagen erhalten hatte, leitete er sie dem betreffenden Bürgermeister zur Stellungnahme weiter, der seinerseits Kopien anfertigte und an die Gemeinderatsmitglieder verteilte. Schließlich brachte der Bürgermeister an zwei Verkündungstafeln einen Anschlag an, in welchem er die Bürger aufforderte, diese Unterlagen einzusehen, die im Versammlungsraum des Dorfgemeinschaftshauses auslagen. In der Weitergabe ihrer Unterlagen, die auch die Namen und Adressen der Petenten enthielten, an den Bürgermeister und den Gemeinderat sowie in der öffentlichen Auslegung sahen die Petenten eine Verletzung datenschutzrechtlicher Vorschriften.

Die Weiterleitung der als Dienstaufsichtsbeschwerde zu qualifizierenden Unterlagen durch den Landrat an den Bürgermeister zur Stellungnahme war nicht zu beanstanden, da das Landratsamt als untere staatliche Verwaltungsbehörde nach Thüringer Kommunalrecht für die Bearbeitung von Dienstaufsichtsbeschwerden gegen Bürgermeister zuständig ist. Nach dem Untersuchungsgrundsatz ist es erforderlich, daß der betroffene Amtsträger die gegen ihn erhobenen Vorwürfe einschließlich der Adressaten zur Kenntnis bekommt, um hierzu umfassend Stellung nehmen zu können. Auch die Übermittlung der Beschwerde an die Mitglieder des Gemeinderates war als erforderlich zur Abgabe einer Stellungnahme des Bürgermeisters anzusehen, da u. a. auch die Arbeit des Gemeinderates kritisiert worden war.

Dagegen war die öffentliche Auslegung der Unterlagen sowie der Aushang eines entsprechenden Hinweises rechtswidrig. Nach einer entsprechenden Aufforderung an die Rechtsaufsichtsbehörde durch den TLfD wurde die Offenlegung der Unterlagen im Dorfgemeinschaftshaus eingestellt. Da nicht zu ermitteln war, ob tatsächlich Bürger von den Unterlagen Kenntnis genommen haben, ist zumindest von einer unzulässigen Nutzung personenbezogener Daten auszugehen (eine Übermittlung würde die Kenntnisnahme voraussetzen), da für die Abgabe der Stellungnahme durch den Bürgermeister in keiner Weise erforderlich war, die Möglichkeit zu schaffen, jedermann Einsicht in diese personenbezogenen Daten zu gewähren. Diese festgestellte Verletzung von Vorschriften über den Datenschutz hat der TLfD gegenüber der Gemeindeverwaltung förmlich beanstandet und um Mitteilung gebeten, welche Vorkehrungen getroffen werden, um derartige Datenschutzverstöße in Zukunft zu vermeiden.

5.1.3.2 Unzulässige Veröffentlichung im Amtsblatt

Ende 1994 wurde der TLfD darauf hingewiesen, daß in einem amtlichen Mitteilungsblatt eine Stadtverwaltung zum Thema “Verkehrssicherheit für Schulkinder” einen Artikel veröffentlicht hatte. Darin informierte sie insbesondere über Gefahrenschwerpunkte im Straßenverkehr (wie fehlende Bürgersteige), begründete die Notwendigkeit für die Festlegung von Parkverboten bei unübersichtlichen Straßenabschnitten, aber auch die bisherige “Untätigkeit” in einigen Fällen.
Diese Form der Information der Bürger ist sicher begrüßenswert, wenn dabei nicht die Kommunalverwaltung über das Ziel hinausgegangen wäre. Im vorliegenden Fall war man davon ausgegangen, daß durchaus jeder Bürger das Recht in Anspruch nehmen kann, darüber informiert zu werden, warum bisher bestimmte Entscheidungen nicht getroffen worden waren bzw. weshalb einige Arbeiten noch nicht durchgeführt wurden. Da in einigen Fällen das Haupthindernis

für eine beabsichtigte Veränderung die noch nicht erfolgte freiwillige Veräußerung von Grundstücksteilen an die Gemeinde zur Schaffung von Bürgersteigen durch bestimmte Eigentümer war, glaubte man berechtigt zu sein, diese im Amtsblatt namhaft zu machen. Ebenso hatte sich im Rathaus ein Handwerksbetrieb, möglicherweise auch in unangemessener Form, gegen das aus seiner Sicht unangemessene und ökonomisch schädigende Parkverbot vor seinem Grundstück geäußert. Diese Verhaltensweisen der betroffenen Bürger, die teilweise im Rahmen von Verwaltungsverfahren zum Ausdruck gebracht worden waren, wurden zum Anlaß genommen, die Einwohner der Stadt ausführlich unter Nennung der Namen von Privatpersonen zu informieren, welche Probleme die Stadtverwaltung ständig zu lösen hat. Diese Verfahrensweise widerspricht jedoch allen Bestimmungen zur Amtsverschwiegenheit der Bediensteten der Stadtverwaltung. Es darf nicht sein, daß Amtsblätter Austragungsort von Verwaltungsangelegenheiten sind, in denen die Kommunalverwaltung von ihrem Standpunkt aus zu Verwaltungsverfahren bzw. zu Fragen des persönlichen Verhaltens von Bürgern Stellung bezieht. Aus diesem Grund wurde seitens des TLfD der Vorgang zum Anlaß genommen, in der Stadtverwaltung ausführlich über die Probleme der Amtsverschwiegenheit zu sprechen. Als Ergebnis wurde festgestellt, daß die Veröffentlichung von personenbezogenen Daten in diesem Artikel auf einer fehlerhaften Auslegung der einschlägigen Datenschutzbestimmungen in bezug auf "das öffentliche Interesse" begründet war. Da es sich um eine kleine Stadt handelte, herrschte dort die Auffassung, daß das Informationsbedürfnis der Bevölkerung eine Veröffentlichung rechtfertigen würde, wobei die Fakten im wesentlichen den Bürgern auch bereits bekannt waren. In Auswertung der Vorfalles mit den Amtsleitern der Stadtverwaltung wurde festgehalten, daß künftig personenbezogene Daten im Amtsblatt nur veröffentlicht werden, wenn dies eine Rechtsvorschrift erlaubt, es sich um öffentlich-zugängliche Daten handelt oder der Betroffene zugestimmt hat. Abschließend sollte an dieser Stelle noch vermerkt werden, daß, obwohl keine Beschwerde der Betroffenen vorlag, sich der Bürgermeister öffentlich für die Namensnennung im folgenden Amtsblatt entschuldigt und darauf hingewiesen hat, daß künftige Namensnennungen unterbleiben werden.

5.1.3.3 Falsch verstandenes öffentliches Interesse

Zwei Kindergärtnerinnen einer Gemeinde wandten sich mit folgendem Problem an den TLfD:
Eltern hatten in einem Kindergarten den zuständigen Bürgermeister sowie die örtliche Presse eingeladen, um die bevorstehende Schließung eines Kindergartens zu verhindern. In seinen Ausführungen begründete der Bürgermeister unter anderem die beabsichtigte Schließung mit der hohen finanziellen Belastung für die Gemeinde. Dabei begnügte er sich nicht mit einer Gesamtdarstellung der Lohnkosten, sondern fühlte sich gegenüber der Öffentlichkeit verpflichtet, detailliert für jede Kindergärtnerin, die monatlichen Gehaltszahlungen bekanntzugeben. Daß er damit gegen geltendes Datenschutzrecht, insbesondere gegen die ihm auferlegte Amtsverschwiegenheit, sowie gegen den Grundsatz der internen Vertraulichkeit von Personaldaten verstoßen hatte, war ihm offensichtlich nicht bewußt. Auch die Dienstaufsichtsbehörde erkannte zunächst die Problematik der unzulässigen Offenbarung von Personaldaten nicht, so daß erst eine entsprechende Nachfrage des TLfD dazu führte, sich erneut mit der Problematik auseinanderzusetzen und den Bürgermeister auf sein gesetzwidriges Handeln hinzuweisen. Von einer Beanstandung seitens des TLfD wurde dennoch aufgrund der Versicherung, daß eine Wiederholung künftig ausgeschlossen wird, abgesehen.

5.1.4 Was darf ein "Staatskommissar" über die Stadträte wissen?

Der Bürgermeister einer Stadt war bei der Abwicklung der Erschließung eines - im nachhinein als überdimensioniert erkannten - Industriegebietes derart überfordert, daß ihm durch die zuständige Rechtsaufsichtsbehörde dieser Aufgabenbereich entzogen werden mußte. Gleichzeitig wurde ihm ein Beauftragter gemäß § 122 Abs. 1 ThürKO beigegeben, der sozusagen als "Staatskommissar" die Funktion des Bürgermeisters für diese Aufgabe übernahm.
In einer Eingabe einer Stadtratsfraktion, die übrigens bis heute noch nicht durch Unterschrift autorisiert ist, wurde bezweifelt, daß der Beauftragte sich die Namen, Adressen, Geburtsort und -datum, Beruf und Parteizugehörigkeit der Stadträte aus den städtischen Unterlagen vorlegen lassen kann. Diese Angaben sind durch die Bekanntmachung der Wahlvorschläge und die Vorstellung der Kandidaten in der Presse allgemein bekannt. Der Beauftragte, der neu in die Stadt kommt, ist zur ordnungsgemäßen Aufgabenerfüllung auf diese Angaben angewiesen, zumal er insoweit partiell in die Funktion des Bürgermeisters eintritt. Sollte die anfragende Stadtratsfraktion Ihre Eingabe noch autorisieren, wird der TLfD sie entsprechend unterrichten.

5.1.5 Verwendung der Kontoverbindung durch die Gemeinde zur Vollstreckung?

Von einem anderen DSB ist die Frage aufgeworfen worden, ob eine Gemeinde die Bankverbindung eines Bürgers zu Vollstreckungszwecken nutzen darf, wenn diese für einen anderen Zweck, z. B. Abbuchung der laufenden Kindergartengebühren, der Gemeinde mitgeteilt worden war. Eine Anfrage des TLfD beim LVwA als oberer Rechtsaufsichtsbe-

hörde ergab, daß dort derartige Problemfälle bisher nicht bekannt sind. Daraus ist jedoch nicht zwingend zu schließen, daß solche zweckändernde Nutzungen in Thüringer Kommunen nicht erfolgen. Für Thüringen stellt sich die Rechtslage wie folgt dar:
Da es sich bei der Verwendung der Kontoverbindung zur Vollstreckung um eine Nutzung zu einem anderen als dem ursprünglichen Zweck handelt, ist dies nur zulässig, sofern eine Rechtsvorschrift dies erlaubt oder der Betroffene hierzu eingewilligt hat (§ 4 Abs. 1 ThürDSG). Hierbei sind drei Fälle zu unterscheiden. Ist der Gemeinde eine Kontoverbindung aus einem Steuerverfahren, das kommunale Steuern oder den Fremdenverkehrsbeitrag betrifft, bekannt, so darf sie diese auch zur Vollstreckung in einem anderen Steuerverfahren verwenden. Dies ergibt sich aus § 15 Abs. 1 Satz 1 Nr. 1c Thüringer Kommunalabgabengesetz (ThürKAG) in Verbindung mit § 30 Abs. 4 Nr. 1 Abgabenordnung. Will die Gemeinde eine Bußgeldentscheidung vollstrecken, so darf sie ihr auch anderweitig bekanntgewordene Kontoverbindungen nach § 20 Abs. 2 Nr. 7 ThürDSG hierzu nutzen. In allen übrigen Fällen ist eine Nutzung von Kontoverbindungen zur Vollstreckung nach § 20 Abs. 2 Nr. 6 ThürDSG zulässig, wenn es zur Abwehr erheblicher Nachteile für das Gemeinwohl erforderlich ist. Ein erheblicher Nachteil für das Gemeinwohl droht nicht immer schon dann, wenn nicht gewährleistet ist, daß die Kommunen ihre Außenstände schnell und kostengünstig eintreiben können. Es muß vielmehr eine konkrete Einzelfallprüfung durchgeführt werden. Dabei ist nicht unbedingt die Höhe der einzelnen gemeindlichen Forderungen ausschlaggebend, da bei einer Häufung von säumigen Schuldnern und der damit verbundenen Außenstände die Funktionsfähigkeit einer Gemeinde gefährdet wäre und somit auch erhebliche Nachteile für das Gemeinwohl zu bejahen sind. Andererseits ist eine erhebliche Gefahr für das Gemeinwohl nicht zu besorgen, solange es in der Gemeinde - abgesehen von Einzelfällen - keine Erfahrungen gibt, daß säumige Schuldner auf Nachfrage nach der Kontoverbindung die Vollstreckung dadurch verzögern oder vereiteln, daß sie die Konten nicht nennen oder diese auflösen.
Hat der Betroffene bei der erstmaligen Bekanntgabe seiner Kontoverbindung gegenüber der Gemeinde nicht schriftlich darin eingewilligt, daß die Gemeinde diese zu Vollstreckungszwecken nutzen darf, so muß die Gemeinde bei einer beabsichtigten Zweckänderung die dargestellte Einzelfallprüfung vornehmen.

5.1.6 Öffentlicher Aushang des Aufgebotes noch zeitgemäß?

In § 12 Ehegesetz (EheG) in Verbindung mit § 3 Personenstandsgesetz (PStG) ist die Verpflichtung der Standesämter zur Veröffentlichung des Aufgebotes vor einer Eheschließung enthalten. Von dem Aufgebot kann gemäß § 12 EheG der Standesbeamte Befreiung erteilen. Aufgrund einer entsprechenden Anfrage hatte sich der TLfD damit zu befassen, ob solch ein Verfahren heute noch erforderlich und zeitgemäß ist, da auf diesem Weg kaum das Ziel, Ehehindernisse zu erkennen, erreicht wird. Daß diese Fragestellung nicht nur in Thüringen aufgeworfen wurde, zeigt eine Erklärung des Bundesinnenministeriums vom 10.02.1995, in der es heißt: “Eine Umfrage bei verschiedenen Standesbeamten ergab, daß in den letzten Jahren nicht ein einziges Mal aufgrund dieses Aushanges dem Standesbeamten ein Ehehindernis mitgeteilt worden war. Die Ermittlung von möglichen Ehehindernissen ist aber der einzige Zweck dieser Regelung.” Nach Rückfrage beim TMJE wurde von dort signalisiert, daß man einer Gesetzesänderung aufgeschlossen gegenüberstehe.
Zwischenzeitlich liegt ein Gesetzentwurf zur Neuordnung des Eheschließungsrechts (Eheschließungsrechtsgesetz) vor. Dieser Entwurf sieht unter anderem die Abschaffung des Aufgebotes vor. Damit wurde nicht nur den Forderungen des Datenschutzes, Eingriffe in das Grundrecht auf informationelle Selbstbestimmung auf das Notwendigste zu beschränken, sondern auch den Vorstellungen der unabhängigen Kommission für Rechts- und Verwaltungsvereinfachung des Bundes entsprochen. Hierbei zeigt sich auch, daß Datenschutz keinesfalls ein Hemmnis der Verwaltung darstellt, sondern durchaus einen wesentlichen Beitrag zur Verringerung des Verwaltungsaufwandes leisten kann.

5.1.7 Anfrage zum Familienbuch

Im Rahmen einer Anfrage zum Verfahren beim Anlegen eines Familienbuches auf Antrag gemäß § 15a PStG wurde der TLfD um die datenschutzrechtliche Prüfung der Erforderlichkeit für eine Datenübermittlung an Dritte bei der im Verfahren vorgenommenen Anhörung gebeten. Gemäß § 12 Abs. 2 Nr. 2 PStG werden in das Familienbuch die Vor- und Familiennamen sowie Wohnort bzw. letzter Wohnort der Eltern der Ehegatten eingetragen. Dazu sind beim Anlegen des Familienbuches auf Antrag nach § 15a Abs. 2 PStG die im Familienbuch einzutragenden Personen vorher anzuhören.
Nach Auskunft der Thüringer Standesämter wird dazu gegenwärtig den Anzuhörenden der Antrag bzw. ein Abdruck davon zur Kenntnisnahme vorgelegt. Im Vordruck zur “Erklärung eines Beteiligten/ Zeugen zum Antrag auf Anlegung eines Familienbuches” soll dieser die Richtigkeit der Angaben bestätigen, insbesondere durch die Ankreuzung unter: “Ich bestätige die Richtigkeit der in diesem Antrag ... gemachten Angaben.” Datenschutzrechtlich bedenklich erscheint es aber, daß durch die Kenntnisgabe des vollständigen Antrages die Daten Dritter (zum Beispiel die Daten der Schwiegerkinder den Schwiegereltern) bekanntgegeben werden. Fraglich ist, inwiefern - im Gegensatz zur Anlegung des Familienbuches im Anschluß an die Eheschließung nach § 12 PStG - bei der Anlegung des Familienbuches auf

Antrag nach § 15a PStG eine Anhörung sämtlicher Personen, die in das Familienbuch eingetragen sind, erforderlich ist. Bei der Anlegung eines Familienbuches auf Antrag ist der Standesbeamte nach § 15a Abs. 2 Satz 2 PStG zwar verpflichtet, sämtliche Personen, die in das Familienbuch einzutragen sind, zu hören. Diese Vorschrift schreibt jedoch nicht vor, daß jeweils allen in das Familienbuch einzutragenden Personen alle einzutragenden Daten mitgeteilt werden müssen. Vielmehr sind die Umstände des jeweiligen Einzelfalls für den Umfang der erforderlichen Anhörung maßgebend.
Der TLfD hat dem TIM deshalb mitgeteilt, daß das im Fall des Beschwerdeführers praktizierte Verfahren, nicht zuletzt im Hinblick darauf, daß Eintragungen in das Familienbuch gemäß § 15b Abs. 1 PStG grundsätzlich aufgrund von Eintragungen in anderen Personenstandsbüchern oder von öffentlichen Urkunden vorzunehmen sind, nicht mit dem Verhältnismäßigkeitsprinzip vereinbar sei. Der TLfD hat angeregt, daß die Standesbeamten, wenn auf andere Weise noch nicht ausreichend belegt, den anzuhörenden Personen stets nur solche Daten bekanntgegeben werden sollten, bei denen feststeht, daß die Anzuhörenden aufgrund von detaillierten Kenntnissen tatsächlich zur Feststellung der Richtigkeit und Vollständigkeit dieser Daten beitragen können. Aus datenschutzrechtlicher Sicht ist wünschenswert, das Verfahren nach § 15a PStG an das der Anlegung des Familienbuches im Anschluß an die Eheschließung nach § 12 PStG insofern anzupassen, daß auf eine Anhörung in den Fällen verzichtet werden kann, in denen die Antragsteller alle Angaben mit Urkunden im Sinne des § 15b Abs. 1 PStG ausreichend belegen können.

In dem in diesem Zusammenhang vom TIM zugeleiteten Entwurf eines Gesetzes zur Neuordnung des Eheschließungsrechts sind zwar auch Änderungen zum Personenstandsgesetz vorgesehen, nicht aber eine Änderung der die Anhörung betreffenden Regelungen. Vom BfD wurde mitgeteilt, daß nach dort vorliegenden Erkenntnissen seitens der mit der Erarbeitung von Vorschlägen für die Änderung des Personenstandsgesetzes beauftragten Bund-Länder-Arbeitsgruppe die Thematik dieser Datenübermittlung im Rahmen der Anhörung zur Anlegung des Familienbuches auf Antrag gemäß § 15a Abs. 2 PStG bereits erörtert wurde und Einigkeit darüber erzielt worden sei, daß nicht sämtliche Familienangehörige gehört werden müssen, wenn der Sachverhalt durch inländische Urkunden hinreichend geklärt werden kann. Der BfD nimmt an, daß ihm das Bundesministerium des Innern in Kürze einen Vorentwurf zur Änderung des Personenstandsgesetzes hinsichtlich einer Anhörung wegen Anlegung eines Familienbuches auf Antrag zur Prüfung zuleiten wird. Der TLfD wird die Angelegenheit weiter verfolgen.

5.1.8 Geburtsdatum als Aktenzeichen auf Abgabebescheid

In einer Eingabe machte ein Petent darauf aufmerksam, daß von einer Stadtverwaltung Bescheide zur Feuerschutzabgabe mit einem Aktenzeichen versehen werden, das sich aus dem Geburtsdatum (Geburtsjahr, -monat, -tag) des Betroffenen zusammensetzt. Aus der Sicht des TLfD war dieses Verfahren datenschutzrechtlich nicht unbedenklich, da nicht auszuschließen war, daß im Rahmen des Schriftverkehrs zum Vorgang (z. B. Einsprüche, Beschwerden usw.) das Geburtsdatum einem Personenkreis zugänglich gemacht wird, der diese Daten zur Aufgabenerfüllung nicht benötigt.
In der Stellungnahme zum Sachverhalt erklärte die Stadtverwaltung, daß die Verwendung des Geburtsdatums des Adressaten als Aktenzeichen seitens der Stadtverwaltung nur bei der Erhebung der Feuerschutzabgabe erfolgt. Es wurde versichert, daß der Feuerschutzabgabebescheid nur dem Empfänger direkt zugestellt wird. Eine anderweitige Verwendung dieses Aktenzeichens erfolge nicht. Als Grund für die Anwendung dieses Aktenzeichens wurde angegeben, daß zur Zahlung der Feuerschutzabgabe nur Bürger mit dem vollendeten 18. Lebensjahr bis zum vollendeten 60. Lebensjahr verpflichtet sind. Somit wird es für die Stadtverwaltung möglich, durch Aufrufung der Jahrgänge nur den betreffenden Personenkreis anzusprechen. Dies ist nach Aussage der Stadtverwaltung die effektivste Möglichkeit, diese Bescheide zu erteilen.
Mit der Maßgabe, daß sicherzustellen ist, daß eine anderweitige Verwendung des Aktenzeichens nicht erfolgt, wurde aus datenschutzrechtlicher Sicht von einer Beanstandung abgesehen. Im Fall einer begründeten Bürgerbeschwerde hat sich aber der TLfD die Beanstandung hinsichtlich der Verwendung des Geburtsdatums als Aktenzeichen ausdrücklich vorbehalten.

5.2 Meldewesen

5.2.1 Thüringer Meldegesetz

Rechtsgrundlage für das Meldewesen in Thüringen ist das Thüringer Meldegesetz vom 23. März 1994, das den Vorgaben des Melderechtsrahmengesetzes einschließlich der Novelle vom 20.03.1994 entspricht (siehe Punkt 1.1.1). Bei der Auslegung und Fortentwicklung des Melderechts ist aus Sicht des Datenschutzes allerdings darauf zu drängen, daß die Übermittlung und Erhebung der Daten auf die jeweilige Aufgabenerfüllung der Behörde beschränkt bleibt und dies auch durchgesetzt wird. Ein erster Schritt hierzu ist die am 01.03.1995 in Kraft getretene Meldescheinverordnung, die alle Meldebehörden zur Verwendung von einheitlichen, den Anforderungen des Meldegesetzes entsprechenden

Formularen verpflichtet. Dies ist zu begrüßen, da hierdurch Fehler bei der Entwicklung eigener Formulare vermieden werden. Um einen unkontrollierten regelmäßigen Meldedatenfluß innerhalb der Landes- und Kommunalbehörden zu vermeiden, wird zur Zeit vom TIM eine erste Thüringer Meldedatenübermittlungsverordnung vorbereitet. Dem TLfD wurde die Möglichkeit eingeräumt, zu einem ersten Entwurf Stellung zu nehmen, wovon auch Gebrauch gemacht wurde. Das TIM hat zwischenzeitlich signalisiert, die gegebenen Hinweise und Anregungen zum größten Teil übernehmen zu wollen.

5.2.2 Unterlagen und Verfahren zur Führung des Melderegisters

Mit Auflösung des Zentralen Einwohnerregisters und Übernahme der Meldedaten in kommunale Verantwortung wurden in den Meldebehörden die unterschiedlichsten Softwareprogramme zur Führung automatisierter Melderegister zur Anwendung gebracht. Dabei wählten viele Landratsämter und Gemeinden die jeweils für sie zu diesem Zeitpunkt kostengünstigste Variante aus. Daß dies auf Dauer nicht unbedingt die zweckmäßigste Lösung ist, zeigt sich nunmehr an den Stellen, an denen aufgrund neuer Rechtsvorschriften Programmänderungen erforderlich werden. Nach Verabschiedung des ThürMeldeG auf der Grundlage des novellierten MRRG bereitete es nach Feststellungen des TLfD einigen Meldeämtern offensichtlich Schwierigkeiten, die vom Gesetzgeber eingeräumte Frist für die erforderliche Anpassung der automatisierten Programme bis zum Jahresende 1995 einzuhalten. Ursachen dafür liegen u. a. in einer teilweise unbefriedigenden Vertragsgestaltung mit den Softwarefirmen sowie auch an fehlenden eigenen EDV-technischen Kapazitäten. Bei allem Verständnis für diese Probleme ist jedoch kritisch anzumerken, daß selbst bei Kontrollen im 3. Quartal 1995 festgestellt wurde, daß von einigen Meldebehörden bisher noch keinerlei Aktivitäten zur Programmänderung erfolgt waren. Es ist zu hoffen, daß dennoch alle Meldebehörden bis Ende 1995 diese Aufgabenstellung erfüllt haben. Dieses zu überprüfen, wird eine der nächsten Aufgaben des TLfD sein.

Neben dem automatisierten Melderegister werden noch zusätzlich in einigen Meldebehörden die vorhandenen Meldekarteien fortgeführt. Es ist nicht Aufgabe des TLfD, die Zweckmäßigkeit zu beurteilen. Zumindest bestehen aus datenschutzrechtlicher Sicht gegen diese Verfahrensweise keine Bedenken, wenn gewährleistet ist, daß die Karteien nur Daten enthalten, die im ThürMeldeG abschließend benannt sind. Da auf den Meldekarteikarten der ehemaligen DDR aus den Jahren vor 1990 weitere Daten (wie z. B. Wehrdienst- und Haftzeiten) eingetragen waren, hatten das TIM sowie das LVwA als zuständige Aufsichtsbehörde mehrmals darauf hingewiesen, daß bei einer beabsichtigten weiteren Nutzung der alten Karteikarten, diese entsprechend zu bereinigen, d. h. die unzulässig gespeicherten Daten gemäß § 11 Abs. 1 ThürMeldeG zu löschen (unkenntlich zu machen) sind. Um alle Mißverständnisse auszuschließen und um den Meldebehörden auch die erforderliche Zeit zur Überprüfung einzuräumen, hatte bereits der Gesetzgeber 1994 in einer Überleitungsbestimmung (§ 43 ThürMeldeG) festgelegt, daß alle Daten, die bei Inkrafttreten des ThürMeldeG in den Melderegistern gespeichert sind und über die in § 3 genannten Daten hinausgehen, innerhalb eines Jahres gelöscht werden müssen. Ungeachtet dieser Regelungen wurde bei Prüfungen in zwei Meldebehörden festgestellt, daß ohne Beachtung der geforderten Löschung die Fortschreibung der alten Meldekarteien erfolgte. Dies wurde gemäß § 39 ThürDSG beanstandet. Die Behörden wurden aufgefordert, unverzüglich die Löschung der Daten vorzunehmen. Gleichzeitig wurde darauf hingewiesen, daß Unterlagen, die für die Aufgabenerfüllung nicht mehr benötigt werden, dem zuständigen Archiv zur Übernahme angeboten werden sollten. Dies ist zwischenzeitlich erfolgt.

5.2.3 Online-Meldedatenabruf in der Gemeindeverwaltung

Im Rahmen der zunehmenden Vernetzung innerhalb der Verwaltung ist festzustellen, daß größere Stadtverwaltungen, die über eigene Meldeämter verfügen, zur Erleichterung ihrer Arbeit automatisierte Abrufverfahren einrichten, durch die einzelnen Ämtern der Stadtverwaltung die Möglichkeit eingeräumt wird, unmittelbar auf Meldedaten zuzugreifen. Dies ist zulässig, da automatisierte Abrufverfahren nur außerhalb der Gemeindeverwaltung in Form regelmäßiger Datenübermittlungen gemäß § 29 ThürMeldeG einer entsprechenden landesrechtlichen Regelung bedürfen. Voraussetzung für die Einrichtung von Online-Verfahren ist, daß diese Ämter die Meldedaten zur Erfüllung der in der Zuständigkeit der Meldebehörde oder in der des Empfängers liegenden Aufgabe benötigen. Aufgrund zusätzlicher Gefahren und Risiken bei automatisierten Abrufverfahren ist vor der Einrichtung eine umfassende Prüfung hinsichtlich der Angemessenheit dieser Maßnahme vorzunehmen. Dazu ist es notwendig, abzuwägen, ob wegen der Dringlichkeit und Häufigkeit von Datenanforderungen die Einrichtung eines Online-Anschlusses anstelle anderer Formen der Weitergabe geboten ist. Selbstverständlich muß der Umfang der Datenweitergabe dem Erforderlichkeitsgrundsatz entsprechen. Ebenso muß den Forderungen der Datensicherheit z. B. durch eine stichprobenartige Protokollierung der einzelnen Abrufe Rechnung getragen werden.
Anhaltspunkte dafür, daß diese Voraussetzungen nicht bei allen Abrufverfahren vorliegen, führten dazu, daß seitens des TLfD Verwaltungen aufgefordert wurden, die Zulässigkeit bereits eingerichteter Abrufverfahren erneut einer Prüfung

zu unterziehen. Dies betrifft zum Beispiel den Online-Zugriff auf Meldedaten durch statistische Ämter. Auf Nachfrage wurde dem TLfD mitgeteilt, daß einem statistischen Amt zur Aufgabenerfüllung der ständige Zugriff auf Meldedaten im Rahmen einer einfachen "Melderegisterauskunft" eingerichtet worden war. Dies erfolgte zum einen für eigene Zwecke, zum anderen "im Auftrag des Meldeamtes zur gelegentlichen Aufbereitung von Gruppenauskünften an Dritte, wenn eine besondere Repräsentativität für diese Auskunft erforderlich ist und dies nach Feststellung des Meldeamtes im öffentlichen Interesse liegt". Als Rechtsgrundlage für die Zulässigkeit wurde auf die Regelungen zur einfachen Melderegisterauskunft verwiesen.
Diese Regelungen gelten jedoch nur für nicht-öffentliche Stellen. Danach können Personen von den Meldebehörden Auskunft über einzelne bestimmte Einwohner oder eine Vielzahl namentlich bezeichneter Einwohner bezüglich des Vor- und Familiennamens, des Doktorgrades und der Wohnanschrift erhalten. Demgegenüber ist die Nutzung der Datenbestände des Meldeamtes durch andere Ämter innerhalb einer Gemeinde nur zulässig, wenn es zur Erfüllung der in der Zuständigkeit des Meldeamtes oder in der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich ist. Für statistische Erhebungen werden personenbezogene Einwohnerdaten ausschließlich für die technische Durchführung als Hilfsmittel benötigt. Auf der Grundlage einer Satzung zur Durchführung einer (bestimmten) Kommunalstatistik nach dem Thüringer Statistikgesetz (ThürStatG) kann die Meldebehörde dem statistischen Amt eine Anschriftenliste von Auskunftspflichtigen übergeben. Ein unmittelbarer Zugriff auf Meldedaten aller Einwohner ist für diese Aufgabenerfüllung nicht erforderlich und deshalb unzulässig. Das trifft selbstverständlich nicht nur für den Zugang zu den Meldekarteien, sondern im besonderen Maße auch auf elektronisch gespeicherte Datenbestände zu. Soweit bevölkerungsstatistische Erhebungen vom statistischen Amt durchgeführt werden, zum Beispiel im Rahmen von Geschäftsstatistiken für das Meldeamt, ist gleichfalls der Zugriff des statistischen Amtes auf Einzeldatensätze nicht erforderlich. Eine Dienstleistung des statistischen Amtes im Rahmen einer Auftragsdatenverarbeitung für das Meldeamt würde gegen § 20 Abs. 1 ThürStatG verstoßen, wonach Statistikstellen keine nichtstatistischen Aufgaben des Verwaltungsvollzuges wahrnehmen dürfen.

5.2.4 Melderegisterauskünfte

5.2.4.1 Kein "Jubiläumsmelderegister" beim Bürgermeister

Häufig wird von Bürgermeistern der Wunsch geäußert, über bestimmte, ständig aktualisierte Meldedaten aller Einwohner der Gemeinde oder des jeweiligen Ortsteiles zu verfügen. Gemäß § 29 ThürMeldeG ist innerhalb der Gemeinde eine Weitergabe von Meldedaten an andere Stellen zulässig, soweit dies zur Erfüllung der in der Zuständigkeit der Meldebehörde oder der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich ist, so daß auch im Einzelfall dem Bürgermeister bzw. Ortsteilbürgermeister Daten aus dem Melderegister zur konkreten Aufgabenerfüllung gemäß § 29 bzw. § 45 ThürKO zweckgebunden übermittelt werden dürfen. Die Führung eines zweiten Melderegisters erlaubt jedoch das ThürMeldeG nicht, ebenso wie jede Datenvorratshaltung. Dementsprechend hat der TLfD bei entsprechenden Anfragen darauf hingewiesen, daß die Führung eines eingeschränkten Meldedatenbestandes und dessen Fortschreibung außerhalb der Meldebehörden bei Bürgermeistern bzw. Ortsteilbürgermeistern unzulässig ist.

5.2.4.2 Datenübermittlung des Meldeamtes an Gemeinderat

Ein Landratsamt wandte sich an den TLfD mit der Bitte um Mitteilung seiner Rechtsauffassung zu einem Streit zwischen den Elternsprechern eines Kindergartens und einem Mitglied des Gemeinderats sowie der zuständigen Meldebehörde. Die Elternsprecher eines Kindergartens beschwerten sich über die ihrer Meinung nach unzulässige Datenübermittlung der Meldebehörde an den Gemeinderat. Gegenstand war eine Liste, auf der alle in der Gemeinde wohnenden Kinder bis zu 6 Jahren mit Namen, Adresse und Geburtstag aufgeführt wurden. Zweck der Übermittlung war es, den Bedarf an zukünftig benötigten Kindergartenplätzen zu ermitteln.
Der TLfD teilte dem Landrat mit, daß gemäß § 29 Abs. 1 ThürMeldeG die Meldebehörde Daten von Einwohnern an öffentliche Stellen übermitteln darf, wenn dies zur Erfüllung der in ihrer Zuständigkeit oder in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Nach § 2 Abs. 2 ThürKO haben die Gemeinden auch die Aufgabe der Sicherung und Förderung eines bedarfsgerechten öffentlichen Angebotes an Kinderbetreuungseinrichtungen. Zu diesem Zweck hätte aber eine überwiegend zahlenmäßige Darstellung, untergliedert nach Geburtsjahrgängen, Wohnort und gegebenenfalls Straße, ausgereicht. Der TLfD wies darauf hin, daß § 29 Abs. 1 ThürMeldeG keine Rechtsgrundlage für die um Übermittlung ersuchende Behörde darstellt, alle hierin abschließend aufgezählten Einwohnerdaten übermittelt zu bekommen. Vielmehr trägt der Empfänger die Verantwortung dafür, bei der Meldebehörde nur die Daten abzufragen, die tatsächlich zur Aufgabenerfüllung im Einzelfall benötigt werden. Die Meldebehörde trägt nur insoweit Verantwortung für die Übermittlung, als erkennbar ist, daß aufgrund einer allgemeinen Plausibilitätsprüfung eine solche Erforderlichkeit generell nicht besteht. Im vorliegenden Fall wäre es nicht erforderlich gewesen, zur Bedarfsplanung

für Kinderbetreuungseinrichtungen die Namen der Kinder zu übermitteln. Für die konkrete Aufgabenerfüllung hätte eine Auflistung der Geburtsjahrgänge und soweit erforderlich der Straßen ausgereicht. Eine Notwendigkeit nach einer Übermittlung der Namen bestand nicht. Dementsprechend handelte es sich insofern um eine unzulässige Datenübermittlung, für die der ersuchende Empfänger gemäß § 21 Abs. 2 Satz 2 ThürDSG die Verantwortung trägt.

5.2.4.3 Auskunftsersuchen bei Vorliegen einer Meldesperre

Im Rahmen der Problemdiskussion zwischen den LfD ergab sich die Frage, wie Auskunftsersuchen bei Vorliegen einer Auskunftssperre, insbesondere bei einer Sperre aufgrund einer vorliegenden Gefahr für das Leben und die Gesundheit, erfolgen muß. Im Unterausschuß "EDV im Einwohnerwesen" der ständigen Konferenz der Innenminister der Länder hatte man sich Mitte 1994 ebenfalls mit diesem Problem beschäftigt und festgestellt, daß eine falsche Auskunft, z. B. "der gesuchte Einwohner ist nicht gemeldet" unzulässig sei. Da aber insbesondere in kleineren Gemeinden der Betroffene leicht ermittelt werden kann, wenn die Meldeämter ein Auskunftsersuchen nur mit dem Hinweis beantworten, daß entsprechend dem Meldegesetz keine Auskunft erteilt werden darf, hatte sich der TLfD mit dieser Frage auch an das TIM gewandt. Die von dort vorgeschlagene Lösung ist sowohl melderechtlich korrekt und datenschutzrechtlich unbedenklich, da für den Anfragenden nicht erkennbar ist, wo sich der Gesuchte aufhält. Danach sollte bei entsprechenden Anfragen an Meldebehörden folgende Antwort gegeben werden: "Die bisherige bzw. gegenwärtige Anschrift ist der Meldebehörde bekannt. Sie darf aufgrund melderechtlicher Bestimmungen nicht mitgeteilt werden. Sollte der begründete Wunsch bestehen, mit dem Betroffenen in Verbindung zu treten, wird diese Bitte von der Meldebehörde an den Betroffenen weitergeleitet."

5.2.4.4 Telefonische Melderegisterauskünfte

Häufig wird nach der Zulässigkeit für die Erteilung telefonischer Melderegisterauskünfte gefragt. Grundsätzlich gibt es keine datenschutzrechtlichen Bedenken, einfache Melderegisterauskünfte an nicht-öffentliche Stellen auch telefonisch vorzunehmen. Ein praktisches Problem besteht allerdings darin, daß diese Auskünfte gebührenpflichtig sind, so daß von dieser Form der Auskunftserteilung nur in Ausnahmefällen Gebrauch gemacht werden kann. Denkbar wäre hier eine Verfahrensweise, nur nach Abschluß entsprechender Vereinbarungen zur Gebührenabrechnung mit bestimmten nicht-öffentlichen Stellen wie Rechtsanwaltsbüros, Kreditauskunfteien o. ä. Auskünfte zu erteilen.
Demgegenüber sollten erweiterte Melderegisterauskünfte aufgrund der Nachweisführung des berechtigten Interesses sowie der im allgemeinen geforderten Benachrichtigung des Betroffenen von der Auskunftserteilung grundsätzlich nicht telefonisch erteilt werden. Hinsichtlich der Datenübermittlungen an öffentliche Stellen gibt es ebenso keine Formvorschriften. Es ist nur zu sichern, daß Unbefugte keine Kenntnis der Daten erhalten. Dies kann bei telefonischen Auskünften z. B. gewährleistet werden, wenn

- der Empfänger persönlich bekannt ist und gesichert ist, daß er von der Behörde autorisiert wurde, entsprechende Daten anzufordern;
- die Übermittlung erst nach Rückruf bei der anfordernden Stelle (Dienstnummer !) erfolgt;
- vor der Datenübermittlung vereinbarte, in regelmäßigen Abständen wechselnde Kennwörter ausgetauscht werden (z. B. Polizeidienststellen, Sozialämter, Finanzämter).

5.2.4.5 Melderegisterauskünfte an Parteien und Wählergruppen

Unsicherheiten gab es in der Vergangenheit in einigen Meldebehörden bei der Anwendung der Bestimmungen in § 33 Abs. 1 ThürMeldeG, wonach Parteien und Wählergruppen im Zusammenhang mit allgemeinen Wahlen sechs Monate vor den Wahlen Adressen von Gruppen von Wahlberechtigten übergeben werden dürfen. So wurde in einer Meldebehörde anläßlich der Kommunalwahl 1994 aufgrund einer Anfrage durch eine Partei ein Ausdruck aus dem Melderegister erstellt, ohne daß die Bürger auf ihr Widerspruchsrecht hingewiesen worden waren. Neben dieser Mißachtung lag ein weiterer Verstoß gegen das Meldegesetz vor, da aufgrund fehlender EDV-technischer Kenntnisse der Mitarbeiter der Meldebehörde sowie einer unzureichenden Software keine Selektion nach Wählergruppen erfolgte. Dieses wurde vom TLfD beanstandet.
Es ist deshalb angeraten, künftig vor der Entscheidung über einen entsprechenden Auskunftsantrag zu prüfen, ob die EDV-technischen Voraussetzungen für die angeforderten Auszüge aus dem Melderegister gegeben sind. Gleichzeitig ist zu gewährleisten, daß Angaben von Personen, die Widerspruch eingelegt haben bzw. für die Auskunftssperren vorliegen (unter Einbeziehung der Personen, die ihren Hauptwohnsitz in Gemeinschaftseinrichtungen haben), von einer Übermittlung ausgeschlossen sind. Ungeachtet dessen bleibt es in der Entscheidungsbefugnis der jeweiligen Meldebehörde, unter Wahrung des Gleichheitsgrundsatzes Melderegisterauskünfte in Vorbereitung von Wahlen an Parteien und Wählergruppen zu erteilen. Eine Verpflichtung, künftig derartige Auskünfte zu erteilen, besteht nach dem geltenden Recht nicht.

5.2.4.6 Melderegisterauskünfte aus Anlaß von Alters- und Ehejubiläen

Schwierigkeiten bereiten teilweise Mitarbeitern der Meldebehörden die Bearbeitung von Melderegisterauskünften in besonderen Fällen. So können nach § 33 Abs. 2 ThürMeldeG aus Anlaß von Alters- und Ehejubiläen parlamentarischen Vertretungskörperschaften, der Presse oder dem Rundfunk entsprechende Melderegisterauskünfte übergeben werden. Diese Regelung erscheint unproblematisch, wenn, wie das Gesetz es vorschreibt, allen Betroffenen die Möglichkeit eingeräumt wird, dagegen Widerspruch einzulegen. Zur Wahrnehmung dieses Rechtes fordert das Gesetz deshalb, daß jährlich hierauf alle Bürger durch eine öffentliche Bekanntmachung hinzuweisen sind. Daß dies nicht in jedem Fall erfolgt, zeigte eine entsprechende Beschwerde eines Bürgers, der mit der Veröffentlichung seines Jubiläums nicht einverstanden war. Aufgrund fehlender Hinweise hatte er aus Unkenntnis sein Widerspruchsrecht nicht in Anspruch genommen.
Bei einer Prüfung der entsprechenden Meldestelle ergab sich weiterhin, daß bei Jubiläen neben den im Gesetz genannten Stellen auch die örtliche Sparkasse darüber informiert wurde. Dies mag zwar auf den ersten Blick durch Übergabe kleiner Präsente seitens der Sparkasse im Interesse des Betroffenen erfolgen, ist aber vom Gesetzgeber so nicht vorgesehen, so daß die Meldestelle aufgefordert wurde, künftig derartige Übermittlungen zu unterlassen. Übersehen wird in diesem Zusammenhang häufig auch von den Meldeämtern die gesetzlich vorgesehene Verpflichtung, daß Personen aus Krankenhäusern, Pflegeheimen und sonstigen Einrichtungen vor einer Übermittlung ihrer Meldedaten zu hören sind.

5.2.4.7 Melderegisterauskunft an Adreßbuchverlage

Eine Reihe von Anfragen, insbesondere aus der Bevölkerung, zeigen immer wieder, daß die Rechtmäßigkeit der Datenübermittlung von den Meldebehörden an Adreßbuchverlage häufig in Frage gestellt wird. Inwieweit das Adreßbuch zeitgemäß oder sinnvoll ist und nicht nur, wie teilweise befürchtet wird, eine Grundlage für den Adreßhandel darstellt, mag dahingestellt bleiben. Sicher ist auch das Argument, vor allem größerer Meldebehörden, nicht von der Hand zu weisen, daß sich durch die Veröffentlichung von Adreßbüchern die Zahl der Melderegisterauskünfte spürbar verringert.
Bei Anfragen hinsichtlich der Zulässigkeit der Datenübermittlung hat der TLfD stets darauf verwiesen, daß nach dem ThürMeldeG derartige Auskünfte zulässig sind, soweit der Betroffene dem nicht widersprochen hat. Danach können Meldebehörden den Adreßbuchverlagen grundsätzlich Vor- und Familiennamen, Doktorgrad und Anschriften sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben, mitteilen. Darauf hat die Meldebehörde mindestens drei Monate vor der Melderegisterauskunft durch öffentliche Bekanntmachung hinzuweisen. Personen, die in Heimen wohnen, sind vorher zu hören. Dennoch sollte vor jeder Datenübermittlung die jeweilige Kommunalverwaltung eine gründliche Interessenabwägung vornehmen, da der Gesetzgeber ihnen die Entscheidungsbefugnis dafür übertragen hat. Letztlich wird durch die entsprechende Veröffentlichung der Daten ein Teil des Melderegisters in ein öffentliches Register überführt, deren Datennutzung sich insbesondere aufgrund der vorhandenen technischen Möglichkeiten (z. B. Einlesen der Daten mittels eines Scanners in Datenbankdateien) jeder Kontrollmöglichkeit entzieht. Zu bedenken ist z. B. auch, daß bereits eine straßenweise und nicht nur alphabetische Auflistung nach Familiennamen in Adreßbüchern nicht mehr von der Begründung für das öffentliche Interesse zur Datenübermittlung an Adreßbuchverlage gedeckt ist. Bei einfachen Melderegisterauskünften besteht der Zweck nur darin, die Anschrift einer namentlich benannten Person zu ermitteln. Demgegenüber werden bei einer Veröffentlichung von Meldedaten, die straßenweise sortiert sind, außerdem Meldedaten über nicht namentlich bezeichnete Einwohner, sogenannte Gruppenauskünfte, bereitgestellt, die nach dem ThürMeldeG sonst nur bestimmte Empfänger erhalten dürfen.
In diesem Zusammenhang sollte auch folgende Problematik nicht unerwähnt bleiben:
Im Rahmen des Gedankenaustausches zwischen den DSB von Bund und Ländern wurde ein Fall diskutiert, in dem ein Verlag eine CD-ROM herausgegeben hatte, die alle Angaben der Telefonbücher der Bundesrepublik Deutschland enthält. Die Abfrage dieser CD-ROM ist so gestaltet, daß die Eingabe einer beliebigen Telefonnummer genügt, um Name und Adresse des Telefonkunden in Sekundenschnelle abzurufen. Da es sich bei diesen Angaben um Daten aus allgemein zugänglichen Quellen handelt (§ 29 Abs. 1 BDSG), dürfte diese Verfahrensweise als mit dem geltenden Datenschutzrecht für vereinbar anzusehen sein. Gleichwohl besteht die Gefahr, daß durch die Zusammenfassung und Veröffentlichung dieser Kundenverzeichnisse ohne großen technischen Aufwand Auswertungen durchgeführt werden können, die weit über den Zweck hinausgehen, für den das Telefonbuch ursprünglich angelegt worden ist. Dem Telefonkunden, der bei Antragstellung der Eintragung in das Telefonbuch nicht widersprochen hat, dürften diese technischen Möglichkeiten nicht bewußt gewesen sein. Andererseits besteht in der Regel ein Bedürfnis, als Telefonanschlußinhaber in einem Telefonbuch zu erscheinen. Anläßlich der Neufassung der Datenschutzverordnung von Telekommunikation und Informationsdiensten haben daher die DSB von Bund und Ländern unter anderem gefordert, daß bei der Antragstellung dem Kunden die Möglichkeit eröffnet wird, der Aufnahme in das elektronisch geführte Kundenverzeichnis gesondert zu widersprechen (siehe Anlage 29).

Für die Adreßbücher bedeutet dies, daß künftig nicht ausgeschlossen werden kann, daß auch Adreßbuchdatenbestände auf moderne Medien übertragen werden. Dadurch lassen sie sich diese z. B. nach beliebigen Begriffen durchsuchen oder sortieren. Bei entsprechenden EDV-Kenntnissen können sie gleichfalls mit anderen Daten verknüpft werden. So wäre es beispielsweise nach einem automatischen Abgleich mit dem elektronischen Telefonbuch sofort möglich, z. B. für einen ausgewählten Stadtteil alle Häuser aufzulisten, in denen vermutlich (soweit nicht Personen einer Eintragung widersprochen haben) nur eine alleinstehende Frau wohnt, die über keinen Telefonanschluß verfügt.
Wegen dieser Mißbrauchsgefahren hat der TLfD in seiner Stellungnahme zur Novelle des ThürMeldeG (siehe Punkt 1.1.1) vorgeschlagen, § 33 Abs. 3 ThürMeldeG so zu fassen, daß Adreßbuchverlagen Meldedaten lediglich zum Zweck einer alphabetischen Auflistung der Einwohner in Adreßbüchern übermittelt werden dürfen.

5.2.4.8 Melderegisterauskunft für Forschungszwecke

Seitens der Meldebehörden wird häufig die Frage an den TLfD gerichtet, wann für Forschungsmaßnahmen Meldedaten nicht namentlich benannter Personen an private Stellen übergeben werden dürfen. Die Datenübermittlung von Meldedaten an nicht-öffentliche Stellen für Forschungszwecke ist in Thüringen in § 32 ThürMeldeG geregelt. Danach darf eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) nur erteilt werden, soweit sie im öffentlichen Interesse liegt. Mitgeteilt werden dürfen für bestimmte Personengruppen Vor- und Familiennamen, Doktorgrade, Alter, Geschlecht, Staatsangehörigkeit sowie Anschriften. Damit ist die Zulässigkeit und der Umfang der Auskunftserteilung abschließend geregelt.
Dies trifft ebenso für Unternehmen der Markt-, Meinungs- und Sozialforschung zu, wobei für diesen Bereich aufgrund einer Vereinbarung der Länder einheitlich der Verfahrensweg geregelt wurde. Danach dürfen Auskünfte nur erteilt werden, wenn der Beauftragte des Unternehmens eine gültige Unbedenklichkeitsbescheinigung vorlegt, die vom Innenministerium des Landes ausgestellt ist, in dem das Unternehmen seinen Sitz hat. Diese Bescheinigung gilt, soweit sie keine Einschränkung enthält, für alle Meldebehörden im Bundesgebiet. Sie wird in der Regel für zwei Jahre ausgestellt und kann jederzeit widerrufen werden. Mit dieser Bescheinigung ist jedoch keinerlei Aussage über das konkrete Vorhaben des Instituts getroffen, sondern lediglich die Zuverlässigkeit des die Auskunft beantragenden Unternehmens bestätigt. Damit soll den Meldebehörden die Entscheidung für die Zulässigkeit der Datenübermittlung nur erleichtert werden. Sie entbindet die Meldebehörde aber nicht von der Pflicht zur Prüfung, ob der Verwendungszweck im öffentlichen Interesse liegt.
Häufig wird dabei von den Antragstellern der Begriff des öffentlichen Interesses sehr weit ausgelegt und mitunter auch mit der Transparenz staatlicher oder kommunaler Arbeit bis zur “Befriedigung allgemeiner Neugier” verwechselt. Da es sich im Meldebereich bei Datenübermittlungen regelmäßig um Eingriffe in das informationelle Selbstbestimmungsrecht der Bürger handelt, bedarf es stets einer verantwortungsbewußten Prüfung, ob die Belange und das Wohl der Allgemeinheit gegenüber den Individualinteressen überwiegen. Unproblematisch ist dies sicher, wenn es sich um Forschungsaufträge öffentlicher Stellen handelt, da man in diesen Fällen davon ausgehen kann, daß eine Auftragserteilung nur erfolgt, wenn diese Frage positiv beantwortet werden kann.
Ausschlaggebend für die Beantwortung der Frage hinsichtlich des öffentlichen Interesses ist letztlich der Verwendungszweck der Daten. Zur Gewährleistung der ausschließlichen Zweckbindung wird empfohlen, den Empfänger bei der Datenübermittlung ausdrücklich darauf hinzuweisen. Gleichzeitig sollte stets geprüft werden, ob insbesondere aus Gründen des Datenschutzes die Auskunftserteilung unter Bedingungen erfolgen oder mit Auflagen (z. B. Löschungsfristen) verbunden werden sollte.

5.2.5 Adreßauskunftsersuchen bei Behörden

Es wird häufig die Frage an den TLfD gerichtet, ob und wie Anfragen von den verschiedensten Seiten bei öffentlichen Stellen hinsichtlich der Übermittlung von Adressen von Personen oder Personengruppen für die unterschiedlichsten Zwecke beantwortet werden können, wenn Rechtsvorschriften dies nicht ausdrücklich erlauben. So ist es beispielsweise durchaus nicht selten, daß ehemalige Schüler oder Studenten zur Organisation von Absolvententreffen an Bildungseinrichtungen mit der Bitte herantreten, ihnen die notwendigen Anschriften mitzuteilen; oder es werden z. B. im Rahmen eines Forschungsprogrammes von einer wissenschaftlichen Einrichtung für eine vorgesehene Befragung ehemaliger Patienten eines Krankenhauses deren Adressen benötigt.
In diesen Fällen fehlen aufgrund der Zweckbindung der Daten häufig die erforderlichen Rechtsgrundlagen zur Datenübermittlung, so daß sich eine Übermittlung der Anschriften an Dritte verbietet. Dennoch kann im Einzelfall ohne Verletzung datenschutzrechtlicher Bestimmungen geholfen werden. Soweit die betreffende Stelle das Anliegen entsprechend ihrer Möglichkeiten unterstützen möchte, können von der anfragenden Person oder Stelle bereits vorfrankierte aber noch nicht adressierte Kuverts mit den zu übersendenden Schriftstücken der Behörde übergeben werden. Dort erfolgt unmittelbar ohne Beteiligung des Anfragenden die Adressierung und die Übergabe an die Post. Dadurch wird verhindert, daß der Anfragende unbefugt Kenntnis der Adressen erhält. Gleichzeitig wird dem Adressaten

bei Interesse die Möglichkeit eingeräumt, sich mit dem Absender in Verbindung zu setzen. Es liegt somit im Ermessen des Adressaten, ob er durch eine entsprechende Rückantwort den Absender über seine Anschrift unterrichtet (sog. Adreßmittlungsverfahren; siehe Punkt 13.3.1).
Selbstverständlich sollte diese Verfahrensweise nur in Ausnahmefällen angewandt werden, da hierbei eine Zweckänderung der Daten (Anschrift) erfolgt, die jedoch gemäß § 20 ThürDSG dann möglich ist, wenn offensichtlich ist, daß es im Interesse des Betroffenen liegt und kein Grund zur Annahme besteht, daß er in Kenntnis der anderen Zwecke seine Einwilligung verweigern würde. Aufgrund der Tatsache, daß die Adresse dem Empfänger (Dritten) nicht übermittelt wurde und somit diesem nicht unbefugterweise zur Kenntnis gegeben wurde, bestehen gegen diese Verfahrensweise aus datenschutzrechtlicher Sicht keine Bedenken.

5.2.6 Wahlen

5.2.6.1 Auslegung von Wählerverzeichnissen

Im Vorfeld der im Oktober 1994 stattgefundenen Bundes- und Landtagswahl in Thüringen wurde der TLfD auf Probleme aufmerksam, die sich im Zusammenhang mit der gesetzlich vorgeschriebenen Auslegung von Wählerverzeichnissen ergeben. Die Wählerverzeichnisse enthalten, nach Stimmbezirken unterteilt, den Familiennamen, Vornamen, Geburtsdatum und Wohnadresse der Wahlberechtigten unter einer fortlaufenden Nummer. Die Daten werden zuvor aus den entsprechenden Melderegistern der Meldebehörden an die für die Führung des Wählerverzeichnisses zuständigen Gemeinden übermittelt. Zu bestimmten Zeiten vor der Wahl ist dieses Wählerverzeichnis öffentlich auszulegen.
Bei einer in diesem Zusammenhang durchgeführten datenschutzrechtlichen Prüfung in einem Wahlamt konnten keine Verstöße gegen datenschutzrechtliche Bestimmungen festgestellt werden. Problematisch ist in diesem Zusammenhang die Veröffentlichung von Personen, die gemäß § 32 Abs. 5 ThürMeldeG von ihrem Recht auf eine Melderegisterauskunftssperre aus Gründen einer Gefahr für Leben, Gesundheit, persönliche Freiheit o. ä. Gebrauch gemacht haben. Der Sinn und Zweck dieser Regelung wird durch die Veröffentlichung in den Wählerverzeichnissen unterlaufen. Für Betroffene und deren Angehörige unangenehm können auch Offenbarungen in Wählerverzeichnissen über bestimmte Aufenthaltsorte sein, z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Einrichtungen usw.

Bei Erarbeitung der Entschließung der 49. Konferenz der DSB hat sich der TLfD deshalb dafür eingesetzt, daß sowohl auf Landes- als auch auf Bundesebene Personen, für die eine Auskunftssperre im Melderegister eingetragen ist, nicht mehr im öffentlichen Wählerverzeichnis aufgenommen werden (siehe Anlage 20).

5.2.6.2 Wahlausschlußgründe

Aus verschiedenen Gründen können Einwohner von ihrem Recht zur Stimmabgabe bei Wahlen ausgeschlossen werden. Dieses kann gegeben sein bei Vorliegen eines entsprechenden Richterspruchs oder in Fällen, bei denen ein Betreuer zur Besorgung aller Angelegenheiten bestellt worden ist.
Zum Zeitpunkt der Vorbereitung sowohl der Bundestags- als auch der Landtagswahl im Oktober 1994 lagen Informationen über Wahlausschlußgründe in den fünf neuen Ländern, wenn überhaupt, nur sehr lückenhaft vor. Die von den Meldebehörden aus der Zeit vor dem 3. Oktober 1990 übernommenen Einwohnermeldedaten sahen eine solche Eintragung nicht vor. Bis zum März 1994 konnten Wahlausschlußgründe nur dann eingetragen werden, wenn die Strafverfolgungsbehörden ihrer Mitteilungspflicht nach der "Anordnung über Mitteilungen in Strafsachen" bzw. die Vormundschaftsgerichte ihre Mitteilungspflicht gemäß der "Anordnung in Zivilsachen" nachkamen. Die einzige Möglichkeit, noch rechtzeitig vor den Wahlen eine vollständige Übersicht über alle Personen zu erhalten, die vom Wahlrecht ausgeschlossen waren, hätte in einer Massenabfrage aller Thüringer Meldebehörden beim BZR bestanden. Es existierte aber keine gesetzliche Grundlage für die allgemeine Übermittlung von Eintragungen im BZR, die zu einem Wahlausschluß führen. Um dieses noch rechtzeitig zu ermöglichen, trat am 27.04.1994 das Dritte BZRÄndG in Kraft. Der TLfD hat die Entscheidung des TIM begrüßt, auf einen Datenabgleich zu verzichten, auch wenn dieser gemäß § 69 BZRG für die im Jahre 1994 stattgefundenen Wahlen möglich gewesen wäre. Nach Einschätzung des TIM wäre bei 2 Millionen Thüringer Wahlberechtigten lediglich mit etwa 5 bis 10 Fällen von Wahlrechtsausschlüssen zu rechnen gewesen. Die Eintragungen im BZR können auch den Ausschluß der Wählbarkeit einer Person (passives Wahlrecht) zur Folge haben. Aufgrund des BZRÄndG wurden in den neuen Bundesländern über Kandidaten, die sich für eine der Wahlen im Jahre 1994 aufstellen ließen, auf Antrag Auskünfte aus dem BZR erteilt. Enthielt das BZR Eintragungen über einen Bewerber, so wurde gemäß § 70 Abs. 2 BZRG das Führungszeugnis für Behörden ausschließlich an das Innenministerium übermittelt. Dabei kam es in Thüringen zu keinen unrechtmäßigen Übermittlungen durch die Registerbehörde direkt an die anfragenden Meldebehörden.

In diesem Zusammenhang erhielt der TLfD die Eingabe einer Stadtverwaltung, die ihn auf formal- und datenschutzrechtlich unzulässige Beschlüsse bei dem Verfahren zur Feststellung eines Ausschlusses vom Wahlrecht hinwies. So bekamen die Wahlämter etwa den vollständigen Beschluß des Vormundschaftsgerichts über die Bestellung eines Betreuers. In einem anderen Fall wurde dem Wahlamt die gesamte 37seitige Urteilsschrift in einer Strafsache übermittelt. Der TLfD wandte sich daraufhin an das TJM mit der Bitte, die Gerichte und Behörden im dortigen Verantwortungsbereich auf die geeignete Form bei Mitteilungen von Wahlausschlußgründen an die Wahlämter hinzuweisen. Die Gerichte wurden aufgefordert, zukünftig die Mitteilungsanordnung strikt zu beachten. Dem TLfD sind daraufhin auch keine weiteren Fälle von nicht ordnungsgemäßen Mitteilungen von Wahlausschlußgründen bekanntgeworden.

5.2.6.3 Nutzung von Adreßdaten der Abfallwirtschaft für einen Wahlaufruf eines Landrates

In Vorbereitung und Durchführung der Kommunalwahlen 1994 hatte ein Landrat zum Erreichen einer möglichst hohen Wahlbeteiligung einen Wahlaufruf an die Haushalte herausgegeben. Dies war jedoch nicht in Form einer Postwurfsendung erfolgt, sondern es war jeder einzelne Haushalt direkt angeschrieben worden. Aufgrund eines Hinweises wurde der TLfD über den Sachverhalt informiert und gebeten, die Herkunft der Adressen zu ermitteln, da der Verdacht bestand, daß das Meldeamt unzulässigerweise diese Daten zur Verfügung gestellt hatte. Die Regelungen des ThürMeldeG erlauben nur zum Zwecke der Wahlwerbung eine Datenübergabe eines ausgewählten Personenkreises an Parteien und Wählergemeinschaften. Im vorliegenden Fall hatte jedoch der Landrat alle Haushalte angeschrieben. Andererseits wäre aufgrund einer fehlenden Aufgabenstellung eine Übermittlung von Meldedaten an den Landrat für die Herausgabe eines Wahlaufrufes als Verwendungszweck nach dem Meldegesetz unzulässig.
Im Ergebnis der Prüfung stellte sich jedoch heraus, daß für die Adressierung keine Meldedaten, sondern die im Amt für Wasser- und Abfallwirtschaft rechtmäßig gespeicherten Daten für die Erteilung von Müllgebührenbescheiden an die Bürger auf ausdrückliche Anweisung des Landrates zweckentfremdet genutzt worden waren. Trotz vorgebrachter Bedenken der Amtsleitung waren die Daten angefordert und für die Adressierung der Wahlaufrufe genutzt worden. Aufgrund der fehlenden Rechtsgrundlage für die Zweckänderung der Daten wurde dieses Verhalten vom TLfD gegenüber dem Landratsamt kritisiert und darüber das LVwA als zuständige Rechtsaufsichtsbehörde in Kenntnis gesetzt. Gleichzeitig wurde darum gebeten, die Auswertung des Vorfalls für die weitere Sensibilisierung der Mitarbeiter für Probleme des Datenschutzes zu nutzen. Da eine weitere mißbräuchliche Nutzung der Daten nach Feststellung des Verstoßes von der Behörde ausgeschlossen wurde und den Betroffenen keine Nachteile entstanden, wurde seitens des TLfD von einer Beanstandung abgesehen.

5.3 Ausländerwesen

5.3.1 Ausländerzentralregister

Das Ausländerzentralregister nach dem Ausländerzentralregistergesetz (siehe Punkt 1.2.3) wird vom Bundesverwaltungsamt als Registerbehörde geführt. Das AZR ist von seiner Funktion her nicht mit dezentralen Meldeeinrichtungen vergleichbar. Sein Zweck besteht in erster Linie darin, die Behörden zu unterstützen, die mit ausländer- und asylrechtlichen Aufgaben betraut sind oder sonstige Aufgaben mit ausländerspezifischem Bezug wahrnehmen. Nach § 22 AZR-G können zum Abruf von Daten im automatisierten Verfahren u. a. Ausländerbehörden zugelassen werden. Die Zulassung des automatisierten Abrufverfahrens bedarf der Zustimmung der für die speichernde und abrufende Stelle jeweils zuständigen obersten Bundes- oder Landesbehörde. Die Registerbehörde (das Bundesverwaltungsamt) hat den BfD von der Zulassung zu unterrichten. Nach § 7 Abs. 3 ThürDSG ist über die Einrichtung eines Abrufverfahrens vorher der TLfD zu unterrichten. Bisher liegt dem TLfD lediglich eine solche Unterrichtung vor.

5.3.2 Einführung einer Asyl-Card

Im Zuge der Diskussion zur Harmonisierung der Verwaltungsabläufe im Asylverfahren ist hinsichtlich des Datenabgleiches und Datenaustausches im Asylverfahren die Einführung einer sogenannten Asyl-Card favorisiert worden. Diese Asyl-Card soll jeder Asylbewerber mit sich führen müssen. Auf dieser Chipkarte sollen neben Namen, Geburtsdatum, Fingerabdruck und Lichtbild auch Daten über das Asylverfahren, das Vorliegen einer Arbeitserlaubnis, der Empfang von Sach- und Geldleistung und weitere Daten erfaßt sein. Sie soll sowohl Kontrollzwecken als auch fürsorglichen Leistungszwecken und darüber hinaus zur Reduzierung des Verwaltungsaufwandes, der Datenfehlerquote, der Möglichkeit, ständig aktuelle Daten bundesweit sofort abrufen zu können, sowie der Reduzierung des mißbräuchlichen Leistungsempfanges dienen.
Die Einführung der Asyl-Card wurde seitens des TIM befürwortet. Der TLfD hat daraufhin folgende Bedenken geäußert: Die Zusammenführung von Daten aus ganz unterschiedlichen Lebensbereichen, die Verknüpfung der teilweise einander beeinträchtigenden Zielsetzungen und die Dokumentation eines gesamten Lebensabschnittes kann

dazu führen, daß vollständige Persönlichkeitsbilder zusammengefügt werden können. Das Bundesverfassungsgericht hat die automatisierte Herstellung von Persönlichkeitsprofilen jedoch für unzulässig erklärt. Alle Bemühungen um Effizienzsteigerung und um Schutz vor mißbräuchlicher Inanspruchnahme staatlicher Leistungen können die Einführung eines derartig umfassenden elektronischen Überwachungssystems keinesfalls rechtfertigen. Der TLfD hat dem TIM gegenüber seine Verwunderung zum Ausdruck gebracht, daß die Einführung der Asyl-Card so unproblematisch gesehen wird. Eine Äußerung des TIM hierzu steht bislang aus. Das Thema war Gegenstand der Konferenz der DSB vom 09./10.03.1995 (siehe Anlage 12) und wird aus datenschutzrechtlicher Sicht auch weiterhin begleitet.

5.3.3 Beantragung von Paßersatzpapieren für Flüchtlinge

Nach § 43b des Asylverfahrensgesetzes hat das BMI oder die von ihm bestimmte Stelle für Ausländer, die in einer Aufnahmeeinrichtung zu wohnen verpflichtet sind, für die Beschaffung der Heimreisedokumente im Wege der Amtshilfe Sorge zu tragen. Die erforderlichen Maßnahmen sind zum frühestmöglichen Zeitpunkt zu treffen. Die Beschaffung von Paßersatzpapieren ist mit einer Weitergabe von Daten an die Auslandsvertretungen des Herkunftsstaates in der Bundesrepublik Deutschland - datenschutzrechtlich als eine Übermittlung an Stellen im Ausland - verbunden. Diese Datenübermittlung ist nach § 23 ThürDSG unter anderem dann zulässig, wenn sie in einer Rechtsvorschrift geregelt ist, was nicht der Fall ist. Bezüglich des frühestmöglichen Zeitpunktes der Datenübermittlung hat der TLfD die Ansicht vertreten, daß die Datenübermittlung nicht vor rechtskräftigem Abschluß des Asylverfahrens erfolgen darf. Dies gründet sich darauf, daß Maßnahmen der Datenverarbeitung in den Schutzbereich von Grundrechten wie das Asylrecht eingreifen können. Das Grundrecht könnte durch Übermittlung von Informationen aus dem Asylverfahren an den Herkunftsstaat beeinträchtigt werden, wenn dadurch eine Verfolgung möglich wird.
Das TIM hat mitgeteilt, daß Paßersatzpapiere, sofern diese nicht vorliegen, grundsätzlich erst mit Wirksamwerden der Ausreisepflicht bei den entsprechenden Konsulaten beantragt werden. Dazu werden grundsätzlich nur die Daten übermittelt, die für die Beantragung erforderlich sind. Gegen die Datenübermittlung zu diesem Zeitpunkt war nichts einzuwenden. Den datenschutzrechtlichen Belangen wird im Freistaat Thüringen daher Rechnung getragen.

5.4 Sparkassen

5.4.1 Datenschutzkontrolle über die gemeinsame Sparkassenorganisation Hessen-Thüringen

Das Land Hessen und der Freistaat Thüringen haben durch den am 01.07.1992 in Kraft getretenen Staatsvertrag eine gemeinsame Sparkassenorganisation gebildet. Dieser gehören neben dem Sparkassen- und Giroverband Hessen-Thüringen sowie der Landesbank Hessen-Thüringen die öffentliche Lebensversicherungsanstalt Hessen-Nassau-Thüringen, die öffentliche Versicherungsanstalt Hessen-Nassau-Thüringen und die Hessisch-Thüringische Brandversicherungsanstalt Kassel-Erfurt an.

Die Staatsaufsicht über diese Sparkassenorganisation üben die Ministerien in Hessen und Thüringen, denen die oberste Sparkassenaufsicht obliegt, im turnusmäßigen Wechsel von 4 Jahren aus. Nach Artikel 34 Abs. 2 Satz 3 des Staatsvertrages folgt die Kontrollbefugnis des jeweiligen LfD diesem Turnus. Ab 01.01.1996 ist daher der TLfD erstmals für die Einhaltung des Datenschutzes bei der Sparkassenorganisation Hessen-Thüringen bis zum 31.12.1999 zuständig. Die Überwachung erfolgt einvernehmlich mit dem jeweils anderen LfD und ist in einer Verwaltungsvereinbarung festgeschrieben, die am 25.09.1995 in Kraft getreten ist. Darin ist insbesondere auch die Beanstandung von Verletzungen datenschutzrechtlicher Vorschriften geregelt, die möglichst im Einvernehmen zustande kommen soll und die der jeweils zuständige LfD gegenüber der Sparkassenorganisation ausspricht. Darüber hinaus unterrichten sich die LfD von Hessen und Thüringen gegenseitig über alle für die Kontrolltätigkeit bedeutsamen Umstände. Schließlich werden die Beiträge zum jeweiligen Tätigkeitsbericht sowie die Bearbeitung von Landtagsanfragen und -petitionen, die die Sparkassenorganisation betreffen, untereinander abgestimmt. Unabhängig von dieser Regelung üben die DSB beider Länder die Kontrolle über die in ihrem Gebiet gelegenen und tätigen Sparkassen aus, wobei sie sich insbesondere über Fragen und Tatsachen von übergreifendem Interesse unterrichten.

5.4.2 Zulässigkeit der Datenerhebung im Rahmen des Geldwäschegesetzes

Sparkassen fallen als öffentlich-rechtliche Wirtschaftsunternehmen unter die Sonderbestimmungen des § 26 ThürDSG. Von dem betrieblichen Datenschutzbeauftragten einer Thüringer Sparkasse wurde der TLfD um Stellungnahme bezüglich der Interpretation des § 4 BDSG in Verbindung mit § 9 Abs. 1 Satz 2 des Geldwäschegesetzes (GwG) gebeten. Der Fragesteller hatte Schwierigkeiten, die Vorschriften des GwG bzw. die Weisungen des Bundesaufsichtsamtes für das Kreditwesen (Kopierpflicht nach § 9 Abs. 1 Satz 2 GwG) mit den Belangen des Datenschutzes in Einklang zu bringen.

In Beantwortung seiner Frage teilte der TLfD mit, daß sowohl das BDSG als auch das GwG den Umgang mit personenbezogenen Daten regeln. Schutzgut des BDSG ist dabei das Recht auf informationelle Selbstbestimmung, Ziel des Geldwäschegesetzes in erster Linie die Bekämpfung der strafbaren Geldwäsche. § 9 GwG bestimmt, daß die bei der Identifizierung zu erhebenden Daten aufzuzeichnen sind und diese Aufzeichnung nach § 9 Abs. 1 Satz 2 GwG, soweit möglich, durch Kopie der zur Feststellung der Identität vorgelegten Dokumente zu erfolgen hat. Diese vorgegebene Handlungsweise beinhaltet aber keinen Verstoß gegen die Schutzvorschriften des BDSG. Gemäß § 4 Abs. 1 BDSG ist die Verarbeitung personenbezogener Daten und deren Nutzung zulässig, wenn eine andere Rechtsvorschrift - in diesem Fall das GwG - es erlaubt oder anordnet. Darüber hinaus wurde der Fragesteller darauf hingewiesen, daß neben der Vorschrift des § 9 Abs. 1 Satz 2 GwG die Regelung des § 7 GwG einzubeziehen ist. Danach kann von einer Identifizierung abgesehen werden, wenn der Betroffene bei dem zur Identifizierung Verpflichteten persönlich bekannt ist oder wenn er bei früheren Gelegenheiten identifiziert worden ist. Der Kunde sollte auf die Ausnahmemöglichkeit dieser Identifizierungspflicht hingewiesen werden, damit er unter Umständen Gründe vortragen kann, die eine eventuelle nochmalige Identifizierung entbehrlich machen. Weiter wurde dem anfragenden bDSB mitgeteilt, daß bei einer normalen Konto- und Depoteröffnung nicht automatisch das GwG als Rechtfertigung für die Ablichtung eines Ausweisdokumentes herangezogen werden kann. Nach dem GwG greift die Pflicht zur Anfertigung derartiger Dokumente erst bei der Durchführung bestimmter Transaktionen, z. B. bei Abgabe von Bargeld im Wert von mindestens 20.000 Deutsche Mark.

6. Personalwesen

6.1 Personalakten

Der Umgang mit personenbezogenen Daten stellt schon im Vorfeld eines Dienst- bzw. Arbeitsverhältnisses ein Problem dar, da nicht nur der private, sondern auch der öffentliche Arbeitgeber im Umgang mit Bewerberdaten mitunter nicht die erforderliche Sorgfalt einhält, die geboten ist. Entweder werden Bewerbungsunterlagen nicht zurückgesandt oder werden weiter vorgehalten, bis sich zu einem späteren Zeitpunkt gegebenenfalls die Möglichkeit ergibt, den Bewerber in einem anderen Verfahren zu berücksichtigen. Es kommt auch vor, daß Bewerbungsunterlagen, ohne Rücksprache mit dem Betroffenen genommen zu haben, an eine andere Behörde weitergegeben werden. Es ist zu begrüßen, daß der Entwurf eines Arbeitsvertragsgesetzes, wie ihn der Freistaat Sachsen im Bundesrat vorgelegt hat, in § 16 ausdrücklich vorsieht, daß personenbezogene Daten und Bewerbungsunterlagen Dritten nur mit Einwilligung des Bewerbers zugänglich gemacht werden dürfen und Bewerbungsunterlagen dem Bewerber unverzüglich auszuhändigen sind, sofern dieser nicht mit ihrer weiteren Aufbewahrung einverstanden ist.
Auch der TLfD hat zu dieser Problematik im Rahmen einer möglichen Änderung des ThürDSG eigene Vorstellungen entwickelt.

6.1.1 Personalaktenführungsrichtlinie

Das TIM hat schon vor Inkrafttreten des Thüringer Beamtengesetzes am 01.07.1994 einen Entwurf für eine Personalaktenführungsrichtlinie vorgelegt, der den obersten Landesbehörden zur Stellungnahme zugeleitet wurde. Inkraftgetreten ist diese Richtlinie bisher allerdings nicht. Seitens des TLfD wird es begrüßt, daß der Versuch unternommen wird, die Grundlage für eine einheitliche Personalaktenführung sicherzustellen. Bei den zahlreichen Kontrollen im Personalwesen, auf die noch einzugehen sein wird, wurde immer wieder festgestellt, daß es in den Personalstellen sowohl in der Landesverwaltung als auch in den Kommunen mitunter Unsicherheiten darüber gibt, was in eine Personalakte aufzunehmen ist. Dies gilt besonders dann, wenn für verschiedene Bereiche der Personalverwaltung unterschiedliche Stellen zuständig sind. Während auf Landesebene die Grundakten im Regelfall bei der personalführenden Dienststelle geführt werden, ist die Zentrale Gehaltsstelle im Geschäftsbereich des TFM für die Zahlbarmachung der Vergütung und Besoldung zuständig. Für Reisekostenabrechnungen und Beihilfeangelegenheiten ist für weite Teile des Landespersonals die Zentrale Beihilfestelle in Stadtroda zuständig, die organisatorisch zum Haushaltsreferat des LVwA und damit zum Geschäftsbereich des TIM zählt.
Für beide Stellen wäre es aus datenschutzrechtlicher Sicht erforderlich, klare Regelungen zur Aufnahme der entsprechenden Unterlagen in die jeweiligen Teilakten zu treffen. Der TLfD hat eine Prüfung bei der Zentralen Gehaltsstelle (siehe Punkt 6.3.1) zum Anlaß genommen, seine Mithilfe bei der Erarbeitung von Regelungen für die Vergütungsakten ausdrücklich anzubieten. Bisher ist lediglich bekannt, daß das TIM beabsichtigt, die Vorschriften der Personalaktenführungsrichtlinie den anderen Ressorts zu empfehlen.
Der TLfD hat das TIM insbesondere auf die Notwendigkeit hingewiesen, klare Regelungen zum Umgang mit "Kaderakten" der ehemaligen DDR zu treffen. Wenn die Kenntnis der Daten zur rechtmäßigen Erfüllung einer in der Zuständigkeit der personalführenden Stelle liegenden Aufgabe nicht mehr erforderlich ist, ist eine weitere Verarbeitung oder Nutzung dieser Daten gemäß § 20 Abs. 1 in Verbindung mit § 31 Abs. 1 ThürDSG unzulässig. Die Akten sind dann

gemäß § 11 Abs. 1 Thüringer Archivgesetz auszusondern und dem zuständigen Archiv zur Übernahme anzubieten. Dies trifft insbesondere auf Unterlagen zur Beurteilung gesellschaftlichen Verhaltens, Nachweise zur Tätigkeit in Parteien und Massenorganisationen oder Unterlagen, die ausschließlich Daten Dritter, wie zum Beispiel Verwandtschaftsaufstellungen, enthalten, zu. Auch Unterlagen vorhergehender Arbeitsstellen, soweit diese nicht im Einzelfall im Zusammenhang mit anerkannten Vordienstzeiten stehen, werden hierzu zu zählen sein. Es kann nur immer wieder betont werden, daß das Fehlen einer entsprechenden Personalaktenführungsrichtlinie in der Praxis zu Problemen führt, die aus datenschutzrechtlicher Sicht vermeidbar wären, wenn hier Regelungen vorlägen.

6.1.2 Personalfragebogen für Bedienstete des Freistaats Thüringen

Anfragen und Kontrollen in Personalverwaltungen ergaben immer wieder, daß die Auslegung der Regelungen des § 97 ThürBG hinsichtlich des erforderlichen Umfangs von Personalaktendaten im Personalbogen Schwierigkeiten bereitet. Da mit den Personalfragebogen umfangreiche Datenerhebungen durch den Dienstherren bei den Beschäftigten durchgeführt werden, bedarf es grundsätzlich einer sorgfältigen Abwägung, ob und welche Daten im Rahmen von Bewerbungen bzw. bei der Aufnahme eines Arbeitsrechtsverhältnisses erhoben werden. Aus diesem Grund unterliegt auch der "Inhalt von Personalfragebögen von Angestellten und Arbeitern" zur Wahrung des Persönlichkeitsrechts der Bediensteten gemäß § 74 Abs. 3 Nr. 8 ThürPersVG der vollen Mitbestimmung des jeweils zuständigen Personalrates. Unabhängig davon wäre es nach Auffassung des TLfD dennoch dienlich, wenn auf Landesebene entsprechende abgestimmte Mustervordrucke empfohlen würden. Dadurch könnten u. a. aufwendige spätere Korrekturen und Probleme weitgehend vermieden werden. So hatten sich im Berichtszeitraum mehrere Mitarbeiter einer Thüringer Hochschule an den TLfD gewandt, mit der Bitte um Prüfung ihres Personalbogens hinsichtlich der Zulässigkeit der geforderten Angaben. Dabei war festzustellen, daß in dieser Hochschule ein Fragebogen mit sehr umfangreichen Datenerhebungen verwendet wurde. Nach Prüfung der einzelnen Fragen wurde im Hinblick auf den Erforderlichkeitsgrundsatz gegen einige dieser im Personalbogen geforderten Angaben, z. B. hinsichtlich Einkünften aus Kapitalvermögen, Vermietung und Verpachtung, Bedenken erhoben. Von der zuständigen Personalleitung wurde dies aufgegriffen und dem TLfD mitgeteilt, daß man sich künftig an dem aktuellen, den Datenschutzbestimmungen genügenden Personalfragebogen für Bedienstete des Landes Thüringen der Zentralen Gehaltsstelle orientieren wird. Gleichzeitig wurde der Bitte des TLfD entsprechend zugesichert, daß die Daten, die aufgrund der bisherigen Personalbogen möglicherweise unzulässig erhoben wurden, gemäß § 16 ThürDSG gelöscht werden.

Durch Anfrage eines Bewerbers für den Schuldienst wurde der TLfD auf einen vom TKM für verbindlich erklärten Personalbogen für Lehrereinstellungen aufmerksam, auf dem Daten erhoben werden, die gleichfalls nach Auffassung des TLfD nicht erforderlich sind. Das betrifft insbesondere Datenerhebungen zum Ehepartner, zu Eltern, zu schwebenden Gerichtsverfahren und Wohnungsanschriften der letzten 20 Jahre, für die eine Notwendigkeit nicht erkennbar war. Das TKM hat unter Verweis darauf, daß es hierzu einer Abstimmung mit dem TIM bedarf, eingeräumt, daß der Personalfragebogen überarbeitet werden muß. Seit dieser Feststellung ist allerdings bereits eine geraume Zeit vergangen, ohne daß eine Entscheidung getroffen wurde. Dies ist insbesondere deshalb problematisch, da die Gefahr besteht, daß mit dem Personalbogen unzulässig erhobene Daten auch Eingang in die Personalakte finden.

6.1.3 Einsichtsrecht des Geheimschutzbeauftragten in Personalakten

Seitens eines Ministeriums wurde die Frage an den TLfD gerichtet, ob dem Geheimschutzbeauftragten nach § 13 der Sicherheitsrichtlinie des Landes Thüringen vom 11.06.1991 das Recht auf Einsichtnahme in die Personalakte eines Bediensteten zusteht. Hierzu wurde vom TLfD mitgeteilt, daß nach § 97 Abs. 3 ThürBG nur Beschäftigte, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten betraut sind, Zugang zur Personalakte haben dürfen und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Da in dem betreffenden Fall der Geheimschutzbeauftragte nicht zu diesem Personenkreis zählte, wurde darauf verwiesen, daß eine Einsichtnahme nur dann vorstellbar erscheine, wenn er nach § 97 Abs. 1 Satz 3 in Verbindung mit § 100 Abs. 2 Satz 1 ThürBG von dem Betroffenen ausdrücklich ermächtigt worden wäre. § 13 Abs. 2 der Sicherheitsrichtlinien für das Land Thüringen sieht vor, daß der Geheimschutzbeauftragte anhand der Personalakte und sonstiger für ihn als geeignet erkennbarer Unterlagen die Vollständigkeit und Übereinstimmung der gemachten Angaben und etwaiger sicherheitserheblicher Umstände prüft. Angesichts der eindeutigen Regelung des ThürBG ist für eine Überprüfung anhand der Personalakten durch den Geheimschutzbeauftragten der betreffenden Behörde keine Möglichkeit mehr gegeben. Mangels anderweitiger Regelungen sind die Vorschriften des ThürBG auch für Tarifbedienstete anzuwenden.

6.1.4 Einsichtsrecht des Rechnungshofes in Personalakten

Aus dem Kreis der LfD ist das Problem diskutiert worden, ob ein Einsichtsrecht des Rechnungshofes in Personalakten besteht. Das ThürBG sieht eine ausdrückliche Ermächtigungsgrundlage für den Rechnungshof nicht vor. Ob man § 95 Abs. 1 LHO, wonach Unterlagen, die der Rechnungshof zur Erfüllung seiner Aufgaben für erforderlich hält, ihm auf Verlangen innerhalb einer von ihm zu bestimmenden Frist zu übersenden oder seinen Beauftragten vorzulegen sind, als eine entsprechende Rechtsgrundlage ansehen kann, sieht der TLfD als zweifelhaft an, zumal eine Personalakte schon begrifflich etwas anderes ist als eine Unterlage. Das TIM wurde vom TLfD auf die Notwendigkeit der Schaffung von Rechtsgrundlagen in diesem Zusammenhang hingewiesen. Das TIM sieht den Rechnungshof als Dritten nach § 101 Abs. 2 ThürBG (§ 90d BBG) an, so daß im Falle einer nicht erteilten Einwilligung eines Beamten zur Auskunftserteilung eine Abwägung zwischen den Interessen des Bediensteten und des Gemeinwohls oder der schutzwürdigen höherrangiger Interessen des Dritten vorgenommen werden muß. Nach Auffassung des TLfD wird man dem Anliegen des Rechnungshofes nicht unbedingt Vorrang gegenüber den Interessen des betreffenden Mitarbeiters an der Wahrung seines Rechtes auf informationelle Selbstbestimmung geben können, wenngleich die Notwendigkeit einer Kontrolle, die sich auch auf Personalakten erstrecken können soll, nicht zu verkennen ist. Angesichts der fehlenden Normenklarheit überrascht daher die Auffassung des TIM, daß kein Erfordernis besteht, eine entsprechende Rechtsgrundlage zu schaffen. Nur übergangsweise ist der TLfD bereit, bei etwaigen Einsichtnahmen des Rechnungshofes in Personalakten von einer Beanstandung abzusehen.

6.1.5 Einsichtsrecht der Hochschule

Der bDSB einer Thüringer Hochschule bat um datenschutzrechtliche Prüfung einer "Einverständniserklärung", die den Mitarbeitern der Hochschule von seiten des TMWFK mit der Bitte um Unterzeichnung zugesandt worden war. Diese Einverständniserklärung beinhaltete, daß der Unterzeichnende zustimmt, daß die dem TMWFK überlassenen Unterlagen über seine Forschungs- und Publikationstätigkeiten einer anderen Hochschule zur Vorbereitung einer möglichen Versetzung nach § 58 Abs. 3 Satz 2 des Thüringer Hochschulgesetzes (ThürHG) zur Verfügung gestellt werden und er mit der Einsichtnahme in seine Personalakte einverstanden ist.
Nach Prüfung der Rechtmäßigkeit der Einverständniserklärung hat der TLfD dem anfragenden bDSB mitgeteilt, daß es gemäß §101 Abs. 1 ThürBG zulässig ist, die Personalakte für Zwecke der Personalverwaltung oder Personalwirtschaft Behörden desselben Geschäftsbereiches ohne Einwilligung des Betroffenen vorzulegen, soweit die Vorlage der Personalakte zur Vorbereitung oder Durchführung von Personalentscheidungen notwendig ist. Da es sich hier um mögliche Versetzungen nach § 58 Abs. 3 Satz 2 ThürHG handelt, die bei Auflösung oder Zusammenschluß von Hochschulen auch ohne Zustimmung der Betroffenen zulässig sind und die genannten Hochschulen demselben Geschäftsbereiches angehören, kommt der vorgenannte § 101 Abs. 1 ThürBG zur Anwendung. Die Vorlage der Personalakte und Auskunft ist somit unter Berücksichtigung der Beschränkung auf den jeweils erforderlichen Umfang (§101 Abs. 3 ThürBG) für Zwecke der Personalverwaltung auch ohne die Einwilligung bzw. Einverständniserklärung des Betroffenen zulässig.

6.1.6 Umgang mit "alten" Kaderakten

Es ist bei Kontrollen immer wieder festzustellen, daß Unklarheiten über die Nutzung und den Verbleib "alter" Kaderakten bestehen. Dies zeigte sich auch anläßlich einer Kontrolle in einem Veterinär- und Lebensmittelüberwachungsamt. Dabei stellte sich heraus, daß nach Auflösung der ehemaligen Kreishygieneinspektionen sowie der Abteilungen Veterinärwesen der Kreise die Kaderakten der ausgeschiedenen Mitarbeiter in den Landratsämtern und teilweise noch als Handakten für eventuelle Rückfragen (insbesondere für Rentenberechnungen) in den staatlichen Veterinär- und Lebensmittelüberwachungsämtern verblieben waren. Aufgrund der Regelungen des ThürDSG stehen diese Unterlagen gemäß § 30 ThürDSG demjenigen Träger öffentlicher Verwaltung zu, der nach dem Grundgesetz für diese Verwaltungsaufgabe zuständig ist. Da dies das LVwA ist, wurde es über das Kontrollergebnis informiert und aufgefordert, alle Personalunterlagen der Mitarbeiter der ehemaligen Kreishygieneinspektionen sowie der Abteilungen Veterinärwesen der Kreise zu übernehmen, was zwischenzeitlich auch erfolgte.

An den TLfD wurde auch das Problem herangetragen, was aus den Personalakten der Mitarbeiter der ehemaligen HO geworden ist und wo man diese einsehen könne. Zuständig für diesen Aufgabenbereich ist der BfD, mit dem sich der TLfD diesbezüglich in Verbindung gesetzt hat. Aus den zahlreichen Anfragen ist zu schließen, daß viele Bürger nicht wissen, wer die hierfür zuständige Stelle ist. Gesprächs- und Auskunftspartner in Thüringen ist die Firma DISOS GmbH, Sorbenweg 3 - 4, 99096 Erfurt, die weitere Außenstellen in Erfurt, Gera und Suhl hat. Deren alleinige Gesellschafterin ist die Bundesanstalt für vereinigungsbedingte Sonderaufgaben als Nachfolgeeinrichtung der aufgelösten Treuhandanstalt. Dort befinden sich u. a. Personalunterlagen und auch Lohnabrechnungsunterlagen ehemaliger Thüringer

volkseigener Betriebe, die entweder aufgelöst oder unter anderer Bezeichnung in neuer Rechtsform weitergeführt wurden. Wie sich der TLfD vor Ort überzeugen konnte, werden dort die Akten eingelagert, aufbewahrt und archiviert. Ratsuchenden Bürgern werden von den Mitarbeitern der DISOS GmbH die erbetenen Auskünfte erteilt.

6.1.7 Veröffentlichung von Personalnachrichten im Justiz-Ministerialblatt für Thüringen

Im Justiz-Ministerialblatt für Thüringen werden in unregelmäßiger Folge Personalnachrichten, gegliedert nach Ministerium, Gerichten und Staatsanwaltschaften, Versetzungen, Ernennungen, Berufungen in das Beamtenverhältnis auf Lebenszeit und ähnliche Mitteilungen, veröffentlicht. Die Veröffentlichung erfolgt durch Benennung des Namens und der Amtsbezeichnung.
Auf Nachfrage hat das TMJE mitgeteilt, die Veröffentlichung der Personalnachrichten erfolge aufgrund der Verwaltungsvorschrift vom 12.10.1993 (JMBl. S. 255). Diese Verwaltungsvorschrift sieht vor, daß eine Veröffentlichung dann erfolgen darf, wenn der Betroffene zugestimmt hat.
Die erforderliche Zustimmung wurde durch das TMJE bislang als vorliegend angenommen, da in einem Schreiben, welches bei einer Ernennung bzw. einer Versetzung dem Betroffenen ausgehändigt wurde, angekündigt wurde, daß beabsichtigt ist, die Personaldaten im Justiz-Ministerialblatt für Thüringen zu veröffentlichen. Der TLfD hat darauf hingewiesen, daß eine Absichtsankündigung formell keineswegs einer Einwilligungserklärung entspricht. Die Veröffentlichung der Personalnachrichten ist daher ohne Rechtsgrundlage erfolgt und damit unzulässig. Höherrangige Interessen, die eine Veröffentlichung zwingend erfordern, sind nicht erkennbar.
Das Vorstelligwerden beim TMJE hat dazu geführt, daß man sich dazu entschlossen hat, künftige Veröffentlichungen nur noch mit schriftlicher Einverständniserklärung der Betroffenen vorzunehmen. Die Gestaltung des Formblattes ist allerdings noch Gegenstand der Diskussion, da nach dem vorgesehenen Formular theoretisch die Veröffentlichung der kompletten Personalakte möglich wäre.
In einigen anderen Ländern wird inzwischen aufgrund der datenschutzrechtlichen Bedenken auf die Veröffentlichung der Personalnachrichten verzichtet.

6.1.8 Bekanntgabe der Prüfungsabsolventen für den gehobenen Forstdienst

In Nummer 13/95 des Thüringer Staatsanzeigers hat das Thüringer Ministerium für Landwirtschaft, Naturschutz und Umwelt (TMLNU) die Namen aller Absolventen der Laufbahnprüfung für den gehobenen Forstdienst veröffentlicht. Rechtsgrundlage hierfür ist § 70 der Thüringer Verordnung über die Ausbildung und Prüfung für die Laufbahn des gehobenen Forstdienstes (ThürAPOgFD), der vorschreibt, daß das Ministerium die Namen der Anwärter, die die Laufbahnprüfung bestanden haben, in alphabetischer Reihenfolge im Staatsanzeiger bekanntgibt. Der TLfD sieht durch diese Vorschrift das informationelle Selbstbestimmungsrecht nach Artikel 6 Abs. 2 der Verfassung des Freistaats Thüringen (VerfThür) als verletzt an. Es ist kein Gesichtspunkt erkennbar, der eine Veröffentlichung dieser personenbezogenen Daten rechtfertigt. Das TMLNU hat zunächst die Veröffentlichungsnotwendigkeit damit begründet, daß die Öffentlichkeit für diese Ausbildung zahle und damit auch ein Recht habe zu erfahren, wer die Ausbildung erfolgreich beendet hat. Es wird nicht in Abrede gestellt, daß der Steuerzahler ein Recht hat zu wissen, ob seine Steuergelder sinnvoll verwandt werden. Die Aufzählung der Namen derjenigen, die eine Prüfung erfolgreich absolviert haben, ist dafür aber nicht als geeignet anzusehen, da Prüfungsergebnisse durch eine Vielzahl von Faktoren bestimmt werden. Auch wenn niemand eine Prüfung besteht, läßt sich daraus nicht die Schlußfolgerung ableiten, daß Steuergelder verschwendet werden, da das Prüfungsergebnis vom Fleiß der Prüflinge und auch psychischen Faktoren abhängt, die bei jedem einzelnen unterschiedlich sind. Den Ansprüchen der Öffentlichkeit wird man gerecht, wenn mitgeteilt wird, wie viele Prüflinge eine Prüfung bestanden haben.
Das TLMNU hat nunmehr mitgeteilt, daß das Prüfergebnis künftig nicht mehr veröffentlicht wird und bei einer Änderung der Ausbildungs- und Prüfungsordnung der in Rede stehende Paragraph ersatzlos gestrichen wird.

6.1.9 Datenschutzrechtliche Überprüfung von Personalakten bei der Landesforstdirektion

Im Rahmen einer datenschutzrechtlichen Kontrolle in der Landesforstdirektion wurde hinsichtlich der Aufbewahrung der Altpersonalakten festgestellt, daß in den Bodenräumen des Behördengebäudes archivierte Altakten bis in das Jahr 1840 zurückgehen. Vom TLfD wurde deshalb die Behörde auf § 103 ThürBG hingewiesen. Danach sind mit Ablauf der in den Absätzen 1 bis 3 geregelten Aufbewahrungsfristen die Personalakten dem Thüringer Staatsarchiv anzubieten. Gemäß § 103 Abs. 4 ThürBG sind die Personalakten nach Ablauf der Aufbewahrungsfrist zu vernichten, sofern sie nicht vom Staatsarchiv übernommen werden.
Außerdem wurde die Behörde aufgefordert, die der aktuellen Personalakte beigehefteten Altakten durchzusehen und alle Teile, die nicht gemäß § 97 ThürBG mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen, aus der Personalakte zu entfernen.

Da die Behörde zukünftig eine Vernetzung mit ihren zugehörigen unteren Ämtern vorsieht, wurde auf die besondere Beachtung des § 7 ThürDSG und auf die dann erforderliche Änderungsmeldung zum Datenschutzregister hingewiesen. Im Rahmen der Prüfung wurde auch festgestellt, daß für die automatisierte Zeit- und Telefongebührenerfassung der Mitarbeiter keine Löschungsfristen festgelegt waren. Gemäß § 16 Abs. 2 ThürDSG sind personenbezogene Daten zu löschen, wenn sie von der speichernden Stelle zur Aufgabenerfüllung nicht mehr benötigt werden.

6.1.10 Kontrolle der Lehrerpersonalverwaltung im Landesverwaltungsamt

Im Berichtszeitraum erfolgte eine Kontrolle in der Personalverwaltung der Lehrer im LVwA. Schwerpunkt bildete dabei die Führung von Teil- und Nebenakten, die Zugriffsberechtigung der Mitarbeiter auf einzelne Unterlagen, Fragen der Aufbewahrung und Archivierung sowie die Nutzung automatisierter Verfahren im Personalbereich.
Im Ergebnis der Prüfung wurde folgendes festgestellt:

Obwohl die zuständige Abteilung im LVwA über einen Arbeitsverteilungsplan verfügt, der hinsichtlich der Zuständigkeiten der Mitarbeiter klare Aufgabenabgrenzungen vorsieht, hatten die Mitarbeiter auch die Möglichkeit, Personaldaten anderer Sachgebiete einzusehen. Begründet wurde dies damit, daß entsprechend der anstehenden Aufgaben übergreifende Arbeitsgruppen gebildet und Vertretungen abgesichert werden mußten sowie die Unterstützung einzelner Bereiche bei größerem Arbeitsanfall zeitweise erforderlich war. Aufgrund der Beanstandung durch den TLfD gemäß § 39 ThürDSG wurde dies zwischenzeitlich abgestellt.
In der Personalverwaltung der Lehrer wurde ein automatisiertes Verfahren angewandt, wofür keine Zustimmung des zuständigen Personalrates vorlag, was aber gemäß § 74 des Thüringer Personalvertretungsgesetzes (ThürPersVG) eine Voraussetzung für die Nutzung automatisierter Verfahren zur Personalverwaltung und Bewirtschaftung ist. Der Einwand, daß dieses Verfahren bereits 1993 und damit vor Inkrafttreten des ThürPersVG eingeführt worden war, konnte insoweit nicht akzeptiert werden, als sich die Mitwirkung des Personalrates nicht nur auf die Einführung bzw. Änderung vorhandener Programme bezieht, sondern ausdrücklich die Anwendung einbezieht, die nach Inkrafttreten des ThürPersVG vorlag. Dementsprechend ergab sich daraus die Verpflichtung der Behördenleitung, für eine weitere Anwendung die Zustimmung des Personalrates einzuholen. Erst nach mehrmaligem Schriftwechsel und Einbeziehung des Kultusministers konnte erreicht werden, daß die Beteiligung des Hauptpersonalrates eingeleitet wurde.
Im Rahmen der Prüfung wurde weiterhin festgestellt, daß die automatisiert erhobenen Personaldaten in regelmäßigen Abständen dem TKM zur Verfügung gestellt wurden. Unbestritten ist, daß das TKM als oberste Schulaufsichtsbehörde für alle Angelegenheiten der Schulaufsicht zuständig ist, die nicht durch Gesetz anderen Behörden zugewiesen sind. Gleichzeitig kann das TKM im Einzelfall im Rahmen seiner Entscheidungsbefugnisse sowie bei der Wahrnehmung seines Kontroll- und Aufsichtsrechts Einsicht in Personalunterlagen nehmen. Im ThürBG heißt es dazu, daß die Personalakte zum Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Aufsichtsbehörde vorzulegen ist. Gemäß § 4 des Gesetzes über die Schulaufsicht ist das LVwA insbesondere zuständig für die laufenden Angelegenheiten der Personalverwaltung für die im Dienst des Landes Thüringen stehenden Mitarbeiter in den staatlichen Schulämtern, Schulleiter, Lehrer, Erzieher, Seminarleiter, Fachlehrer und Lehramtsanwärter. Dementsprechend ist eine regelmäßige, den gesamten Lehrerbestand umfassende, aktuelle Übermittlung von Personaldaten an die Aufsichtsbehörde nicht erforderlich. Aufgrund der Kritik des TLfD an dieser Verfahrensweise wurde inzwischen eine weitere Datenübermittlung in dieser Form ausgeschlossen und der vorhandene Datenbestand im TKM gelöscht.

Hinweise und Anfragen von Lehrern ergaben, daß bisher von Personalunterlagen und Urkunden bis zu fünf Exemplaren abgefordert worden waren (Schule, Schulamt, Landesverwaltungsamt, Kultusministerium, Zentrale Gehaltsstelle). Die Stichprobenkontrolle in einem Schulamt bestätigte das insoweit, als dort Nebenakten geführt wurden, die u. a. Abdrucke von Geburtsurkunden, Heiratsurkunden, Scheidungsurteilen, Ablichtungen von Pässen, Personalausweisen, Wehrdienstausweisen, Gesundheitszeugnissen u. a. enthielten, die das Schulamt zur Wahrnehmung seiner Aufgaben nicht benötigt.
Aufgrund der Feststellungen und der Tatsache, daß abschließende Regelungen über die Führung von Teil- und Nebenakten im Kultusbereich nicht vorliegen, wurde die Personalverwaltung im LVwA aufgefordert, entsprechende Regelungen zu treffen. Im Ergebnis dessen erfolgte vom LVwA zwischenzeitlich die Aufforderung an alle Schulen, vorhandene Personalnebenakten an die Schulämter zur Weiterleitung an das LVwA zu übergeben. Eine Führung von Nebenakten ist in der Schule künftig nicht mehr zulässig. Im weiteren wurden die Schulämter verpflichtet, alle vorhandenen Nebenakten zu sortieren und verpackt bereitzustellen, damit sie in Kürze vom LVwA übernommen werden können. Dort werden dann vorhandene doppelte Unterlagen, Zeugnisse und Belege im Zuge der Umsetzung des Besoldungsgesetzes für die Lehrer in Thüringen ausgesondert und nach Prüfung an die Bediensteten zurückgegeben. Von einer Neuregelung zur Personalnebenaktenführung an den Schulämtern wird derzeit abgesehen, da die Überprüfung der Geschäftsverteilung im Bereich des TKM, in dem auch die Aufgaben der staatlichen Schulämter und der für die Personalbewirtschaftung zuständigen Abteilung des LVwA berührt werden, noch nicht abgeschlossen ist.

Im Rahmen der Prüfung im LVwA wurde festgestellt, daß dort weder Personal- bzw. Kaderakten von den vor 1990 aus dem Schuldienst ausgeschiedenen Lehrern und Erziehern aufbewahrt werden noch Übersichten der Aufbewahrungsorte dieser Unterlagen vorliegen. Gemäß § 30 ThürDSG stehen personenbezogene Daten aus ehemaligen Einrichtungen, die vor dem 03.10.1990 nach ihrer Zweckbestimmung überwiegend für Verwaltungsaufgaben gespeichert waren, die nach dem Grundgesetz von Ländern wahrzunehmen sind, demjenigen Träger öffentlicher Verwaltung zu, der nach dem Grundgesetz für die Verwaltungsaufgaben zuständig ist. Entsprechend dem Thüringer Gesetz über die Schulaufsicht, in dem die Gesamtheit der staatlichen Aufgaben zur inhaltlichen, organisatorischen und planerischen Gestaltung und die Beaufsichtigung des Schulwesens als Aufgabe der Schulaufsicht benannt wird, ist das LVwA für die laufenden Personalangelegenheiten der im Dienst des Freistaats stehenden Lehrer und Erzieher zuständig. Daraus ergibt sich, daß das LVwA nach § 30 ThürDSG auch für die Altakten des o. g. Personenkreises zuständig ist. Obwohl der TLfD bereits Ende 1994 auf dieses Problem hingewiesen hatte, erfolgten weder vom LVwA als zuständige Stelle noch vom TKM als Fachaufsichtsbehörde ausreichende Aktivitäten.
Es kann sicher akzeptiert werden, daß aufgrund der laufenden Prüfung der Organisationsstrukturen im Bereich des TKM gegenwärtig noch keine abschließende Aussage zur künftigen Art und Weise der Verwahrung dieser Unterlagen getroffen werden kann. Dessen ungeachtet wurde das LVwA aufgefordert, seiner Verantwortung für eine ordnungsgemäße Verwahrung und Nutzung der Daten auch gegenwärtig bereits im vollen Umfang gerecht zu werden. Dazu ist es erforderlich, auf der Grundlage einer Bestandsaufnahme kurzfristig die notwendigen Regelungen zu treffen, um künftig zu sichern, daß vom LVwA alle diesbezüglichen Anfragen ehemaliger Lehrer und Erzieher, die vor 1990 aus dem Schuldienst ausgeschieden waren (z. B. zur Durchsetzung von Rentenansprüchen), beantwortet werden können.
Soweit die Akten auch künftig außerhalb des Verantwortungsbereiches des LVwA (z. B. in Kreisarchiven) aufbewahrt werden, müssen die Bestimmungen gemäß § 8 ThürDSG zur Auftragsdatenverarbeitung beachtet werden. Der TLfD wird die Realisierung dieser Forderungen weiterhin beobachten und entsprechend vor Ort kontrollieren.

6.1.11 Personalverwaltung im Polizeipräsidium

Das Thüringer Polizeipräsidium führt sämtliche Personalakten der Thüringer Polizeibeamten und der Angestellten und Arbeiter im Polizeibereich. Ende März 1995 wurde das Thüringer Polizeipräsidium im Bereich der Personalverwaltung einer datenschutzrechtlichen Prüfung unterzogen. Aus datenschutzrechtlicher Sicht wurde eine Fülle von Mängeln festgestellt.
Zum Zeitpunkt der Prüfung war für das Polizeipräsidium kein bDSB bestellt. Es lagen auch keine internen Datenschutzregelungen vor, die vorhandene Datenverarbeitungstechnik wurde in datenschutzrechtlicher Hinsicht nicht betreut, besondere Datensicherungsmaßnahmen fehlten.

In Anbetracht der im Gebäude der Personalverwaltung des Polizeipräsidiums vorhandenen sensiblen personenbezogenen Daten (Personalakten, Vergütungsakten, Disziplinarvorgänge usw.) und deren besonderer Schutzwürdigkeit genügte die vorgefundene Sicherung der Räumlichkeiten in keiner Weise den Anforderungen an eine ordnungsgemäß gesicherte Unterbringung. Das Gebäude war insgesamt leicht zugänglich. Zu fordern war auch eine Schlüsselordnung und ein Nachweis über den Verbleib von Schlüsseln. Das Polizeipräsidium hat inzwischen die erforderlichen Sicherungsmaßnahmen durchgeführt bzw. zugesagt.

Auch der Umgang mit den sensiblen Personalaktendaten mußte kritisiert werden. Die Personalstammdaten wurden mittels eines automatisierten Verfahrens verwaltet, welches nicht gemäß § 34 Abs. 2 ThürDSG freigegeben war. Die nach dem ThürPersVG erforderliche Beteiligung des Personalrats lag ebenfalls nicht vor. Die fehlende Freigabe war gemäß § 39 ThürDSG zu beanstanden. Die Freigabe durch das TIM ist inzwischen erfolgt. Die datenschutzrechtliche Beanstandung in diesem Punkt ist daher behoben.

Die Einsichtnahme in verschiedene Ordner mit der Beschriftung “Bewerbungen” ergab, daß Bewerbungsunterlagen vorgehalten wurden, obwohl die Bewerbungsverfahren abgeschlossen waren. Bewerbungsunterlagen von nicht eingestellten Bewerbern dürfen aber über den Zeitpunkt des Abschlusses des Bewerbungsverfahrens hinaus nicht vorgehalten werden, wenn keine entsprechende Einwilligung der Betroffenen vorliegt. Die Vorhaltung ohne Einwilligung als Speicherung ist nicht erforderlich und damit unzulässig und war daher gemäß § 39 Abs. 1 ThürDSG in Verbindung mit § 20 Abs. 1 ThürDSG zu beanstanden. Das Thüringer Polizeipräsidium wurde aufgefordert, die Bewerbungsunterlagen umgehend zurückzugeben oder, soweit nicht zustellbar, zu vernichten. Das Thüringer Polizeipräsidium hat inzwischen mitgeteilt, daß die entsprechenden Ordner überarbeitet wurden und Unterlagen, soweit erforderlich, vernichtet sind.
In verschiedenen Dienstzimmern befanden sich unter anderem auch Kartons und Ordner mit ungeordneten Unterlagen, die im unmittelbaren Zusammenhang mit dem Dienstverhältnis der Betroffenen standen. Diese müssen jeweils zur Personalakte genommen werden. Nachgereichte Geburtsurkunden und Heiratsurkunden, die in der zentralen Aktenre-

gistratur zunächst in einem offenen Karteikasten abgelegt waren , müssen auf die Erforderlichkeit zur Aufnahme in die Personalakte oder zur Weiterleitung an die Gehaltsstelle überprüft werden. Sollten diese Unterlagen bereits vorhanden sein, so sind sie den Betroffenen zurückzugeben. Andere Vorgänge - ebenfalls ungeordnet - in Ordnern oder Kartons müssen aufbereitet oder ggf. vernichtet werden.
Den Personalakten aus dem Angestelltenbereich und dem Beamtenbereich waren, sofern die Mitarbeiter aus dem Beschäftigungsverhältnis übernommen worden waren, Unterlagen des dem Dienstverhältnis mit dem Freistaat Thüringen vorangegangenen Beschäftigungsverhältnis vorgeheftet. Darin waren auch Unterlagen enthalten, die für das gegenwärtige Arbeitsverhältnis nicht erforderlich sind. Darüber hinaus fanden sich in den Akten auch Mehrfertigungen von Urkunden und Unterlagen. Zur Personalakte gehören nur die Unterlagen, die in einem unmittelbaren Zusammenhang mit dem Beschäftigungsverhältnis der betreffenden Person stehen (§ 97 Abs. 1 Satz 2 ThürBG), alle anderen Unterlagen sind zu entfernen.
In allen vier Sachgebieten und einer zugeordneten Organisationseinheit befanden sich jeweils Kopien bzw. Mehrfertigungen der Unterlagen aus den Personalakten, was als unzulässige Doppel- und Nebenakten zu werten ist. Nebenakten dürfen nach § 97 Abs. 2 Satz 2 ThürBG nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für den Beamten zuständig sind, was für das Polizeipräsidium jedoch nicht zutrifft. Angesichts des Vorhandenseins der gesamten Personalakte mit allen für die Aufgabenerfüllung erforderlichen Unterlagen in der zentralen Personalaktenverwaltung in demselben Gebäude und somit der Möglichkeit des Zugriffs der zuständigen Bediensteten auf die jeweilig für die Aufgabenerfüllung erforderlichen Teile besteht keinerlei Erforderlichkeit zur Führung von Doppel- bzw. Nebenakten in den verschiedenen Sachgebieten. Doppel- bzw. Nebenakten sind zu vernichten. Auch von Disziplinarvorgängen oder Ermittlungsergebnissen waren neben den sich in der zentralen Personalaktenregistratur befindlichen Disziplinarakten Zweitschriften unverschlossen in Ordnern auf einem Schrank in einem Dienstzimmer vorhanden. Dies war zum einen als unzulässige Nebenakten und zum anderen wegen des fehlenden Schutzes gegen unbefugten Zugriff zu beanstanden.
Aufgrund der vorgefundenen gravierenden datenschutzrechtlichen Verstöße hat sich der TLfD veranlaßt gesehen, die gesamte Personalaktenführung zu beanstanden. Das Thüringer Polizeipräsidium wurde aufgefordert, die vorhandenen Personalakten entsprechend den §§ 97 ff. ThürBG vollständig zu überarbeiten, wobei alle wesentlichen und notwendigen Bestandteile aufgenommen und unzulässige Teile sowie Mehrfachfertigungen entfernt werden müssen. Hierzu wären entsprechende Richtlinien hilfreich, die jedoch noch ausstehen (siehe Punkt 6.1.1).
Das Polizeipräsidium hat auf den hohen Arbeitsaufwand und das Fehlen des hierfür erforderlichen Personals verwiesen, so daß eine Bereinigung der Personalakten zunächst nur im laufenden Dienstbetrieb möglich sei. Dies darf aber nicht dazu führen, daß der überwiegende Teil der Personalakten bei der Umstrukturierung des Polizeipräsidiums im kritisierten Zustand, der immerhin schon seit der Durchführung der datenschutzrechtlichen Kontrolle bekannt ist, an andere Stellen weitergegeben wird. Diese Stellen erhielten dann ebenfalls Kenntnis der unzulässigen Teile, was wiederum problematisch ist.
Der TLfD wird die Realisierung der geforderten Maßnahmen gegebenenfalls im Rahmen einer Kontrolle überprüfen.

6.1.12 Personalakten der Strafvollzugsbediensteten

Der Aufbau der Personalakten der Strafvollzugsbediensteten richtet sich nach der Verwaltungsvorschrift des Thüringer Justizministeriums vom 01.10.1992. Danach gliedern sich die Personalakten in Personalhauptakten, Personalbei- und Personalnebenakten. Die Personalhauptakten werden beim TMJE geführt, Personalnebenakten führen die Justizvollzugsanstalten. Zu den Haupt- und Nebenakten gehören auch jeweils Beihefte. Anläßlich einer datenschutzrechtlichen Kontrolle in einer JVA konnte von den Mitarbeitern des TLfD in die dort geführten Personalnebenakten zunächst keine direkte Einsicht genommen werden. Anhand der Schilderung des Inhaltes der Personalnebenakten wurde seitens des TLfD der Schluß gezogen, daß es sich dabei um eine vollständige Kopie der im TMJE geführten Akten handeln mußte. Demgemäß war die Führung von unzulässigen Doppelakten zu beanstanden, da eine Nebenakte nach § 97 Abs. 2 Satz 3 ThürBG nur solche Unterlagen enthalten darf, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist, keinesfalls aber den Umfang einer Personalhauptakte haben darf. Hierzu wurde vom TMJE ausgeführt, es handle sich nicht um die vollständige Kopie der im Ministerium geführten Unterlagen, die Personalhauptakte sei in jedem Fall umfänglicher.
Daraufhin wurde im TMJE eine datenschutzrechtliche Kontrolle gemäß § 37 ThürDSG durchgeführt. Es wurde festgestellt, daß die Personalhauptakten in der Tat umfänglicher waren. Dies lag vor allem daran, daß die alten "Kaderakten" weitergeführt wurden. Dies erfolgte dergestalt, daß jeweils die alte Personalakte aus "DDR-Zeiten" vollständig übernommen, entsprechend der Verwaltungsvorschrift in die Hefter eingeordnet und um die neuen Bestandteile des aktuellen Beschäftigungsverhältnisses ergänzt wurde. So befanden sich in den aktuellen Personalhauptakten auch handschriftliche Bewerbungsschreiben zum Dienst im Strafvollzug der DDR, Ermittlungsberichte, Leistungseinschätzungen mit Aussagen zur politischen Zuverlässigkeit und zum Teil auch "Unterhaltungsblätter" über aufgetauchte Differenzen im Zusammenhang mit der Tätigkeit aus "DDR-Zeiten". Jeweils mit eingeheftet war auch der

Personalbogen aus der Altakte mit der gesamten Familienübersicht inklusive Angaben über Parteimitgliedschaften von Familienmitgliedern, über Schwiegereltern und Geschwister des Ehepartners sowie deren Ehegatten.
Eine Zulässigkeit der Speicherung von Unterlagen aus den Altakten kann jedoch auf Grund der Erforderlichkeit für die Aufgabenerfüllung nur für die Urkunden gesehen werden, die zum Nachweis eines lückenlosen Lebenslaufs dienen können (Abschlußzeugnisse u. ä.) und nur für die Unterlagen, die für die Übernahme in die Dienstlaufbahn relevant waren. Alle übrigen Altunterlagen sind umgehend aus der Hauptpersonalakte zu entfernen, da sie gemäß § 97 Abs. 1 Satz 2 ThürBG nicht in die Personalakte aufgenommen werden dürfen. Unterlagen mit politischem Charakter oder den privaten Bereich berührend könnten schon aufgrund der Verwaltungsvorschrift über die Führung von Personalakten ohne Zustimmung des Beamten grundsätzlich nicht aufgenommen werden. Da hier jedoch § 97 Abs. 1 Satz 2 ThürBG eine Regelung getroffen hat, nach der diese Unterlagen eindeutig nicht aufgenommen werden können, ist eine Zustimmung des Betroffenen zum Verbleib der unzulässigen Unterlagen unbeachtlich, denn der Verbleib in der Personalakte untersteht nicht der Disposition des Betroffenen. Die Weiterführung der alten Kaderakten ohne Überprüfung auf die Erforderlichkeit der Unterlagen durch das TMJE wurde demgemäß beanstandet.

Die Personalnebenakten wurden sodann hinsichtlich der Erforderlichkeit zur Aufgabenerfüllung in der JVA erneut kontrolliert. Anhand einer Aufstellung der Aufgaben einer JVA wurde eine Vielzahl von Unterlagen als für die Aufgabenerfüllung nicht erforderlich festgestellt. Im Vergleich zu den im TMJE geführten Personalhauptakten ergab sich darüber hinaus, daß in den in der JVA geführten Nebenakten lediglich die alten “Kaderakten” fehlten, auf die es jedoch zur Beurteilung der Zulässigkeit der Nebenakten nicht ankommen kann, da die Unterlagen aus den Kaderakten, wie ausgeführt, in weiten Teilen für eine Personalakte unzulässig sind.
Die Bestimmung der Verwaltungsvorschrift zur Führung von Personalakten, daß in Personalnebenakten nur solche Vorgänge aufgenommen werden dürfen, die auch in den Personalhauptakten oder Personalbeiakten enthalten sind, führt dazu, daß die aufgrund der Aufgabenerledigungen in der JVA anfallenden Unterlagen auch zur Personalhauptakte gegeben werden müssen, obwohl im TMJE keine Aufgaben hierzu zu erledigen sind. So kommt es zu einer Doppelung von Unterlagen in nicht erforderlicher Weise, indem die jeweils aufgabenerfüllende Stelle der anderen Stelle Unterlagen zukommen läßt, die dann abgeheftet werden.
Der TLfD hat angeregt, die Möglichkeit zu prüfen, für die Aufgaben, die ausschließlich von einer Stelle wahrgenommen werden, Teilakten zu bilden und diese nur bei dieser Stelle zu führen. Die Verwaltungsvorschrift zur Führung von Personalakten ist dringend auf die Vereinbarkeit mit dem Thüringer Beamtengesetz und dem Erforderlichkeitsgrundsatz wegen der festgestellten Unstimmigkeiten zu überprüfen.

6.1.13 Zeugnis und Ausbildungsnachweise für Referendare

Im Kreise der DSB des Bundes und der Länder wurde der TLfD auf die Problematik hingewiesen, daß in Referendarzeugnissen krankheits- und urlaubsbedingte Abwesenheitszeiten nur dann aufgenommen werden sollten, wenn diese Zeiten Einfluß auf die Beurteilung haben, weil der Ausbildungszeitraum durch sie zu stark verkürzt worden ist. Der TLfD hat diesen Hinweis gegenüber dem TMJE aufgegriffen, das hierzu eine andere Auffassung vertritt. Das TMJE ist der Ansicht, daß diese Daten erforderlich sind, weil sie zur Beurteilung der Tatsachengrundlage der in den Zeugnisformularen getroffenen Bewertung geeignet seien und bei häufiger Unterbrechung bzw. Fehltagen in kurzen Ausbildungsabschnitten das mildeste Mittel darstellten, da nicht der Grund der Abwesenheit genannt wird. Diese Auffassung überzeugt nicht, da Unterbrechungen und Fehltage der personalverwaltenden Stelle zu melden sind und auch der Ausbilder davon Kenntnis erhält. Der Zeugnisinhalt sollte neben dem Zeitraum, in welchem die Ausbildung absolviert wurde, enthalten, was dort geleistet wurde und wie diese Leistung benotet wurde. Es ist nicht erkennbar, welchen Zweck die Kenntnis der Unterbrechungszeiträume haben soll, so daß die Erforderlichkeit hier zu verneinen ist.

6.1.14 Aushändigung von Personalakten an das Rechtsamt

An den TLfD herangetragen wurde die Frage nach der Zulässigkeit der Aushändigung von Personalakten an das Rechtsamt, das für die Behörde einen Prozeß führt. Bei formaler Betrachtungsweise ließe sich die Ansicht vertreten, daß dies unzulässig sei, da das Rechtsamt im Rahmen der Personalverwaltung nicht mit der Bearbeitung von Personalangelegenheiten betraut ist, sondern nur fallweise zur Bearbeitung hinzugezogen wird. Dieser Auffassung ist jedoch nicht beizupflichten. Hier ist der Bearbeiter im Rechtsamt im Sinne der beamtenrechtlichen Vorschriften des § 97 Abs. 3 ThürBG, der § 56 Abs. 3 BRRG entspricht, als mit der Bearbeitung von Personalangelegenheiten beauftragt anzusehen, so daß die Aushändigung der Personalakte keinen Bedenken unterliegt. Für den Fall, daß Teilakten gebildet sind, sind jedoch die Teilakten auszusondern, auf die es bei der Führung des Prozesses nicht ankommt. Wenn beispielsweise Prozeßgegenstand die Genehmigung zu einer Dienstreise ist, ist im Regelfall nur die entsprechende Teilakte auszuhändigen, während bei einem das Beamtenverhältnis selbst betreffenden Verfahren die Teilakten üblicherweise nicht erforderlich sind. Auch bei der Diskussion, die zu diesem Thema bundesweit geführt wurde, ist diese Auffassung weitgehend vertreten worden.

6.1.15 Datenübermittlung aus Personalakten zum Zwecke der Rechtsberatung einer Behörde

Im Auftrage mehrerer Fraktionen eines Stadtrates wurde der TLfD gebeten, zu prüfen, inwieweit es zulässig ist, daß ein Bürgermeister dem Justitiar der Stadtverwaltung sowie dem Justitiar der Wohnungsgesellschaft, deren Gesellschafteranteile sich vollständig in der Hand der Stadt befinden, Teile der Personalakte eines Mitarbeiters der Stadtverwaltung (einschließlich des Überprüfungsergebnisses zur persönlichen Eignung) zur Einsichtnahme überläßt. Der Bürgermeister war auf Beschluß des Stadtrates mit der Überprüfung der Mitarbeiter auf eine eventuelle Tätigkeit für das Ministerium für Staatssicherheit der ehemaligen DDR beauftragt und hatte sich von den Justitiaren zur arbeitsrechtlichen Bewertung des Überprüfungsergebnisses des Bediensteten beraten lassen. Beide Personen hatten im weiteren die Stadt in der ersten Instanz des betroffenen Arbeitsgerichtsverfahrens, für das kein Anwaltszwang besteht, vertreten. Dazu war es erforderlich und zulässig, den Beauftragten Einblick im Vorfeld in die für ein eventuelles Gerichtsverfahren erheblichen Unterlagen zu gewähren, so daß eine Übergabe der Unterlagen an die Justitiare möglich war. Durch entsprechende Empfangsbekenntnisse, die vorlagen und in denen ausdrücklich der Verwendungszweck sowie die Einhaltung der Vertraulichkeit festgehalten wurde, war den Anforderungen des Datenschutzes hinreichend Rechnung getragen worden.

6.1.16 Verlust einer Personalakte

Die Personalakten sind als besonders sensible Daten auch besonders zu schützen, insbesondere auch vor unbefugter Einsicht. Ein Verlust der Unterlagen bedeutet für einen Betroffenen, daß er sämtliche für die Personalverwaltung oder Personalwirtschaft erforderlichen Unterlagen nachreichen muß, damit die Voraussetzungen für die Aufgabenerfüllung der personalführenden Stelle vorliegen. Ohne Personalakten können keine Ernennungen, Beförderungen bis hin zu Gehaltszahlungen erfolgen. Der Verlust bedeutet für den Betroffenen immer Unannehmlichkeiten.
Ein Petent hat sich, nachdem seine Nachfragen und Bemühungen seit Juni 1992 zur Auffindung seiner Personalakte erfolglos geblieben waren, an den TLfD gewandt. Die Bemühungen des TLfD haben nicht zum Auffinden der Personalakte geführt.
Bei den durchgeführten Kontrollen wurden folgende datenschutzrechtliche Bedenken festgestellt:
Zu berücksichtigen war die Aufbausituation in den Behörden eines neuen Bundeslandes.
Bei Dienstantritt des Betroffenen Anfang März 1992 war die Personalakte in der Behörde als personalverwaltende Stelle vorhanden. Personalakten mußten zwecks Einstellung dem zuständigen Ministerium vorgelegt werden. Zum fraglichen Zeitpunkt waren weder im Personalreferat der Behörde noch des Ministeriums schriftliche Aufzeichnungen darüber angefertigt worden, welche Personalakten aus- bzw. eingegangen sind. Die fehlende Dokumentation war aus datenschutzrechtlicher Sicht als organisatorischer Mangel zu kritisieren. Seit Anfang 1993 wird im Ministerium und seit Ende 1992 in der Behörde die erforderliche Dokumentation zum Verbleib von Personalunterlagen geführt. Insofern sind die damaligen Mängel zwischenzeitlich behoben, so daß von einer Beanstandung gemäß § 39 Abs. 3 ThürDSG abgesehen werden konnte.
In der Behörde wurde darüber hinaus festgestellt, daß mangels Auffindbarkeit der Originalpersonalakte vom Betroffenen nachgereichte Kopien und Duplikate geführt wurden. Die Voraussetzungen zur Zulässigkeit der Führung einer Nebenakte lagen jedoch nicht vor, so daß diese Unterlagen als unzulässige Doppel- bzw. Nebenakte zu werten waren. Im Laufe der Kontrolle hat die Behörde nunmehr formell festgestellt, daß die Originalpersonalakte tatsächlich nicht vorhanden ist, und die vorhandenen Unterlagen als Ersatzakte geführt werden. Insofern ist auch dieser datenschutzrechtliche Mangel behoben worden.

6.2 Beihilfe

6.2.1 Kontrolle der Zentralen Beihilfestelle

Im Rahmen der Kontrolltätigkeit des TLfD wurde die Zentrale Beihilfestelle in Stadtroda geprüft. Sie ist insbesondere zuständig für die Beihilfebearbeitung für die Landesbeamten mit Ausnahme der Justiz und der Finanzverwaltung. Aus datenschutzrechtlicher Sicht ist die Einrichtung einer von der übrigen Verwaltung getrennten, zentralen Organisationseinheit zur Beihilfebearbeitung, wie dies die Zentrale Beihilfestelle in Stadtroda darstellt, eine optimale Lösung zur Gewährleistung der Forderung des ThürBG, daß nur die Beschäftigten der Beihilfestelle Zugang zu den Beihilfeakten erhalten dürfen.
Beihilfeakten sind regelmäßig Unterlagen mit höchst sensiblen persönlichen Daten über Krankheiten, Diagnosen, Behandlungen und Medikationen der Bediensteten, die bei einer unbefugten Offenbarung zu spürbaren Nachteilen für den Betroffenen führen können. Eine Verarbeitung und Nutzung der Daten muß deshalb ausschließlich auf das Beihilfeverfahren beschränkt bleiben. In § 98 ThürBG ist deshalb bestimmt, daß die Beihilfebearbeitung in einer von der übrigen Personalverwaltung getrennten Organisationseinheit erfolgen soll. Insoweit ergab die Kontrolle in der Zentralen Beihilfestelle, daß dort das vom Gesetzgeber geforderte Abschottungsprinzip strikt eingehalten wird.

6.2.2 Verwendung von Beihilfestammdaten für Besoldungszwecke

Im Rahmen der Bund-Länder-Diskussion erhielt der TLfD Kenntnis davon, daß Überlegungen bestehen, § 56a Satz 4 BRRG, dem § 98 ThürBG wortgleich entspricht, um eine Regelung zu ergänzen, die es ermöglicht, Daten aus Beihilfeakten auch für Besoldungszwecke zu nutzen. Die Verwendung der Beihilfedaten für andere als Beihilfezwecke wäre eine Zweckdurchbrechung, die nur dann zulässig ist, wenn der Beihilfeberechtigte oder der bei der Beihilfegewährung zu berücksichtigende Angehörige im Einzelfall in eine entsprechende Datenübermittlung einwilligte. Für eine Durchbrechung dieser Zweckbindung wird jedoch keine Notwendigkeit gesehen. Hinzu kommt, daß es dem Beihilfeberechtigten unbenommen bleibt, beim Beihilfeantrag ein vom Gehaltskonto abweichendes Konto zu wählen, so daß eine regelmäßige Datenübermittlung von der Beihilfestelle an die Zentrale Gehaltsstelle diese Daten erhielte, die nicht erforderlich wären. Eine Anfrage beim TIM zeigte, daß dieses ebenfalls keinen Bedarf zur Änderung der auf strikte Zweckbindung ausgerichteten Regelungen sieht.

6.2.3 Beihilfebearbeitung in den Landkreisen und Kommunen

Nach Erkenntnis des TLfD sind im kommunalen Bereich häufig Beihilfestellen unmittelbar in Personalämter bzw. Personalstellen eingebunden. Gemäß § 98 ThürBG soll allerdings die Beihilfebearbeitung in einer von der übrigen Personalverwaltung getrennten Organisationseinheit erfolgen. Mit dieser Regelung soll jede Vermischung zwischen Personalverwaltung und Beihilfebearbeitung ausgeschlossen werden. Das bedeutet aber, daß auch im Rahmen der Fachaufsicht Mitarbeiter oder Leiter der Personalverwaltungen keinen Zugang zu Beihilfeunterlagen haben dürfen, was natürlich bei einer organisatorischen Zugehörigkeit der Beihilfestelle zum Personalbereich regelmäßig nicht gegeben ist. Spätestens dann, wenn z. B. Beihilfeanträge vom Beihilfesachbearbeiter bearbeitet, aber die Bescheide vom Leiter der Personalstelle unterzeichnet werden, wenn Mitarbeiter der Personalverwaltung Zugang zu den Räumen der Beihilfestelle erhalten, wenn Widersprüche, Beschwerden und Eingaben bei der Beihilfestelle durch den Leiter der Personalstelle bearbeitet und entschieden werden oder wenn Mitarbeiter in Vertretungsfällen in beiden Bereichen eingesetzt werden, ergeben sich datenschutzrechtlich bedenkliche Konfliktsituationen, die vom Gesetzgeber nicht gewünscht sind.
Obwohl in besonderen, begründeten Ausnahmefällen Abweichungen aufgrund der “Sollvorschrift” möglich sind, wie insbesondere bei kleineren Behörden, bei denen die erforderliche Abschottung nur mit großem personellen und materiellen Aufwand sichergestellt werden kann, sollte jedoch aus datenschutzrechtlicher und sicher auch aus wirtschaftlicher Sicht eher darüber nachgedacht werden, “zentrale” bzw. “gemeinsame” Beihilfestellen einzurichten.

6.3 Zentrale Gehaltsstelle

6.3.1 Prüfung der Zentralen Gehaltsstelle

Bei einer Kontrolle der Zentralen Gehaltsstelle Thüringen (ZGT) wurde festgestellt, daß die seinerzeitige räumliche Unterbringung nicht den Mindeststandard, der für den Umgang mit personenbezogenen Daten erforderlich ist, gewährleistet. Über eine allgemein zugängliche Feuerleiter war es möglich, Zugang zu den Räumlichkeiten und damit zu den Besoldungsakten der Beschäftigten des Freistaats Thüringen zu erhalten. Der TLfD hat hier eine Beanstandung ausgesprochen. Der TLfD geht davon aus, daß der Mangel behoben wurde, indem ein Umzug in ein anderes Gebäude zwischenzeitlich erfolgte.
Der Postweg ist bei der ZGT so organisiert, daß die Post bei der Oberfinanzdirektion Erfurt (OFD), zu der die ZGT organisatorisch zählt, eingeht und von dort an die ZGT weitergeleitet wird. Auf diese Weise erhalten Mitarbeiter der Poststelle der OFD, ohne daß hierfür eine Notwendigkeit besteht, Kenntnis von personenbezogenen Daten, so daß von seiten des TLfD eine datenschutzgerechte Organisation des Postweges gefordert wird. Nach Mitteilung der ZGT beabsichtigt sie, dieser Forderung nachzukommen. Auch bei einigen anderen Fällen hat die ZGT datenschutzrechtlich problematische Zustände abgestellt, so daß die Forderungen des TLfD weitgehend erfüllt wurden.
Bei der Einsichtnahme in Vergütungsakten von Mitarbeitern des Freistaats Thüringen stellte sich heraus, daß Ablichtungen und Unterlagen in diesen Akten enthalten waren, für deren Aufnahme keine eindeutigen Regelungen vorhanden sind. Der TLfD vertritt die Auffassung, daß die Aufnahme von Personalunterlagen aus den Grund- bzw. Teilakten in Nebenakten die Ausnahme sein muß und nur dann erfolgen sollte, wenn dies unbedingt für die Aufgabenerfüllung erforderlich ist. Schon im Jahre 1994 hat der TLfD darauf hingewiesen, daß hier klare und eindeutige Regelungen zu treffen sind, was bis zum heutigen Tage noch nicht erfolgt ist. Es wird noch nach einem Entwurf von Vollzugsbestimmungen verfahren. Seitens des TLfD wurde die Empfehlung ausgesprochen, angesichts des Umstandes, daß es sich bei den Vergütungsakten um Teilakten von Personalakten handelt, das TIM bei der Erarbeitung einer entsprechenden Richtlinie einzubeziehen. Ob beabsichtigt ist, diese Anregung aufzugreifen, wurde bisher nicht deutlich.

6.3.2 Auskunftserteilung durch die Zentrale Gehaltsstelle

Von der Zentralen Gehaltsstelle des Freistaats Thüringen wurde an den TLfD die Frage herangetragen, ob an das Landesamt für Verfassungsschutz Auskünfte zu bestehenden Pfändungs- und Einziehungsverfügungen bei einem Betroffenen zu erteilen sind, der einer Sicherheitsüberprüfung unterzogen wird. Eine nähere Überprüfung ergab, daß der Betreffende erhebliche Zahlungsverbindlichkeiten hatte und in der Sicherheitserklärung Fragen nach vorliegenden Zwangsvollstreckungsmaßnahmen zu Unrecht verneint hatte. Im vorliegenden Fall bestanden gegen die Auskunftserteilung keine Bedenken, da aufgrund vorliegender Pfändungen beim Betroffenen die Vermutung der Überschuldung bestand, und damit ein sicherheitsrelevanter Aspekt gegeben war. Der TLfD hat diesen Vorgang zum Anlaß genommen, mit den Beteiligten eine grundsätzliche Regelung für künftige Verfahren zu treffen. Einvernehmen wurde hier erzielt, daß künftig bei derartigen Auskunftsersuchen nur mit dem für Änderungen und Abtretungen zuständigen Referenten der ZGT direkt Kontakt aufgenommen wird, um den Kreis derjenigen, die Kenntnis davon erhalten, daß für einen Beschäftigten des Freistaats Thüringen eine Sicherheitsüberprüfung durchgeführt wird, möglichst klein zu halten.

6.4 Datenerhebung bei Ortszuschlagsberechnung

Vom Personalrat einer Dienststelle wurde an den TLfD das Problem herangetragen, daß die Dienststelle zur Berechnung des Ortszuschlages Angaben über das Beschäftigungsverhältnis des Ehepartners erhebt. In dem konkreten Fall begegnete das hierzu verwandte Formular zwar datenschutzrechtlichen Bedenken, in der Sache selbst vertritt der TLfD allerdings die Auffassung, daß die Bezügestelle zur Prüfung der Voraussetzung für die Zahlung des Ortszuschlages nach den §§ 40, 62 BBesG und § 29 BAT sowie § 41 MTL II in die Lage versetzt werden muß, zu prüfen, ob die Voraussetzungen für die Gewährung des entsprechenden Ortszuschlages gegeben sind. In der Bund-Länder-Diskussion wird teilweise die Auffassung vertreten, daß eine bereichsspezifische besoldungsgesetzliche Regelung geschaffen werden müsse, was dem TLfD allerdings nicht vorrangig erscheint.

6.5 Stasi-Überprüfung

6.5.1 Nutzung von Stasi-Unterlagen im Personalwesen

Der Thüringer Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (TLStU) hat im August 1994 “Empfehlungen zur Verfahrensweise bei Personalüberprüfungen - Umgang mit den Auskünften des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik” herausgegeben. Adressat sind (insbesondere) öffentliche Stellen, die ihr Personal auf Verstrickung mit dem alten System hin überprüfen (müssen). Darin werden die Rechtsgrundlagen zur Überprüfung, das Verfahren zur Auskunftserteilung bei der Gauck-Behörde sowie Entscheidungshilfen zur Einzelfallüberprüfung gegeben. In diesen Empfehlungen sind auch eine Reihe von Fragestellungen angesprochen, die in datenschutzrechtlicher Hinsicht bereits mehrfach diskutiert wurden.

6.5.1.1 Sind Überprüfungsunterlagen Bestandteil der Personalakte?

Diese Frage ist mit § 97 Abs. 5 ThürBG ganz klar mit ja zu beantworten. Danach sind Unterlagen, die für die Prüfung der persönlichen Eignung im Sinne des § 6 Abs. 1 Nr. 3 und 4 und des § 8 Abs. 3 ThürBG (Vermutung der Nichteignung) bestimmt waren, in einer gegen unbefugten Zugriff besonders gesicherten Teilakte zu führen, wobei eine Nutzung einer strengen Zweckbindung unterliegt. Eine Einsichtnahme durch die personalführenden Stellen ist nach der bestandskräftigen Entscheidung über die Einstellung/ Übernahme des Betroffenen nur dann zulässig, wenn begründete Zweifel an der Richtigkeit der Angaben (z. B. durch neue Erkenntnisse der Gauck-Behörde) bestehen. Dies erscheint sachgerecht, da es sich um äußerst sensible personenbezogene Daten handelt. Hierauf bezieht sich ebenfalls das Einsichtsrecht des Betroffenen mit der Einschränkung, daß alle personenbezogenen Daten über Dritte bei der Einsichtnahme unkenntlich zu machen sind.

6.5.1.2 Regelüberprüfung der Mitarbeiter des öffentlichen Dienstes in Thüringen

Die durch den Thüringer Gesetzgeber wie auch durch die Thüringer Landesregierung geschaffenen rechtlichen Regelungen sehen vor, daß sich alle Bewerber für den öffentlichen Dienst des Landes durch eine Anfrage bei der Gauck-Behörde überprüfen lassen müssen. Für Kommunalbedienstete gibt es eine diesbezügliche Empfehlung, der nach Kenntnis des TLfD überwiegend gefolgt wird.

Rechtsgrundlage hierfür war zunächst der Einigungsvertrag, der u. a. eine Tätigkeit für das frühere Ministerium für Staatssicherheit/Amt für Nationale Sicherheit als außerordentlichen Kündigungsgrund festgeschrieben hat. Daran anknüpfend wurde im Stasi-Unterlagengesetz (§ 1 Abs. 1 Nr. 4 i. V. m. § 21 Abs. 1 Nr. 6d StUG) als bereichsspezifische Rechtsvorschrift geregelt, daß öffentliche Stellen Stasi-Unterlagen zur Überprüfung von Mitarbeitern im öffentlichen Dienst, insbesondere zur Feststellung, ob sie hauptamtlich oder inoffiziell für den Staatssicherheitsdienst tätig waren, verwenden dürfen. Diese Regelungen gehen davon aus, daß vor Einstellung eines Bediensteten, aber auch während des Dienstverhältnisses, die Eignung des Mitarbeiters hinsichtlich relevanter Verfehlungen in der Vergangenheit durch die Dienststellen zu überprüfen sind.
Hierzu hat die Thüringer Landesregierung am 23.06.1992 einen Runderlaß über die Prüfung der persönlichen Eignung für den öffentlichen Dienst (ThürStAnz Nr. 34 S. 1122; sog. “Eignungserlaß”) beschlossen. Danach ist bei allen Bewerbern durch die jeweilige oberste Dienstbehörde oder die von ihr ermächtigte nachgeordnete Behörde beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR mit Zustimmung des Bewerbers anzufragen. Den Gemeinden, Landkreisen und sonstigen der Aufsicht der Landes unterstehenden Körperschaften und Anstalten und Stiftungen des öffentlichen Rechts wird empfohlen, entsprechend zu verfahren. Der hierzu verwendete Erhebungsbogen enthält die ausdrückliche Zustimmungserklärung des Betroffenen zur Einholung von erforderlichen Auskünften bei der Gauck-Behörde.
In der Folgezeit wurden im Thüringer Beamtenrecht diese Grundsätze ebenfalls verankert. Außerdem sieht Artikel 26 Abs. 2 der Verfassung des Freistaats Thüringen vor, daß die Eignung zur Einstellung und zur Weiterbeschäftigung im öffentlichen Dienst grundsätzlich jeder Person fehlt, die mit dem früheren Ministerium für Staatssicherheit/Amt für Nationale Sicherheit zusammengearbeitet hat oder für diese tätig war.
Dieses wird in § 8 Abs. 3 des ThürBG dahin gehend konkretisiert, daß bei hauptamtlichen und inoffiziellen Mitarbeitern des MfS/AfNS sowie einer Vielzahl weiterer ehemals staatstragender Organisationen die Nichteignung für die Berufung in das Beamtenverhältnis vermutet wird, die im Einzelfall widerlegbar ist. Dieser Grundsatz findet schließlich seine konsequente Fortsetzung in § 13 Abs. 1 Nr. 3 ThürBG, der zwingend vorsieht, daß eine Ernennung eines Beamten zurückzunehmen ist, wenn er gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen hat oder die vermutete Nichteignung des § 8 Abs. 3 ThürBG nicht widerlegt werden konnte.

6.5.1.3 Umgang mit Gauck-Unterlagen bei Nichteignung für den öffentlichen Dienst

Immer wieder wenden sich Betroffene wie auch öffentliche Stellen an den TLfD mit Fragen hinsichtlich der Nutzung und Aufbewahrung von Auskunftsunterlagen des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR. Vieles davon wäre vermeidbar, wenn seitens aller öffentlichen Stellen diese Problematik immer mit der notwendigen Sensibilität behandelt werden würde und wenn insbesondere auch Hinweise, Erläuterungen bzw. landeseinheitliche Vorschriften zur Verfahrensweise (z.B. in einer Personalaktenführungsrichtlinie) zur Verfügung ständen bzw. zumindest die diesbezüglichen Empfehlungen des Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR überall Beachtung fänden. Damit wäre das Verfahren für alle Betroffenen überschaubarer und gleichzeitig frei von subjektiven Entscheidungen.
Daß Unsicherheiten und fehlende Regelungen unverhältnismäßig viel Aufwand, aber insbesondere auch Ärger und Verdruß bei den Betroffenen hervorrufen können, zeigte z.B. eine Eingabe aus dem nachgeordneten Bereich des TMWFK. Dort hatte der Leiter einer Einrichtung die Nachfrage eines nicht in den öffentlichen Dienst übernommenen ehemaligen Mitarbeiters zum Umgang mit dessen “Gauck”-Unterlagen mit dem Hinweis beantwortet, daß diese gut verwahrt wären und er (der Leiter) sich noch keine Gedanken darüber gemacht habe und z. Zt. nicht bereit sei, Festlegungen zum weiteren Umgang zu treffen.
Ungeachtet der sehr fragwürdigen Form der Beantwortung spiegelte sich in diesem Verhalten die bedenkliche Haltung wider, als sei die Einhaltung des Datenschutzes eine Ermessensfrage. Dies zeigte sich auch bei der weiteren Bearbeitung der Eingabe, indem eine abschließende Klärung erst nach einem einjährigen umfangreichen Schriftverkehr unter Einbeziehung des zuständigen Ministeriums erreicht werden konnte. Sie bestand letztlich darin, daß in Ermangelung landesweit geltender Vorschriften zur Umsetzung des StUG sowie des ThürBG das TMWFK für den eigenen Geschäftsbereich eine gesonderte Dienstanweisung zum Umgang mit den Überprüfungsunterlagen des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR erlassen hat. Darin wird, wie auch in den Empfehlungen des Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR und im Einklang mit der Auffassung des TIM sowie des TLfD, entsprechend den Bestimmungen des § 19 Abs. 7 StUG darauf hingewiesen, daß alle vom Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR den ersuchenden Stellen übergebenen Unterlagen nach der rechtskräftigen Auflösung des Arbeitsrechtsverhältnisses, bei Arbeitsplatzwechsel bzw. Nichteinstellung oder auch, wenn nach den Erkenntnissen eine Weiterbeschäftigung als zulässig erachtet wird, an den Bundesbeauftragten zurückzusenden sind bzw. im Einvernehmen mit dem Bundesbeauftragten nachweislich von der öffentlichen Stelle vernichtet werden.

6.5.2 Überprüfung der Landtagsabgeordneten

Das Thüringer Abgeordnetengesetz sieht in § 1 Abs. 2 vor, daß Abgeordnete ihre Mitgliedschaft im Thüringer Landtag verlieren, wenn sie wissentlich als hauptamtliche oder inoffizielle Mitarbeiter mit dem Ministerium für Staatssicherheit, dem Amt für Nationale Sicherheit oder Beauftragten dieser Einrichtungen zusammengearbeitet haben. Weitere Ausführungsbestimmungen zur praktischen Handhabung dieser Norm fehlen. Am 18.05.1995 hat der Thüringer Landtag einen Beschluß gefaßt, wonach alle Abgeordneten von der Gauck-Behörde überprüft werden sollen. Darunter befinden sich auch Abgeordnete, die in eine Überprüfung durch die Gauck-Behörde nicht eingewilligt haben. Unter Namensnennung wurde in den Medien über persönliche Erklärungen berichtet, die diese Abgeordneten gegenüber dem Landtagspräsidenten abgegeben hatten. Von den Abgeordneten wurde ein Verstoß gegen Datenschutzvorschriften vermutet, so daß sie sich an den TLfD gewandt haben. Nach § 37 Abs. 4 ThürDSG unterliegt der Landtag der Kontrolle durch den Landesbeauftragten für den Datenschutz nur, soweit er in Verwaltungsangelegenheiten tätig wird. Die Grenze zwischen Verwaltungstätigkeit und dem der Kontrolle des DSB entzogenen parlamentarischen Bereich kann im Einzelfall schwierig zu ziehen sein. Während die Personalverwaltung für die Mitarbeiter der Landtagsverwaltung eindeutig Verwaltungstätigkeit darstellt, ist bei der Schreibtätigkeit im Schreibdienst danach zu unterscheiden, was geschrieben wird. Das Erstellen einer Vorlage ist dem parlamentarischen Bereich zuzuzählen, während des Fertigen eines Entwurfes für eine verwaltungsinterne Dienstanweisung Verwaltungshandeln darstellt. Im konkreten Sachverhalt hat der TLfD seine Kontrollkompetenz für nicht gegeben angesehen.

6.5.3 Überprüfung kommunaler Mandatsträger

Bis zum Inkrafttreten der Thüringer Kommunalgesetze am 01.07.1994 erfolgte die Überprüfung der kommunalen Mandatsträger in der Weise, daß Gauck-Abfragen durch die jeweiligen Gemeindevertretungen bzw. Kreistage veranlaßt wurden. Mit Inkrafttreten der Kommunalgesetze änderte sich dieses Verfahren. Den Bewerbern für ein kommunales Wahlamt werden vor der Wahl Erklärungen abverlangt, ob sie wissentlich mit dem MfS/AfNS zusammengearbeitet haben (offiziell oder inoffiziell). Wird diese Erklärung wahrheitswidrig verneint, so ist zu differenzieren (Bei Bejahung hat der Wähler zu entscheiden, siehe Punkt 5.1.1):

- Bei Bewerbern für die Gemeinderäte und Kreistage entfällt die Wählbarkeit. Die Rechtsaufsichtsbehörde stellt dann den Mandatsverlust nach positivem Gauck-Bescheid und entsprechender Prüfung fest.

- Bei den Bürgermeistern und Landräten stellt die wahrheitswidrige Verneinung der Frage nach § 6 Abs. 2 Nr. 1 ThürKWBG einen Entlassungsgrund dar. Liegen der Rechtsaufsichtsbehörde Anhaltspunkte für solche wahrheitswidrige Angaben vor, so hat sie eine Prüfung vorzunehmen, die die Anforderung von Auskünften der Gauck-Behörde umfaßt.

6.5.4 Datenschutz beim Thüringer Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

Der Thüringer Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR, der mit dem am 01.04.1993 in Kraft getretenen Thüringer Landesbeauftragtengesetz (ThürLBStUG) eingeführt wurde, darf die zur Erfüllung seiner Aufgaben erforderlichen personenbezogenen Daten nach Maßgabe des StUG bearbeiten. Das Thüringer Datenschutzgesetz findet mit Ausnahmen über die Datenschutzkontrolle keine Anwendung (§ 2 ThürLB-StUG).

7. Polizei

7.1 Polizeiaufgabengesetz

Das am 13.06.1992 in Kraft getretene Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (Polizeiaufgabengesetz - PAG -) vom 4. Juni 1992 enthält u. a. gesetzliche Einschränkungen des informationellen Selbstbestimmungsrechts von Betroffenen durch die Polizei. Die Grundsätze der Datenerhebung zur Aufgabenerfüllung der Polizei sind in den §§ 31 ff. PAG geregelt. Die Datenerhebung muß demnach zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, zum Schutz privater Rechte, zur Vollzugshilfe oder zur Erfüllung von der Polizei durch andere Rechtsvorschriften übertragenen Aufgaben erforderlich sein, sofern die §§ 12 bis 47 PAG keine besonderen Regelungen vorsehen. Die Erhebung personenbezogener Daten kann durch Befragung, Identitätsfeststellung und erkennungsdienstliche Behandlung, aber auch durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder Aufzeichnungen erfolgen. Besondere Mittel der Datenerhebung finden sich in § 34 Abs. 1 PAG

(längerfristige Observation, verdeckter Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen, verdeckte Ermittler und Vertrauenspersonen). Dabei können auch Dritte, sofern dies nicht vermeidbar ist, betroffen werden. Die §§ 38 bis 47 PAG betreffen die für derartige intensive Eingriffe in das informationelle Selbstbestimmungsrecht notwendigen bereichsspezifischen datenschutzrechtlichen Regelungen über die Speicherung, Veränderung und Nutzung von Daten, die Dauer der Datenspeicherung, die Zweckbindung, die Datenübermittlung, das automatisierte Abrufverfahren, den Datenabgleich, die Rasterfahndung, die Berichtigung, Löschung und Sperrung von Daten sowie die Erforderlichkeit von Errichtungsanordnungen für automatisierte Dateien und das Auskunftsrecht der Betroffenen.

7.2 Umgang mit Altdaten aus der ehemaligen DDR im Polizeibereich

Mit Inkrafttreten des ThürDSG bzw. des ThürArchivG war der rechtliche Rahmen zum Umgang mit Altdaten gesetzt. Im Juli 1994 hat der TLfD die Problematik der Altdaten im Polizeibereich aufgegriffen. Bei den Altdaten handelt es sich um Vorgänge, die im Zusammenhang stehen mit der Auflösung der Dienststellen der ehemaligen Deutschen Volkspolizei aus der Zeit vor dem 03.10.1990.
Zu klären war zunächst der Umfang des Altaktenbestandes, der Inhalt und die Frage, wo sich die Altakten befinden. Hierzu waren sowohl ein intensiver Schriftwechsel mit dem TIM als auch klärende Gespräche notwendig.
Da verschiedene Polizeidienststellen des Freistaats Thüringen ihren Altaktenbestand bereits den zuständigen Archiven übergeben hatten, sind auch die Staatsarchive zur Frage des Verbleibs einbezogen worden.
Dabei wurde folgendes festgestellt:
Detaillierte Fragen zur weiteren Verwendung und dem Inhalt der als Altakten bezeichneten Vorgänge der einzelnen Polizeidienststellen konnten bislang noch nicht detailliert beantwortet werden. Zu berücksichtigen war, daß mangels entsprechender Regelungen Altakten in verschiedenen Dienststellen vernichtet wurden, ohne daß hierüber genaue Angaben möglich sind. Seitens des TIM wurde versichert, daß sich beim TIM selbst keinerlei Altunterlagen aus dem Polizeibereich befinden.
Die Kaderakten der ehemaligen Bediensteten der Volkspolizei sind beim Polizeipräsidium Thüringen und dort im Personalaktenarchiv archiviert. Eine datenschutzrechtliche Kontrolle hatte keine datenschutzrechtlichen Bedenken hinsichtlich der Aufbewahrung ergeben.
Die Übergabe der Altdaten aus dem Paß- und Meldewesen aus dem Bereich der Polizei-Kreisämter an die zuständigen Kommunalverwaltungen ist durch den Erlaß des TIM (Hinweise zur Behandlung von Meldeunterlagen des ehemaligen Paß- und Meldewesens der Polizei-Kreisämter) vom 10. 08. 1994 geregelt worden. Es liegen keine Hinweise vor, daß nicht entsprechend verfahren wurde.
Bei Ein- und Ausreisevorgängen war zu unterscheiden, welche Vorgänge sich bei den Polizeidienststellen befanden (Ausreisen z. B. nach Schweden, Frankreich etc. sowie Ausländereheschließungen) und welche Vorgänge von der Kommunalverwaltung, Abteilung Inneres, bearbeitet worden waren (sämtliche anderen Ausreisen, auch Übersiedlungen in das Gebiet der Bundesrepublik und West-Berlin). Über den Verbleib dieser Unterlagen besteht noch keine endgültige Klarheit.
Straftatenvorgänge, für die das TMJE zuständig ist, sind zunächst aufgrund der großen Anzahl bei den Polizeidienststellen verblieben. Über den Bestand dieser Akten sind Verzeichnisse von den Polizeidienststellen an das TMJE übergeben worden, um die beabsichtigte Aussonderung der Unterlagen durch einmonatigen Aushang an der jeweiligen Gerichtstafel bekanntzugeben. Dieses Aushangverfahren ist, soweit bekannt, ebenfalls abgeschlossen, so daß eine Übergabe an das Staatsarchiv vorgenommen werden kann.

Die personenbezogenen Sammlungen in der Kriminalpolizei wurden vom zuständigen LKA übernommen und entsprechend den Regelungen des PAG bereinigt.
Das TIM hat gegenüber dem TLfD versichert, daß es der Problematik erhebliche Bedeutung zumißt und bemüht ist, den verbliebenen Aktenbestand recht schnell den Staatsarchiven anzubieten. Es besteht Einigkeit darüber, daß den Staatsarchiven der komplette Altaktenbestand der verbliebenen Akten zur Übernahme angeboten wird. Die Staatsarchive entscheiden dann, welche Altakten sie übernehmen und welche Altakten in den Polizeidienststellen verbleiben. Eine Entscheidung über die weitere Verwendung desjenigen Altaktenbestandes, der von den Staatsarchiven nicht übernommen wird, soll nach Mitteilung des TIM erst dann getroffen werden, wenn bekannt ist, um welche konkreten Altakten es sich handelt. Hierzu ist beabsichtigt, eine Arbeitsgruppe einzusetzen, die Entscheidungsvorschläge erarbeitet. Aus Sicht des TLfD ist der Umstand, daß die umfassende Aufarbeitung des Altaktenbestandes noch nicht abgeschlossen ist, schwer nachvollziehbar.
Der TLfD wird weiterhin auf die abschließende Entscheidung zum weiteren Umgang mit den verbleibenden Altakten aus dem Polizeibereich dringen und die Durchführung kontrollieren.

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

Vom TIM wurde dem TLfD der Entwurf der Neufassung der o. a. Verwaltungsvorschriften zur Stellungnahme zugesandt. Darin ist vorgesehen, daß unter Verzicht auf die Übermittlung von Anschrift, Geburtsjahr und Geburtsmonat eine Ausfertigung des Protokolls an die Untersuchungsstelle übersandt wird. In einer Besprechung mit den beteiligten Ministerien und Dienststellen wurde Einvernehmen dahin gehend erzielt, daß hierbei auch die Angabe des Berufes entbehrlich ist, da dieser für die Blutalkoholkonzentrationsbestimmung nicht erforderlich ist. Auch sind bei den näheren Angaben zum Ort der Alkohol-/ Medikamenten-/ Drogenaufnahme konsequenterweise dann lediglich Ankreuzmöglichkeiten in dem Formular vorgesehen worden, um zu verhindern, daß die nicht erforderlichen Daten unnötigerweise übermittelt werden. Die entsprechend überarbeitete Verwaltungsvorschrift ist am 01.12.1995 in Kraft getreten.

7.4 Datenübermittlung von der Polizei an Fußballvereine zur Erteilung von Stadionverboten

Die Bundesarbeitsgemeinschaft Fanprojekte, ein Zusammenschluß aller bundesdeutschen Fanprojekte, die sich um die Betreuung und Begleitung jugendlicher Fußballzuschauer kümmern und zwischen den beteiligten Vereinen, der Polizei sowie den Fußballfans vermitteln, hat sich an die DSB der Länder gewandt, um folgenden Sachverhalt aus datenschutzrechtlicher Sicht bewerten zu lassen:
Die Einführung des “Nationalen Konzeptes Sport und Sicherheit” sieht als eine Maßnahme gegen Gewalt rund um den bezahlten Fußball sogenannte “bundesweite Stadionverbote” für auffällig gewordene Fußballfans vor. Ein bundesweites Stadionverbot wird auf Antrag eines örtlichen Fußballvereines vom Deutschen Fußball-Bund (DFB) ausgesprochen, wenn Informationen über Fehlverhalten eines Fußballzuschauers im Rahmen einer Sportveranstaltung oder in deren Umfeld (Anfahrtsweg, Gastronomie im Umfeld, öffentliche Verkehrsmittel) vorliegen. Gängige Praxis sei, daß der Fußballverein die notwendigen Informationen entweder durch den eigenen Ordnungsdienst oder durch die Polizei erhält. Diese Information umfasse sämtliche personenbezogenen Daten und den betreffenden Vorfall. Die Frage nach der Rechtsgrundlage für die Weitergabe persönlicher Daten an den Fußballverein durch die Polizei konnte für Thüringen aus der Sicht des TLfD für den öffentlichen Bereich wie folgt beantwortet werden:
Nach § 41 Abs. 3 Satz 2 Thüringer Polizeiaufgabengesetz ist eine Übermittlung personenbezogener Daten an nichtöffentliche Stellen und an Einzelpersonen durch die Polizei möglich. Voraussetzung ist, daß die Datenübermittlung der Erfüllung polizeilicher Aufgaben oder der Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder für die schutzwürdigen Belange einzelner erforderlich ist. Inwiefern die Voraussetzungen vorliegen, ist vom jeweiligen Einzelfall abhängig. Grundsätzlich könnte jedoch die Datenübermittlung von der Polizei an den Verein zur Verhütung von Störungen bei Sportgroßveranstaltungen, insbesondere wenn Fehlverhalten von einzelnen Fußballfans in der vorangegangenen Zeit bekannt sind, in Frage kommen.

In diesem Zusammenhang sei auf die bundesweite Datei “Gewalttäter Sport” hingewiesen. In dieser Verbunddatei werden durch die Polizei Fälle erfaßt, wenn bestimmte Straftaten im Zusammenhang mit Sportveranstaltungen begangen worden sind oder auch polizeiliche Maßnahmen zur Gefahrenabwehr gegen einzelne Personen ergriffen wurden. Diese Datei ist 1992 und 1993 eingehend diskutiert worden, wobei die Landesbeauftragten grundsätzlich Bedenken an der Geeignetheit und Erforderlichkeit dieser Datei und an einzelnen Regelungen zu den Speicherungsvoraussetzungen, den Speicherungsfristen und den Zugriffsrechten, die in der Errichtungsanordnung vorgesehen waren, geltend gemacht haben. Auf diese Datei haben die Polizeidienststellen bundesweit Zugriff. Für den Freistaat Thüringen hat das TIM mitgeteilt, daß die Datei “Gewalttäter Sport” nicht genutzt wird.

7.5 Verkehrsordnungswidrigkeitenverfahren

7.5.1 Anhörungsbogen

Seit November 1995 wird in Thüringen im Rahmen von Verkehrsordnungswidrigkeitenverfahren bei Überschreitung der zulässigen Höchstgeschwindigkeit das vom Fahrer gefertigte Foto auf dem Anhörungsbogen aufgedruckt und an den jeweiligen Fahrzeughalter versandt.
Da zunächst nach Auffassung des TLfD eine Versendung des Lichtbildes aufgrund datenschutzrechtlicher Bedenken regelmäßig nur vorgenommen werden sollte, wenn seitens des Fahrzeughalters im Rahmen der Anhörung die Tat verneint wird, erfolgte vor Einführung des Verfahrens ein Meinungsaustausch zwischen dem TIM und dem TLfD. Dabei wurde Einvernehmen erzielt, daß zunächst der Versand der Lichtbilder auf dem Anhörungsbogen in einer Pilotphase erfolgt, um zu prüfen, ob durch dieses Verfahren das Ziel, den Verwaltungsaufwand (Reduzierung von Widersprüchen und Nachforschungen durch die Polizei) deutlich zu verringern, erreicht werden kann. Unter diesem Aspekt kann aus datenschutzrechtlicher Sicht bei einer Interessenabwägung einer regelmäßigen Lichtbildversendung zugestimmt

werden. Ist der Halter selbst auf dem Foto abgebildet, werden ihm ohnehin keine Daten übermittelt, da er selbst der Betroffene ist. Insoweit ist dieser Fall datenschutzrechtlich unproblematisch. Hat aber zum Zeitpunkt der Verkehrsübertretung eine andere Person das Fahrzeug geführt, können sich Probleme ergeben, wenn der Halter die Führung des Fahrzeuges einer verfügungsberechtigten Person und diese wiederum einer dritten Person überlassen hat. Bisher mußte der Halter davon nichts erfahren, da der Halter zunächst der Bußgeldstelle allenfalls den Verfügungsberechtigten im Anhörungsbogen mitgeteilt hat, der wiederum bei seiner Anhörung auf den tatsächlichen Fahrer verwies. Im Einzelfall mußten weitere Ermittlungen durch die Polizei vorgenommen werden.
Bei dem neuen Verfahren wird nun der Halter regelmäßig durch den Lichtbildversand der Bußgeldstelle über den Fahrzeugführer informiert. Dabei wird, um keine schutzwürdigen Interessen Dritter zu beeinträchtigen, zugesichert, daß auf dem Foto ausschließlich der Fahrer abgebildet wird.
Eine abschließende datenschutzrechtliche Bewertung des Verfahrens wird der TLfD nach Abschluß der Testphase auf der Grundlage eines Ergebnisberichtes des TIM vornehmen.

Im Rahmen der Bearbeitung einer Beschwerde hatte sich Ende 1994 der TLfD bereits mit dem Anhörungsbogen bei der Verfolgung von Verkehrsordnungswidrigkeiten beschäftigt. Dabei wurde festgestellt, daß, obwohl von dem Betroffenen auch "freiwillige Angaben" erhoben werden, ein entsprechender Hinweis auf den Zweck der Speicherung bzw. auf eine ggf. vorgesehene Übermittlung, wie dies in § 4 ThürDSG gefordert wird, auf dem Vordruck fehlt. Eine Rückfrage bei der Zentralen Bußgeldstelle ergab, daß ein Teil der Angaben weder für das Verfahren noch in irgendeiner anderen Form, z. B. für statistische Auswertungen, derzeit genutzt wird. Aus diesem Grund wurde das TIM gebeten, zur Erforderlichkeit der Datenerhebung Stellung zu nehmen. Im Ergebnis konnte auch von dort keine ausreichende Begründung zur Erforderlichkeit für die Erhebung dieser Daten abgegeben werden, so daß die Aufforderung seitens des TLfD an das TIM erging, den Anhörungsbogen entsprechend zu überarbeiten.
Trotz mehrfacher Nachfrage liegt jedoch bis zum gegenwärtigen Zeitpunkt kein überarbeiteter Anhörungsbogen vor. Dies ist um so unverständlicher, als im Rahmen der Einführung des Lichtbildversandes bei Verkehrsordnungswidrigkeiten das Fahrerfoto in den gegenwärtigen Anhörungsbogen integriert, aber nicht gleichzeitig der Anhörungsbogen den datenschutzrechtlichen Bestimmungen angepaßt wurde. Es bleibt zu hoffen, daß dies kurzfristig nachgeholt wird.

7.5.2 Lichtbildabgleich mit Melderegister

Der TLfD wurde darauf aufmerksam gemacht, daß aufgrund eines Beschlusses des Bund-Länder-Fachausschusses für Straßenverkehrsordnungwidrigkeiten verschiedene Länder beabsichtigen, den Abgleich des Beweisfotos (z. B. Geschwindigkeitsüberschreitung) mit dem im Personalausweis- und Paßregister abgelegten Paßbild auch bei Verstößen im Verwarnungsbereich zuzulassen. Bisher war dieser Abgleich auf erheblichere Verstöße beschränkt, die zur Eintragung in das Verkehrszentralregister geführt haben.
Der TLfD hat die Auffassung vertreten, daß ein Abgleich von Beweisfotos mit den im Personalausweis- und Paßregister abgelegten Paßbildern keinen datenschutzrechtlichen Bedenken begegnet, sofern unter Beachtung des Verhältnismäßigkeitsgrundsatzes zuerst eine Identifizierung beim Betroffenen selbst ergebnislos versucht wurde, denn eine Identifizierung durch Befragung Dritter im Umfeld des Betroffenen (z. B. Nachbarn) stellt einen weitaus einschneidenderen Eingriff in das Persönlichkeitsrecht dar.
Das TIM hat auf die Anfrage, ob im Freistaat Thüringen gleiches beabsichtigt ist, die Auffassung vertreten, einer gesonderten Zulassung bedürfe es nicht. Diese Maßnahme komme ohnehin nur zum Tragen, wenn es im Streitfall notwendig würde, zu beweisen, welcher Fahrer die Ordnungswidrigkeit begangen habe. Es wird auch keine Unverhältnismäßigkeit darin gesehen, direkt ohne Versuch der Identitätsfeststellung beim Betroffenen einen Abgleich mit dem Paßbild im Register vorzunehmen. Ob dies auch praktisch durchgeführt wird, ist bisher nicht mitgeteilt worden.

7.5.3 Privatisierung der Überwachung im Straßenverkehr

Von DSB anderer Länder wurde der TLfD darüber informiert, daß es dort Überlegungen gibt, die Verfolgung von Ordnungswidrigkeiten im Straßenverkehr und die allgemeine Verkehrsüberwachung zum Teil zu privatisieren, um eine Entlastung der Polizei herbeizuführen. Vom TLfD ist hierzu die Auffassung vertreten worden, daß eine Privatisierung auf verfassungsrechtliche Bedenken stößt. Zum einen unterliegt die Verfolgung von gesetzlich sanktionierten Verstößen gegen allgemeine Rechtsvorschriften und die generelle Aufrechterhaltung der öffentlichen Sicherheit dem staatlichen Monopol für die Ausübung von Zwangsgewalt, das nur in Ausnahmefällen eine Durchbrechung erlaubt. Ein solcher ist hier nicht gegeben. Zweifel hinsichtlich der Zulässigkeit sind auch aufgrund des Opportunitätsgrundsatzes nach § 47 OWiG begründet, wonach die Behörde bei der Verfolgung und Ahndung nach pflichtgemäßem Ermessen zu verfahren hat. Bei einer Übertragung auf Private wäre dieser Ermessensgebrauch eingeschränkt, da für die Entscheidung, ob und in welchem Fall und wie eine Ordnungswidrigkeit verfolgt werden soll, sämtliche Umstände des Falles herangezogen werden müssen, was durch die Verlagerung der Entscheidung auf Private nur eingeschränkt möglich

wäre. Die von den privaten Unternehmen ermittelten Tatsachen sind zwar nachprüfbar, wobei sich die Nachprüfung aber auch nur auf die von dem Privaten als rechtserheblich angesehenen Umstände beschränken könnte. Viel spricht dafür, daß angesichts der Anzahl zu ahndender Verkehrsverstöße diese Feststellungen dann automatisch übernommen werden. Auf Anfrage des TLfD hat das TIM mitgeteilt, daß es der Auffassung zustimmt, daß aus rechtlichen Gründen die Übertragung der Ahndung von festgestellten Ordnungswidrigkeiten nicht an private Unternehmen erfolgen kann. Seitens des TLfD wird beobachtet werden, ob im Zuge zunehmender Privatisierungsüberlegungen diese Absichten ggf. wieder aufgegriffen werden.

7.6 Automatisiertes Fingerabdruckidentifizierungssystem

Im Freistaat Thüringen wird, wie in anderen Bundesländern auch, eine Landesdatei über Fingerabdrücke geführt. Die aufgrund erkennungsdienstlicher Behandlung in den Ländern gewonnenen Fingerabdruckbögen werden auch in das Automatisierte Fingerabdruckidentifizierungssystem (AFIS), das beim BKA geführt wird, übernommen. Wenn also an einem Tatort in Thüringen Fingerabdruckspuren festgestellt werden, so können sie mit den im BKA-Zentralrechner gespeicherten Fingerabdrucksätzen abgeglichen werden. Aus dem Kreise der DSB des Bundes und der Länder wird kritisiert, daß AFIS bis heute ohne entsprechende Errichtungsanordnung geführt wird. Ein Problem im Zusammenhang mit AFIS stellt die Forderung aus datenschutzrechtlicher Sicht dar, daß polizeiliche Recherchen im Bestand von AFIS nach dem Asylverfahrensgesetz protokolliert werden, damit eine Kontrolle, ob die tatbestandlichen Voraussetzungen nach § 16 Abs. 5 Asylverfahrensgesetz vorlagen, ermöglicht wird. Für die Länderpolizeien, die der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen, sind keine solchen Protokolle vorgesehen. Auf Protokolle beim BKA besteht jedoch keine Möglichkeit des Zugriffs für die LfD. Für eine effektive Kontrolltätigkeit der LfD müssen sie jedoch die Möglichkeit der Einsicht in Zugriffsprotokolle haben.

7.7 Kontrolle einer Polizeidirektion

Auch in Polizeidirektionen werden in einem nicht unerheblichen Maß personenbezogene Daten verarbeitet, zum einen in der eigenen Verwaltung und zum anderen in der Wahrnehmung polizeilicher Aufgaben.
Anläßlich der Kontrolle gemäß § 37 ThürDSG in einer Polizeidirektion wurden folgende datenschutzrechtliche Mängel festgestellt:
Gemäß § 34 Abs. 2 ThürDSG bedarf der erstmalige Einsatz von automatisierten Verfahren einer datenschutzrechtlichen Freigabe. Eine solche Freigabe lag für die in der Personalverwaltung geführten automatisierten Dateien nicht vor. Dies war gemäß § 39 Abs. 1 ThürDSG zu beanstanden. Die Beanstandung wurde durch die Freigabe des Verfahrens durch das TIM behoben.
Im technischen und organisatorischen Bereich wurden ebenfalls Mängel festgestellt, die jedoch nicht so gravierend waren, daß sie zu einer datenschutzrechtlichen Beanstandung geführt hätten. Nach § 9 ThürDSG sind für die Verarbeitung technische und organisatorische Maßnahmen zur Datensicherung zu treffen und schriftlich niederzulegen. Ein weiterer Aspekt war die Sicherung des Zugangs, wozu der TLfD eine Schlüsselordnung gefordert hat. Bei der Entsorgung von Unterlagen mit personenbezogenen Daten durch eine Privatfirma wurde empfohlen, sich vor Ort über die ordnungsgemäße Entsorgung zu informieren.

7.8 Erfolgskontrolle polizeilicher Befugnisse bei steigender Kriminalität

Die Aufgabe der beim BKA eingerichteten Rechtstatsachensammelstelle ist die Erhebung von Rechtstatsachenmaterial zu Erfahrungen der Polizei mit bestimmten Instrumenten der Informationsgewinnung bei der Kriminalitätsbekämpfung, wie z. B. den Einsatz verdeckter Ermittler oder den Einsatz technischer Mittel (Abhörgeräte, Videokameras usw.). Diese Stelle soll auch bei sich konkret abzeichnenden rechtspolitischen Entwicklungen mit polizeipraktischem Bezug tätig werden, um gesetzgeberischen Handlungsbedarf zu begründen. Die Einrichtung einer Rechtstatsachensammlung als objektives Instrument zur Bewertung polizeilicher Eingriffsbefugnisse ist auch mit dem Entschließungsvorschlag zur 49. Konferenz der DSB (siehe Anlage 13) aus datenschutzrechtlicher Sicht grundsätzlich begrüßt worden. Die DSB haben eine ergebnisoffene Überprüfung der bestehenden Befugnisse vorgeschlagen und erwarten, daß sich die Polizeien der Diskussion über die Erforderlichkeit und Angemessenheit weitreichender Befugnisse zu Eingriffen in das Persönlichkeitsrecht nicht entziehen werden. Das TIM hat Übereinstimmung erklärt mit der auf der 49. Konferenz geäußerten Auffassung, daß diese Sammlung nicht einseitig den Zweck verfolgen darf, Forderungen der Polizei zur Einführung zusätzlicher Befugnisse argumentativ zu unterstützen.
Inwiefern die Forderungen der DSB umgesetzt werden, bleibt abzuwarten.

7.9 EUROPOL

Die Staaten der Europäischen Union haben im Vertrag über die Europäische Union den Aufbau eines unionsweiten Systems zum Austausch von Informationen im Rahmen eines Europäischen Polizeiamtes (EUROPOL) für den Bereich der polizeilichen Zusammenarbeit zur Bekämpfung und Verhütung des Terrorismus, schwerwiegender Formen der internationalen Kriminalität und des illegalen Drogenhandels vorgesehen. EUROPOL soll folgende Aufgaben wahrnehmen:

- Informationen und Erkenntnisse zu sammeln, zusammenzustellen, zu analysieren und auszuwerten,
- die nationalen Dienststellen über die sie betreffenden Informationen hinsichtlich der in Erfahrung gebrachten Zusammenhänge von Straftaten unverzüglich zu unterrichten,
- Ermittlungen in den Mitgliedstaaten durch die Übermittlung aller sachdienlichen Informationen an den nationalen Stellen zu unterstützen und
- eine automatisiert geführte Sammlung von Informationsbeständen zu unterhalten, die sowohl von den nationalen Behörden übermittelte als auch von EUROPOL selbst eingespeicherte Daten enthält.

Ein Problem der Datenspeicherung in EUROPOL für den Freistaat Thüringen liegt darin, daß Thüringer Daten über das LKA an das BKA geleitet werden, so daß die Notwendigkeit besteht, eine datenschutzrechtliche Kontrolle der Übermittlung sicherzustellen. Die DSB des Bundes und der Länder haben in einer Entschließung (siehe Anlage 8) deutlich gemacht, daß das Übereinkommen der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen muß und die materielle Verantwortung für die Datenverarbeitung, soweit die Daten von Landesbehörden erhoben worden sind, dort weiterhin liegt. Außerdem ist die Forderung erhoben worden, daß die Regelungen zur Bearbeitung personenbezogener Daten präzise sein müssen und dem Grundsatz der Verhältnismäßigkeit entsprechen. Die in bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen erfüllen diese Voraussetzungen nicht. Der Bundesrat hat klargestellt, daß nach der geltenden Rechtslage für die Übermittlung dieser Daten das Landesrecht maßgeblich ist, so daß der datenschutzrechtlichen Verantwortung der Länder Rechnung zu tragen ist. Eine Beteiligung der Landesbeauftragten ist dadurch vorgesehen, daß der gemeinsamen Kontrollinstanz nach Artikel 24 des EUROPOL-Übereinkommens neben dem BfD der LfD Sachsen-Anhalt als Vertreter der Länder angehören wird.

8. Verfassungsschutz

8.1 Sicherheitsüberprüfung

Das Sicherheitsüberprüfungsgesetz (SÜG) des Bundes ist im April 1994 in Kraft getreten. § 23 SÜG sieht vor, daß eine Auskunft über im Rahmen einer Sicherheitsüberprüfung gespeicherte personenbezogene Daten oder die Einsicht in die Sicherheitsüberprüfungsakte versagt werden kann, wenn der Inhalt der Akten Rückschlüsse auf die Organisation und Arbeitsweise des Verfassungsschutzes zuläßt oder ihre Kenntnis die Funktionsfähigkeit des Verfassungsschutzes einschließlich der Zusammenarbeit mit anderen Behörden gefährden oder erhebliche Beeinträchtigungen von überwiegenden berechtigten Interessen Dritter mit sich bringen. Da das Vorliegen dieser Gründe sehr weit gefaßt werden kann, besteht das Problem für einen Betroffenen, der eine Sicherheitsüberprüfung nicht bestanden hat, daß ihm die Überprüfung dieses Ergebnisses wegen fehlender Auskünfte zu den entscheidungserheblichen Kriterien praktisch unmöglich gemacht wird. Zu dieser Problematik vertritt der TLfD die Ansicht, daß dem Betroffenen die Sicherheitsüberprüfungsakte zwar nicht mit allen Angaben vorgelegt werden muß, zur Gewährung des Individualrechtsschutzes eine entsprechend konkrete Auskunft zur Überprüfbarkeit einer Entscheidung aber zu erteilen ist. Es muß eine Abwägung der im Spannungsfeld stehenden öffentlichen und privaten Interessen durchgeführt werden. Das aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung schützt den einzelnen umfassend gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten. Im überwiegenden allgemeinen Interesse muß der einzelne jedoch verfassungsgemäß gesetzliche Einschränkungen, vor allem nach dem Grundsatz der Verhältnismäßigkeit, hinnehmen. Zur Prüfung der Rechtmäßigkeit von Eingriffen in dieses Recht ist aus dem Rechtsstaatsgedanken eine wirksame Kontrolle in tatsächlicher und rechtlicher Hinsicht notwendig. Dieser Kontrolle kann sich nach Auffassung des TLfD auch der Verfassungsschutz nicht grundsätzlich entziehen.

Der Freistaat Thüringen hat bislang kein entsprechendes Landesgesetz. Sicherheitsüberprüfungen werden anhand von Richtlinien vorgenommen, die den Anforderungen als gesetzliche Regelung bei so einschneidenden Eingriffen in das informationelle Selbstbestimmungsrecht nicht genügen. Das TIM wurde vom TLfD auf die dringende Erforderlichkeit eines entsprechenden Landesgesetzes hingewiesen.

Die DSB der neuen Länder haben am 20.09.1994 folgenden Beschluß im Rahmen des AK Neue Bundesländer verabschiedet:

- Auch die Verfassungsschutzbehörden der neuen Länder dürfen für Zwecke der Sicherheitsüberprüfungen nur Daten verarbeiten und nutzen, die sie zur Erfüllung der ihnen gesetzlich vorgeschriebenen Aufgaben auch tatsächlich benötigen.
- Bürger aus den westlichen und östlichen Bundesländern dürfen im Rahmen von Sicherheitsüberprüfungen nicht unterschiedlich behandelt werden. Insbesondere sind die DSB der neuen Länder der Auffassung, daß allein die Mitgliedschaft in der SED oder einer der anderen Blockparteien nicht grundsätzlich als sicherheitserheblicher Sachverhalt zu werten ist.
- Datenerhebungen zu Sicherheitsüberprüfungen dürfen nur im Rahmen des Sicherheitsüberprüfungsgesetzes erfolgen.
- Die Landesregierungen der neuen Länder werden gebeten, dafür Sorge zu tragen, daß möglichst kurzfristig Sicherheitsüberprüfungsgesetze der Länder verabschiedet werden.

Einige Bundesländer haben inzwischen die Forderungen nach einer gesetzlichen Regelung aufgegriffen und entsprechende Gesetzentwürfe erarbeitet. Eine Beteiligung des TLfD an einem Gesetzentwurf für Thüringen hat bisher noch nicht stattgefunden.

8.2 Maßhalten beim vorbeugenden personellen Sabotageschutz

Die DSB des Bundes und der Länder haben in einem gemeinsamen Beschluß (siehe Anlage 15) auf der Konferenz der DSB gefordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren.
Die Verfassungsschutzbehörden des Bundes und der Länder sind in die Sicherheitsüberprüfungen derjenigen Beschäftigten einbezogen, die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen (personeller Sabotageschutz). Spezialgesetzlich geregelt sind solche Überprüfungen gegenwärtig für den Atombereich und für Flughäfen. Angesichts der Überlegungen des Bundesministeriums des Innern, diese Überprüfungen auch auf Beschäftigte "lebens- und verteidigungswichtiger Einrichtungen" auszudehnen, wobei als "lebenswichtig" bereits Stellen angesehen werden, die für das Funktionieren des Gemeinwesens unverzichtbar sind, sind die DSB der Meinung, daß das Persönlichkeitsrecht hier doch Maßhalten fordert. Eine besondere Zurückhaltung muß besonders bei vorbeugenden Sicherheitsüberprüfungen auferlegt werden. Um nicht Sicherheitsüberprüfungen auch für Einrichtungen, die "für das Funktionieren des Gemeinwesens unverzichtbar sind", rechtlich zuzulassen, ist insbesondere eine eindeutige Auslegung des Begriffs der "sicherheitsempfindlichen Stellen" solcher Einrichtungen erforderlich. So sollte bei allen Vorhaben, bei denen eine Erweiterung der Sicherheitsüberprüfung beim vorbeugenden personellen Sabotageschutz beabsichtigt ist, stets bedacht werden, daß hier besonders sensible personenbezogene Daten erhoben werden, ohne daß der Betroffene dazu Anlaß gegeben hat.

8.3 Personenbezogene Datenübermittlung zwischen Verfassungsschutzbehörden

Ein anderer LfD informierte, daß bei einer Überprüfung im dortigen Landesamt für Verfassungsschutz festgestellt worden sei, daß bei der Übersendung von Berichten an andere Verfassungsschutzbehörden mit personenbezogenen Angaben über verschiedene Personen häufig keine Prüfung der Erforderlichkeit mit einer gegebenenfalls notwendigen Teilanonymisierung erfolgt sei. Auf eine entsprechende Anfrage des TLfD beim TLfV wurde von dort mitgeteilt, daß man sich mit den anderen Verfassungsschutzbehörden einig sei, daß die Übermittlung von Informationen im Sinne von § 3 Bundesverfassungsschutzgesetz in den Verfassungsschutzbehörden nur dann nicht erforderlich sei, wenn erkennbar sei, daß die Informationen für die Aufgabenerfüllung der Empfängerbehörden nicht relevant sind oder sein können. Diese Auffassung teilt der TLfD vom Grundsatz her, beabsichtigt jedoch, die Einhaltung dieser Praxis bei Gelegenheit zu überprüfen.

8.4 Kontrollbesuch beim Landesamt für Verfassungsschutz

Im Berichtszeitraum wurde auch das Landesamt für Verfassungsschutz (LfV) einer datenschutzrechtlichen Kontrolle durch den TLfD unterzogen.
Bei der stichprobenartigen Kontrolle im Personalbereich zeigte sich, daß dort Unterlagen Aufnahme in eine Personalakte gefunden hatten, ohne daß hierfür eine Erforderlichkeit bestand. Die Bearbeitung dieser Vorgänge liegt in der ausschließlichen Zuständigkeit der ZGT, so daß eine zusätzliche Erhebung und Vorhaltung der personenbezogenen Daten bei der nicht zuständigen Personalverwaltung des LfV vom TLfD kritisiert wurde. Seitens des TIM wurde zwischenzeitlich mitgeteilt, daß hier den Forderungen des TLfD, diese Unterlagen zu entfernen, entsprochen wird.

Nach Feststellung des TLfD hält das LfV Daten von Bewerbern, die sich mehrfach bewerben, vor, ohne daß es bis zum jetzigen Zeitpunkt hierzu aus datenschutzrechtlicher Sicht notwendige Regelungen hinsichtlich der Löschung gibt. Es ist vom TIM in Aussicht gestellt worden, daß hierzu eine Regelung getroffen wird, die auch in die in Ausarbeitung befindliche Personalaktenführungsrichtlinie Eingang finden soll, was seitens des TLfD begrüßt wird.
Nach einer Prüfung von Sach- und Personenakten sollte sich die Prüfung auch auf Sicherheitsüberprüfungsakten erstrecken. Aufgrund einer Entscheidung des TIM wurde die Einsichtnahme in diejenigen Sicherheitsüberprüfungsakten, bei denen eine Belehrung der einbezogenen Personen (Ehe- bzw. Lebenspartner) sowie der Auskunfts- und Referenzpersonen (noch) nicht stattgefunden hat, verweigert. Dies hat der TLfD gemäß § 39 Abs. 1 ThürDSG beanstandet. Bei dieser vom TIM getroffenen Entscheidung wird davon ausgegangen, daß als "Betroffener", dem ein Widerspruchsrecht zusteht, auch Auskunfts- und Referenzpersonen anzusehen sind. Diese Auffassung findet im Gesetz keine Rechtsgrundlage und widerspricht sowohl § 37 Abs. 2 ThürDSG als auch § 38 Abs. 1 Satz 1 ThürDSG. Zudem hängt die Kontrollmöglichkeit des TLfD nach Ziffer 37.2 VVThürDSG nicht von der Unterrichtung des Betroffenen über das Widerspruchsrecht ab. Der TLfD als unabhängige Kontrollinstanz kann sich in seinen Prüfungen vor Ort keinen Beschränkungen unterwerfen, die durch das geltende Recht nicht gedeckt sind.
Das TIM hat seine Rechtsauffassung zwischenzeitlich insofern modifiziert, als die Verweigerung der Einsichtnahme in diejenigen Sicherheitsüberprüfungsakten, bei denen eine Belehrung der nach Auffassung des TIM einzubeziehenden Personen nicht stattgefunden hat, nicht länger aufrechterhalten bleibt. Es hat jedoch mitgeteilt, daß künftig auch die einzubeziehenden Personen sowie Auskunfts- und Referenzpersonen über das nach Auffassung des TIM bestehende Widerspruchsrecht belehrt bzw. unterbliebene Belehrungen nachgeholt werden. Es stellt sich hier die Frage der zukünftigen Handhabung, wenn von der sicherheitszuüberprüfenden Person kein Widerspruch eingelegt wurde, aber beispielsweise von einer Referenzperson. Soll für diesen Fall keine Kontrollmöglichkeit des TLfD gegeben sein? Die Antwort darauf von seiten des TIM steht noch aus.

9. Finanzen, Steuern, Rechnungsprüfung

9.1 Finanzverwaltung

9.1.1 Eintragung eines Freibetrages auf der Lohnsteuerkarte

Wenn ein Steuerpflichtiger erstmalig mit einem "Antrag auf Lohnsteuerermäßigung" den Freibetrag für Behinderte nach § 33b Einkommenssteuergesetz (EStG) geltend macht, wird dieser vom örtlich zuständigen Finanzamt eingetragen (§ 39a Abs. 4a EStG). Unabhängig davon, ob der Steuerpflichtige in den Folgejahren wiederum einen "Antrag auf Lohnsteuerermäßigung" stellt, wird die Wohnsitzgemeinde - soweit bekannt - durch das Finanzamt über den Anspruch auf Eintragung eines Freibetrages für Behinderte und damit über die Tatsache einer vorhandenen Behinderung unterrichtet. Obwohl dieses Verfahren sicherlich in den meisten Fällen eine bürgerfreundliche Lösung darstellt, gibt es auch Fälle, in denen der Steuerpflichtige nicht wünscht, daß der Gemeindeverwaltung seine Behinderung bekannt wird. Gleiches gilt gegenüber dem Arbeitgeber bei Eintritt einer Behinderung während eines bestehenden Arbeitsverhältnisses. Die ausschließlich zweckgebundene Kenntnis der Behinderung erscheint besonders dann nicht in jedem Fall gesichert, wenn der Steuerpflichtige in einer kleinen Gemeinde wohnt, in der Gemeindebedienstete und Steuerpflichtiger sich persönlich kennen. Der Arbeitgeber kann unter Umständen darüber hinaus auch von der Höhe eines auf der Lohnsteuerkarte eingetragenen Freibetrages wegen der Behinderung auf den Behinderungsgrad zurückschließen. Auf diese, sich eventuell nachteilig auf den Arbeitnehmer auswirkenden Informationen hat der Arbeitgeber in vielen Fällen keinen Anspruch. Der besonderen Schutzwürdigkeit der Sozialdaten Behinderter entspräche es daher, den Behinderten zumindest ein Wahlrecht einzuräumen. Er sollte selbst entscheiden können, ob er den Freibetrag vom Finanzamt auf der Lohnsteuerkarte eintragen lassen möchte - mit der Folge einer Datenübermittlung an die Wohnsitzgemeinde - oder ob er der künftigen Datenübermittlung an die Gemeinde widersprechen und den Eintrag des Freibetrages auf der Lohnsteuerkarte durch das Finanzamt über einen jährlichen Antrag auf Lohnsteuerermäßigung erreichen möchte.
Das um Stellungnahme zu diesem Vorschlag gebetene TFM erklärte, daß diese Angelegenheit bereits Gegenstand der Besprechung der Lohnsteuerreferatsleiter des Bundes und der Länder war. Dabei war entschieden worden, daß im Vordruck "Antrag auf Lohnsteuerermäßigung" kein Auswahlkästchen aufgenommen werden soll, wonach der Steuerpflichtige wählen kann, ob der Pauschbetrag für Behinderte - verbunden mit dem entsprechenden Datenfluß - unmittelbar von der Gemeinde bei Ausstellung der Lohnsteuerkarte eingetragen werden soll oder nicht. Statt dessen wurde beschlossen, auf dem Antrag die Versicherung des Betroffenen um folgenden Wortlaut zu ergänzen: "Mir ist bekannt, daß erforderlichenfalls Angaben über Kindschaftsverhältnisse und Pauschbeträge für Behinderte der für die Ausstellung von Lohnsteuerkarten zuständigen Gemeinde mitgeteilt werden."
Nach Aussage des TFM wird diese Angelegenheit im Kreis der Lohnsteuerreferatsleiter des Bundes und der Länder erneut zur Diskussion gestellt. Die Angelegenheit wird der TLfD weiter verfolgen.

9.1.2 Zustellung von Lohnsteuerkarten

Aus anderen Bundesländern wurde bekannt, daß die Lohnsteuerkarten für Ehegatten und ihre minderjährigen Kinder von seiten der Meldebehörden in einem Briefumschlag versandt werden. Diese Art der Zustellung der Lohnsteuerkarten wird für datenschutzrechtlich bedenklich gehalten, da den Ehegatten und den Kindern vom Absender die Möglichkeit eröffnet wird, die Angaben über Steuerdaten untereinander zur Kenntnis zu nehmen. Diese Informationen dürften zwar in der Regel untereinander bekannt sein, es sind aber durchaus Fälle denkbar, in denen einzelne Familienmitglieder dies nicht wünschen.
Nach Aussage des TFM ist es den Meldebehörden hinsichtlich der Übermittlung (Aushändigung) freigestellt, ob sie die Lohnsteuerkarten durch Bedienstete der Gemeinde zustellen lassen, per Post versenden oder private Dienstleistungsunternehmen mit dem Versand beauftragen. Nach Erfahrung des TFM wird bei Versand per Post pro Arbeitnehmer ein Briefumschlag verwendet, da der sonst nötige Verwaltungsaufwand beim Kuvertieren die eventuelle Kostenersparnis beim Versand übersteigt. Es wurde bislang von seiten des TFM davon ausgegangen, daß gleiches auch für die anderen Versandarten gilt.
Da jedoch nicht auszuschließen ist, daß insbesondere in Gemeinden, die mittels Gemeindeboten zustellen, ein Briefumschlag für mehrere Familienangehörige verwendet wird - eine Verwaltungsanweisung existiert in Thüringen zu diesem Problem noch nicht - wurde das LVwA in seiner Funktion als Aufsichtsbehörde gebeten, die Landratsämter und die Meldeämter auf dieses Problem bei der Zustellung hinzuweisen und damit die gemäß § 9 Abs. 1 ThürDSG erforderlichen technischen und organisatorischen Maßnahmen, die erforderlich sind, um die Ausführung der Vorschriften des Datenschutzgesetzes zu gewährleisten, zu treffen.

9.1.3 Unterlagenübersendung des Finanzamts an den falschen Empfänger

Ein Beschwerdeführer übergab in der Dienststelle des TLfD persönliche Unterlagen eines ihm unbekannten Ehepaars, die ihm von einem Finanzamt zugesandt worden waren. Da die Übermittlung von Unterlagen mit personenbezogenen Daten an den offensichtlich falschen Adressaten eine Verletzung datenschutzrechtlicher Bestimmungen darstellt, bat der TLfD das Finanzamt um eine Stellungnahme zum Sachverhalt.
Vom Finanzamt wurde dazu mitgeteilt, daß sich der Sachverhalt leider nicht mehr aufklären lasse. Es wurde versichert, daß Unterlagen im Amt stets nur an denjenigen verschickt werden, für den sie bestimmt sind (Regelfall). Im Einzelfall könne aber nicht immer vollständig ausgeschlossen werden, daß durch ein ungewolltes und nicht beabsichtigtes Versehen Belege vertauscht werden oder aber ineinander rutschen. Es wurde darauf verwiesen, daß das Steuerverfahren ein Massenverfahren ist. Die Fehlerquote wurde für vernachlässigbar gehalten.

Da die Mitarbeiter des Finanzamtes an das Steuergeheimnis gemäß § 30 Abgabenordnung (AO) gebunden sind und mit sehr sensiblen personenbezogenen Daten arbeiten, wurde das Finanzamt auf die Dringlichkeit einer Auswertung und eines Nachvollzugs der Angelegenheit hingewiesen. Dies war um so notwendiger, da es sich hier um eine Bürgerbeschwerde handelte. Vom Finanzamt wurde daraufhin mitgeteilt, daß den Mitarbeitern nochmals unter anderem auch die besondere Bedeutung von § 30 AO nahegebracht wurde.
Auch künftig wird sich der TLfD darüber informieren, wie in der Praxis mit dem Steuergeheimnis umgegangen wird und gegebenenfalls geeignete Maßnahmen anregen, um solche Vorkommnisse auszuschließen.

9.1.4 Namensverwechslung

Von einem Thüringer Bürger wurde dem TLfD geschildert, daß er bei der Beantragung eines neuen Personalausweises Schwierigkeiten mit der Meldebehörde hatte. Trotz Vorlage der noch gültigen alten Dokumente konnten von den Behördenmitarbeitern die Daten des Antragstellers im Register nicht gefunden werden. Erst nach totaler Neuanmeldung als Bürger deutscher Nationalität wurde sein Antrag auf Anfertigung eines neuen Personalausweises und Passes bearbeitet. Da er kurze Zeit später erfuhr, daß beim Finanzamt ein Bescheid wegen nicht gezahlter Lohnsteuer gegen ihn vorlag, er sich aber keines steuerlichen Vergehens bewußt war, wandte er sich mit der Bitte um Prüfung des Sachverhaltes an den TLfD. Er nahm an, daß hier ein Mißbrauch seiner persönlichen Daten durch eine andere Person vorlag.
Eine Nachfrage bei der Meldebehörde ergab, daß durch einen Fehler des zuständigen Mitarbeiters der Meldebehörde bei der Abmeldung eines Bürgers die gleichzeitige Abmeldung des Beschwerdeführers vorgenommen worden war. Beide Personen tragen den gleichen Namen und sind am gleichen Tag geboren. Dieser Fehler des Meldeamtes wurde zwischenzeitlich beseitigt. Unabhängig von der Verwechslung im Meldeamt führte die Namens- und Geburtstagsgleichheit auch im Finanzamt zu einem Irrtum. Dort wurden bei einem automatischen Kassenabgleich innerhalb des Finanzamtes lediglich die Namen, jedoch nicht weitere Merkmale (wie z. B. Adresse) verglichen, so daß der Beschwerdeführer die Mahnung erhielt, die für den Namensvetter bestimmt war. Dies wurde vom Finanzamt korrigiert.

Der Beschwerdeführer wurde über die Sachlage informiert. Der TLfD behält sich vor, sowohl den Vorgang eines Kassenabgleiches in einem Finanzamt, als auch einer An- bzw. Abmeldung im Meldeamt zu prüfen.

9.1.5 Zeichnungsvorbehalt des Vorstehers eines Finanzamtes gemäß § 23 der Geschäftsordnung für die Finanzämter

Nach § 23 Abs. 1 Nr. 4 der Geschäftsordnung für die Finanzämter (FAGO) hat der Vorsteher eines Finanzamtes die steuerlichen Angelegenheiten von Amtsangehörigen zu zeichnen, um gegebenenfalls Begünstigungen und Steuerhinterziehungen begegnen zu können.
Diese Vorschrift stößt aber auf datenschutzrechtliche Bedenken, weil hierdurch das informationelle Selbstbestimmungsrecht beeinträchtigt werden kann. Der Dienstvorgesetzte bekommt auf diese Weise Auskunft über die Einkommens- und Vermögensverhältnisse seiner Amtsangehörigen.
Das TFM hat deshalb verfügt, daß Amtsangehörige, deren Beschäftigungsfinanzamt gleichzeitig das für Ihre steuerlichen Angelegenheiten zuständige Finanzamt ist, die Besteuerung durch ein Nachbarfinanzamt beantragen können. Diesen Anträgen, die keine Begründung enthalten müssen, haben die Finanzämter durch Abschluß einer Zuständigkeitsvereinbarung mit diesem Nachbarfinanzamt zu entsprechen.
Obwohl die von Seiten des TFM getroffene Verfügung begrüßt wird, ist weiterhin, auch im Hinblick darauf, daß eine nur verwaltungsintern getroffene Regelung jederzeit wieder geändert werden kann, eine entsprechende ergänzende Regelung des § 27 AO geboten.

9.1.6 Einsichtsrecht in Einkommenssteuerbescheide bei Unterhaltsansprüchen

Der Ehepartner einer Petentin war im Ergebnis einer Klage dazu verurteilt worden, seiner Tochter aus erster Ehe (Klägerin) Auskunft über die Höhe seiner Einkünfte zu erteilen und darüber Belege, unter anderem auch den Einkommenssteuerbescheid, vorzulegen. Da sich wegen Zusammenveranlagung mit ihrem Ehepartner auf diesem auch Angaben zu ihrer Person befanden, wandte sich die Beschwerdeführerin daraufhin ratsuchend an den TLfD. Sie war nicht bereit, der Klägerin ihre detaillierten personenbezogenen Daten (Höhe ihres Einkommens, Konfession u. ä.) zur Kenntnis zu geben und bat deshalb um Überprüfung der Zumutbarkeit eines solchen Urteils aus datenschutzrechtlicher Sicht

Zur Verfahrensweise bei einer gemeinsamen Veranlagung des Auskunftspflichtigen mit einem neuen Ehepartner ist zum Schutz des Persönlichkeitsrechts des nicht betroffenen Ehepartners folgende Verfahrensweise nach einem Urteil des BGH aus dem Jahre 1983 zulässig: “Umfaßt der Auskunftsanspruch die Vorlegung des Einkommenssteuerbescheides, so muß der Auskunftspflichtige den Bescheid zwar auch dann vorlegen, wenn er zusammen mit seinem Ehegatten veranlagt worden ist. Er darf dabei jedoch solche Angaben abdecken oder unkenntlich machen, die ausschließlich seinen Ehegatten betreffen oder in denen Werte für ihn und seinen Ehegatten zusammengefaßt sind, ohne daß sein eigener Anteil daraus entnommen werden kann.” (BGH, Urt. v. 13.04.1983 - IV b ZR 374/81 (KG)

Dies wurde der Petentin auf ihre Anfrage zur Gewährleistung des Datenschutzes mitgeteilt.

9.1.7 Kontrollbesuch in einem Finanzamt

Zur Kontrolle der Einhaltung der Vorschriften des ThürDSG sowie Vorschriften über den Datenschutz im Zusammenhang mit der Finanz- bzw. Steuerverwaltung wurde ein Thüringer Finanzamt der Prüfung durch den TLfD unterzogen.
Im Ergebnis der Kontrolle wurden folgende Mängel festgestellt und behoben:
Im Finanzamt war bisher kein Datenschutzbeauftragter benannt worden. Dieser wurde unter Beachtung der Verwaltungsvorschriften zu § 34 ThürDSG bestellt.
Die Datenverarbeitung in der Finanzverwaltung erfolgt gegenwärtig unter Nutzung des integrierten - automatisierten - Besteuerungsverfahrens. Für dieses Verfahren lag in der Behörde keine Freigabe und kein Verfahrensverzeichnis vor. Die Freigabe der Verfahren konnte, ebenso wie das Verzeichnis der Datenverarbeitungsanlagen, mittlerweile vorgelegt werden. Noch ungeklärt blieben folgende Sachverhalte:
Im Finanzamt existieren keine Regelungen zur Aufbewahrung bzw. Archivierung der Unterlagen. Von seiten der Finanzverwaltung wurde dazu Verbindung mit dem Thüringer Staatsarchiv aufgenommen. Aufgrund der umfangreichen Materie konnte bislang noch keine abschließende Festlegung getroffen werden.
In der Geschäftsstelle des Finanzamtes werden Personalnebenakten (§ 27 Abs. 4 FAGO) geführt. Dem Finanzamt werden von seiten der OFD nur in sehr begrenztem Umfang Aufgaben der Personalbewirtschaftung übertragen, so daß gegen diese praktizierte Form der Führung von Personalnebenakten im Finanzamt aus datenschutzrechtlicher Sicht erhebliche Bedenken bestehen. Da derzeit - auch mit anderen Behörden - über eine grundlegende Regelung hinsichtlich der Führung von Personalnebenakten diskutiert wird, soll dieses Problem an dieser Stelle nicht vertieft werden.

Im Finanzamt wird die Einhaltung der durch Erlaß des TFM geregelten Gleitarbeitszeit der Mitarbeiter durch eine elektronische Zeiterfassungsanlage kontrolliert. Es fehlten hierzu die erforderliche schriftliche Freigabe durch das TFM (§ 34 Abs. 2 ThürDSG) und die erforderliche Zustimmung des Personalrates zur Einführung des Verfahrens.
Das Finanzamt hat dem TLfD zugesichert, in den noch offengebliebenen Fragen unaufgefordert nach Eingang einer Mitteilung vom Ministerium zu berichten.

9.1.8 Bereichsspezifischer Datenschutz in der Abgabenordnung

Der BfD ist an das BMF herangetreten, um ihm die von den DSB des Bundes und der Länder zum Entwurf für ein Abgabenordnungsänderungsgesetz diskutierten Vorschläge, Regelungen zur Ergänzung der Abgabenordnung im Rahmen des Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetzes und andere datenschutzrechtliche Anliegen zu unterbreiten.
Vor allem der Umgang mit Daten, die dem Steuergeheimnis unterliegen, muß klarer als bislang geregelt werden.
So bedarf z. B. der § 30 AO der Ergänzung über die Bindung der von der Finanzverwaltung erhobenen oder gespeicherten Daten an den Erhebungs- und Speicherzweck. In § 27 AO muß in Erweiterung zum bisherigen Inhalt festgelegt werden, daß auf Antrag eines bei einer Finanzbehörde Beschäftigten eine andere Finanzbehörde die Zuständigkeit übernimmt, wenn die Beschäftigungsbehörde nach den Steuergesetzen für ihn örtlich zuständig ist. Weiterhin bedürfen die §§ 30, 31a, 88a und 105, 138, 208 AO der Ergänzung bzw. Präzisierung.
Der TLfD wird den Fortgang der Gesetzesinitiative beobachten.

9.1.9 Nutzung des ePost-Verfahrens

Bei der Deutschen Post AG handelt es sich im datenschutzrechtlichen Sinne nach § 2 Abs. 1 BDSG um eine öffentliche Stelle des Bundes. Das Errichten und Betreiben von Einrichtungen zur entgeltlichen Beförderung von schriftlichen Mitteilungen oder sonstigen Nachrichten von Person zu Person ist dem Nachfolgeunternehmen der Deutschen Bundespost Postdienst nach § 2 Abs. 1 Postgesetz bis zum Auslaufen des Beförderungsvorbehaltes ausschließlich vorbehalten.
Durch das ePost-Verfahren (elektronischer Briefservice) bietet die Deutsche Post AG den Postkunden die Möglichkeit, von DV-Einrichtungen zeichencodierte Nachrichten elektronisch an Partner ohne unmittelbar erreichbare Endgeräte zu versenden. Der Kunde kann zeichencodierte Nachrichten für jeden Empfänger jederzeit elektronisch bei der für ihn zuständigen ePost-Station einliefern. Die elektronischen Informationen werden über Fernmeldeleitungen an die empfängernahen ePost-Stationen weiterübermittelt. Nach Umwandlung der zeichencodierten in körperliche Nachrichten werden die Sendungen entsprechend dem Wunsch des Kunden als Briefe oder Infopost weiterbefördert und an den Empfänger ausgeliefert. Da die Deutsche Post AG u. a. auch für Behörden den Ausdruck von Bescheiden sowie deren Kuvertierung und Versand übernimmt, wurde im Kreis der DSB des Bundes und der Länder im Berichtszeitraum diskutiert, inwiefern datenschutzrechtliche Bedenken gegen diese ePostdienste der Deutschen Post AG bestehen.
Als datenschutzrechtliche Probleme könnten sich insbesondere folgende Sachverhalte herausstellen:

- Die Allgemeinen Geschäftsbedingungen der ePost enthalten keine Festlegungen über Speicherdauer bzw. Löschung der Inhalts- und Adreßdaten nach erfolgter Übertragung und Briefproduktion.
- Den Nutzern des ePost-Verfahrens werden keine transparenten Angaben über die Verwendung von Verbindungsdaten, Übertragungsprotokollen und Abrechnungsdaten gemacht.
- Regelungen zur Löschung dieser Datenspuren sind nicht vorhanden, insbesondere fehlen Regelungen zum Umgang mit den Adreßdaten des Empfängerkreises.
- Dem Nutzer des ePost-Verfahrens wird nicht deutlich gemacht, daß eine anonyme Benutzung des Verfahrens, wie etwa vergleichbar beim klassischen Briefpostdienst, nicht möglich ist.

Der TLfD wird die Nutzung des ePost-Verfahrens weiter im Auge behalten, um möglichen Datenschutzverstößen begegnen zu können.

9.2 Offene Vermögensfragen

9.2.1 Datenabfrage beim ARoV

Der Amtsleiter eines Landratsamtes (LRA), in dem auch das Amt zur Regelung offener Vermögensfragen (ARoV) untergebracht ist, wandte sich wegen eines speziellen Datenschutzproblems mit der Bitte um Prüfung des Sachverhaltes an den TLfD.
Von dem bDSB des ARoV war der Amtsleiter anläßlich der Präsentation der neuen Anwendersoftware des LRA auf ein datenschutzrechtliches Problem angesprochen worden. Er fand es bedenklich, daß ein an das Netz des ARoV

angeschlossener PC-Arbeitsplatz nicht in der Behörde selbst, sondern in dem Liegenschaftsamt (außerhalb des LRA) eingerichtet wurde und den dortigen Mitarbeitern zur Verfügung stehen sollte. Innerhalb dieses bestehenden Datennetzes besteht die grundsätzliche Möglichkeit, den gesamten Datenbestand des ARoV abzufragen und den einzelnen Antragstellern persönlich zuzuordnen. Da der bDSB annahm, diese theoretische Möglichkeit eines Zugriffs auf den Gesamtdatenbestand des ARoV einschließlich genannter Zuordnungsmöglichkeit sei auch für die Bediensteten des Liegenschaftsamtes jederzeit gegeben, forderte er, die Einrichtung des dem ARoV zugehörigen PC-Arbeitsplatzes im Liegenschaftsamt rückgängig zu machen. Aus seiner Sicht stellte sich die Zugriffsmöglichkeit auf diesen Datenbestand zugunsten einer anderen Behörde (Liegenschaftsamt) als eine "Datenübermittlung innerhalb des öffentlichen Bereiches" nach § 21 ThürDSG dar.
Auf Bitte des TLfD um Auskunft, welche personenbezogenen Daten durch das Liegenschaftsamt über diesen PC abrufbar sind und recherchiert werden können, wurde mitgeteilt, daß das im ARoV eingesetzte EDV-Verfahren alle durchgeführten Abfragen/Recherchen mit der Angabe des jeweiligen Sachbearbeiters protokolliert. Das EDV-Verfahren läßt es zu, den einzelnen Sachbearbeitern unterschiedliche Rechte zu geben und diese mit Kennung und Paßwort zu sichern, d. h., daß jeder Arbeitsplatz der EDV-Anlage nur Zugriff auf spezielle Daten hat.
Da über den im Liegenschaftsamt stationierten "Auskunfts-PC" nur Name und Anschrift des Anmelders abrufbar sind, bestätigte sich die Vermutung des bDSB - die Möglichkeit einer Datenabfrage im Netz sei für die Mitarbeiter des Liegenschaftsamtes für den gesamten Datenbestand möglich - nicht.

Dem anfragenden Amtsleiter konnte mitgeteilt werden, daß Art und Weise und auch der Umfang, in welchem die Datenabfrage von seiten des Liegenschaftsamtes im Verfahren der Erteilung einer Grundstücksverkehrsgenehmigung erfolgt, als nicht problematisch anzusehen war.

9.2.2 Datenübermittlung zwischen dem ARoV und Sozialamt

Ein Thüringer Sozialamt trat mit dem aus seiner Sicht verständlichen, aber aus datenschutzrechtlicher Sicht unzulässigen Ansinnen an den TLfD heran, die Ergebnisse von Rückübertragungsverfahren direkt vom ARoV ohne Wissen des Betroffenen übermittelt zu bekommen. Das Sozialamt argumentierte damit, daß es sich bei den Ergebnissen der Rückübertragungsverfahren um Daten aus allgemein zugänglichen Quellen handele, weil diese Angaben im Grundbuch als einem allgemein zugänglichen Register jederzeit eingesehen werden könnten.
Grundlage zur Datenübermittlung von ARoV an Sozialbehörden im Wege der Amtshilfe sind die Vorschriften des ThürDSG, da keine spezialgesetzlichen Übermittlungsbefugnisse vorliegen sowie die Vorschriften über die Amtshilfe (§§ 4 ff. ThürVwVfG) gemäß § 2 Abs. 4 ThürDSG keine Anwendung finden. Nach § 21 Abs. 1 ThürDSG ist die Übermittlung personenbezogener Daten an andere öffentliche Stellen nur 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 zulassen würden. Für die ÄRoV ist eine solche Datenübermittlung regelmäßig nicht erforderlich. Die Erforderlichkeit der Daten für die Erfüllung der Aufgaben der Sozialämter ist jedoch nicht schon allein deshalb zu verneinen, weil das Sozialamt die Daten beim Betroffenen selbst erheben könnte, sondern es sind die Voraussetzungen für eine Erhebung ohne Mitwirkung des Betroffenen gemäß § 19 Abs. 2 Satz 2 ThürDSG zu prüfen. Dies brauchte hier nicht weiter geprüft zu werden, da bereits die Voraussetzungen für eine zweckfremde Nutzung nach § 20 Abs. 2 nicht vorliegen. Insbesondere handelt es sich um keine Daten, die gemäß § 20 Abs. 2 Nr. 5 aus allgemein zugänglichen Quellen entnommen werden können. Öffentliche Register zählen nur dann zu den allgemein zugänglichen Quellen, wenn die Einsichtnahme nicht von einem besonderen berechtigten Interesse abhängig ist. Nach § 12 Abs. 1 Grundbuchordnung kann jedoch nur derjenige Einsicht in das Grundbuch nehmen, der ein berechtigtes Interesse darlegt. Das Sozialamt muß also diese Daten bei seinen Antragstellern erfragen. Dies könnte allenfalls durch eine Einwilligung des Betroffenen gegenüber dem ARoV erreicht werden. Die Neigung hierzu dürfte sich angesichts des drohenden Zugriffs des Sozialamts auf den rückübertragenen Vermögenswert wohl aber in Grenzen halten.

9.2.3 Auskunft des ARoV nach der Grundstücksverkehrsordnung

Sowohl die Bundesanstalt für vereinigungsbedingte Sonderaufgaben (BVS) als auch ein Landkreis haben sich an den TLfD gewandt, da seitens des Landesamtes zur Regelung offener Vermögensfragen (ThLARoV) die Übermittlung von Namen und Anschriften der Anmelder an die Stellen, die für die Erteilung einer Grundstücksverkehrsgenehmigung nach der GVO zuständig sind, für datenschutzrechtlich unzulässig gehalten wurde.
Der TLfD hat zu der angesprochenen Frage die Auffassung vertreten, daß auf die Erforderlichkeit abzustellen sei, da die Grundstücksverkehrsordnung hierzu keine Regelung enthält. Entscheidend ist die Durchführung des Verfahrens, aus dem sich die Erforderlichkeit der Datenübermittlungen entnehmen läßt. Soll eine Grundstücksverkehrsgenehmigung nach § 1 Abs. 2 Satz 2 GVO erteilt werden und liegen Restitutionsanträge vor, die offensichtlich unbegründet sind, bedarf es vor Erlaß dieses Verwaltungsaktes, weil geltend gemachte Restitutionsansprüche unbegründet sind, nach

§ 28 VwVfG der Anhörung der Restitutionsanmelder. Vollständige und sichere Auskünfte sind hier nur von der Stelle zu bekommen, bei der die Anmeldungen vorliegen, so daß die Verpflichtung der Auskunftserteilung durch das ThLARoV zu bejahen ist. Dieser Auffassung hat sich auch das TFM angeschlossen, das eine entsprechende Weisung an das ThLARoV gegeben hat.

9.2.4 Datenschutz bei der Durchführung des Gesetzes zur Regelung offener Vermögensfragen

Durch eine Beschwerde erhielt der TLfD Kenntnis, daß im Rahmen einer Mitteilung des ThLARoV über die beabsichtigte Entscheidung bezüglich einer Rückübertragung von Grundstücken gemäß § 32 Abs. 1 VermG allen Verfügungsberechtigten der betroffenen Grundstücke eine vollständige Liste mit der Bezeichnung der Grundstücke, der Fläche, des Namens des Eigentümers bzw. Nutzers und Verfügungsberechtigten, der Angabe eines Ausschlußgrundes und des Datums der Grundbucheintragung zugesandt wurde. Es handelte sich im konkreten Fall um über dreihundert Empfänger. Die namentlich genannten Personen waren an diesem Restitutionsverfahren Drittbeteiligte, auf die die Vorschriften des VermG als Nutzer oder als bereits im Grundbuch eingetragene Eigentümer zutreffen. Als Beteiligte sind sie auch berechtigt, die Namen der übrigen an dem Verfahren Beteiligten zu erfahren. Das ThLARoV hat "die betroffenen Rechtsträger oder staatlichen Verwalter sowie Dritte, deren rechtliche Interessen durch den Ausgang des Verfahrens berührt werden können, über die Antragstellung, auf Antrag unter Übersendung einer Abschrift des Antrages und seiner Anlagen, zu informieren und zu dem weiteren Verfahren hinzuzuziehen" (§ 31 Abs. 2 VermG). Da in diesem Fall für die Feststellung von Drittbeteiligten auch die Bezeichnung des Grundstückes ausreichend erscheint, hat sich das ThLARoV bereit erklärt, in derartigen Fällen den Drittbeteiligten nur noch einen Bescheid mit einer Liste ohne Namen zuzustellen.

9.2.5 Nachweis des berechtigten Interesses gemäß § 32 Abs. 5 VermG

Das TFM hat sich zur Auslegung und Handhabung des § 32 Abs. 5 VermG an den TLfD gewandt. Nach § 32 Abs. 5 VermG kann jedem, der ein berechtigtes Interesse glaubhaft darlegt, Name und Anschrift eines Antragstellers sowie der Vermögenswert mitgeteilt werden, auf den sich die Anmeldung des Rückübertragungsantrags bezieht. Zuvor muß das ARoV den Antragsteller auf diese Möglichkeit hinweisen und eine Frist für einen möglichen Widerspruch gegen die Bekanntgabe der personenbezogenen Daten von zwei Wochen einräumen. Das TFM hat hierzu die Auffassung vertreten, daß der Begriff des "berechtigten Interesses" nicht allzuweit auszulegen sei und hierzu auf die Begründung der Bundesregierung zum Entwurf des 2. Vermögensrechtsänderungsgesetzes verwiesen. Diese Auffassung wird seitens des TLfD geteilt. Zur Frage, wie zu verfahren ist, wenn die Zustimmung widerrufen wird oder zweckwidrig die übermittelten Angaben durch den Auskunftersuchenden weitergegeben werden, wurde wie folgt Stellung genommen: Die Zweckbindung des Auskunftersuchenden ergibt sich aus § 22 Abs. 4 Satz 1 ThürDSG. Danach darf der Empfänger die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt worden sind. Eine Weitergabe der Daten durch den Auskunftersuchenden an Dritte ist nicht zulässig, weil die Übermittlung zum Zwecke der Durchführung eines konkreten Investitionsvorhabens des Auskunftersuchenden, nicht aber zur Weitergabe an Dritte erfolgt. Auf diese Zweckbindung hat die übermittelnde Stelle den Auskunftersuchenden gemäß § 22 Abs. 4 Satz 2 ThürDSG hinzuweisen. Selbst wenn eine Übermittlung an den Dritten nach § 32 Abs. 5 VermG zulässig wäre, müßte die übermittelnde Stelle gemäß § 22 Abs. 4 Satz 3 ThürDSG vor der Übermittlung zustimmen. Darüber hinaus ist gemäß § 43 Abs. 2 Nr. 2 ThürDSG die unbefugte Datenübermittlung strafbewehrt. Beim Widerruf der stillschweigend oder auch ausdrücklich erteilten Zustimmung ist nach den allgemeinen Grundsätzen des Verwaltungsverfahrensgesetzes davon auszugehen, daß dies zulässig ist. Dies hat zur Folge, daß rückwirkend die Rechtsgrundlage für die Datenübermittlung entfällt und der Widerspruch durch die datenspeichernde Stelle für die Zukunft zu beachten ist. Praktisch dürfte dies jedoch nur in den Fällen werden, in denen bei Eingang des Widerrufs die Auskunft noch nicht erteilt worden ist. In den anderen Fällen ist der Anmelder durch die Zweckbindung davor geschützt, daß die Angaben nicht an Dritte übermittelt werden. Der TLfD hat angeregt, Hinweise auf die Zweckbindung und die strafrechtlichen Folgen eines Verstoßes ergänzend in den in § 32 Abs. 5 VermG ergangenen Erlaß aufzunehmen.

9.2.6 Datenfälschung in einem Vermögensamt

Durch Presseberichte wurde der TLfD darauf aufmerksam gemacht, daß eine Routineüberprüfung des ThLARoV in einem ARoV ergeben hat, daß es dort zu Datenfälschungen gekommen ist. Eine Anfrage beim zuständigen Landratsamt ergab, daß vier Mitarbeiter des ARoV Vorgänge in der Weise manipuliert hatten, daß den jeweiligen Akten im Datenverarbeitungssystem neue (falsche) Namen zugeordnet wurden. Dadurch war es nicht mehr möglich, diese Akten unter dem korrekten Namen in der Datenverarbeitungsanlage aufzufinden. Parallel hierzu haben diese Mitarbeiter die entsprechenden Akten innerhalb des Amtes so beiseite gelegt, daß sie in der normalen Bearbeitung nicht auffindbar waren. Diese Manipulation fiel dadurch auf, daß bei der Vergabe der "neuen" (falschen) Namen die betreffenden Mitarbeiter ihre eigenen Namen verwendet hatten, was Kollegen aufgefallen war.

Dieser Vorfall hatte zur Folge, daß den entsprechenden Mitarbeitern fristlos gekündigt wurde. Die zuständige Staatsanwaltschaft hat ein Ermittlungsverfahren eingeleitet, das noch nicht abgeschlossen ist. Von dieser Manipulation waren nach bisherigen Erkenntnissen allerdings nur 29 von etwa 10.000 Akten betroffen. Dieser Fall zeigt, daß noch so viele Datenschutzvorschriften keinen wirksamen Schutz des informationellen Selbstbestimmungsrechts des einzelnen bewirken können, wenn sich die Mitarbeiter der öffentlichen Stellen über diese Vorschriften hinwegsetzen. Für das ARoV wird zur Zeit in Auswertung des Vorfalls ein neues Datenschutzkonzept erarbeitet.

9.2.7 Recherchen von Privatfirmen für das Thüringer Landesamt zur Regelung offener Vermögensfragen

Dem TLfD wurde von einem Landratsamt mitgeteilt, daß eine Privatfirma mit der zur Durchführung des gesetzlichen Auftrages der Vermögensämter erforderlichen Recherche beauftragt wurde. Da Bedenken gegen diese Vorgehensweise bestanden, wurde der TLfD um Überprüfung und Würdigung des Sachverhaltes gebeten.
Da sich diese Firma entsprechend § 8 Abs. 6 ThürDSG vertraglich der Kontrolle durch den TLfD unterworfen hatte, wurde sie zur Klärung der Angelegenheit einer datenschutzrechtlichen Prüfung unterzogen.
Das TFM, als oberste Landesbehörde, hat im Ergebnis der Prüfung bestätigt, daß die Auftragsvergabe zur Grundstücksrecherche und -dokumentation an private Unternehmen als Hilfe und Unterstützung für die ÄRoV im Sinne von Ziffer 8.5.1 der VVThürDSG unerläßlich ist und bis zum Ablauf des Jahres 1995, für das ThLARoV darüber hinaus bis Ablauf 1996, erforderlich sein wird. Um sicherzustellen, daß nicht nur die Firmen, die sich bereits entsprechend § 8 Abs. 6 ThürDSG vertraglich zur Einhaltung der Bestimmungen dieses Gesetzes verpflichtet und der Kontrolle durch den Landesbeauftragten unterworfen haben, sondern auch deren Mitarbeiter über die einzuhaltende datenschutzrechtliche Regelung informiert werden, hat das TFM das ThLARoV gebeten, eine Erklärung zur Einhaltung des Datenschutzgeheimnisses von allen Mitarbeitern der beauftragten Recherchefirmen einzuholen.

9.3 Datenschutzkontrolle bei den Rechnungsprüfungsbehörden

Im Kreis der DSB des Bundes und der Länder wurde diskutiert, inwieweit sich die Kontrollbefugnis der DSB auch auf die Rechnungsprüfungsbehörden erstreckt. Nach dem Wortlaut des § 37 Abs. 4 ThürDSG ist die Kontrollbefugnis des TLfD bei den Thüringer Rechnungsprüfungsbehörden nicht beschränkt.
Der Rechnungshof ist eine selbständige, nur dem Gesetz unterworfene oberste Landesbehörde. Die Mitglieder des Thüringer Rechnungshofes besitzen nach Artikel 103 Abs. 1 der Verfassung des Freistaats Thüringen richterliche Unabhängigkeit. Der TLfD vertritt deshalb die Auffassung, daß eine datenschutzrechtliche Kontrolle im Kernbereich der Tätigkeit der Rechnungsprüfungsbehörden durch den TLfD nicht uneingeschränkt möglich ist, da sie als Eingriff in die Unabhängigkeit der Rechnungsprüfer verstanden werden könnte.
Der TLfD geht aber auch im umgekehrten Fall davon aus, daß eine Prüfung des Landesrechnungshofes im Geschäftsbereich des TLfD bezüglich der Einhaltung haushaltsrechtlicher Bestimmungen zwar grundsätzlich zulässig ist, Art und Umfang der Kontrolltätigkeit des Landesbeauftragten sich aber einer Bewertung durch den Rechnungshof entziehen.
Im übrigen vertritt der TLfD die Auffassung, daß elementare Teile des Umgangs der Rechnungsprüfungsbehörden mit personenbezogenen Daten - wie z. B. technische Sicherungsmaßnahmen bei der Aufbewahrung und Archivierung - der Verwaltungstätigkeit der Rechnungsprüfungsbehörden zuzurechnen sind und damit auch der Kontrollbefugnis des TLfD unterliegen. Soweit die reine Verwaltungstätigkeit zu überprüfen ist, dürfte die gegenseitige Kontrolltätigkeit außer Frage stehen. Auf Anfrage des TLfD beim Thüringer Rechnungshof wurde mitgeteilt, daß diese Auffassung geteilt wird.

10. Justiz

10.1 Fehlende bereichsspezifische Regelungen im Bereich der Justiz

Nach Ablauf von nunmehr zwölf Jahren seit dem Volkszählungsurteil fehlen im Bereich der Justiz wesentliche bereichsspezifische Regelungen. Das Bundesverfassungsgericht hat zwar als Ausnahme dem Gesetzgeber eine Übergangsfrist eingeräumt, die fehlenden gesetzlichen Grundlagen, die einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung zulassen, zu schaffen, das Ende der Frist ist indessen nicht ausdrücklich bestimmt worden. Dieser Übergangsbonus ist aus datenschutzrechtlicher Sicht und auch aufgrund inzwischen mehrfach ergangener Feststellungen der Rechtsprechung abgelaufen. Seit geraumer Zeit fordern die DSB des Bundes und der Länder die verfassungsmäßigen gesetzlichen Grundlagen zur Einschränkung des informationellen Selbstbestimmungsrechts im Bereich der Justiz. Seitens der Justiz sind mehrfach Gesetzentwürfe angekündigt worden, konkret liegen jedoch noch keine vor. Schon in der 47. Konferenz (siehe Anlage 2) haben die DSB daran erinnert, daß sie bereits 1981 Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren unterbreitet haben. In der 48. Konferenz (siehe Anlage 10) haben die DSB erneut darauf hingewiesen, daß gesetzliche Regelungen im Bereich der Justiz

überfällig sind. Es fehlen weiterhin ausreichende gesetzliche Regelungen für die
- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz),
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen, wie die Dauer der Speicherung in automatisierten Dateien.

Auf der 49. Konferenz (siehe Anlage 16) haben die DSB zu den bis dahin bekanntgewordenen Entwürfen zu einem Strafverfahrensänderungsgesetz, die nur unzureichende Generalklauseln bezüglich der Aufbewahrung von Akten und der Speicherung personenbezogener Daten in Dateien enthalten, Forderungen nach konkreten gesetzlichen Regelungen in diesem Bereich erhoben. In der 50. Konferenz (siehe Anlage 25) haben die DSB Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien erhoben. Insbesondere auch in diesem Bereich sind bei fehlerhafter Abwägung der Übermittlung von personenbezogenen Daten besonders tief einschneidende Folgen im privaten und beruflichen Bereich von Opfern, Beschuldigten bzw. Angeklagten und deren Angehörigen zu erwarten.

Ein Entwurf eines Justizmitteilungsgesetzes war in der letzten Legislaturperiode zwar eingebracht worden, aufgrund des Ablaufes der Legislaturperiode aber der Diskontinuität verfallen. Der Gesetzentwurf soll nun in veränderter Form noch in diesem Jahr als Regierungsentwurf für ein erneutes Gesetzgebungsverfahren verabschiedet werden. Insbesondere soll künftig im Vergleich zum früheren Regierungsentwurf ein niedrigerer Datenschutzstandard gelten. Im Hinblick auf die einschneidenden Belastungen der Betroffenen durch Justizmitteilungen haben die DSB in der 50. Konferenz für künftige Gesetzgebungsverfahren eine rechtzeitige Unterrichtung und Beteiligung der DSB angemahnt und sich diesbezüglich in einem Schreiben an die Konferenz der Justizministerinnen und Justizminister gewandt.

10.2 Altdatenbestände der betrieblichen Konfliktkommissionen

Die Konfliktkommissionen nach dem Gesetz über die gesellschaftlichen Gerichte der DDR (GBl. I 1982 S. 269) waren gesellschaftliche Organe zur "Erziehung und Selbsterziehung der Werktätigen", die über die Einhaltung der Gebote der sozialistischen Moral, private Streitfälle und geringfügige Straftaten von Betriebsangehörigen entschieden. Durch die Konfliktkommissionsordnung war die zweijährige Aufbewahrung und anschließende Abgabe von Unterlagen an das zuständige Kreisgericht geregelt. Nach Inkrafttreten des Einigungsvertrages ist offensichtlich mangels Regelung ein Teil der Unterlagen der ehemaligen Konflikt- und auch Schiedskommissionen, insbesondere aus den beiden letzten Jahren vor der Wende, noch in den Händen der Kommissionen verblieben. Die DSB der neuen Länder haben sich darauf geeinigt, die zuständigen Stellen aufzufordern, dafür Sorge zu tragen, daß die Unterlagen entsprechend der jeweiligen Landesvorschriften den zuständigen Stellen übergeben werden.
Das TMJE hat den TLfD darüber informiert, daß nach Berichten der Amtsgerichte die Akten der ehemaligen gesellschaftlichen Gerichte bei den meisten Amtsgerichten noch aufbewahrt werden. Teilweise wurden sie jedoch bereits komplett vernichtet. Über den besonderen Vertraulichkeitsgrad dieser Akten ist belehrt worden. Obwohl das Thüringer Archivgesetz keine gesonderten Regelungen zur Sicherung bzw. zum Umgang mit Akten der ehemaligen gesellschaftlichen Gerichte enthält, scheinen die getroffenen Sicherheitsvorkehrungen bei der Archivierung ausreichend. Im Freistaat Thüringen ist kein Fall bekanntgeworden, in dem sich Unterlagen noch bei ehemaligen Kommissionsmitgliedern befinden sollen.

10.3 Altbestände von Karteien bei den Staatsanwaltschaften

Die Altbestände von Karteikarten der früheren Bezirks- und Kreisstaatsanwaltschaften sind als "Vorgänge der Staatsanwaltschaften" im Sinne von Ziffer 3.1 der Verwaltungsvorschrift des Thüringer Justizministeriums (JMBl. für Thüringen 1994, 76) bis auf weiteres aufzubewahren. Im Kreise der DSB der neuen Länder war diskutiert worden, daß eine Aufbewahrung über einen Zeitraum, in dem eine Erforderlichkeit als Zulässigkeitsvoraussetzung vorliegt, unzulässig ist. Die entsprechenden Karteikarten müßten, sofern keine Erforderlichkeit mehr vorliegt, ausgesondert werden. Auf Anfrage des TLfD hinsichtlich der Situation in Thüringen hat das TMJE mitgeteilt, daß für die weitere Aufbewahrung der Karteikarten der zentralen Namenskartei der Staatsanwaltschaften weiterhin eine Erforderlichkeit bezüglich Rehabilitierungsverfahren, Haftzeitbestätigungen und ähnlichen Vorgängen besteht. Im Hinblick auf die noch bestehende Situation in einem neuen Bundesland hat der TLfD der weiteren Aufbewahrung zugestimmt. Es wurde jedoch angeregt, sobald die gegenwärtig bestehenden Bedenken ausgeräumt sind, abweichend von den bisher geltenden Aufbewahrungsbestimmungen generell die Karteikarten
- zehn Jahre nach ihrem Anlegen endgültig auszusondern,
- bereits nach fünf Jahren auszusortieren und in eine jahrgangsweise geführte "Archivdatei" zu übernehmen.

Die weitere Erforderlichkeit der Aufbewahrung der Altbestände der Karteikarten der Staatsanwaltschaften wird im Rahmen einer datenschutzrechtlichen Kontrolle zu überprüfen sein.

10.4 Akteneinsicht in Gerichtsakten und staatsanwaltschaftliche Ermittlungsakten

Die Gewährung von Akteneinsicht, insbesondere in Strafakten, ist derzeit in den Richtlinien für das Straf- und Bußgeldverfahren näher geregelt. Diese Richtlinien sind vornehmlich für die Staatsanwaltschaft bestimmt, einige Hinweise wenden sich aber auch an Richter. Die DSB haben den Bundesgesetzgeber aufgerufen, die Gewährung von Einsicht in Strafakten in der Strafprozeßordnung präzise und unter Berücksichtigung des Persönlichkeitsrechts der Beteiligten zu regeln. Richtlinien genügen nicht den vom Bundesverfassungsgericht geforderten gesetzlichen Grundlagen. Die Gewährung der Akteneinsicht Dritter kann aus datenschutzrechtlicher Sicht im Einzelfall hingenommen werden, wenn dem Erforderlichkeits- und Verhältnismäßigkeitsgrundsatz Rechnung getragen wird. Vom Grundsatz her sollte in alle Strafakten nur dann Akteneinsicht gewährt werden, wenn eine Auskunft aus diesen Akten nicht ausreicht oder einen unverhältnismäßig großen Aufwand bedeutet.
Nach den Richtlinien kann Akteneinsicht grundsätzlich nur einem Rechtsanwalt oder Rechtsbeistand nach Darlegung eines berechtigten Interesses (z. B. für die Prüfung bürgerlich-rechtlicher Ansprüche oder zur Vorbereitung eines Verwaltungsstreitverfahrens) gewährt werden. Darüber hinaus dürfen keine schutzwürdigen Interessen des Beschuldigten oder eines Dritten entgegenstehen. Problematisch ist die Akteneinsicht insbesondere bei Groß- und Sammelverfahren, da hier nicht für jeden Täter und den jeweiligen Tatvorwurf einzelne Akten angelegt werden, so daß jeweils auch personenbezogene Daten Dritter im Zuge der Akteneinsicht wahrgenommen werden können. Gegen eine Aufteilung der Akten wird seitens der Justiz geltend gemacht, daß bei einer gesonderten Aktenführung für jeden einzelnen Täter in diesen Verfahren der Überblick über den gesamten Komplex nicht mehr gewährleistet werden kann. Jedoch sollte in jedem Fall bei Akteneinsicht in diese Akten geprüft werden, ob nicht die Einsicht in einzelne Teile ausreichen kann.
Das Akteneinsichtsrecht ist im Entwurf eines Strafverfahrensänderungsgesetzes 1994 in den §§ 474 ff. StPO zur gesetzlichen Regelung vorgesehen. Der Gesetzentwurf wurde im Bundesrat vom Freistaat Thüringen mitinitiiert. Nach übereinstimmender Auffassung des Bundesrats wird damit den Erfordernissen des Datenschutzes Rechnung getragen.

Im Bereich der Verwaltungsgerichtsbarkeit besteht ebenfalls ein Akteneinsichtsrecht. In einer Eingabe beschwerte sich ein Bürger darüber, daß durch eine Stadtverwaltung personenbezogene Daten über die Anmeldung von Rückübertragungsansprüchen einem Antragsteller nach dem Investitionsvorranggesetz übermittelt worden seien. Dies sei aus einem Antrag an das Verwaltungsgericht im Rahmen eines Verfahrens nach § 80 VwGO zu entnehmen, der von eben jenem Antragsteller gestellt worden sei. Der Petent sah in der Bekanntgabe dieser Daten an eine Privatperson einen Verstoß gegen elementare Bestimmungen des Verwaltungsverfahrensgesetzes und des BDSG.
Die Nachfrage bei der Stadtverwaltung hat ergeben, daß der Antragsteller im Rahmen des Verfahrens nach § 80 VwGO beim Verwaltungsgericht Akteneinsicht genommen hatte. In den Gerichtsakten war unter anderem auch der vermögensrechtliche Antrag des Anmelders enthalten. Nach § 99 VwGO sind die Behörden grundsätzlich zur Vorlage von Urkunden oder Akten und zu Auskünften gegenüber dem Verwaltungsgericht verpflichtet. Zu diesen Akten gehörte auch der Antrag auf Rückübertragung des vom Investitionsvorrangantrag betroffenen Grundstückes. In § 100 Abs. 1 VwGO ist geregelt, daß die Verfahrensbeteiligten neben den Gerichtsakten auch die dem Gericht von den Behörden vorgelegten Akten einsehen können. Im Verwaltungsgerichtsverfahren liegt demnach eine gesetzliche Regelung vor, nach der die Einsichtnahme zulässig ist. Der Eindruck des Petenten, eine Verwaltungsbehörde habe unzulässigerweise personenbezogene Daten offenbart, hatte sich nicht bestätigt. Der Petent wurde hierüber informiert.

10.5 Staatsanwaltschaftliches Verfahrensregister

Nach der Einfügung der §§ 474 ff. StPO durch das Verbrechensbekämpfungsgesetz besteht die Regelung, daß beim BZR ein Zentrales Staatsanwaltschaftliches Verfahrensregister geführt wird. Gemäß § 476 Abs. 5 StPO bestimmt das Bundesministerium der Justiz mit Zustimmung des Bundesrats in einer Errichtungsanordnung die näheren Einzelheiten, insbesondere die Art der zu verarbeitenden Daten, die Anlieferung der zu verarbeitenden Daten, die Voraussetzung, unter der in der Datei verarbeitete Daten an welche Empfänger und in welchem Verfahren übermittelt werden, die Einrichtung eines automatisierten Abrufverfahrens und die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen. Die DSB haben an der allgemeinen Verwaltungsvorschrift über eine Errichtungsanordnung für das länderübergreifende staatsanwaltschaftliche Verfahrensregister in der Fassung der Bundesratsdrucksache verschiedene Punkte kritisiert. Insbesondere war die Auslegung von anderen zur Identifizierung geeigneten Merkmalen, das Fehlen der Voraussetzungen und des Verfahrens für Übermittlungen aus dem Register sowie der Verzicht auf konkrete Ausführung der nach § 9 BDSG geforderten Maßnahmen zur Datensicherung problematisch. Der Entwurf der Errichtungsanordnung hat inzwischen die Bundesratsausschüsse passiert. Die Forderungen der DSB haben in der Beschlußfassung des Bundesrats weitgehend keine Berücksichtigung gefunden.

10.6 Betriebssicherungsdienst der Deutschen Post AG

Aufgrund eines im Berichtszeitraum ergangenen Beschlusses des Hanseatischen Oberlandesgerichtes Hamburg waren Fragen zur Stellung des Betriebssicherungsdienstes der Deutschen Post AG bei der Strafverfolgung aufgetaucht. In diesem Beschluß hat das Oberlandesgericht beschlossen, daß nach der Privatisierung der Post mit Inkrafttreten des Postneuordnungsgesetzes keine Grundlage mehr für die Bestellung von Mitarbeitern des Betriebssicherungsdienstes der Deutschen Post AG als Hilfsbeamte der Staatsanwaltschaften besteht und damit weiterhin auch keine Rechtfertigung mehr für einen weiteren Verbleib von Ermittlungsakten im Gewahrsam des Betriebssicherungsdienstes gegeben ist.
Zur Begründung führt das Oberlandesgericht aus, daß § 152 Abs. 2 GVG die Übertragung der Hilfsbeamteneigenschaft nur auf den öffentlichen Dienst (im Sinne einer funktionalen Einheit aller Personen, die für den Staat handelnd in staatlicher Regie öffentliche Aufgaben besorgen) zulasse. Mit der Privatisierung der Post gehöre der Betriebssicherungsdienst i. d. S. jedoch nicht mehr zum öffentlichen Dienst. Mit dem Funktionsvorbehalt nach Artikel 33 Abs. 4 GG sei es darüber hinaus nicht vereinbar, wenn hoheitliche Befugnisse im Bereich der Strafverfolgung auf Private übertragen würden. Infolge des Wegfalls der Hilfsbeamtenstellung wurde vom Oberlandesgericht die Entfernung der Ermittlungsakten, die dem Betriebssicherungsdienst der Deutschen Post AG vor Inkrafttreten des Postneuordnungsgesetzes in ihrer Funktion als Hilfsbeamte der Staatsanwaltschaft überlassen worden waren, aus dem Gewahrsam des Betriebssicherungsdienstes gefordert.
Der TLfD hat sich daraufhin an das TMJE gewandt, mit der Bitte, zu überprüfen, ob auch in Thüringen bereits vor Inkrafttreten des Postneuordnungsgesetzes der Betriebssicherungsdienst der Deutschen Post AG in einschlägigen Ermittlungsverfahren von der Staatsanwaltschaft beauftragt worden ist und damit ggf. staatsanwaltschaftliche Akten beim Betriebssicherungsdienst vorliegen. Weiter hat der TLfD darum gebeten, die Staatsanwaltschaften dazu zu verpflichten, die Ermittlungsakten aus dem Gewahrsam der Betriebssicherungen der Deutschen Post AG zu entfernen und bis auf weiteres keine Beamten des Betriebssicherungsdienstes mit Ermittlungsaufgaben zu beauftragen. Das TMJE hat dem TLfD mitgeteilt, daß eine unverzügliche Änderung der Verordnungen über die Hilfsbeamten der Staatsanwaltschaften mit dem Ziel der Streichung des Abschnittes über die Hilfsbeamteneigenschaft von Beamten- und Angestelltengruppen der Deutschen Post AG angestrebt wird. In diesem Sinne wurde vom TMJE ein Entwurf einer Neufassung der Thüringer Verordnung über die Hilfsbeamten der Staatsanwaltschaft erarbeitet, der neben anderen notwendigen Änderungen u. a. auch die ersatzlose Streichung des angesprochenen Abschnitts hinsichtlich der Stellung der Beamten und Angestellten im Betriebssicherungsdienst der Deutschen Post AG vorsieht.
Unabhängig davon hat das TMJE durch Erlaß die Thüringer Staatsanwaltschaften über den genannten Beschluß des Hanseatischen Oberlandesgerichts informiert und diese angewiesen, von einer Beauftragung der Angestellten und Beamten des Betriebssicherungsdienstes der Deutschen Post AG mit Ermittlungshandlungen abzusehen.

10.7 Weitergabe personenbezogener Daten an gemeinnützige Einrichtungen

Nach § 153a StPO kann bei einem Vergehen vorläufig von der Erhebung der öffentlichen Klage abgesehen werden oder eine bereits erhobene Klage vorläufig eingestellt werden. Dies wird mit der Auflage verbunden, daß der Beschuldigte bzw. Angeklagte einen Geldbetrag zugunsten einer gemeinnützigen Einrichtung oder der Staatskasse zu zahlen hat. Soll an eine gemeinnützige Einrichtung gezahlt werden, so wird regelmäßig auf dem entsprechenden Überweisungsformular der Name des Betroffenen, seine Anschrift, die Höhe des zu zahlenden Geldbetrages sowie das Geschäftszeichen der Staatsanwaltschaft bzw. des Gerichtes aufgenommen. Neben dem Beschuldigten wird auch der Zahlungsempfänger mittels Formblatt darüber informiert, daß vom Betroffenen unter dem Geschäftszeichen ein bestimmter Geldbetrag zugehen wird. Da es sich in diesen Fällen der Einstellung des Verfahrens nur um einen geringen Schuldvorwurf handeln kann, besteht keinerlei Erfordernis, die Tatsache, daß jemand Beschuldigter in einem Strafverfahren war, an unbeteiligte Dritte, hier eine gemeinnützige Einrichtung, zu übermitteln.
Im Kreise der DSB wurde im Interesse der Betroffenen daher die Möglichkeiten diskutiert, anstelle des Namens des Beschuldigten nur das Geschäftszeichen oder ein Codewort mitzuteilen, um die erfolgte Zahlung als Erfüllung der Auflage zuordnen zu können. Darüber hinaus könnte auch in Erwägung gezogen werden, die Zahlungen nur noch an die Staatskasse zuzulassen und aus dem Gesamtbetrag den gemeinnützigen Einrichtungen Anteile zuzuweisen. Der TLfD hat die Variante der Angabe des Geschäftszeichens unter Verzicht auf die Angabe des Namens favorisiert, da dies zur Individualisierung der Zahlung ausreichend erscheint.
Das TMJE betrachtet die Übermittlung des Namens eines Beschuldigten an einen Zahlungsempfänger als unverzichtbar zur ordnungsgemäßen Aufgabenerfüllung. Insbesondere bei Großverfahren mit mehreren Beschuldigten sei eine Überwachung des Zahlungseingangs nicht mehr möglich. Die Vergabe eines Codes wird abgelehnt, da dies sowohl bei der Information des Zahlungsempfängers als auch bei der Kontrolle der Zahlungseingänge zu einer enormen Arbeitsbelastung und Erschwerung des Verfahrens führen würde.
Hier muß noch eine Regelung im Einklang mit den Belangen des Datenschutzes gefunden werden.

10.8 Eintragung der Schuldunfähigkeit in das Bundeszentralregister

Nach § 11 Abs. 1 Nr. 1 des Bundeszentralregistergesetzes (BZRG) ist im BZR einzutragen, daß eine gerichtliche Entscheidung und Verfügung einer Strafverfolgungsbehörde, durch die ein Strafverfahren wegen erwiesener oder nicht auszuschließender Schuldunfähigkeit oder auf Geisteskrankheit beruhender Verhandlungsunfähigkeit, ohne Verurteilung abgeschlossen wird. Aus der Eintragung ist nicht ersichtlich, ob es sich um eine dauernde oder nur vorübergehende Schuldunfähigkeit gehandelt hat. Diese Eintragung bleibt in der Regel bis zur Vollendung des 90. Lebensjahres des Betroffenen bestehen, auch wenn längst keine Schuldunfähigkeit mehr vorliegt. Die Eintragung taucht dann regelmäßig in Führungszeugnissen für Behörden auf, was zu beruflichen Nachteilen beim Betroffenen führen kann. Es fehlen geregelte Tilgungsfristen für Schuldunfähige. Sie sind damit gegenüber Schuldfähigen, für die Tilgungsfristen nach § 45 ff. BZRG bestehen, benachteiligt. Daß bei Schuldunfähigen über einen sehr viel längeren Zeitraum hinaus Daten aus dem BZR abgerufen bzw. übermittelt werden können, ist aus datenschutzrechtlicher Sicht nicht gerechtfertigt. Das Bundesministerium der Justiz hat schon im Mai 1994 die Vorlage eines entsprechenden Gesetzentwurfes angekündigt. Sobald dieser vorliegt, wird er aus datenschutzrechtlicher Sicht begleitet werden.

10.9 Niederlegung von Suchvermerken im Bundeszentralregister

Von einem anderen Landesdatenschutzbeauftragten wurde dem TLfD mitgeteilt, daß die Meldebehörden seines Landes beabsichtigen, eine Niederlegung von Suchvermerken im BZR zur Ermittlung der Aufenthaltsorte der Personen, die ohne ordnungsgemäße Abmeldung im Zeitraum von November 1989 bis Ende 1990 in die alten Bundesländer abgewandert sind, vorzunehmen.
Nach den Vorschriften des Bundeszentralregistergesetzes (BZRG) ist zwar jede Behörde der Bundesrepublik Deutschland im Rahmen der ihr obliegenden hoheitlichen Aufgaben befugt, befristet Suchvermerke im Register niederzulegen, eine Niederlegung von Suchvermerken zum Zwecke der Vervollständigung der Melderegister erscheint aber aus datenschutzrechtlicher Sicht nicht unbedenklich. Aus diesem Grund wurde das TIM um Mitteilung gebeten, ob in Thüringen die Niederlegung von Suchvermerken in vergleichbaren Fällen ebenfalls vorgesehen ist.
Vom TIM wird die Auffassung vertreten, daß von der Möglichkeit zur Niederlegung von Suchvermerken nur in gravierenden Einzelfällen Gebrauch gemacht werden sollte, um z. B. Unterhalts- und andere Schuldner ausfindig machen zu können. Eine generelle Notwendigkeit, Suchvermerke auch für Personen, die zwischen 1989 und 1990 ohne Abmeldung verzogen sind und bei denen keine Rückmeldung vorliegt, vorzunehmen, wurde vom TIM nicht gesehen. Von seiten des TIM ist nicht beabsichtigt, die Meldebehörden von dieser an sich durch Gesetz gegebenen Möglichkeit zu unterrichten und ihnen entsprechendes Tätigwerden anheim zu stellen. Das TIM geht davon aus, daß der mit der Niederlegung der Suchvermerke angestrebte Erfolg in keinem angemessenen Verhältnis zum Aufwand steht und nur im geringen Umfang zur Vervollständigung der Melderegister führen würde.
Diese Auffassung des TIM wird vom TLfD geteilt, wenn auch der datenschutzrechtliche Aspekt im Vordergrund steht und nicht der vom Ministerium als Begründung angeführte Verwaltungsaufwand.

10.10 Versendung von Einstellungsbescheiden in Ermittlungsverfahren gegen unbekannte Täter

Im Kreise der DSB wurde das Problem aufgeworfen, ob Einstellungsbescheide in Ermittlungsverfahren gegen unbekannte Täter durch die Staatsanwaltschaft durch sogenannte “Info-Post” versendet werden können. Die Einstellungsbescheide enthalten Angaben zum Tatort, zur Tatzeit, zum Delikt und auch die Adresse eines Anzeigenerstatters. Durch den Verbund dieser Daten kann nicht von unsensiblen Daten gesprochen werden.
Die Versandform als “Info-Post” oder auch “Info-Brief” gestattet der Post, diese Briefe stichprobenweise zu öffnen. Da es sich bei den Daten um schützenswerte Daten handelt, ist § 9 Abs. 3 ThürDSG anzuwenden. Danach sind bei der Verarbeitung personenbezogener Daten in nichtautomatisierten Dateien oder in Akten Maßnahmen zu treffen, die verhindern, daß Unbefugte auch beim Transport auf die Daten zugreifen können. Im Falle der “Info-Post” ist durch die Möglichkeit der stichprobenweisen Öffnung der Zugriff von Bediensteten der Post, die mit dem Vorgang an sich nichts zu tun haben, nicht verhindert.
In Thüringen werden Einstellungsbescheide in Ermittlungsverfahren gegen unbekannte Täter generell als Brief versandt. Eine Ausnahme bilden die Einstellungsmitteilungen an die Geschädigten bei Diebstählen und Sachbeschädigungen. Der TLfD hat gegenüber dem TMJE darauf hingewiesen, daß durch Versand dieser Einstellungsbescheide als “Info-Post” die datenschutzrechtlichen Bestimmungen nicht eingehalten werden. Eine Einhaltung wäre dann gegeben, wenn die Post auf das Öffnen der Briefe verzichten würde, wozu jedoch keine Bereitschaft besteht. Der TLfD hat zum Ausdruck gebracht, daß diese Versandform der Einstellungsbescheide aus datenschutzrechtlicher Sicht als unzulässig betrachtet wird.

10.11 Datenschutz im Strafvollzug

Im Strafvollzug ist ebenfalls das Grundrecht auf informationelle Selbstbestimmung zu beachten. Bislang fehlt es jedoch an bereichsspezifischen Datenschutzregelungen für den Strafvollzug (siehe Punkt 10.1). Die Datenerhebung, -verarbeitung und -nutzung ist bisher in der Vollzugsgeschäftsordnung geregelt. Im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichtes zum Grundrecht auf informationelle Selbstbestimmung ist die Regelung in einer Verwaltungsvorschrift, wie sie die Vollzugsgeschäftsordnung darstellt, nur für eine Übergangszeit hinnehmbar. Diese Übergangszeit besteht nunmehr schon seit zwölf Jahren. Ein entsprechendes Änderungsgesetz zum Strafvollzugsgesetz liegt jedoch noch nicht vor. Die DSB fordern seit langem normenklare Datenschutzbestimmungen, wobei besonders darauf zu achten ist, daß sich die Erhebung von Daten über Strafgefangene ebenso wie die Datenerhebung über Dritte am Maßstab der Erforderlichkeit orientiert.

10.11.1 Kontrolle in einer Justizvollzugsanstalt

Anläßlich einer Kontrolle gemäß § 37 ThürDSG in einer Justizvollzugsanstalt (JVA) wurden folgende datenschutzrechtliche Probleme festgestellt:
Es begegnete erheblichen Bedenken, daß in der JVA alte Gefangenenpersonalakten bis zu 43 Jahre nach dem Entlassungstermin aufbewahrt werden. In Übereinstimmung mit dem Thüringer Archivgesetz und der Praxis in anderen Bundesländern wurde angeregt, die Akten nach 30 Jahren dem zuständigen Archiv anzubieten. Seitens der JVA und des TMJE wurde dem entgegengehalten, daß die Akten für Auskünfte über Rentenansprüche, die Bestätigung von Haftzeiten, den Nachweis versicherungspflichtiger Tätigkeit sowie für die Geltendmachung eventuell gegebener Schadensersatzansprüche benötigt werden und daher entsprechend den Aufbewahrungsbestimmungen bis auf weiteres aufbewahrt werden. Für 1996 ist eine zentrale Auskunftsstelle, bei der eine Speicherung der Daten vorgenommen werden soll, angestrebt. Im Hinblick darauf kann die weitere vorübergehende Aufbewahrung in der JVA aus datenschutzrechtlicher Sicht hingenommen werden.
Da in archivierten Gefangenenpersonalakten des entlassenen Jahrgangs 1993 sich zum Teil mehrere Lichtbilder des Gefangenen befanden, hat das TMJE inzwischen die Anstaltsleiter darauf hingewiesen, die Gefangenen nicht nur beim Aufnahmegespräch gemäß § 86 Abs. 3 Strafvollzugsgesetz und Nr. 23 Abs. 4 Vollzugsgeschäftsordnung auf die Möglichkeit der Vernichtung der Lichtbilder nach der Entlassung hinzuweisen, sondern diesen Hinweis bei der Entlassung aus dem Vollzug zu wiederholen.

Bei der Erstaufnahme wird über jeden Gefangenen eine Personalakte (sogenannte Gefangenenpersonalakte) angelegt. Die Gefangenenpersonalakten sind in drei Heftnadeln gegliedert und enthalten vor allem die von der Vollzugsgeschäftsordnung vorgeschriebenen Formblätter, aber auch andere Schriftstücke wie z. B. vollständige Urteile, gerichtliche Verfügungen über die Briefkontrolle, Anträge des Gefangenen usw. Kernstück bildet der Personalbogen A, worauf alle Grunddaten des Gefangenen (Name, Geburtsdatum, Anschrift, Angehörige usw.) bei dessen Zugang festgehalten werden. Von diesem Bogen werden mehrere Durchdrucke erstellt, die an die verschiedenen Abteilungen in der JVA verteilt werden. Die Erforderlichkeit der Angaben auf diesen Durchdrucken für die Aufgabenerfüllung in den verschiedenen Abteilungen wird bei den nächsten Kontrollen in Justizvollzugsanstalten überprüft werden.
Problematisch aus datenschutzrechtlicher Sicht ist insbesondere, daß in die Gefangenenpersonalakten mit der Vielzahl von sensiblen personenbezogenen Daten grundsätzlich allen Bediensteten der JVA die Einsichtnahme gestattet ist. Eine konkrete gesetzliche Regelung des Zugriffs auf die Gefangenenpersonalakten steht weiterhin aus. Daher wird der Zugriff allein auf die weitgehende Auslegung des Strafvollzugsgesetzes und der Vollzugsgeschäftsordnung gestützt. Es ist aber auch das Datenschutzgesetz heranzuziehen, das die Voraussetzung der Erforderlichkeit des Zugriffs enthält. Die Argumentation, die Verfolgung des Vollzugszieles erfordere, daß jeder Bedienstete genau wisse, mit wem er es zu tun hat und wie er zu behandeln ist, rechtfertigt indes einen uneingeschränkten Zugriff nicht. Aus Gründen des Datenschutzes ist der Zugriff auf die Teile der Personalakte zu beschränken, deren Kenntnis zur Aufgabenerfüllung erforderlich ist. Jeder darüber hinausgehende Einblick ist unzulässig. Zur Nachprüfbarkeit der Erforderlichkeit der Einsichtnahme ist auch eine Protokollierung mit Namen und Datum und des Grundes der Einsicht notwendig. Entsprechend der Anregungen des TLfD wird nach Mitteilung des TMJE derzeit ein gesondertes Programm entwickelt, das eine differenzierte Einsicht in Gefangenendaten ermöglicht. Dies kann aber erst bei der Umstellung der Vollzugsgeschäftsstelle auf EDV eingesetzt werden. Bis dahin wurde die geforderte Protokollierung entsprechend der Empfehlung des TLfD geregelt.
Die Gefangenenpersonalakten wurden ebenfalls zur Schulung von Bediensteten im Rahmen der Umstellung auf automatisierte Datenverarbeitung genutzt. Nach der entsprechenden Kritik wurde sofort zugesagt, zu diesem Zweck Musterakten herzustellen. Eine Einsicht von anderen Bediensteten war im übrigen auf keinen Fall zu rechtfertigen.

Eine Besonderheit im Rahmen dieser Kontrolle bestand darin, daß die Einsichtnahme der Mitarbeiter des TLfD in die Gefangenenpersonalakten von einer Genehmigung seitens des TMJE abhängig gemacht wurde. Nach § 38 Abs. 1 ThürDSG hat der TLfD und seine Beauftragten Einsicht in alle Unterlagen und Akten, die im Zusammenhang mit der Kontrolle nach § 37 ThürDSG stehen. Die durch die Vollzugsgeschäftsordnung vorgesehene Genehmigung kann seitens des Ministeriums nicht versagt werden. Daher besteht aus Sicht des TLfD auch kein Erfordernis der Einholung einer entsprechenden Genehmigung. Sie ist vielmehr entbehrlich. Dies, verbunden mit einer zeitlichen Verzögerung bei der Durchführung der Kontrolle und dem Umstand, daß die Kontrolle nicht reibungslos durchgeführt werden konnte, hat dem TLfD Anlaß zur Beanstandung gemäß § 39 ThürDSG gegeben. Die Beanstandung wurde dadurch behoben, daß die Bediensteten nach Mitteilung des TMJE darüber belehrt wurden, daß der TLfD und seine Mitarbeiter gemäß § 37 ThürDSG Einsicht nehmen können, ohne daß hierfür die Genehmigung der Aufsichtsbehörde notwendig ist.

10.11.2 Kontrolle in der EDV-Leitstelle Justizvollzug

Da die Einführung von moderner Rechentechnik in den Justizvollzugsanstalten sich noch in der Aufbauphase befindet, soll nachfolgend nur auf den derzeitigen Zwischenstand eingegangen werden:
Für die Thüringer Justizvollzugsanstalten wurde eine Verwaltungsabteilung "EDV-Leitstelle für den Justizvollzug" eingerichtet, die der Fachaufsicht des TMJE und der Dienstaufsicht des örtlichen Leiters der JVA unterliegt. Die EDV-Leitstelle ist verantwortlich für die gesamte IT-Beschaffung und den IT-Einsatz in den Thüringer Justizvollzugsanstalten. Die rechentechnische Grundlage werden LANs (Lokale Netzwerke) in den fünf Thüringer Justizvollzugsanstalten bilden, welche 1995 und 1996 aufgebaut werden sollen. Die Software wird von der EDV-Leitstelle JVA Thüringen in Zusammenarbeit mit der EDV-Leitstelle JVA Sachsen erarbeitet. Geplant ist, daß jede JVA im Freistaat Thüringen ihr eigenes Rechnernetz besitzt. Nach Angabe des Leiters der EDV-Leitstelle ist keine Datenübertragung von personenbezogenen Daten zwischen den einzelnen Justizvollzugsanstalten vorgesehen. Die EDV-Leitstelle wird die Fernwartung für alle Netzwerke übernehmen.
Während der Kontrolle wurde festgestellt, daß auf dem Rechnernetz in der örtlichen JVA Software mit Daten von Gefangenen zu Testzwecken eingesetzt wurde, ohne daß eine Verfahrensfreigabe nach § 34 ThürDSG vorlag. Die Anträge auf Verfahrensfreigabe sind für das erste Halbjahr 1996 angekündigt. Da offensichtlich für einige Programme die Testphase mit fiktiven personenbezogenen Daten abgeschlossen war, bemängelte der TLfD die hierfür noch nicht ordnungsgemäß eingerichteten Zugriffsrechte und Paßwortgestaltungen für die jeweils zuständigen Mitarbeiter der JVA (siehe Punkt 15.14.2). Ein Teil der Zugriffsrechte und Paßwortregelungen wurde sofort korrigiert, für die übrigen wurde die Realisierung zugesagt. Die Beschaffung eines noch fehlenden Sicherheitsschrankes wurde ebenfalls zugesagt, sobald die Haushaltsmittel zur Verfügung stehen. Damit wurde den Anregungen und Forderungen des TLfD entsprochen.

10.11.3 Beschwerden von Gefangenen

Wenn jemand an seiner Wohnungstür, Haustür oder an seinem Briefkasten seinen Namen anbringt, so erfolgt dies freiwillig und in der Regel zu dem Zweck, daß er von Besuchern gefunden wird und seine Post richtig abgegeben werden kann. Im Justizvollzug stellt sich dies etwas anders dar. Der Name in Verbindung mit der Tatsache, daß er sich an einer Haftraumtür in einer Justizvollzugsanstalt befindet, offenbart einem Besucher, daß sich der Betreffende im Justizvollzug befindet, was eine nicht erforderliche Datenübermittlung darstellt. Mehrere Beschwerden von Gefangenen richteten sich dagegen, daß in einer JVA anläßlich eines Besuches von anstaltsfremden Personen die Namensschilder an den Haftraumtüren nicht umgedreht waren, so daß die Möglichkeit bestand, die Namen der Gefangenen zur Kenntnis zu nehmen. Auf Anfrage hat die Anstaltsleitung mitgeteilt, daß die Namen an den Haftraumtüren anläßlich eines Besuches durch anstaltsfremde Personen ohne Aufgabenbezug im Strafvollzug üblicherweise weisungsgemäß umgedreht werden, um den datenschutzrechtlichen Anforderungen Rechnung zu tragen. Ob dies bei dem den Beschwerden zugrundeliegenden Besuch der Fall war, war im nachhinein mangels Dokumentation des Umdrehens der Namensschilder nicht feststellbar. Auf Anregung des TLfD hat die Anstaltsleitung der JVA die Anweisung zum Umdrehen, Abnehmen oder Abdecken der Namensschilder von Gefangenen an den Haftraumtüren bei Besuchen der Anstalt durch Personen ohne Aufgabenbezug im Strafvollzug inzwischen schriftlich erlassen.
Die grundsätzliche Erforderlichkeit des Anbringens von Namensschildern an Haftraumtüren ist jedoch in Frage zu stellen, zumal zumindest in einer JVA in Thüringen und auch in verschiedenen anderen Ländern darauf verzichtet wird. Die Anstaltsleitung hat hierzu dargelegt, daß es für jeden Justizvollzugsbediensteten aus Gründen der Ordnung und Sicherheit sowie aus "behandlerischen und betreuerischen Gründen" unabdingbar sei, die Namen der Gefangenen zu kennen und in der Anrede zu benutzen, nicht zuletzt, um an der Erreichung des Vollzugszieles, nämlich den Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen (§ 2 StVollzG), mitzuwirken. Dies sei am besten durch diese Namensschilder gewährleistet. Im Laufe der Diskussion hat die Anstaltsleitung mitgeteilt, die große Mehrheit der Gefangenen in der betroffenen JVA habe die Einwilligung zur Anbringung des Schildes mit ihren Namen an der Haftraumtür erklärt. Verweigert jedoch ein Gefangener dieses Einverständnis, so besteht die Möglichkeit, daß er nur mit der Nummer seines Haftraumes angesprochen wird.

Problematisch in diesem Zusammenhang war auch, daß seitens der Anstaltsleitung keine Erforderlichkeit zum Umdrehen der Namen an den Haftraumtüren bei Besuchen von Justizvollzugsbediensteten aus anderen Justizvollzugsanstalten gesehen wurde. Der TLfD hat darauf hingewiesen, daß die Kenntnisnahme der Namen nur zulässig sein kann, wenn eine konkrete dienstliche Aufgabe wahrgenommen wird, zu der die Kenntnisnahme erforderlich ist.

Eine weitere Beschwerde war gegen die Überwachung des Schriftverkehrs von Gefangenen mit Rechtsanwälten gerichtet.
§ 29 StVollzG geht von dem Grundsatz aus, daß das grundgesetzlich geschützte Briefgeheimnis auch für den Strafgefangenen Gültigkeit hat. Der Schriftwechsel des Gefangenen mit seinem Verteidiger ist ebenso wie Schreiben des Gefangenen an Volksvertretungen des Bundes und der Länder sowie an deren Mitglieder und die europäische Kommission für Menschenrechte von der Überwachung ausgenommen. Der übrige Schriftwechsel darf aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt überwacht werden. Verteidigerpost muß nach der Verwaltungsvorschrift zu § 29 StVollzG deutlich sichtbar gekennzeichnet sein. Briefe von Rechtsanwälten, die nicht mit “Verteidigerpost” gekennzeichnet sind, dürfen aber nach Auffassung des TLfD nicht ohne weiteres im Zuge der Überwachung des übrigen Schriftwechsels geöffnet werden. Sollte ein Brief nämlich ungekennzeichnet dennoch Verteidigerpost beinhalten, würden unbefugt personenbezogene Daten erhoben. Die JVA muß sich in diesen Fällen zunächst rückversichern, ob es sich um Verteidigerpost handelt oder nicht. Werden diese Briefe ohne eine entsprechende Rückversicherung geöffnet, so ist das Briefgeheimnis, das den besonderen Schutz personenbezogener Daten enthält, verletzt.

Dem TLfD ist seitens eines Gefangenen auch mitgeteilt worden, daß das Schreiben des TLfD an ihn der Briefüberwachung unterzogen wurde. Nach Angaben der Anstaltsleitung erfolgt die Überwachung des “übrigen Schriftverkehrs” jedoch nur stichprobenweise. Da sich gemäß § 11 Abs. 1 ThürDSG jedermann an den TLfD mit dem Vorbringen wenden kann, daß bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen seine schutzwürdigen Belange beeinträchtigt werden und nach § 11 Abs. 2 ThürDSG niemand benachteiligt oder gemaßregelt werden darf, weil er von diesem Recht Gebrauch macht, sieht der TLfD keine Veranlassung, daß seine Schreiben von einer JVA, wenn auch nur stichprobenweise, kontrolliert werden.

10.12 Ehescheidungsverbundurteile

Ehescheidungsverbundurteile sind von den Parteien (Betroffene) bei verschiedenen Behörden und sonstigen Stellen (Meldebehörde, Standesamt, Finanzamt, Arbeitgeber) vorzulegen. Wenn das vollständige Urteil vorgelegt wird, erhält die betreffende Stelle neben den von ihr benötigten Angaben zwangsläufig eine Vielzahl von Informationen (personenbezogene Daten der Partei), die zur Aufgabenerfüllung nicht benötigt werden.
In den Personalakten bzw. Besoldungs- und Vergütungsakten befinden sich zum Teil vollständige Scheidungsverbundurteile oder auch Unterhaltsvergleiche. In diesen Urteilen bzw. Vergleichen sind auch oft Daten von unbeteiligten Dritten aufgenommen. Die Anforderung und Aufnahme der Urkunden in die Personalakten stellen in diesen Fällen eine Erhebung von Daten dar, die nicht für die Aufgabenerfüllung erforderlich sind. Die Daten zu erheben ist somit unzulässig.
Dieses hat der TLfD zum Anlaß genommen, sich mit einem Schreiben an die obersten Landesbehörden, das LVwA, die Landratsämter und kreisfreien Städte des Freistaats Thüringen zu wenden. Um die datenschutzrechtliche Problematik in Zukunft zu vermeiden, wurde eine Anregung des TMJE aufgegriffen und die Personalverwaltungen darauf aufmerksam gemacht, daß bei der Anforderung eines solchen Urteils beim Betroffenen darauf hinzuweisen ist, daß eine auszugsweise Ausfertigung zur Aufgabenerfüllung ausreicht. Aufgrund der genauen Bezeichnung des Zwecks der benötigten Urkunde kann das Gericht die Belange des Datenschutzes dadurch gewährleisten, daß den Betroffenen nur entsprechende Auszüge versandt werden. Auch soll der Betroffene bei der Anforderung einer solchen Unterlage darauf hingewiesen werden, daß Angaben über Dritte, die für die Personalstelle nicht relevant sind, geschwärzt werden können.

Von den LfD anderer Bundesländer ist mitgeteilt worden, daß nach entsprechender Umstellung der Gerichte auf automatisierte Verfahren beabsichtigt ist, den Betroffenen mit der Versendung eines Scheidungsverbundurteiles darauf hinzuweisen, daß die Möglichkeit besteht, für die im Urteil geregelten Folgesachen, also die Sachen, die nicht den Scheidungsausspruch selbst betreffen, Auszüge und Teilausfertigungen des Urteils zu beantragen.

10.13 Einsicht in das Grundbuch

Nach § 12 der Grundbuchordnung (GBO) kann jeder, der ein berechtigtes Interesse darlegt, Grundbuchinformationen über Eigentumsverhältnisse in Form der Datenübermittlung einer öffentlichen Stelle an einen Dritten erhalten. Die DSB des Bundes und der Länder haben übereinstimmend die Protokollierung der Einsichtnahmen gefordert. Damit wäre

nachvollziehbar, wer, unter Umständen auch aus welchem Grund, Einsicht in die Grundbuchinformationen genommen hat. Einer Protokollierung sämtlicher Einsichtnahmen in die Grundbücher aufgrund der großen Nachfrage insbesondere in den neuen Bundesländern stehen wegen zahlreicher Grundstückserwerbsvorgängen und auch hinsichtlich der oft unklaren Rechtslage von Grundstückseigentum die Justizverwaltungen der Länder in Anbetracht des Aufwandes kritisch gegenüber.
Da das Grundbuch im Freistaat Thüringen künftig automatisiert geführt werden soll, wird dann auch die technische Möglichkeit geschaffen, die Einsichtnahme automatisiert zu protokollieren. Die Einführung des automatisierten Grundbuches soll ab Anfang 1996 schrittweise erfolgen. Mit der Einführung des automatisierten Grundbuches besteht auch die Möglichkeit, die bisherigen Grundbücher in Papierform in das automatisierte Grundbuch aufzunehmen. Den Forderungen aus datenschutzrechtlicher Sicht zur Protokollierung der Einsichtnahme könnte dann nachgekommen werden.

10.14 Datenverarbeitung durch Notare

Auch die Notare des Freistaats Thüringen unterliegen der Kontrolle des TLfD. Bei den Notaren des Freistaats werden üblicherweise auch automatisierte Dateien zur Aufgabenerfüllung geführt. Die Bundesnotarordnung, das Beurkundungsgesetz und auch die bundeseinheitliche Dienstordnung für Notare enthalten keinerlei datenschutzrechtliche Bestimmungen zur automatisierten Datenverarbeitung. Entsprechende Regelungen und damit Rechtsgrundlagen sind jedoch dringend erforderlich. Ebenso wie sich der BfD und andere LfD an die jeweilige Justizverwaltung gewandt haben, wurde dem TMJE das Anliegen, bei einer Änderung der entsprechenden Gesetze auch datenschutzrechtliche Bestimmungen aufzunehmen, mitgeteilt. Der TLfD wird weiterhin darauf dringen.

10.15 Zweite Zwangsvollstreckungsnovelle

Der Entwurf eines Zweiten Gesetzes zur Änderung zwangsvollstreckungsrechtlicher Vorschriften (2. Zwangsvollstrekkungsnovelle) wurde in der 12. Legislaturperiode nicht mehr im Bundestag behandelt. Der Entwurf der 2. Zwangsvollstreckungsnovelle ist nunmehr als Gesetzentwurf des Bundesrates erneut in den Bundestag eingebracht worden. Gegenstand der Kritik aus datenschutzrechtlicher Sicht ist nach wie vor § 829 Abs. 1 ZPO. Dieser regelt den Pfändungsbeschluß bezüglich Geldforderungen gegenüber einem Dritten, der dem Schuldner Geld schuldet. Hier soll ein Satz angefügt werden, wonach ein einheitlicher Pfändungsbeschluß auf Antrag des Gläubigers gegenüber mehreren Drittschuldnern ergehen soll, soweit dies für Zwecke der Vollstreckung geboten erscheint und kein Grund zu der Annahme besteht, daß schutzwürdige Interessen der Drittschuldner entgegenstehen. Diese Regelung ist trotz des Hinweises auf die Interessen der Drittschuldner datenschutzrechtlich unzureichend. Soweit weiterhin ein einheitlicher Pfändungsbeschluß ergehen soll, wird dies im Ergebnis regelmäßig erfolgen. Jede Mitteilung des Namens und der Anschrift eines Drittschuldners an einen anderen Drittschuldner bedeutet einen Eingriff in dessen Persönlichkeitsrecht. Voraussetzung für die Zulässigkeit eines Eingriffs in das Persönlichkeitsrecht ist jedoch, daß er erforderlich ist. Es ist indessen nicht erforderlich, daß jemand erfährt, wer einer Person noch Geld schuldet. Daher sollte vom Grundsatz getrennter Pfändungsbeschlüsse für jeden einzelnen Drittschuldner ausgegangen werden und nur ausnahmsweise, soweit dies für Zwecke der Vollstreckung erforderlich ist und kein Grund zu der Annahme besteht, daß schutzwürdige Interessen der Drittschuldner entgegenstehen, hiervon abgewichen werden. Dies scheint eine Sollvorschrift nicht sicherzustellen. Bei der Zustellung von Pfändungs- und Überweisungsbeschlüssen durch Gerichtsvollzieher bei Unternehmen ist darauf zu achten, daß, zur Vermeidung der Kenntnisnahme des Inhaltes durch unberechtigte Dritte bei Ersatzzustellung durch Übergabe des Schriftstückes an einen Mitarbeiter, sich diese in einem verschlossenen Umschlag befinden.

10.16 Einsatz von EDV-Systemen im Geschäftsbereich der Gerichtsvollzieher

Die Verwaltungsvorschrift des TMJE über den “Einsatz von EDV-Systemen im Geschäftsbereich des Gerichtsvollziehers” wurde im Berichtszeitraum überarbeitet und neu gefaßt. Dies geschah nach Mitteilung des TMJE in erster Linie, um eine Angleichung der entsprechenden Verwaltungsvorschriften der Länder Bayern, Sachsen, Sachsen-Anhalt und Thüringen zur Erleichterung der gemeinsamen Gerichtsvollzieherausbildung herbeizuführen. Diese Verwaltungsvorschrift regelt den Einsatz von EDV-Technik zur Führung der Geschäftsbücher der Gerichtsvollzieher. Da die Gerichtsvollzieher personenbezogene Daten verarbeiten, sind die Bestimmungen des ThürDSG zu beachten. Vor allem besteht für die Gerichtsvollzieher die Pflicht der Meldung der automatisierten Dateien zum Datenschutzregister. Die grundsätzlichen Bestimmungen der Verwaltungsvorschrift waren bereits in der ursprünglichen Form der Verwaltungsvorschrift enthalten. Die Neufassung der Verwaltungsvorschrift wurde dem TLfD zum Zwecke der Beteiligung vorgelegt. Hinsichtlich der Einführung der Verwaltungsvorschrift bestanden aus datenschutzrechtlicher Sicht keine Bedenken.

11. Gesundheits- und Sozialdatenschutz

11.1 Änderungen von Rechtsgrundlagen

11.1.1 Novelle des Sozialdatenschutzes

Nach längerer Diskussion, an der sich auch die DSB von Bund und Ländern intensiv beteiligt hatten, ist am 01.07.1994 das Zweite SGB-Änderungsgesetz in Kraft getreten. Hauptgegenstand der Novelle war aus Sicht des Datenschutzes die Neufassung des 2. Kapitels des Zehnten Buches ("Schutz der Sozialdaten"). Die Anpassung der bisherigen Vorschriften an die neuere Entwicklung des Datenschutzrechtes erfolgte zunächst dadurch, daß die Verweisungen auf das BDSG durch die Übernahme dieser Bestimmungen in den Text des SGB X ersetzt wurden. Eine vorangestellte Vorschrift mit Begriffsbestimmungen soll die Handhabung des Gesetzes erleichtern.
Diesen Begriffsbestimmungen folgen Regelungen zur Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung. Daran schließen sich detaillierte Vorschriften zum Schutz der Sozialdaten vor unbefugter Übermittlung an. Hierbei hat sich der Gesetzgeber insbesondere bei der Festschreibung der Zweckbindung der Datenverwendung eng an das BDSG angelehnt. Dennoch erforderten bereichsspezifische Besonderheiten des Sozialrechts gegenüber dem BDSG modifizierte Übermittlungsregelungen. Die Einführung einer Vorschrift zur Einrichtung automatisierter Abrufverfahren (§ 79 SGB X) ist neu und trägt ebenfalls den neueren Entwicklungen sowohl in der Datenverarbeitungstechnik wie auch im Datenschutz Rechnung. Hinzuweisen ist noch auf die Verbesserung der Kontrollbefugnis der LfD. Durch die Verweisung auf das BDSG in der früheren Fassung waren die Kompetenzen der LfD bei ihren Kontrollen nicht eindeutig geklärt. Man behalf sich mit einer verfassungskonformen Auslegung, daß die jeweiligen landesrechtlichen Regelungen maßgeblich sein sollten. Diese Auslegung wurde nun mit dem neuen § 81 Abs. 2 Satz 3 SGB X durch den Bundesgesetzgeber als geltendes Recht bestätigt.

11.1.2 Einordnung der gesetzlichen Unfallversicherung in das Sozialgesetzbuch (SGB VII)

Die Bundesregierung hat im Sommer 1995 einen Gesetzentwurf vorgelegt, der die Einordnung der Vorschriften der RVO bezüglich der gesetzlichen Unfallversicherung in das Sozialgesetzbuch als Siebtes Buch vorsieht.
Ein bereits Anfang 1995 vorgelegter Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung gab den DSB von Bund und Ländern Anlaß zur Kritik. So war unter anderem die Beschränkung einer als zu weitgehend empfundenen Auskunftspflicht der behandelnden Ärzte gegenüber den Unfallversicherungsträgern gefordert worden. Darüber hinaus sind noch eine Vielzahl weiterer Kritikpunkte aus datenschutzrechtlicher Sicht benannt worden. Die wesentlichen Forderungen sind in einer Entschließung der 49. Konferenz der DSB des Bundes und der Länder enthalten (siehe Anlage 18).
Der in Kenntnis dieser Entschließung vorgelegte Regierungsentwurf trägt den Bedenken der DSB von Bund und Ländern jedoch nur teilweise Rechnung. Unter Federführung des BfD mit Unterstützung der LfD werden die noch nicht berücksichtigten Forderungen im derzeit stattfindenden Gesetzgebungsverfahren vorgetragen.

11.2 Gesetzliche Kranken- und Pflegeversicherung

11.2.1 Mitgliederwerbung durch Krankenkassen?

Da ab 01.01.1996 die Mitglieder der gesetzlichen Krankenversicherung das Recht haben, die Mitgliedschaft in einer gesetzlichen Krankenkasse frei zu wählen, stehen ab diesem Zeitpunkt die Krankenkassen im Wettbewerb zueinander. Dies führt zu dem Bedürfnis der Krankenkassen, um ihre Mitgliedschaft zu werben. Unter den DSB des Bundes und der Länder wurde daher die Frage erörtert, ob es zulässig ist, daß die Krankenkassen sich personenbezogene Daten beschaffen dürfen, um anschließend mit diesen Daten potentielle neue Mitglieder zu werben. Dabei bestand Einigkeit darin, daß die Krankenkassen im Rahmen ihrer Aufklärungs- und Beratungspflicht nach den §§ 13 und 14 SGB I befugt sind, allgemein gehaltene Werbung durch Veranstaltungen sowie Annoncen etc. zu betreiben. Einer gezielten personenbezogenen Werbung steht jedoch der abschließende Katalog des § 284 Abs. 1 SGB V entgegen, der die Erhebung und Speicherung von Daten für Werbezwecke der Krankenkassen nicht erlaubt. Anläßlich eines Informationsgespräches, das der TLfD mit der Geschäftsführung der AOK Thüringen im Herbst letzten Jahres führte, wurde mitgeteilt, daß zur Zeit keine personenbezogene Mitgliederwerbung beispielsweise in Schulen oder durch Betreuungsbeauftragte durchgeführt wird. Man beschränke sich auf die Bewerbung eigener Mitglieder im Rahmen von Aufklärungsschriften und Gesundheitskursen.
Die DSB von Bund und Ländern haben in Gesprächen mit dem zuständigen Bundesministerium für Gesundheit die Forderung erhoben, § 284 Abs. 1 SGB V um eine Datenerhebungsbefugnis zur personenbezogenen Werbung zu ergänzen. Solange es keine solche Befugnis gibt, ist davon auszugehen, daß die Krankenkassen keine Mitgliederwerbung mittels zu erhebender oder gespeicherter personenbezogener Daten betreiben dürfen.

11.2.2 Mißverständnisse über Pflichtmitgliedschaft bei der AOK

Eine Geschäftsstelle der AOK Thüringen begrüßte mit einem Schreiben ihr neues Mitglied, das zuvor eine Lehrstelle angetreten hatte, und beglückwünschte es zu seiner guten Wahl. Der Betreffende argwöhnte hierbei jedoch eine unzulässige Datenübermittlung durch seinen Arbeitgeber an die AOK: Er hatte sich bei Antritt seiner Lehre für eine andere Ersatzkasse entschieden, an die seine Beiträge abgeführt wurden.
Die Überprüfung des Sachverhaltes von seiten des TLfD bei der AOK ergab, daß der Petent sich tatsächlich bei einer anderen Ersatzkasse versichert hatte, ihm jedoch nach geltender Rechtslage ein solches Wahlrecht nicht zustand. Dieses war der AOK als zuständiger "Pflichtkrankenkasse" im Rahmen ihrer Überwachung der ordnungsgemäßen Beitragsabführung aufgefallen. Die Angaben über das Arbeitsverhältnis wurden daher durch den Arbeitgeber gemäß § 98 Abs. 1 SGB X zu Recht der zuständigen "Pflichtkrankenkasse" mitgeteilt.

11.2.3 Geschäftsstellenübergreifender Zugriff auf Versichertendaten durch die AOK?

Bei der datenschutzrechtlichen Prüfung von AOK-Geschäftsstellen wurde durch mehrere LfD festgestellt, daß aufgrund der zentralen Verarbeitung von Versichertendaten und der Einrichtung von Online-Zugriffen für alle Geschäftsstellen auf Daten aller Versicherten zugegriffen werden kann. Aufgrund datenschutzrechtlicher Bedenken hinsichtlich der Erforderlichkeit eines landesweiten oder überregionalen Zugriffes auf Versichertendaten wurde von den DSB des Bundes und der Länder in ihrer 49. Konferenz (siehe Anlage 19) darauf hingewiesen, daß ohne ein schriftliches Einverständnis der Versicherten nur der Zugriff auf einen Stammdatensatz für vertretbar gehalten wird. Dabei wird anerkannt, daß sowohl aus Wettbewerbsgründen wie auch im Interesse der Versicherten die Möglichkeit des Zugriffs von verschiedenen Geschäftsstellen nicht grundsätzlich verwehrt werden darf. Voraussetzung ist jedoch, daß der Versicherte dieses wünscht. Ob dies dadurch erreicht wird, daß der Betroffene schriftlich seine Zustimmung abgibt oder ein Zugriff auf die Daten nur durch Eingabe der Chipkarte des Versicherten möglich wird, ist dabei unerheblich. Eine abschließende Klärung konnte bisher noch nicht erreicht werden, da die Argumente der gesetzlichen Krankenkassen gegen eine Beteiligung der Versicherten beim Zugriff nach Auffassung der LfD nicht stichhaltig genug waren.

11.2.4 Übermittlung medizinischer Daten durch den Medizinischen Dienst der Krankenversicherung (MDK)

Gemäß § 275 SGB V sind die Krankenkassen in gesetzlich bestimmten Fällen verpflichtet, gutachterliche Stellungnahmen des MDK einzuholen. Nach § 277 SGB V hat der MDK das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund mitzuteilen. Der Versicherte kann der Mitteilung zum Befund an den Leistungsbringer widersprechen.
Im Rahmen der Kontrolltätigkeit des TLfD wurde bei den gesetzlichen Krankenkassen festgestellt, daß seitens der Gutachter des MDK der Begriff "gutachterliche Stellungnahme" sehr weit gefaßt wurde, indem nicht nur das Gesamtergebnis und die erforderlichen Angaben zum Befund, sondern alle dem Gutachter zur Verfügung stehenden Anamnese- und Befunddaten aufgenommen wurden. Eine Rückfrage beim MDK Thüringen ergab, daß von dort zwischenzeitlich zur Gewährleistung der Erfordernisse des Sozialdatenschutzes eine Dienstanweisung zu den Problemen des EDV-Einsatzes, des Datenschutzes und der Datensicherheit herausgegeben worden war. Eingeschlossen darin ist die Übergabe einheitlicher Vordrucke an die Gutachter, die so gestaltet sind, daß eine Datenübermittlung über das erforderliche Maß hinaus künftig ausgeschlossen werden kann. Aufgrund der Feststellungen des TLfD wurden vom MDK Thüringen nochmals nachdrücklich alle Beratungsstellen auf die Beschränkung bei der Datenübermittlung auf das gesetzlich vorgegebene erforderliche Maß hingewiesen. Die Einhaltung dieser Hinweise wird der TLfD in Zukunft kontrollieren.

11.2.5 Übersendung von Befund- und Entlassungsberichten an die gesetzlichen Krankenkassen zur Anspruchsprüfung

Auf Grund einer Anfrage hatte sich der TLfD mit der Frage zu beschäftigen, ob und in welchem Umfang Befund- und Entlassungsberichte zur Anspruchsprüfung der Krankenhäuser an die gesetzlichen Krankenkassen übergeben werden müssen. Gemäß § 39 SGB V haben Versicherte einen Anspruch auf Behandlung in einem zugelassenen Krankenhaus, wenn das Behandlungsziel nicht ambulant, teilstationär oder vor- oder nachstationär erreicht werden kann. In § 301 SGB V ist geregelt, daß die Krankenhäuser verpflichtet sind, den Krankenkassen bei einer Krankenhausbehandlung die medizinischen Angaben wie die Einweisungsdiagnose und die Aufnahmediagnose als Nachweis der Notwendigkeit der stationären Behandlung zu übermitteln. Ebenso ist bei einer Überschreitung der je nach Behandlung zugeordneten bestimmten Verweildauer darüber hinaus dies der Krankenkasse gegenüber zu begründen. Die dafür notwendigen Angaben zur Datenübermittlung an den Leistungsträger sind in § 301 SGB V abschließend geregelt. Dementsprechend dürfen zur Klärung der Kostenübernahme die Krankenkassen von den Krankenhäusern keine Entlassungsberichte anfordern.

Es ist jedoch immer wieder festzustellen, daß Krankenhäuser, teilweise aus Vereinfachungsgründen, von sich aus Befunde und Entlassungsberichte als medizinische Begründung zur Klärung der Kostenübernahme übersenden. Dies ist nicht zulässig, da durch diese Verfahrensweise den Krankenkassen Daten übermittelt werden, die für deren Aufgabenerfüllung nicht erforderlich sind. Demgegenüber bestehen selbstverständlich aus datenschutzrechtlicher Sicht keine Bedenken, wenn die gesetzliche Krankenkasse zur Prüfung der Voraussetzung, Art und Umfang der Krankenhausbehandlung nach § 275 SGB V eine gutachterliche Stellungnahme des MDK einholt. Der medizinische Dienst ist befugt, die Räume der Krankenhäuser zu betreten, in Krankenunterlagen Einsicht zu nehmen und soweit erforderlich, den Versicherten zu untersuchen. Aufgrund des Einsichtsrechts des medizinischen Dienstes ist es auch zulässig, ersatzweise in Einzelfällen Auszüge aus den Krankenunterlagen, insbesondere auch Entlassungsberichte, an den MDK, nicht jedoch an die Krankenkasse, zu übersenden. Eine Weiterleitung der Krankenhausentlassungsberichte an die Krankenkasse ist aufgrund der Rechtslage nicht möglich.

11.2.6 Verfahren zur Feststellung der Pflegebedürftigkeit

Das nach langem und zähem Ringen verabschiedete Pflegeversicherungsgesetz vom 26.04.1994 sieht vor, daß ab 01.04.1995 Leistungen im Rahmen der häuslichen Pflege sowie ab 01.06.1996 Leistungen im Rahmen der stationären Pflege erbracht werden. In diesem Zusammenhang hatte sich der TLfD - entsprechend seinem Zuständigkeitsbereich - mit der Erhebung und Übermittlung von personenbezogenen Daten bei der Feststellung der Pflegebedürftigkeit auseinanderzusetzen. Dies bezieht sich zunächst nur auf die Feststellung der Pflegebedürftigkeit hinsichtlich der häuslichen Pflege. Die Problematik betrifft jedoch auch die zweite Stufe der Pflegeversicherung. Die Praxis bei der Feststellung der Pflegebedürftigkeit weicht von den gesetzlichen Vorgaben ab.
Voraussetzung für die Inanspruchnahme von Leistungen der Pflegeversicherung ist die Pflegebedürftigkeit (§ 14 SGB XI), die vorliegt, wenn Personen "wegen einer körperlichen, geistigen oder seelischen Krankheit oder Behinderung für die gewöhnlichen und regelmäßigen wiederkehrenden Verrichtungen im Ablauf des täglichen Lebens auf Dauer ... der Hilfe bedürfen". Diese Pflegebedürftigen werden nach § 15 SGB XI in drei Stufen eingeteilt: erheblich Pflegebedürftige, schwer Pflegebedürftige und Schwerstpflegebedürftige. Ob die Voraussetzungen der Pflegebedürftigkeit vorliegen, lassen die Krankenkassen nach der Antragstellung durch den Versicherten vom MDK gemäß § 18 SGB XI überprüfen. Dieser untersucht den Versicherten in der Regel in dessen häuslicher Umgebung. Ist die Aktenlage eindeutig, so kann diese Untersuchung ausnahmsweise unterbleiben.
Die Einzelheiten zur Abgrenzung der Merkmale der Pflegebedürftigkeit und der Pflegestufen sowie zum Verfahren der Feststellung der Pflegebedürftigkeit haben die Spitzenverbände der Pflegekassen unter Beteiligung des MDK, der Kassenärztlichen Bundesvereinigung sowie weiterer Verbände in den sogenannten "Pflegebedürftigkeits-Richtlinien" vom 07.11.1994 verbindlich geregelt. Die Anlage zu diesen Richtlinien enthält ein Formular, in das alle Befunde über aktuelle Erkrankungen sowie über Vorerkrankungen, die für die Pflegebedürftigkeit von Bedeutung sind, eingetragen werden. Außerdem sind detaillierte Angaben über das noch vorhandene oder nicht mehr vorhandene "Funktionieren" des Versicherten zu machen. Es handelt sich dabei um eine Vielzahl intimster persönlicher Daten, wie z. B. "Essen und Trinken können", "Ausscheiden können" oder "Funktionelle Einschränkungen der Psyche". Die Richtlinien sehen vor, daß der MDK das in diesem Formular zusammengefaßte Gutachten der Pflegekasse zu übermitteln hat. Die Richtlinien regeln weiter, daß die Pflegekasse über die Mitwirkungspflicht sowie die Folgen fehlender Mitwirkung aufklärt und den Antragsteller auffordert, dem MDK die Einwilligung zur Einholung von Auskünften bei seinen behandelnden Ärzten zu erteilen. Der Umfang der erforderlichen Einwilligung des Versicherten in die Offenbarung seiner Daten über Vorerkrankungen ist nicht näher umschrieben.
Diese Unbestimmtheit des Umfangs der Daten, in deren Offenbarung eingewilligt werden soll, könnte in der Praxis dazu führen, daß vom MDK bei sämtlichen Ärzten, die den Antragsteller je behandelt haben, Befunddaten angefordert werden, was gegen § 18 Abs. 3 SGB XI verstieße, wonach nur die für die Begutachtung der Pflegebedürftigkeit wichtigen, also erforderlichen Angaben bei dritten Ärzten eingeholt werden dürfen. Daher sind die Formulare, auf denen der Antragsteller seine Einwilligung erklärt, so zu fassen, daß es dem Antragsteller möglich ist, bei seiner Einwilligung die Beiziehung von Arztunterlagen, die nicht mit der Pflegebedürftigkeit in Zusammenhang stehen, auszuschließen. Darüber hinaus ist es problematisch, wenn durch den MDK den Pflegekassen die vollständigen Gutachtenformulare zur Kenntnis gegeben werden, da § 18 Abs. 5 Satz 1 lediglich davon spricht, den Pflegekassen "das Ergebnis seiner Prüfung mitzuteilen". Die Auslegung des Wortlautes wird durch die Aufgabenverteilung zwischen Pflegekassen und MDK gestützt. Danach bedienen sich die Pflegekassen des MDK, der den Versicherten in seinem Wohnbereich untersucht und der Pflegekasse das Ergebnis seiner medizinischen Begutachtung mitteilt. Die Weitergabe sämtlicher Einzelbefunde, wie sie die Anlage zu den Richtlinien vorsehen, ist nicht erforderlich. Eine Übermittlung der vollständig erhobenen Daten kann allenfalls zur Überprüfung in Einzelfällen möglich sein. Dagegen liefe die Übermittlung aller Angaben zur Prüfung durch die Pflegekassen auf eine doppelte Aufgabenerledigung hinaus, die vom Gesetzgeber so nicht gewollt sein dürfte.

Dem TMSG wurden diese Bedenken vorgetragen. Es wurde gebeten, auf Bundesebene auf eine Änderung der Pflegebedürftigkeits-Richtlinien hinzuwirken. Dieses teilt die letztgenannten Bedenken nicht, da die Pflegekassen als Entscheidungsbefugte Anspruch auf Vorlage sämtlicher entscheidungserheblichen Unterlagen habe. Dieser Auffassung kann sich der TLfD nicht anschließen, da dies gerade dazu führen würde, daß die Begutachtung durch zwei Stellen erfolgen würde. Hier bedarf es - auch auf Bundesebene - weiterer Überzeugungsarbeit.

11.3 Umgang mit Patientendaten im Gesundheitswesen

11.3.1 Altdaten aus ehemaligen Polikliniken und Ambulanzen

Bei der Auflösung der staatlichen Einrichtungen des Gesundheitswesens der ehemaligen DDR, wie Polikliniken, Ambulatorien, Betriebssanitätsstellen, wurden auf Landesebene keine gesonderten Regelungen zum Umgang mit den Patientenunterlagen getroffen. So haben nach Auflösung der ehemaligen Gesundheitseinrichtungen der DDR Ärzte, die bis zu diesem Zeitpunkt angestellt waren, Akten bisheriger Patienten ohne deren Zustimmung in ihre Niederlassung mitgenommen. Diese Verfahrensweise kann sicher im Interesse des Patienten aus datenschutzrechtlicher Sicht gebilligt werden, soweit der Patient durch sein schlüssiges Verhalten (erneuter Arztbesuch beim niedergelassenen Arzt) seine Zustimmung bekundet hat. Wurde demgegenüber der Arzt vom Patienten nach seiner Niederlassung nicht mehr aufgesucht bzw. liegt keine Einwilligung vor, ist eine weitere Verwahrung der Unterlagen bei diesem Arzt unzulässig, es sei denn, daß dieser im Auftrag der Kommunalverwaltung handelt. Dazu bedürfte es aber zunächst einer Bestandsaufnahme, gegenseitiger Informationen sowie entsprechender Vereinbarungen. Weitere Akten (vermutlich der überwiegende Teil) wurden nach Auflösung der ehemaligen Gesundheitseinrichtungen von den Kommunen oder Landratsämtern übernommen. Dies erfolgte jedoch mehr oder weniger sporadisch, so daß ein Gesamtüberblick bis zum heutigen Tag nicht vorliegt.
Trotz ständiger Bemühungen seitens des TLfD um eine patientengerechte und datenschutzrechtlich akzeptable einheitliche Regelung in Thüringen konnte bisher kein befriedigendes Ergebnis erreicht werden. Nach Auffassung des TLfD stehen gemäß § 30 ThürDSG die alten Patientenunterlagen aus ehemaligen Gesundheitseinrichtungen den Kommunen als demjenigen Träger öffentlicher Verwaltung zu, der nach dem Grundgesetz für die Verwaltungsaufgabe zuständig ist. Aufgrund fehlender Nachfolgeeinrichtungen sollte jedoch aus datenschutzrechtlicher Sicht aufgrund der Sensibilität der dem Arztgeheimnis unterliegenden medizinischen Daten eine weitere Verwahrung der Unterlagen unter der Verantwortung eines Arztes (zweckmäßigerweise im jeweils zuständigen Gesundheitsamt) erfolgen. Zwischenzeitlich durchgeführte Kontrollen und Rückfragen des TLfD ergaben, daß sich in Thüringen die Gesundheitsämter auch ohne weitere Regelungen grundsätzlich dieser Aufgaben gestellt haben, wobei die Arbeitsweise, das Engagement und das Ergebnis in den einzelnen Kreisen große Unterschiede erkennen läßt. Als Hauptproblem erweist sich auch aufgrund strittiger Zuständigkeiten das Verfahren zur Bestandsaufnahme, da sich mit wachsendem zeitlichen Abstand seit Auflösungen der Gesundheitseinrichtungen die Kenntnis über den Verbleib der Patientenakten immer mehr verringert.

Das alles interessiert jedoch den betroffenen Bürger nicht. Er erwartet, daß mit Auflösung des ehemaligen staatlichen oder kommunalen Gesundheitswesens dafür Sorge getragen wird, daß auch weiterhin seine Patientenakten vor unbefugter Einsichtnahme sicher verwahrt werden und er bei Bedarf, wie bei jedem Behandlungsverhältnis mit einem Arzt, im Rahmen der Aufbewahrungsfristen Einblick bzw. Auszüge daraus erhalten kann und nicht, daß seine Unterlagen wie herrenloses Gut behandelt werden und Bauarbeiter seine Akte beim Abbruch eines Hauses finden oder diese gemeinsam mit alten Autoreifen oder Baumaterialien in Kellerräumen von Landratsämtern, zu denen auch Hausmeister, Kraftfahrer oder Handwerker Zutritt haben, ungeordnet lagern. Daß dies durchaus keine theoretischen Vorstellungen sind, zeigten Überprüfungen in den letzten zwei Jahren. Selbstverständlich hat der TLfD bei entsprechenden Feststellungen von den zuständigen Stellen sofortige Abhilfe gefordert. Unabhängig davon wurde aber auch wegen der grundsätzlichen Bedeutung dieses Problems das TMSG aufgefordert, gemeinsam mit dem TIM Regelungen und Empfehlungen zum Umgang mit Patientenunterlagen aus ehemaligen staatlichen und kommunalen Einrichtungen zu erlassen. Da trotz mehrmaliger Erinnerung durch den TLfD kein zufriedenstellendes Ergebnis erreicht werden konnte, wurde dies gemäß § 39 ThürDSG beanstandet.
Zwischenzeitlich wurde vom TMSG der Entwurf eines gemeinsamen Runderlasses des Ministeriums für Soziales und Gesundheit und des Innenministeriums über Hinweise und Empfehlungen zur datenschutzrechtlichen Behandlung von Patientenunterlagen, Zentralkarteien, Zentralen Registern und Zentraldateien mit patientenbezogenem medizinischen Inhalt vorgelegt. Die Prüfung der Unterlagen ergab jedoch, daß darin die Fragen hinsichtlich der Verantwortlichkeiten, zum Verfahren der Bestandsaufnahme, der Art und Weise der Verwahrung und der Nutzung der Unterlagen noch nicht eindeutig und ausreichend beantwortet werden. Dies wurde dem TMSG, mit der Bitte um eine entsprechende Überarbeitung des Entwurfes, mitgeteilt.
Da nunmehr (fast fünf Jahre nach Auflösung der Gesundheitseinrichtungen) der Entwurf eines gemeinsamen Runderlasses des TMSG und des TIM vorliegt, bleibt zu hoffen, daß auch in Kürze im Interesse aller Betroffenen eine

datenschutzgerechte und vor allem auch praxisbezogene Lösung gefunden wird und Meldungen, daß "Patientenakten aufgefunden" wurden, der Vergangenheit angehören werden. Der TLfD wird diesen Bereich weiterhin kritisch und beratend beobachten.

11.3.2 Gesundheitsakten von Strafvollzugsbediensteten

Im DDR-Strafvollzug wurden neben den Personalakten auch Gesundheitsakten über Bedienstete, die durch den Anstaltsarzt behandelt wurden, angelegt. Da diese Gesundheitsakten im Januar 1991 abgeschlossen wurden und gegenwärtig in den Justizvollzugsanstalten aufbewahrt werden, hat das TMJE den TLfD um Stellungnahme zum weiteren Verbleib dieser Akten gebeten.
Der TLfD hat hierzu ausgeführt, daß diese Gesundheitsakten, wie Patientenakten anderer Ärzte auch, nach der Berufsordnung für Ärzte zehn Jahre nach Abschluß der Behandlung aufzubewahren sind. Bei Gesundheitsakten ist davon auszugehen, daß sie sehr sensible Daten enthalten und gegen unbefugten Zugriff in ärztlicher Obhut gesondert gesichert sein müssen. Daher scheidet eine Übergabe an die Betroffenen selbst aus. Auf Wunsch der Betroffenen könnten sie jedoch dem jeweils weiterbehandelnden Arzt übergeben werden.
Wenn die Gesundheitsakten nicht an weiterbehandelnde Ärzte übergeben werden können, so ist mit diesen Unterlagen nach § 16 ThürDSG zu verfahren. Die Daten sind zunächst zur Aufgabenerfüllung einer JVA nicht erforderlich. Sie wären demnach grundsätzlich gemäß § 16 Abs. 1 Nr. 1 ThürDSG nach Ablauf der Aufbewahrungsfrist von zehn Jahren nach Abschluß der Behandlung zu löschen. Vor einer Löschung sind sie jedoch dem zuständigen Archiv zur Übernahme anzubieten. Sollte das Archiv die Übernahme ablehnen, unterbleibt dennoch die Löschung nach § 16 Abs. 4 Nr. 1 ThürDSG, wenn im Einzelfall Grund zur Annahme besteht, daß schutzwürdige Interessen des Betroffenen, etwa wegen möglicher haftungsrechtlicher Ansprüche, beeinträchtigt werden. Aus datenschutzrechtlicher Sicht können die Gesundheitsakten zunächst weiterhin für die Dauer der Aufbewahrungsfrist in gesicherter Verwahrung der Justizvollzugsanstalten des Freistaats Thüringen verbleiben.

11.3.3 Die ärztliche Schweigepflicht besteht auch gegenüber der Polizei

In einer Eingabe beschwerte sich ein Bürger über einen Amtsarzt, der verschiedene Anamnesedaten über ihn an eine Polizeiinspektion übermittelt hatte. Die nähere Untersuchung des Falls ergab, daß der Amtsarzt auf telefonische Anfrage eines Polizeibeamten ein Schreiben an die betreffende Polizeiinspektion sandte, in dem er nicht nur über den psychischen Krankheitszustand des Bürgers informierte, sondern auch medizinische Sachverhalte über dessen Frau übermittelte. Nach Aussagen des Amtsleiters der Polizeiinspektion erfolgte das Auskunftsersuchen, weil der Bürger häufig Strafanzeigen erstattete, die als offensichtlich unbegründet erschienen.
In einem persönlichen Gespräch mit dem ehemaligen Amtsarzt ging dieser von der Zulässigkeit seiner Übermittlung aus. Er führte hierzu aus, daß die von ihm übermittelten Informationen und Sachverhalte "allgemein bekannt" gewesen wären und die Übermittlung nur im Interesse des Bürgers gelegen hätten. Er stützte sich hierbei auf § 4 Abs. 2 der Verordnung über den öffentlichen Gesundheitsdienst für die Aufgaben der Gesundheitsämter in den Landkreisen und kreisfreien Städten. Darin heißt es, daß personenbezogene Daten an die zuständigen Behörden mitgeteilt werden dürfen, wenn dies zur Abwehr von Gefahren für Leben oder Gesundheit erforderlich ist. Dieser Ansicht konnte der TLfD aber nicht folgen. Entsprechend der besonderen Verschwiegenheitspflicht der Ärzte gemäß § 2 der Ärztlichen Berufsordnung der Landesärztekammer Thüringen, die durch die Regelungen des § 203 Abs. 1 Nr. 1 und Abs. 2 Nr. 1 StGB strafrechtlich bewährt ist, mußte der TLfD davon ausgehen, daß es sich hierbei um einen groben Verstoß gegen datenschutzrechtliche Bestimmungen handelt. Die um Auskunft ersuchende Polizeiinspektion wurde aufgefordert, sich künftig bei Auskunftsersuchen an Stellen, die einer besonderen Schweigepflicht unterliegen, zur Vermeidung des Verdachts einer Anstiftung zu einer strafbaren Handlung zu vergewissern, daß die begehrte Auskunft keine Verletzung von Privatgeheimnissen im Sinne des § 203 StGB darstellt.

11.3.4 Negative Bekenntnisfreiheit im Krankenhaus

Der bDSB eines Landesfachkrankenhauses für Psychiatrie und Neurologie übersandte dem TLfD ein von ihm erstelltes Datenschutz-Merkblatt zur Prüfung. Darin war u. a. zu lesen, daß die Klinikmitarbeiter dem Seelsorger neben dem Namen und der Aufenthaltsstation auch die Konfession des Patienten mitteilen dürfen, wenn dies der Patient nicht ausdrücklich untersagt hat. Nach Artikel 136 Abs. 3 Satz 1 der Weimarer Reichsverfassung (WRV), der nach Artikel 140 GG weiter gilt, ist niemand verpflichtet, seine religiöse Überzeugung zu offenbaren. Dies ist eine Wiederholung des bereits nach Artikel 4 Abs. 1 GG gewährleisteten Grundrechts auf negative Bekenntnisfreiheit, das heißt dem Recht, die eigene religiöse Überzeugung gegenüber anderen zu verschweigen. Ist das Bekenntnis des Patienten den Mitarbeitern des Krankenhauses bekannt, so ist ein wirksamer Schutz des Rechts auf negative Bekenntnisfreiheit durch einen Widerspruch des Patienten allein nicht gewährleistet. Vielmehr ist hierfür die ausdrückliche Zustimmung des Patienten

zu einer solchen Datenübermittlung erforderlich. Dieser Hinweis wurde dem bDSB des Krankenhauses mitgeteilt. Es ist davon auszugehen, daß nunmehr entsprechend verfahren wird.

11.3.5 Bekanntgabe der Zahl der HIV-Infizierten in der Zeitung

Im Jahr 1994 wurden in mehreren Presseveröffentlichungen Zahlen über HIV-Infizierte und Aidserkrankte in Thüringen, darunter auch für die Zeit vor 1989 in den ehemaligen Bezirken Erfurt, Gera und Suhl, genannt. Bei einer Rückfrage beim zuständigen Ministerium für Soziales und Gesundheit wurde der TLfD auf einen Bestand anonymisierter HIV-Daten der ehemaligen Bezirke Erfurt, Gera und Suhl verwiesen. Da weitere Angaben nicht erfolgten, sah sich der TLfD veranlaßt, vor Ort den Datenbestand zu prüfen. Die Durchsicht der Unterlagen ergab, daß es sich bei diesem Material bereits um aggregierte Daten von HIV-Erkrankungen handelte, die den ehemaligen Bezirkshygieneinspektionen von der damaligen Zentralstelle in Berlin als Informationsmaterial zur Verfügung gestellt worden waren. Die Aufstellungen selbst ließen aufgrund der Aggregationen keinerlei Rückschlüsse mehr auf einzelne Patienten zu. Insoweit handelte es sich nicht mehr, wie vom TMSG mitgeteilt worden war, um anonymisierte Daten, sondern, da keine reanonymisierbaren Einzeldatensätze vorhanden waren, um eine reine Statistik der HIV-Infizierten bzw. Aidserkrankten. Insoweit gab es hinsichtlich der weiteren Verwahrung und Nutzung dieser Materialien aus datenschutzrechtlicher Sicht keinerlei Bedenken.

11.4 Übermittlung von Blutspenderdaten

Bundesweit kam es in der Vergangenheit durch Bluttransfusionen bei den Empfängern zu einer HIV Übertragung. In einem anderen Bundesland hat ein durch eine Blutübertragung HIV-infizierter Patient verlangt, daß ihm die Spenderdaten übermittelt werden. Er bezog sich dabei auf ein Urteil des Landessozialgerichts Niedersachsen. Danach ist der ärztliche Leiter eines Bluttransfusiondienstes als Arzt zwar schweigeverpflichtet, aber in seiner Eigenschaft als behördlicher Leiter des Transfusionsdienstes zur Herausgabe der Spenderdaten verpflichtet.
Nach Angaben des TMSG sind in Thüringen bislang keine Fälle bekannt, in denen die personenbezogenen Daten der Blutspender verlangt wurden. Die Spenderdaten unterliegen der ärztlichen Schweigepflicht und sind außer dem ärztlichen Leiter des Herstellers der Konserve niemandem zugänglich.
Der übermittelten Rechtsauffassung des TMSG ist zuzustimmen. Weiterhin kann eine Pflicht zur Offenbarung nur durch § 34 StGB (rechtfertigender Notstand) sowie § 385 Abs. 2 ZPO und § 53 Abs. 2 StPO (Entbindung von der Verschwiegenheitspflicht) gegeben sein. Eine Trennung des ärztlichen Leiters in Arzt mit Schweigepflicht und in behördlichen Leiter ohne Schweigepflicht ist nach Auffassung des TLfD nicht möglich.
Zur Wahrung ihrer Rechte benötigt die durch die Blutspende HIV-infizierte Person die Daten des Spenders nicht. Für den Blutempfänger besteht damit an der Offenbarung dieser Daten kein rechtliches Interesse.

11.5 Aufnahme von Personalien durch Lebensmittelüberwachungsamt

Im Rahmen einer Prüfung in einem Staatlichen Veterinär- und Lebensmittelüberwachungsamt wurde festgestellt, daß bei der Abgabe von Lebensmittelproben durch einen Bürger dessen Personalien auf einem Vordruck “Beschwerdeprobe” festgehalten werden. Dagegen bestehen natürlich keine Bedenken, da selbstverständlich der Beschwerdeführer über das Ergebnis informiert werden möchte bzw. im Notfall auch informiert werden muß. Als problematisch wurde jedoch vom TLfD der Umfang der Datenerhebung angesehen, da die Erforderlichkeit für eine Erhebung des Berufes, des Familienstandes und der Staatsbürgerschaft des Beschwerdeführers nicht begründet werden konnte.
Im Ergebnis einer Rückfrage im LVwA als zuständiger Aufsichtsbehörde wurde dem TLfD mitgeteilt, daß die Veterinär- und Lebensmittelüberwachungsämter aufgrund des Hinweises angewiesen wurden, ab sofort auf die Ausfüllung dieser Angaben zu verzichten und künftig diese Merkmale auf dem Vordruck nicht mehr enthalten sein werden.
Da ein Durchschlag des Vordruckes mit der Lebensmittelprobe dem Veterinär- und Lebensmittelinstitut übergeben wird, hatte der TLfD gleichzeitig angeregt, künftig auf die Übermittlung der Personalien des Beschwerdeführers zu verzichten und statt dessen eine entsprechende Proben- bzw. Identifikationsnummer zu verwenden. Dieser Vorschlag wurde gleichfalls vom LVwA aufgegriffen und mit der Bitte an das TMSG weitergeleitet, dieses bei der Überarbeitung der Thüringer Richtlinien für die Probennahme von Lebensmitteln, Tabakerzeugnissen, kosmetischen Mitteln und sonstigen Bedarfsgegenständen zu prüfen.

11.6 Meldungen der Gesundheitsämter nach dem Bundesseuchengesetz

Durch den ständigen Erfahrungsaustausch zwischen den DSB des Bundes und der Länder wurde der TLfD darauf hingewiesen, daß seit 1994 im Rahmen der Ausdehnung meldepflichtiger Krankheiten nach dem Bundesseuchengesetz auf die humanen spongiformen Enziphalopathien (Creutzfeldt-Jakob-Krankheit) die zuständigen Gesundheitsämter von den Ärzten Meldungen auf einem einheitlichen Formblatt erhalten, welches unter anderem den Namen, den Vornamen, die Straße, die Postleitzahl, den Ort, den Beruf, das Geschlecht, die Staatsangehörigkeit sowie das Geburts- und Sterbedatum der betroffenen Person enthalten. Gemäß § 1 Abs. 3 der Verordnung über die Ausdehnung der Meldepflicht übersendet das zuständige Gesundheitsamt die Formblätter in anonymisierter Form über die zuständige Landesbehörde an das Robert-Koch-Institut. Die faktische Anonymisierung soll dadurch erreicht werden, daß der Name, der Vorname, die Straße, der Ort und die zwei letzten Stellen der Postleitzahl sowie der genaue Tag der Geburt nicht übermittelt werden.
Dabei ist jedoch zu beachten, daß aus den Angaben zum Beruf, wie z. B. Schornsteinfegermeister o. ä., in Verbindung mit den drei ersten Stellen der Postleitzahl sowie dem Geburtsmonat und Jahr oder auch durch seltene Staatsangehörigkeiten im Einzelfall Identifizierungen möglich sein könnten. Aus diesem Grund ist zur Vermeidung jedes Reidentifikationsrisikos der Beruf entsprechend zu verallgemeinern.
Dieser Hinweis des TLfD wurde vom TMSG unmittelbar aufgegriffen und den Gesundheitsämtern zur künftigen Beachtung übermittelt.

11.7 Muß der ärztliche Leiter des Rettungsdienstes Patientendaten speichern?

Bei einem Notarzteinsatz oder einem Rettungstransport ist eine Notarzteinsatzprotokollierung durchzuführen. Dabei handelt es sich um einen standardisierten Erfassungsbogen mit zwei Durchschlägen, der u. a. auch personenbezogene Daten des Notfallpatienten enthält. In einem Rundschreiben an alle Landkreise und kreisfreien Städte legte das TIM fest, daß das Original des Bogens für die medizinische Einrichtung zur Weiterbehandlung des Patienten bestimmt ist, der erste Durchschlag beim Notarzt verbleibt und der zweite Durchschlag der ärztliche Leiter des Rettungswesens zu Zwecken der Qualitätssicherung behält. In einem Schreiben der Thüringer Notärzteschaft wurde der TLfD gebeten, sich dafür einzusetzen, daß auch der ärztliche Leiter Rettungswesen einen nicht anonymisierten Durchschlag des Notarzteinsatzprotokolls erhält. Da aber das Rundschreiben des TIM der Rechtslage gemäß § 20 Abs. 3 ThürRettG entspricht, bestand aus der Sicht des TLfD kein Anlaß, auf eine Änderung des o. g. Rundschreibens Einfluß zu nehmen. Zehn Monate später wurde dem TLfD das DIVI-Notarztprotokoll der Deutschen Rettungsflugwacht zur datenschutzrechtlichen Prüfung vorgelegt. Dabei zeigte sich eine weitgehende Übereinstimmung mit dem in Thüringen nicht mehr in Anwendung kommenden Notarzteinsatzprotokoll. Wieder war vorgesehen, daß der Leiter der Luftrettung ebenfalls verschiedene personenbezogene Daten des Notfallpatienten erhalten würde. Die Deutsche Rettungsflugwacht wurde darauf hingewiesen, daß die Rechtslage gemäß § 20 Abs. 3 ThürRettG völlig eindeutig ist und dazu aufgefordert, den zweiten Durchschlag in anonymisierter Form zu gestalten.

11.8 Bekanntgabe der Sozialversicherungs-Wahlergebnisse

Der Wahlausschuß bei der Landesausführungsbehörde für Unfallversicherung Thüringen hat im Thüringer Staatsanzeiger die Ergebnisse der allgemeinen Sozialversicherungswahl 1993 in der Weise bekanntgemacht, daß die Namen, Amtsbezeichnungen, Adressen sowie die Geburtsdaten der gewählten Mitglieder sowie deren Stellvertreter abgedruckt wurden. Ein hier Genannter stellte dem TLfD die Frage, ob die Veröffentlichung in diesem Umfang zulässig sei. Rechtsgrundlage für die Veröffentlichung der gewählten Mitglieder und Stellvertreter bei den Sozialversicherungswahlen ist § 59 Abs. 2 der Wahlordnung für die Sozialversicherung (v. 23.02.1992, BGBl. I S. 116 ff.). Danach sind durch den Wahlausschuß nach Feststellung des endgültigen Wahlergebnisses Familienname, Vorname, Geburtsdatum, Wohnort und Wohnung der Mitglieder und ihrer Stellvertreter öffentlich bekanntzugeben. Bei einer Novelle dieser Verordnung sollte sich der Bundesverordnungsgeber überlegen, ob zur Unterrichtung der Versicherungsmitglieder das genaue Geburtsdatum erforderlich ist, da es für den Versicherten wohl nur von Bedeutung sein dürfte, welcher Altersgruppe “sein” Vertreter angehört.
Von § 59 Abs. 2 nicht abgedeckt ist allerdings die Veröffentlichung der jeweiligen Amtsbezeichnung. Eine Erforderlichkeit zur Unterrichtung der Versicherungsmitglieder über die Amtsbezeichnung der Gewählten ist nicht ersichtlich. Da es sich bei diesen Angaben um Sozialdaten handelt, ist nach § 67b Abs. 1 SGB X eine Übermittlung nur zulässig, wenn der Bewerber zuvor ausdrücklich seine Einwilligung abgegeben hat. Dem TMSG als zuständiger Aufsichtsbehörde wurde dies mitgeteilt und darum gebeten, sicherzustellen, daß bei künftigen allgemeinen Sozialversicherungswahlen die Amtsbezeichnungen der Gewählten nur nach deren vorheriger Einwilligung veröffentlicht werden.

11.9 Soziales

11.9.1 Rundfunkgebührenbefreiung aus sozialen Gründen durch das Sozialamt?

Durch die Anfrage eines Sozialamtes wurde der TLfD auf die Praxis bei der Befreiung von der Rundfunkgebührenpflicht aufmerksam. Nach § 5 Abs. 2 Satz 3 der Thüringer Rundfunkgebührenbefreiungsverordnung entscheidet die Rundfunkanstalt (MDR) über die Befreiung aus sozialen Gründen auf Vorschlag der Sozialbehörden. § 5 Abs. 2 Satz 4 der Verordnung eröffnet die Möglichkeit, daß die Rundfunkanstalt die Sozialbehörden zur Aushändigung des Befreiungsbescheides ermächtigen darf. Hiervon hat der MDR Gebrauch gemacht. Mit dieser Praxis wird die Entscheidung über die Befreiung von der Rundfunkgebührenpflicht von den Sozialbehörden gegenüber dem Antragsteller rechtsverbindlich getroffen, ohne daß der MDR den Vorgang vor Aushändigung des Befreiungsbescheides zur Kenntnis genommen hat. Im Anschluß an die ausgesprochene Befreiung fordert der MDR von den Sozialämtern die Vorlage sämtlicher Nachweise, die für die Befreiung von der Rundfunkgebührenpflicht von Bedeutung sind.

Nach § 6 Abs. 4 des Rundfunkgebührenstaatsvertrages kann die Entscheidungszuständigkeit für die Befreiung auch auf andere Stellen als die Landesrundfunkanstalt übertragen werden. Dies ist jedoch in der geltenden Befreiungsverordnung nicht vorgesehen, insbesondere sind auch keine Regelungen getroffen, welche personenbezogenen Daten die für die Entscheidung zuständige Stelle an die Landesrundfunkanstalt zu übermitteln hat. Der vom MDR erhobene Anspruch auf Übermittlung aller Daten, die dem Vorschlag und der Entscheidung der Sozialbehörde zugrunde lagen, entbehrt daher einer Rechtsgrundlage. Diese Rechtsauffassung wird von den für den Einzugsbereich des MDR zuständigen LfD in Sachsen, Sachsen-Anhalt und Thüringen geteilt. Da aufgrund des Rundfunkgebührenstaatsvertrages die Rundfunkgebührenbefreiungsverordnungen der Länder übereinstimmen sollen, haben die drei genannten LfD die für das Rundfunkrecht zuständigen Landesressorts auf die rechtswidrige Praxis hingewiesen und darum gebeten, sich für eine übereinstimmende Änderung der Rundfunkgebührenbefreiungsverordnungen einzusetzen. Bei der notwendigen Änderung des Verfahrens ist aus datenschutzrechtlicher Sicht insbesondere folgendes zu beachten:

- Es ist an dem datenschutzrechtlichen Grundsatz festzuhalten, daß die Erhebung und Verarbeitung von personenbezogenen Daten nur durch die Behörde erfolgen darf, die für die Entscheidung zuständig ist.

- § 6 Abs. 4 Rundfunkgebührenstaatsvertrag eröffnet die Möglichkeit, daß eine andere Behörde als die Rundfunkanstalt über den Antrag auf Gebührenbefreiung entscheidet. In diesem Zusammenhang muß in einer Rechtsverordnung geregelt werden, welche Daten erforderlichenfalls an den MDR übermittelt werden.

- Bei einer solchen Novellierung der Rundfunkgebührenbefreiungsverordnung bieten sich wegen der besonderen Sensibilität der Daten die Sozialbehörden als bürgernahe Entscheidungsträger an. Das Verfahren wird damit erheblich vereinfacht und entspricht dem verfassungsrechtlichen Gesichtspunkt der Transparenz gegenüber dem Antragsteller.

Anlaß für die Anforderung von sämtlichen für die Beurteilung der Rundfunkgebührenbefreiung erforderlichen Unterlagen durch den MDR ist sicher, daß damit die möglicherweise zu großzügig ausgesprochenen Befreiungen nachträglich durch den MDR kontrolliert und ggf. revidiert werden sollen.
Dieselbe Motivationslage führte auch in der Vergangenheit dazu, daß die Rundfunkanstalten zur Ermittlung von "Schwarzhörern" eine regelmäßige Übermittlung der Daten aller volljährigen Einwohner an die GEZ begehrten. Entsprechende Rechtsgrundlagen enthielten nur die Meldedatenübermittlungsverordnungen Hessens und Nordrhein-Westfalens. Die 46. Konferenz der DSB des Bundes und der Länder hat am 26./27.10.1993 festgestellt, daß eine solche Regelung zu einem bundesweiten Melderegister bei Volljährigen führen könnte und überdies gegen das Verhältnismäßigkeitsprinzip verstoßen würde. Der Entwurf einer Thüringer Meldedatenübermittlungsverordnung, der derzeitig vom TIM vorbereitet wird, enthält in der dem TLfD bekannten Fassung keine solche Regelung und trägt damit dem Beschluß der 46. Datenschutzkonferenz Rechnung. Dies wird begrüßt.

11.9.2 Adoptionsgeheimnis gilt auch bei Überprüfung des Kindergeldanspruches

Das Erste Gesetz zur Umsetzung des Spar-, Konsolidierungs- und Wachstumsprogrammes vom 21.12.1993 sah unter anderem vor, die eingeengten Voraussetzungen für das Weiterbestehen eines Kindergeldanspruches ab 01.01.1994 zu überprüfen. Hierzu wurde vom zuständigen Bundesministerium für Familie und Senioren ein einheitlicher Vordruck an die zuständigen Landesstellen gegeben. In diesem Erfassungsbogen sind die Antragsteller unter anderem danach gefragt worden, ob das Kind, für das Kindergeld bezogen wird, ein leibliches Kind oder ein Adoptivkind ist. Daneben sah der Erfassungsbogen vor, daß über 16 Jahre alte Kinder diesen Erfassungsbogen unterschreiben müssen.

Nach § 1754 BGB sind Adoptivkinder den leiblichen Kindern rechtlich gleichgestellt. Die Frage danach ist nicht zulässig, da sie für die Feststellung des Kindergeldanspruches nicht erforderlich ist. Durch diese Fragestellung wird das Adoptionsgeheimnis nach § 1758 BGB verletzt, weil der Antragsteller annehmen muß, daß er zur Offenbarung der Adoption deshalb verpflichtet ist, weil er mit seiner Unterschrift die Vollständigkeit der Angaben zu versichern hat.
Dieser Sachverhalt wurde von den DSB in Bund und Ländern einhellig kritisiert und gefordert, die bereits erhobenen Angaben zu Adoptionen wieder zu löschen. In Thüringen wurde ein entsprechender Vordruck von der ZGT verwendet. Das TFM wurde gebeten, die erhobenen Adoptionsdaten zu löschen bzw. zu sperren. Das TFM hat daraufhin durch Erlaß die ZGT angewiesen, entsprechend zu verfahren. Darüber hinaus ist eine Änderung des entsprechenden Vordrucks erfolgt.

11.9.3 DDR-Antragsformulare für Kindertagesstättenplatz sind überholt

Aufgrund einer Bürgereingabe erhielt der TLfD Kenntnis von noch in Anwendung befindlichen Anträgen auf Einweisung in eine Kinderkrippe, einen Kindergarten oder ein Kinderwochenheim. Darin wurden Angaben zu Geschwisterkindern sowie zum erlernten Beruf und zur jetzigen Tätigkeit (einschließlich der Anschrift der Arbeitsstelle, der Telefonnummer sowie der täglichen Arbeitszeit) der Eltern erhoben. Da gemäß § 22 Abs. 1 Kindertageseinrichtungsgesetz (KitaG) jedes Kind im Alter von zwei Jahren und sechs Monaten bis zum Schuleintritt einen Rechtsanspruch auf einen Kindergartenplatz besitzt, werden vom Gesetzgeber keine Bedingungen für die Zuweisung eines Kindergartenplatzes an die Eltern gestellt, so daß die o. g. Datenerhebung nicht für die Prüfung erforderlich ist.
Gemäß § 19 Abs. 1 ThürDSG ist das Erheben personenbezogener Daten nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Ist diese Voraussetzung nicht erfüllt, so ist auch eine Erhebung, die mit Einwilligung des Betroffenen durchgeführt wird, bereits unzulässig. Die Stadtverwaltung hat daraufhin eine Dienstanweisung erlassen, in der alle Kindertagesstättenleiterinnen darauf hingewiesen werden, daß alte Anträge nicht mehr verwendet werden dürfen.

11.9.4 Mißachtung des Datenschutzes durch den nachgeordneten Bereich eines Jugendamtes

Im Berichtszeitraum erreichte den TLfD eine Eingabe, in der sich ein Bürger darüber beschwerte, daß er nach Unterbringung seines Kindes in einem Heim über dessen Unfall durch einen an der Wohnungstür angebrachten und für jedermann lesbaren Zettel informiert wurde. Neben der Mitteilung über den Unfall war die Anschrift des Klinikums bzw. des Kinderheimes für eventuelle Rückfragen angegeben. Nach Prüfung des Vorganges mußte aus datenschutzrechtlicher Sicht dem Petenten bestätigt werden, daß aufgrund der Form der Datenübermittlung auch unbefugte Dritte Zugang zu den Informationen erhalten hatten. Die Begründung der Erzieherin des Heimes, daß sie im Interesse der Gesundheit der Tochter sowie der bestehenden Rechtslage eine umgehende Information der Eltern für erforderlich hielt und davon ausgegangen war, daß mit einer Benachrichtigung an der Wohnungstür (bei vorgefundenem gefüllten Briefkasten) dieses Ziel am schnellsten erreichbar war, konnte aus datenschutzrechtlicher Sicht nicht akzeptiert werden.
Im vorliegenden Fall hätte es ausgereicht, nur einen Hinweis auf eine dringende Nachricht an der Wohnungstür anzubringen oder die Bitte um einen dringenden Rückruf unter einer Telefonnummer zu hinterlassen. Eine öffentlich zugängliche Information, daß die Tochter in einem bestimmten Heim wohnt sowie der Umstand, daß sie verunglückt war und wo sie sich gegenwärtig aufhält, stellte eine unzulässige Offenbarung dar. In diesem Sinne wurde das zuständige Jugendamt und die Heimleitung informiert und gebeten, den Vorfall zum Anlaß zu nehmen, die Mitarbeiter nochmals entsprechend zu belehren, damit Wiederholungen ausgeschlossen sind.

11.10 Chipkarte im Gesundheitswesen

In den vergangenen Jahren hat sich eine rasante Entwicklung bei den maschinenlesbaren Speicher- und Prozessorkarten vollzogen. Die Entwicklung von den Magnetstreifenkarten wie z. B. EC-Karte hin zur Speicherchipkarte wie zum Beispiel der Telefonkarte (siehe hierzu auch Punkt 15.10) hat auch vor dem Gesundheitswesen nicht haltgemacht.

11.10.1 Krankenversichertenkarte

Die erste Pflichtkarte schreibt § 291 SGB V seit dem 01.01.1995 für alle Mitglieder der Krankenkassen vor. Obwohl die Kassen überwiegend eine Chipkarte verwenden, ist im SGB V hierzu keine Regelung getroffen. Die Krankenversichertenkarte soll den althergebrachten Krankenschein in Papierform ersetzen und dabei zum Nachweis der Berechtigung zur Inanspruchnahme von Leistungen sowie zur Abrechnung dienen. Der Gesetzgeber hat hierbei einen abschließenden Datensatz vorgegeben, der auf dieser Karte enthalten sein darf (Ausstellende Krankenkasse; Name, Geburtsdatum und Anschrift des Versicherten; Krankenversichertennummer; Versichertenstatus; Zeitraum des Versicherungsschutzes). Medizinische Daten dürfen also nicht auf der Krankenversichertenkarte gespeichert werden. Der

Gesetzgeber erhofft sich mit der Einführung der Krankenversicherungskarte Einsparungen durch eine rationellere Ausstellung der Krankenscheine bzw. vereinfachte Abrechnungsmöglichkeit sowie die Erschwerung von Leistungsmißbrauch. Angesichts der klaren gesetzlichen Regelungen und der Tatsache, daß keine medizinischen Daten gespeichert werden, bestehen gegen die Krankenversichertenkarte keine Bedenken aus datenschutzrechtlicher Sicht.

11.10.2 Gesundheitskarte/ Freiwillige Patientenkarte

Im Berichtszeitraum bemühten sich zahlreiche Anbieter (z. B. Ärzte, Apotheker, Krankenkassen etc.), neben der Krankenversichertenkarte als Pflichtkarte eine freiwillige Patientenkarte einzuführen. Die Zwecke und daraus resultierend die gespeicherten Daten auf diesen Karten sind breit gefächert:

Auf Notfallkarten sollen neben einem Stammdatensatz (Name, Adresse etc.) Notfalldaten wie Blutgruppe, Rhesusfaktor, Allergien, Impfungen usw. gespeichert werden, die im Notfall schnell abrufbar sein sollen.
Daneben werden in zahlreichen Pilotprojekten Patientenkarten für besondere Patientengruppen erprobt. Bei chronisch Kranken sowie bei Patienten, die nach Operationen einer intensiven Nachsorge bedürfen, soll die Kommunikation unter den behandelnden Ärzten sowie mit den Betreuungs- und Nachsorgeeinrichtungen verbessert werden. So wird von der Medizinischen Hochschule Hannover und weiteren Nachsorgestellen der Einsatz einer Smart-Card getestet, die zur Überwachung von Patienten mit implantierten Defibrillatoren (Elektroschock-Geräte zum Einsatz bei Herz-Kreislauf-Stillstand) dient. Diese sogenannte Defi-Card nimmt der Patient zu jeder Nachsorgemaßnahme mit, die dann auf der Karte dokumentiert wird. Weitere Beispiele solcher Karten für besondere Patientengruppen sind eine Krebsnachsorgekarte, die durch das Deutsche Krebsforschungszentrum getestet wurde, sowie eine sogenannte Diabcard, die im Rahmen eines Projektes der EG-Kommission unter Beteiligung von Deutschland, Italien, Spanien und Österreich vorgesehen ist und die eine Dokumentation aller Test- und Therapiedaten bezüglich der Behandlung von Diabetes enthält.
Von verschiedenen Krankenkassen ist die Einführung von Gesundheitskarten geplant, die neben den Stammdaten und Notfalldaten auch Parameter wie Blutdruck, Blutzucker und Cholesterinwert enthalten. Eine von den Spitzenverbänden der Apotheker geplante A-Card soll sämtliche Medikamente enthalten, die der Patient in Apotheken erworben hat. Schließlich wird in Neuwied von der kassenärztlichen Vereinigung Koblenz eine persönliche Patientenkarte erprobt, die anamnestische Basisdaten wie bestehende chronische Krankheiten, durchgeführte Operationen, Dauermedikation sowie Allergien aufnehmen soll und für die Aufnahme weiterer medizinischer Daten aus der Arztpraxis oder Apotheke vorbereitet ist.

Allen diesen Kartenprojekten ist gemeinsam, daß die Daten auf freiwilliger Basis erhoben und verarbeitet werden sollen. Wegen der Sensibilität von Gesundheitsdaten, die auf der Chipkarte gespeichert werden sollen, und den mit der Mobilität der Chipkarte verbundenen erhöhten Mißbrauchsgefahren kommt der Freiwilligkeit besondere Bedeutung zu. Die DSB des Bundes und der Länder haben die bisherigen Pilotprojekte und Planungen der freiwilligen Patientenchipkarten kritisch begleitet. Zentraler Punkt der Kritik war die Freiwilligkeit der Verwendung dieser Chipkarten. Eine Einwilligung des Patienten setzt eine umfassende Aufklärung über den Inhalt, Umfang und die Tragweite der Datenverarbeitung voraus. Diese Aufklärung dürfte sich jedoch in der Praxis häufig auf die mit der Karte verbundenen Vorteile beschränken, und die Risiken werden, wenn überhaupt, nur am Rande erwähnt. Werden die Vorteile der Kartenverwendung mit anderen Vorteilsgewährungen bzw. mit einer Benachteiligung von Nicht-Karteninhabern gekoppelt, ist eine Freiwilligkeit der Entscheidung nicht mehr gegeben, sondern durch einen faktischen Zwang ersetzt. Ein Beispiel hierfür ist die Vergabe von Bonuspunkten durch eine Krankenkasse an diejenigen Patienten, die bei Aktionstagen ohne ärztliche Behandlung medizinische Daten wie Blutzucker, Cholesterin, Blutdruck usw. messen und auf der Chipkarte eintragen lassen.
Ebenso wie bei der Erhebung und Speicherung medizinischer Daten auf der Chipkarte besteht hinsichtlich des Offenbarens der gespeicherten Daten ebenfalls die Gefahr, daß die freie Entscheidung des Patienten durch einen faktischen Zwang ersetzt wird. Wenn die Patientenchipkarte in großer Zahl “freiwillig” verwendet wird, dürfte es z. B. dem Bewerber für eine Arbeitsstelle schwerfallen, die Chipkarte nicht vorzuzeigen, wenn er damit rechnen muß, daß sein Konkurrent eingestellt wird, der seine Gesundheitsdaten freiwillig offenbart hat. Zur Freiwilligkeit der Verwendung der Chipkarte mit den darauf gespeicherten Daten durch den Versicherten gehört auch, daß der Versicherte in jedem Einzelfall entscheiden kann, welche Daten aufgenommen und von wem zu welchem Zeitpunkt gelesen werden können. Außerdem muß der Versicherte jederzeit die Karte selbst lesen können. Darüber hinaus muß er die Möglichkeit haben, Änderungen und Löschungen der gespeicherten Daten auf der Karte zu veranlassen.

In der Diskussion um die Patientenchipkarte wird davon gesprochen, daß der Patient durch die Chipkarte nunmehr “Herr seiner Daten” sei. Dies ist im Grundsatz richtig, jedoch sind damit ebenso Risiken verbunden. Seit alters her kam dem Arzt die Aufgabe zu, im Rahmen des Arzt-Patienten-Verhältnisses unter Wahrung der ärztlichen Schweigepflicht die Patientendaten so aufzubewahren, daß keine Unbefugten Zugriff darauf hatten. Diese Pflicht würde nun auf den

Patienten abgewälzt, mit dem zusätzlichen Risiko, daß das mobile Speichermedium für Mißbrauch anfälliger ist als die Akte in den Schränken der verschiedenen behandelnden Ärzte und Krankenhäuser.
Schließlich muß der Versicherte bei der Entscheidung, ob er in die Verwendung der Chipkarte einwilligt, bedenken, ob die Behandlung bei einem Arzt nicht dadurch einen Qualitätsverlust erleidet, daß der Arzt sich bei der Behandlung mehr auf die Liste der auf der Karte eingetragenen Diagnosen als auf seine eigene Untersuchung des Patienten verläßt, wobei die Karte wegen der Freiwilligkeit keinen Anspruch auf Vollständigkeit erheben kann.

Auf diese Gesichtspunkte haben die DSB des Bundes und der Länder in einer Entschließung (siehe Anlage 4) hingewiesen und Anforderungen formuliert, die solche Patientenchipkarten erfüllen müssen. Dieser Beschluß wurde von der 50. Konferenz der DSB des Bundes und der Länder durch eine weitere Entschließung (siehe Anlage 26) bekräftigt und ergänzt. So wurden die jeweiligen Gesetzgeber aufgefordert, die notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu erlassen.

11.11 Gesundheitsberufe

11.11.1 Offenlegung der Einkünfte von Ärzten gegenüber der Ärztekammer

Ein Thüringer Arzt wandte sich an den TLfD mit einer Frage zur Praxis der Beitragsfestsetzung durch die Landesärztekammer. Die Kammerversammlung habe beschlossen, daß für die Ermittlung der Beiträge durch die Ärzte Steuererklärungen der zurückliegenden Jahre vorgelegt werden müßten. Dies hielt er aus datenschutzrechtlicher Sicht für bedenklich und bat um Prüfung.
Eine Nachfrage bei der Landesärztekammer hat ergeben, daß nach § 2 Abs. 3 Satz 4 der Beitragsordnung der Landesärztekammer jeder Arzt im Rahmen der Selbsteinstufung eine Kopie des entsprechenden Auszuges des Einkommenssteuerbescheides des Bezugsjahres der Beitragsbemessung oder eine schriftliche Bestätigung eines Steuerberaters über die Richtigkeit der Selbstveranlagung beilegen muß. Allerdings erfolgt die Selbsteinstufung lediglich aus den Einkünften aus ärztlicher Tätigkeit (§ 2 Abs. 2 Beitragsordnung). Daraus ergibt sich, daß auf der Kopie des Einkommenssteuerbescheides alle Angaben zu anderen Einkunftsarten sowie die Einkünfte des Ehepartners geschwärzt werden können. Es besteht also nicht die Pflicht, eine Kopie des vollständigen Steuerbescheides vorzulegen. Darüber hinaus braucht keine Kopie des Steuerbescheides vorgelegt zu werden, wenn ein Steuerberater die Selbsteinstufung bestätigt. Daß allerdings Angaben über die Einkünfte aus ärztlicher Tätigkeit gemacht werden müssen, ist wegen der Anknüpfung der Beitragsbemessung an diesen Tatbestand erforderlich und hat seine Rechtsgrundlage in der Satzung der Landesärztekammer. Die Landesärztekammer hat zu Recht darauf hingewiesen, daß dieses Verfahren den geringeren Eingriff gegenüber der Möglichkeit des § 31 Abs. 1 der Abgabenordnung darstellt, die es dem Finanzamt ermöglicht, der Landesärztekammer diese Angaben auch ohne Wissen des Arztes mitzuteilen.
Der TLfD hat die Landesärztekammer sowie den Arzt hiervon unterrichtet und die Landesärztekammer gleichzeitig gebeten, in dem noch zu erstellenden Vordruck den Hinweis nach § 19 Abs. 3 ThürDSG aufzunehmen, aufgrund welcher Vorschrift das Kammermitglied zum Nachweis seines Einkommens aus ärztlicher Tätigkeit verpflichtet ist.

11.11.2 Vorlage eines polizeilichen Führungszeugnisses für die Zulassung als Vertragsarzt

Aufgrund von Feststellungen anderer LfD wurde der TLfD darauf aufmerksam, daß mit dem Antrag für die Zulassung zur vertragsärztlichen Tätigkeit gemäß § 18 Abs. 2b der Zulassungsordnung für Vertragsärzte (Ärzte-ZV) auch ein sogenanntes polizeiliches Führungszeugnis beizufügen ist. Dabei verlangen einige Zulassungsausschüsse für Ärzte nicht das einfache Führungszeugnis, welches jeder Bürger bei der Meldestelle beantragen kann, sondern den umfangreicheren Auszug aus dem BZR (Behördenführungszeugnis) gemäß § 31 BZRG.
Eine Anfrage bei der Kassenärztlichen Vereinigung Thüringen ergab, daß in Thüringen ebenfalls ein Behördenführungszeugnis gefordert wird. Dies steht jedoch im Widerspruch zu § 18 Abs. 2b Ärzte-ZV, wonach ausdrücklich die Beifügung eines polizeilichen Führungszeugnisses notwendig ist. Behördenführungszeugnisse können aber nicht beigefügt werden, da sie unmittelbar vom BZR der Behörde oder aber vorher einem Amtsgericht zur Einsichtnahme durch den Betroffenen zugeleitet werden. Die Kassenärztliche Vereinigung in Thüringen verlangt nun diejenige Form des Führungszeugnisses (Belegart O), bei der dem Betroffenen keine vorherige Einsichtnahme gestattet ist. Insoweit kann der TLfD die Rechtsauffassung und die gegenwärtig praktizierte Verfahrensweise durch den Zulassungsausschuß für Ärzte in Thüringen nicht teilen.
Wie einem Entwurf zur Änderung der Zulassungsordnung für Vertragsärzte, der dem TLfD vorliegt, zu entnehmen ist, soll künftig, um einen effektiven Schutz der Patienten vor einer unangebrachten Zulassung von Ärzten zur vertragsärztlichen Versorgung zu gewährleisten, der Nachweis dafür durch ein Behördenführungszeugnis erfolgen. Dabei soll dem Recht auf informationelle Selbstbestimmung des Antragstellers dadurch Rechnung getragen werden, daß dieser die Möglichkeit erhält, vor Weiterleitung des Führungszeugnisses an den Zulassungsausschuß beim Amtsgericht Einsicht

zu nehmen und ggf. einer Weiterleitung zu widersprechen. Es bleibt zu hoffen, daß diese notwendige Klarstellung in Kürze durch Änderung der gegenwärtig geltenden Rechtsvorschriften erfolgt.

12. Statistik

In seinem Urteil zur Volkszählung 1993 hat das Bundesverfassungsgericht in seinen Leitsätzen festgestellt, daß Einschränkungen des Rechtes auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse unter Beachtung der Grundsätze der Normenklarheit sowie der Verhältnismäßigkeit zulässig sind. Dementsprechend bedarf es auch zur Durchführung von Landes- bzw. Kommunalstatistiken entsprechender landesgesetzlicher Regelungen. Diesen Forderungen folgend wurde im Juli 1992 das Thüringer Statistikgesetz (ThürStatG) verabschiedet. Damit hatte der Freistaat als erstes der neuen Bundesländer ein Landesstatistikgesetz und somit bereichsspezifische bzw. spezialgesetzliche Regelungen zum Umgang mit personenbezogenen Daten im Rahmen der Durchführung von Landes- bzw. Kommunalstatistiken. Damit ist ergänzend zu den Bestimmungen des Gesetzes über die Statistik für Bundeszwecke die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für statistische Zwecke im Rahmen der Durchführung amtlicher Statistiken abschließend geregelt.

12.1 Gebäude- und Wohnungszählung 1995

Gemäß § 3 des Gesetzes über Gebäude- und wohnungsstatistische Erhebungen (Wohnungsstatistikgesetz) wurde mit Stand vom 30.09.1995 in den neuen Bundesländern (einschließlich Berlin) eine Totalerhebung von Wohngebäuden und Wohnungen durchgeführt. Sie war damit in den neuen Bundesländern die bisher umfangreichste amtliche Statistik mit Auskunftspflicht.
Zur Bewältigung der Aufgabe bedurfte es der Einrichtung zahlreicher Erhebungsstellen außerhalb des für die Durchführung von Bundesstatistiken zuständigen Thüringer Landesamts für Statistik (TLS). Die Erhebungsstellen wurden entsprechend den Vorgaben durch den Gesetzgeber in den Gemeinden bzw. Verwaltungsgemeinschaften eingerichtet. Entsprechend den Forderungen zur statistischen Geheimhaltung war es notwendig, diese Erhebungsstellen von der übrigen Verwaltung sowohl personell wie auch räumlich abzuschotten, um zu gewährleisten, daß keinerlei Informationen, die im Rahmen der Durchführung dieser Statistik gewonnen wurden, der übrigen Verwaltung zur Kenntnis gelangten.
Erwähnenswert ist in diesem Zusammenhang, daß der TLfD seitens der beteiligten Stellen stets über den aktuellen Sachstand informiert wurde und bei der Erarbeitung der erforderlichen Organisationsmittel gehört wurde. Die Anregungen des TLfD wurden stets umgesetzt. Gleichzeitig konnten Fragen aus der Bevölkerung immer aktuell und sachgerecht beantwortet werden.
Selbstverständlich wurde durch mehrere Kontrollen vor Ort geprüft, ob die diesbezüglichen Richtlinien des TLS in der Praxis auch entsprechend umgesetzt wurden. Dabei konnte in den kontrollierten Erhebungsstellen eine strikte personelle und räumliche Trennung der Erhebungsstelle von der übrigen Verwaltung festgestellt werden. Kritikpunkte gab es ausschließlich hinsichtlich teilweiser nicht ausgeschöpfter Möglichkeiten zur Datensicherheit. Dies betraf insbesondere die sichere Verwahrung der Unterlagen und Sicherheitskopien.
Eine Erhebungsstelle, in der sich noch Bewerbungsunterlagen von nicht zum Einsatz gelangten Erhebungsbeauftragten befanden, wurde vom TLfD aufgefordert, diese den Betroffenen zurückzugeben. Gleichzeitig wurde das TLS gebeten, alle übrigen Erhebungsstellen entsprechend zu informieren.

12.2 Mikrozensus

Seit 1957 werden in der Bundesrepublik Erhebungen über die Bevölkerung und den Arbeitsmarkt in Form einer einprozentigen Stichprobe der Bevölkerung durchgeführt. Dabei wird ein Rotationsverfahren angewendet, bei dem die Erhebungseinheit jeweils nach vier Jahren wechselt. Die Erhebung erfolgt bei der überwiegenden Zahl von Merkmalen auf der Grundlage einer Auskunftspflicht sowie bei einem geringen Teil von Angaben auf freiwilliger Basis. Die Ergebnisse des Mikrozensus über die wirtschaftliche und soziale Lage der Bevölkerung, Familien und Haushalte sowie den Arbeitsmarkt werden als Informationsbasis für die Politik, die Verwaltung, die Wirtschaft und die Wissenschaft benötigt.
Ende 1995 trat das Mikrozensusgesetz 1990 außer Kraft. Nach teilweise kontroverser Diskussion zwischen dem Bundesinnenministerium und den statistischen Ämtern sowie den DSB hinsichtlich des Umfanges der Datenerhebung und des Anteiles von Pflichtauskünften liegt nunmehr ein Gesetzentwurf zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt sowie die Wohnsituation der Haushalte (Mikrozensusgesetz) vor, der die weiteren Erhebungen auf repräsentativer Grundlage als Bundesstatistik bis in das Jahr 2004 regeln soll. Aus datenschutzrechtlicher Sicht ist zu begrüßen, daß man weitgehend den Hinweisen der DSB gefolgt ist und die Auskunftspflicht nicht wesentlich erweitert hat.

Die Gestaltung der Erhebungsvordrucke obliegt den Statistischen Ämtern. Eine Entscheidung über deren künftiges Aussehen wurde aufgrund der bisher fehlenden Rechtsgrundlage noch nicht getroffen. 1995 waren die Fragebögen von den DSB kritisiert worden, da entgegen der bisherigen Praxis 1995 keine körperliche Trennung der Pflichtfragen und freiwilligen Fragen im Erhebungsvordruck vorgenommen worden war und sich nach Auffassung der DSB der Hinweis auf die Freiwilligkeit nicht im ausreichenden Maß im äußeren Erscheinungsbild des Vordruckes heraushob. Begründet wurde dies von den Statistischen Ämtern damit, daß der thematische Zusammenhang von Pflicht- und freiwilligen Angaben durch die absolute Trennung verloren gehen würde.
Ungeachtet dessen besteht die datenschutzrechtliche Forderung nach einer optisch wesentlich deutlicher hervorgehobenen Unterscheidung der beiden Fragengruppen. Dies soll, wie das TLS dem TLfD zwischenzeitlich mitteilte, insbesondere dadurch erfolgen, daß künftig bei freiwilligen Auskünften auch die Alternativantwort "keine Angabe" in den Erhebungsbogen aufgenommen wird.

12.3 Wahlstatistiken

Gemäß § 67 Abs. 1 Thüringer Landeswahlgesetz ist das Ergebnis der Landtagswahl statistisch zu bearbeiten. Weiterhin kann der Landeswahlleiter bestimmen, daß in von ihm zu benennenden Wahlbezirken auch Statistiken über das Wahlverhalten aufzustellen sind. Dazu erfolgt eine Einteilung der Wahlberechtigten nach Altersgruppen und Geschlecht. Es werden somit für jedes Geschlecht fünf Altersklassen gebildet, also insgesamt zehn Gruppen. Selbstverständlich muß das Wahlgeheimnis bei diesem Verfahren stets gewährleistet sein.
In diesem Zusammenhang wurde innerhalb der DSB des Bundes und der Länder diskutiert, wie viele Wähler ein Wahlbezirk mindestens enthalten muß, damit die Gefahr einer Deanonymisierung ausgeschlossen werden kann. Dabei ergibt sich ein Spannungsverhältnis zwischen den Statistischen Ämtern einerseits, die das Wahlverhalten in Dörfern und kleineren Gemeinden miterfassen wollen, und den Forderungen des Datenschutzes andererseits, die Anonymität der Wahl in allen Fällen zu gewährleisten. Je mehr Wahlberechtigte in einem Wahlbezirk vorhanden sind, um so größer ist die Sicherheit, daß das Wahlgeheimnis gewahrt bleibt.
1994 wurde bei der Europawahl eine repräsentative Wahlstatistik bezüglich der Wahlbeteiligung und des Stimmverhaltens nach Geschlecht und Alter durchgeführt. Dem Thüringer Landeswahlleiter wurde die vom TLfD mitgetragene Entschließung der DSB des Bundes und der Länder zum "Datenschutz bei Wahlen" zur Kenntnis gegeben (siehe Anlage 20) in der die Landeswahlleiter aufgefordert werden, nur Wahlbezirke zu bestimmen, die ausreichend Wahlberechtigte aufweisen, um bei der Erstellung einer Wahlstatistik das Wahlgeheimnis mit Sicherheit zu gewährleisten. In seiner Stellungnahme zu der Entschließung brachte der Landeswahlleiter zum Ausdruck, daß alle dort gegebenen Hinweise bei der Erstellung der Wahlstatistik zur Europawahl 1994 grundsätzlich Beachtung fanden. Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse erfolgte hier nicht durch den Wahlvorstand, sondern im TLS.
Der TLfD wird sich rechtzeitig vor der nächsten Landtagswahl über eine in allen Bereichen datenschutzrechtlich korrekte Verfahrensweise bei der Durchführung einer repräsentativen Wahlstatistik mit dem Landeswahlleiter verständigen.

12.4 Erhebung von Daten für die Sozialhilfestatistik

Bei der Prüfung eines Sozialamtes wurde festgestellt, daß Antragsteller bzw. Sozialhilfeempfänger neben ihrem üblichen Antrag auf Gewährung von Hilfe zum Lebensunterhalt nach dem Bundessozialhilfegesetz (BSHG) einen zusätzlichen Fragebogen ausfüllen müssen. Inhalt des Zusatzbogens sind Angaben über die Schul- und Berufsausbildung sowie zur Arbeitslosigkeit. Eine Rückfrage ergab, daß diese Daten bei allen Sozialhilfeempfängern erhoben werden. Bei der Sozialhilfestatistik, die seit 1994 als Bundesstatistik gemäß den §§ 127 ff. BSHG durchgeführt wird, handelt es sich um eine Sekundärstatistik. Das bedeutet, daß die Erhebungsmerkmale nicht bei den Betroffenen erhoben werden, sondern es werden dafür nur Daten, die im Sozialamt zur Antragsbearbeitung auf Sozialhilfe im Rahmen des Verwaltungsvollzuges vorliegen, statistisch aufbereitet. Somit sind die Träger der Sozialhilfe und nicht die Sozialhilfeempfänger auskunftspflichtig. Gleichfalls verbietet sich jede weitere Datenerhebung nur für statistische Zwecke bei den Antragstellern.
Nach § 128 BSHG sind Angaben über die Schul- und Berufsausbildung sowie zur Arbeitslosigkeit für 15- bis unter 65jährige Leistungsempfänger Erhebungsmerkmale zur Durchführung der Bundesstatistik. Die Kenntnis dieser Daten ist aber für die Träger der Sozialhilfe nur dann zur Aufgabenerfüllung erforderlich, wenn gemäß § 40 BSHG Hilfsmaßnahmen bezüglich einer Schul-, Berufsausbildung oder einer möglichen Wiedereingliederung in das Arbeitsleben in Betracht gezogen werden können. Dies trifft selbstverständlich in der Praxis nicht auf alle Personen dieser Altersgruppe zu (z. B. Personen im Erziehungsurlaub oder pflegebedürftige Sozialhilfeantragsteller).
Aus diesen Gründen ist eine undifferenzierte Datenerhebung der o. g. Daten bei allen Sozialhilfeantragstellern bzw. -empfängern unzulässig.

Auf Nachfrage teilte das TLS mit, daß dies auch von einem Teil der Sozialämter bisher entsprechend umgesetzt wurde, indem sie die Erhebungsmerkmale in diesen Fällen als "unbekannt" ausgewiesen haben. Diese datenschutzrechtliche Wertung und Verfahrensweise wird auch vom TMSG geteilt, so daß dies künftig von den Sozialämtern zu beachten ist.

12.5 Erhebung personenbezogener Daten für statistische Zwecke durch öffentliche Stellen

Wiederholt mußte im Berichtszeitraum festgestellt werden, daß öffentliche Stellen für die Erhebung personenbezogener Daten für statistische Zwecke aus Unkenntnis das ThürDSG als Rechtsgrundlage heranziehen. Dies führt insbesondere dazu, daß davon ausgegangen wird, daß nur eine Informationspflicht der Betroffenen hinsichtlich des Zweckes der Erhebung ausreicht, wenn Auskünfte auf freiwilliger Basis eingeholt werden.
Aus diesem Grund mußte vom TLfD des öfteren darauf hingewiesen werden, daß für die Durchführung von Landes- oder Kommunalstatistiken das ThürStatG als spezialgesetzliche Regelung zu beachten ist. Danach bedarf z. B. jede statistische Erhebung im Kommunalbereich einer entsprechenden Satzung. Gleichzeitig sind durch Satzung Statistikstellen einzurichten, die nicht in die Wahrnehmung nichtstatistischer Aufgaben des Verwaltungsvollzugs einbezogen werden dürfen. Zur Gewährleistung des Statistikgeheimnisses bedarf es einer strikten Abschottung in personeller und räumlicher Hinsicht. In den Satzungen sind nähere Bestimmungen zu treffen über die Art der Erhebung, den Kreis der zu Befragenden, die durch Erhebungsmerkmale zu erfassenden Sachverhalte, die Hilfsmerkmale, den Berichtszeitraum, den Berichtszeitpunkt, die Häufigkeit der Erhebung sowie die Art und den Umfang der Auskunftspflicht. Gleichzeitig ist zu gewährleisten, daß die zu Befragenden schriftlich darüber zu informieren sind.
Entsprechendes gilt selbstverständlich auch für die Durchführung von Landesstatistiken, für die in der Regel nach dem ThürStatG das TLS zuständig ist. Wenn in den im Gesetz genannten Fällen die Durchführung einer Statistik keiner Rechtsvorschrift bedarf, hat der statistische Genehmigungsausschuß beim TLfS zu prüfen, ob die vorgesehene Landesstatistik rechtlich zulässig und zweckmäßig ist, insbesondere, ob sie methodisch sachgerecht durchgeführt wird, ob ihre organisatorischen, personellen und finanziellen Folgen für den Freistaat Thüringen vertretbar sind und ob sie im Konflikt mit anderen Statistiken steht.
Leider ist immer wieder festzustellen, daß diese Vorschriften von Landesbehörden oder kommunalen Einrichtungen unbeachtet bleiben und somit unzulässige Datenerhebungen vorgenommen werden. So wurde z. B. durch den Hinweis eines Bürgers festgestellt, daß von der Thüringer Landesanstalt für Umwelt eine Erhebung zum Stand der Technik bei nicht genehmigungsbedürftigen Betriebs- und Produktionsanlagen durchgeführt wurde, die nicht den gesetzlichen Anforderungen einer amtlichen Statistik entsprach. Dies lag daran, daß die zu Befragenden nicht, wie es das ThürStatG ausdrücklich fordert, außer auf den Zweck, die Art und den Umfang der Erhebung auch auf die Rechtsgrundlage für die Erhebung, die Geheimhaltung, die Festlegung, ob es sich um eine Auskunftspflicht oder um eine freiwillige Auskunftserteilung handelt, sowie die Trennung und Löschung der Hilfsmerkmale schriftlich hingewiesen worden waren.
Da die mangelnde Aufklärung der Betroffenen im besonderen Maße den vom Bundesverfassungsgericht zum Volkszählungsurteil vom 15.12.1993 aufgestellten Leitsätzen zur Gewährleistung des Grundrechts auf informationelle Selbstbestimmung widerspricht, wurde auf Veranlassung des TLfD die Erhebung eingestellt und das vorhandene Datenmaterial, soweit dies nicht bereits anonymisiert war, gelöscht.

12.6 Verkehrserhebung

Eine Stadtverwaltung wandte sich an den TLfD mit der Bitte einer datenschutzrechtlichen Überprüfung einer durchzuführenden Verkehrserhebung. Zweck der Erhebung war die Ermittlung der Verkehrsverteilung, des Mobilitätsverhaltens und der Informationsgewinnung für die ÖPNV-Nutzung.

Der Stadtverwaltung wurde mitgeteilt, daß für die Durchführung statistischer Erhebungen durch Kommunalverwaltungen als spezialgesetzliche Rechtsvorschrift zum Datenschutz das ThürStatG gilt. Gemäß § 23 Abs. 1 ThürStatG bedarf es zur Durchführung von Statistiken durch Gemeinden oder in deren Auftrag regelmäßig einer Satzung, soweit nicht die Ausnahmefälle nach den Nummern 1 und 2 zutreffen. Das Verfahren zur Durchführung von Erhebungen ist in § 25 ThürStatG abschließend geregelt. Im weiteren wurde darauf hingewiesen, daß bei der Vergabe statistischer Arbeiten gemäß § 7 ThürStatG die Regelungen des ThürDSG bezüglich der Datenverarbeitung im Auftrag zu beachten sind. Nach § 8 Abs. 3 ThürDSG darf der Auftragnehmer die Daten nur im Rahmen der Weisung des Auftraggebers erheben, verarbeiten oder nutzen. Insoweit muß der Auftraggeber, also die Stadtverwaltung, auf der Grundlage des ThürStatG dem Auftragnehmer die entsprechenden Vorgaben, zum Beispiel Termin der Übergabe der Daten oder Vernichtung des Materials, erteilen. Ferner wurde der Stadtverwaltung der Entwurf einer Satzung zur Verkehrszählung zugesandt.

In dem Satzungsentwurf der Stadtverwaltung wurde vorgeschlagen, die Merkmale "Adresse des Haushaltes" und "Vorname" zu streichen, da aus datenschutzrechtlicher Sicht die Hilfsmerkmale auf das notwendige Maß zu beschrän-

ken sind. Gemäß § 15 Abs. 2 ThürDSG sind sie daher von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen und gesondert aufzubewahren. Aus diesem Grund sind die genannten Angaben auf einem gesonderten Blatt zu erfassen, das über eine Identifikationsnummer mit dem Erhebungsbogen notfalls für Rückfragen zusammengeführt werden kann. Zur Löschung der Hilfsmerkmale gilt gemäß § 15 Abs. 3 Satz 1 ThürStatG, daß die Hilfsmerkmale zu löschen sind, sobald die Überprüfung der Erhebungs- und Hilfsmerkmale auf Schlüssigkeit und Vollständigkeit abgeschlossen ist.

13. Bildung, Wissenschaft und Forschung

13.1 Bildung

13.1.1 Verordnung über statistische Erhebung im Kultusbereich

Für Analysen, Prognosen, Bedarfsberechnung, d. h. insbesondere für Planungszwecke, benötigt das TKM zur Durchsetzung der Aufgaben der Bildungspolitik eine Reihe von Daten über Schüler und Lehrer. Diese Daten werden in zusammengefaßter, aggregierter Form vom statistischen Bundesamt sowie der Kultusministerkonferenz angefordert und ausgewertet.
Durch die im Grundgesetz geregelten Zuständigkeiten gibt es für den Kultusbereich keine einheitliche Bundesstatistik auf der Grundlage eines Bundesgesetzes. Aus diesem Grund muß jedes einzelne Bundesland eigenständig durch Landesgesetzgebung, entsprechend der Beschlüsse der Kultusministerkonferenz, statistische Erhebungen festlegen, deren Ergebnisse auf Bundesebene zusammengefaßt werden können bzw. vergleichbar sind. Auf der Grundlage des Thüringer Schulgesetzes (ThürSchulG) ist das TKM ermächtigt, durch Verordnung Erhebungen mit Auskunftspflicht für Schule, Lehrer und Schüler zu bestimmen. Die bisherige Praxis, die Schulen durch entsprechende Verwaltungsvorschriften dazu zu verpflichten, entsprechende Daten in Form von Sekundärstatistiken zur Verfügung zu stellen, bildete keine ausreichende Rechtsgrundlage für die Erhebungen.
Auf Drängen des TLfD wurde deshalb vom TKM für die jährlich erforderliche Statistik die Verordnung über die statistische Erhebung von personenbezogenen Daten im Kultusbereich erarbeitet. Um den datenschutzrechtlichen Belangen bei der Erhebung Rechnung zu tragen, gab es bereits in der Phase der Erarbeitung des Entwurfes intensive Kontakte zwischen dem TLfD und der Statistikstelle des TKM. Den Hinweisen des TLfD stand man jederzeit aufgeschlossen gegenüber, so daß die zwischenzeitlich verabschiedete Verordnung den datenschutzrechtlichen Anforderungen einer statistischen Erhebung von personenbezogenen Daten gerecht wird.

13.1.2 Übermittlung von Daten zur Erstellung eines wissenschaftlichen Gutachtens

Das TKM führt in Thüringen gemäß § 58 Abs. 1 ThürSchulG die Erhebung und Verarbeitung von schulbezogenen Daten zu statistischen Zwecken durch. Die Thüringer Verordnung über die statistische Erhebung von personenbezogenen Daten im Kultusbereich vom 5. August 1994 bestimmt dabei eine jährliche Durchführung dieser Statistik. In diesem Rahmen diente für das Jahr 1995 die Statistik zur Ermittlung des künftigen Lehrkräftebedarfs. Hierfür wird ein umfangreicher Fragebogen genutzt, der in einen Schul-, Klassen- und Lehrerbogen unterteilt ist. Für die Erstellung eines Bedarfsgutachtens war die Pädagogische Hochschule Erfurt vorgesehen. Das TKM wandte sich mit der Frage an den TLfD, ob die erhobenen Daten als Einzeldatensätze oder nur in aggregierter Form an die Pädagogische Hochschule Erfurt übermittelt werden dürfen. Insbesondere bestand Unsicherheit über die Interpretation der in § 18 Abs. 5 ThürStatG getroffenen Regelungen, wonach Einzelangaben für die Durchführung wissenschaftlicher Vorhaben nur dann übermittelt werden dürfen, "wenn die Einzelangaben nur mit unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können".
Der TLfD erläuterte in seiner Stellungnahme an das TKM, daß der unbestimmte Rechtsbegriff "unverhältnismäßig hoher Aufwand an Zeit, Kosten und Arbeitskraft" dann Anwendung findet, wenn die Daten aus einem abgeschotteten statistischen Bereich übermittelt werden, wobei sich dies an dem Verhältnis von Aufwand und Wert der zu erlangenden Information bemißt. Die Entscheidung über die Zulässigkeit der Übermittlung trifft die übermittelnde Stelle. Diese vom Gesetzgeber verordnete faktische Anonymisierung der Daten ist darauf gerichtet, das Recht auf informationelle Selbstbestimmung unter Beachtung des Grundrechts auf Freiheit von Wissenschaft und Forschung zu gewährleisten. Dementsprechend stellt nicht die Menge der Daten bzw. der Betroffenen, sondern die Gefährdung des einzelnen das bestimmende Entscheidungskriterium dar. Insoweit hat der TLfD keine grundsätzlichen Bedenken gegen eine Übermittlung der Einzeldatensätze, soweit bei diesen kein unmittelbarer Personenbezug hergestellt werden konnte. Im vorliegenden Fall bestanden jedoch insbesondere gegen die Übermittlung der Einzeldatensätze aus den Lehrerbögen von seiten des TLfD erhebliche Bedenken. Auch unter Löschung des Namens, des Vornamens und der Personalnummer wäre durch die Kenntnis der Schulnummer, der Fachkombination sowie des Geburtsdatums eine Deanonymisierung der einzelnen Datensätze problemlos möglich gewesen, wenn die Schule bekannt ist. Das TKM wurde vom TLfD

aufgefordert, die für die Erstellung des Gutachtens notwendigen Rechenprozesse bezüglich der Lehrerdaten in der Statistikstelle des TKM auf der Grundlage der Anforderungen durch die Pädagogische Hochschule durchzuführen.

13.1.3 Datenerhebung im Rahmen der Schulgesundheitspflege

In § 55 ThürSchulG werden die Schüler verpflichtet, sich den Maßnahmen des schulärztlichen und schulzahnärztlichen Dienstes zu unterziehen. Gleichzeitig wird geregelt, daß im Rahmen der Schulgesundheitspflege die für die Durchführung der schulärztlichen Untersuchung erforderlichen personenbezogenen Daten erhoben, verarbeitet und genutzt werden dürfen. Soweit ist für alle Betroffenen klar, daß entsprechende schulärztliche Untersuchungen rechtlich begründet sind. Problematisch wird es jedoch, wenn man als Schüler oder Erziehungsberechtigte wissen möchte, an welchen konkreten Maßnahmen und Untersuchungen der Schüler teilnehmen muß. Hierzu heißt es in § 55 ThürSchulG, daß das Nähere durch Rechtsverordnung des Ministers für Soziales und Gesundheit im Einvernehmen mit dem Kultusminister geregelt wird.
Verabschiedet wurde das ThürSchulG im August 1993. Auch Ende 1995 ist das "Nähere" noch nicht ausreichend geregelt. Das bedeutet, daß erhebliche Unsicherheiten zum Zeitpunkt und Inhalt sowie hinsichtlich der Erhebung, Verarbeitung und Nutzung von Daten bei Schuluntersuchungen bestehen. Das betrifft insbesondere auch die Übermittlung von Untersuchungsergebnissen an die Schule, da nach § 57 ThürSchulG der schulärztliche Dienst der Schule nur das Ergebnis der Pflichtuntersuchungen übermitteln darf. Daraus ergibt sich jedoch sofort die Frage: Wann findet eine Pflichtuntersuchung statt? Aufgrund der fehlenden Verordnung ist dieses gegenwärtig nur für die Schuleinführungsuntersuchung gemäß § 5 ThürSchulG eindeutig bestimmt. Da unbestritten Vorsorgeuntersuchungen der gesundheitlichen Versorgung der Kinder und Jugendlichen im Schulalter und der Früherkennung von Gesundheitsgefährdungen, Gesundheitsschädigungen oder Erkrankungen der Kinder dienen, hat der TLfD zur Beseitigung der bestehenden Rechtsunsicherheit bei allen Beteiligten das TMSG dringend auf den Erlaß der längst überfälligen Verordnung hingewiesen. Vom TMSG erfolgte daraufhin die Zusage, noch im Jahre 1995 eine Rechtsverordnung zur Schulgesundheitspflege zu erlassen. Der Entwurf sollte vorher dem TLfD zu Stellungnahme zugeleitet werden. Beides steht noch immer aus.

Daß die fehlenden Regelungen zu Unsicherheiten hinsichtlich der Zulässigkeit von Untersuchungen in Schulen sowie Fehlentscheidungen führen können, zeigte auch nachfolgender Fall.
Der Vater einer Schülerin beschwerte sich darüber, daß in einer Schule Ultraschalluntersuchungen der Schilddrüse an Schülern und Schülerinnen vorgenommen worden waren. Vorher waren die Eltern der betroffenen Kinder von der geplanten Maßnahme schriftlich unterrichtet und um ihr Einverständnis für diese Maßnahme gebeten worden. Das Informationsblatt wies jedoch aus datenschutzrechtlicher Sicht einige Mängel auf. Insbesondere enthielt es keinen direkten und unmißverständlichen Hinweis auf die Freiwilligkeit der Teilnahme an der Untersuchung, da die im Schreiben formulierte Bitte um das Einverständnis den diesbezüglichen gesetzlichen Anforderungen noch nicht gerecht wird. Im weiteren fehlten im Anschreiben auch konkrete Aussagen zur Datenspeicherung und -nutzung. Dies war insoweit besonderes problematisch, weil aufgrund der Tatsache, daß die Maßnahme in Zusammenarbeit mit der Schule durchgeführt wurde, bei den Betroffenen der Eindruck entstehen konnte, es würde sich um eine Maßnahme der Schulgesundheitspflege handeln.
Nur durch den Hinweis im Informationsblatt, daß zur Aufklärung der Bevölkerung und zur Empfehlung wirksamer Maßnahmen zur Verhinderung von Schilddrüsenerkrankungen eine genaue Kenntnis über Strumavorkommen und die Jodversorgung erforderlich ist und sich deshalb der AK Jodmangel der Bundesrepublik Deutschland um die Erhebung von Untersuchungsbefunden zur Schilddrüsengröße bemüht, ließen darauf schließen, daß neben der unmittelbaren Vorsorgeuntersuchung insbesondere auch ein wissenschaftliches Interesse verfolgt wurde. So begrüßenswert die Durchführung von Vorsorgeuntersuchungen (auch wenn sie mit Forschungsprojekten verbunden werden) sind, so muß es doch, wenn es sich um keine Pflichtuntersuchung handelt, dem Betroffenen überlassen bleiben, ob er sich an diesen Maßnahmen beteiligt oder nicht. Gleichzeitig muß bekannt sein, wie mit den erhobenen Daten umgegangen wird. Zur Entscheidungsfindung bedarf es deshalb für den Betroffenen stets einer entsprechenden Aufklärung, die im vorliegenden Fall nicht ausreichte.
Die Rückfrage beim TKM bestätigte die Vermutung, daß es sich um ein wissenschaftliches Forschungsprogramm handelte. Der Verantwortliche dafür hatte als Mitglied o. g. Arbeitskreises das TKM über die geplante Untersuchung in Kenntnis gesetzt und um dessen Zustimmung gebeten. Gemäß § 57 ThürSchulG kann aber eine Genehmigung für ein wissenschaftliches Forschungsvorhaben in Schulen nur erteilt werden, wenn dieses ein erhebliches wissenschaftliches Interesse im Hinblick auf den Bildungsauftrag der Schule erkennen läßt. Dementsprechend hatte das TKM aufgrund der Nichtgenehmigungsfähigkeit den Antrag abgelehnt. Gleichzeitig hatte es darauf hingewiesen, daß die geplante Untersuchung als nichtschulische Maßnahme die ausdrückliche Freiwilligkeit der beteiligten Eltern und Schüler voraussetzt. Dennoch war die Maßnahme von der Schule unterstützt worden. Dies stellte zwar kein Verstoß gegen datenschutzrechtliche Bestimmungen dar, aber es war dadurch aufgrund der mangelhaften Information die

Vermutung bei den Betroffenen gestützt worden, daß es sich um eine "schulische Pflichtuntersuchung" handeln würde. Um ähnliche Wiederholungen künftig zu verhindern, hat deshalb das TKM nochmals alle Schulämter schriftlich auf Bestimmungen des ThürSchulG hinsichtlich der Zulässigkeit von wissenschaftlichen Untersuchungen und Befragungen in Schulen hingewiesen.
Ungeachtet dessen wäre natürlich eine genaue Kenntnis des Umfanges von Pflicht- bzw. freiwilligen Untersuchungen, die im Rahmen der Schulgesundheitspflege durchgeführt werden, hilfreich, um mögliche Mißverständnisse bei allen Beteiligten zu vermeiden. Dazu bedarf es allerdings des baldigen Erlasses der noch immer ausstehenden Rechtsverordnung.

13.1.4 Schulpsychologischer Dienst

Das TKM übersandte dem TLfD einen Entwurf einer Verwaltungsvorschrift zur Arbeit des Schulpsychologischen Dienstes zur Stellungnahme. Hierzu wurde dem TKM mitgeteilt, daß die bis dahin vorgesehene Weitergabe der Daten des Schulpsychologischen Dienstes an Schulen oder Lehrer bzw. eine Datenübermittlung an sonstige Stellen grundsätzlich der Einwilligung des Betroffenen bedarf. Dem Schulpsychologischen Dienst ist gemäß § 53 ThürSchulG eine Beratungsaufgabe übertragen worden. Es ist deshalb davon auszugehen, daß alle im Rahmen der Beratungstätigkeit erhobenen Daten der Schüler und Eltern freiwillige Angaben der Betroffenen im Sinne des § 4 Abs. 1 ThürDSG darstellen. Die daraufhin am 13. April 1995 vom TKM erlassene Verwaltungsvorschrift berücksichtigt sämtliche datenschutzrechtliche Verbesserungsvorschläge des TLfD.

13.1.5 Notenbekanntgabe

Ein Bürger wandte sich mit der Beschwerde an den TLfD, daß mit dem Hinweis auf Datenschutzbelange in der Schule keine Notenspiegel und Durchschnittsnoten mehr von Klassenarbeiten angefertigt werden würden. Der TLfD hält aus datenschutzrechtlichen Gründen die Bekanntgabe von Notenspiegeln für unbedenklich. Der Zensurenspiegel muß dabei anonymen Charakter haben, so daß keine Rückschlüsse auf bestimmte Schüler möglich sind. In diesem Zusammenhang ist auch auf das ThürSchulG zu verweisen. Gemäß § 48 Abs. 3 Satz 4 ThürSchulG ist die Transparenz der Notengebung für Schüler und Eltern zu gewährleisten. Auf Anfrage bestätigte das TKM, daß die Bekanntgabe der Durchschnittsnote bzw. des Notenspiegels ein geeignetes Mittel ist, den umfassenden Informationsanspruch der Eltern hinsichtlich der Leistung des eigenen Kindes geltend zu machen. Eine mögliche gegenteilige Festlegung der Schulkonferenz bezieht sich nur auf die generelle Linie der jeweiligen Schule. Im Einzelfall können Eltern selbstverständlich die Anfertigung des Zensurenspiegels verlangen.

13.1.6 Schuljubiläen

Eine Schule wandte sich an den TLfD mit der Frage, ob zum 100jährigen Bestehen des Gymnasiums in die zu diesem Anlaß zu erstellende Jubiläumszeitung auch eine Liste mit allen Schülern, die ihr Abitur an der entsprechenden Schule bestanden haben, veröffentlicht werden darf. Um dies zu ermöglichen, ohne daß dafür von jedem Betroffenen eine schriftliche Zustimmung eingeholt werden muß, hat der Gesetzgeber eigens dafür eine Regelung in das ThürSchulG aufgenommen. Unter Beachtung des Rechts auf informationelle Selbstbestimmung der Betroffenen wurde unter Abwägung aller Interessen bestimmt, daß eine Veröffentlichung personenbezogener Daten der Schüler und Eltern in Form von Jubiläums- und Jahresberichten oder Klassenübersichten zulässig ist, soweit der Veröffentlichung nicht widersprochen wurde. Selbstverständlich ist Gleiches auch hinsichtlich der Veröffentlichung von Angaben über Lehrer und Erzieher zu beachten. Ebenso ist dabei zu berücksichtigen, daß personenbezogene Daten auch in Form von Bildmaterial vorliegen können. Gemäß § 57 Abs. 6 ThürSchulG sind die Betroffenen in geeigneter Weise auf ihr Widerspruchsrecht hinzuweisen.

13.1.7 Umfrage zur Teilzeitarbeit bei Lehrern

Aufgrund des bevorstehenden Rückgangs der Schülerzahlen entwickelte das TKM einen Erhebungsbogen, mit dem die grundsätzliche Bereitschaft aller Lehrerinnen und Lehrer in Thüringen zur Aufnahme einer Teilzeitbeschäftigung untersucht werden sollte. Den TLfD erreichten mehrere Anfragen von betroffenen Lehrern sowie der Presse, ob der datenschutzrechtliche Umgang mit diesen Erhebungsbögen gewährleistet sei. In einem Schreiben wurde das TKM gebeten, bis zur Klärung der offenen Fragen die Erhebung auszusetzen bzw. nach einer Klärung den Lehrern weitere Informationen zu den anstehenden Fragen zu übergeben.

Das TKM bestritt völlig überraschend, daß mit dem Erhebungsbogen überhaupt personenbezogene Daten erfaßt werden. Es steht jedoch völlig außer Frage, daß es sich bei der Umfrage zunächst durch die Gestaltung der Fragebögen,

bei der der Name, der Vorname und die Schule jedes Lehrers erfaßt wurde, um eine Erhebung personenbezogener Daten im Sinne des § 2 Abs. 1 ThürDSG und nicht um eine Landesstatistik handelte. Aufgrund der den Betroffenen bislang vorgelegten Informationen, war von einer unzulässig durchgeführten Datenerhebung auszugehen. Dies wurde dem TKM mitgeteilt, das in seiner Antwort die Bedenken nicht ausräumen konnte. Daraufhin fand ein Gespräch mit Mitarbeitern des TKM zu der in Rede stehenden Meinungsumfrage statt. Da alle Fragebögen bereits im Umlauf waren, wurde der Vorschlag gemacht, die Anonymisierung durch Unkenntlichmachung der Namen der Lehrer und Lehrerinnen unverzüglich durchzuführen. Das TKM erließ dann eine Änderung der Auszählungsanweisung, wonach alle ausgefüllten Mitteilungen vor einer Auswertung zu anonymisieren waren, indem der obere Teil des Erhebungsbogens mit dem Namen und Vornamen abgeschnitten und sofort vernichtet wurde. Um zu überprüfen, ob die geänderte Auszählungsanweisung auch umgesetzt wurde, führte der TLfD zeitgleich bei mehreren Schulämtern unangemeldete Kontrollen durch. Hierbei wurde festgestellt, daß die Anweisung ausnahmslos befolgt worden war.

Die datenschutzrechtliche Zulässigkeit von Personalbefragungen im Zusammenhang mit Organisationsuntersuchungen war auch Gegenstand der Erörterungen im Kreis der DSB. Vom Grundsatz her bestehen keine Bedenken, wenn diese Daten zum frühestmöglichen Zeitpunkt anonymisiert und nicht für andere Zwecke verwendet werden. Soweit der Personenbezug herstellbar bleibt, muß eine frühestmögliche Löschung erfolgen. Je nach Art und Gegenstand der Mitarbeiterbefragung können sich hierbei im Einzelfall abweichende Anforderungen ergeben.

13.2 Wissenschaft

13.2.1 Datenübermittlung zwischen BAföG-Ämtern und Ausbildungsstätten

In Thüringen herrschte bislang kein einheitliches Verfahren bezüglich einer Zusammenarbeit zwischen Schulen und BAföG-Ämtern bei der Behandlung von Schulabbrechern, die eine Schulbescheinigung zur Beantragung von BAföG erhalten hatten. Ein Teil der Schulen meldete diese Schulabbrecher generell dem zuständigen Amt für Ausbildungsförderung, während andere Schulen von den BAföG-Ämtern eine Liste mit sämtlichen BAföG-Empfängern der Schule anforderten. Schulabbrecher, die auf dieser Liste aufgeführt waren, wurden dann dem Amt für Ausbildungsförderung mitgeteilt. Beide genutzten Verfahrensweisen sind aus datenschutzrechtlicher Sicht nicht unproblematisch. Im ersten Fall werden die Daten von allen Schulabbrechern an das BAföG-Amt übermittelt, obwohl ein Großteil der Schüler, die eine Besuchsbescheinigung verlangt haben, entweder kein BAföG erhalten oder die Bescheinigung für andere Sachverhalte benötigen. Aus datenschutzrechtlicher Sicht ist die Übermittlung von nicht benötigten personenbezogenen Daten gemäß § 21 Abs. 1 ThürDSG nicht zulässig. Im zweiten Fall ist eine routinemäßige Übermittlung von Listen mit allen Schülern, die BAföG empfangen, aus Gründen des Sozialdatenschutzes gemäß § 69 Abs. 1 Satz 1 SGB X ebenfalls bedenklich.
Aus diesem Grund wurde dem TKM vorgeschlagen, mit Aushändigung der Schulbesuchsbescheinigung den einzelnen Schüler über die Datenübermittlung bei einem unentschuldigten Fernbleiben vom Unterricht Kenntnis zu geben und auf eine Widerspruchsmöglichlichkeit aufmerksam zu machen. Diejenigen Schüler, die einer möglichen Datenübermittlung widersprechen, müssen dann in regelmäßigen Abständen eine Schulbesuchsbescheinigung einholen.
Weiterhin war auf Grundlage des bis dahin gültigen § 47 Abs. 2 BAföG eine Verpflichtung zur Unterrichtung der BAföG-Ämter durch die Schulen von Amts wegen nicht zu entnehmen. Eine solche Verpflichtung richtete sich vielmehr ausschließlich an den BAföG-Empfänger. Wegen dieser Problematik hat der Bundesgesetzgeber im Zuge eines Siebzehnten Gesetzes zur Änderung des Bundesausbildungsförderungsgesetzes einen dritten Absatz in § 47 BAföG eingefügt. Hierin heißt es:
“(3) Ist dem Auszubildenden von einer der in § 2 Abs. 1 Nr. 1 bis 4 bezeichneten oder diesen nach § 2 Abs. 3 als gleichwertig bestimmten Ausbildungsstätten für Zwecke dieses Gesetzes bescheinigt worden, daß er sie besucht, so unterrichtet die Ausbildungsstätte das Amt für Ausbildungsförderung unverzüglich, wenn der Auszubildende die Ausbildung abbricht.”

Die in Kraft getretene gesetzliche Änderung stößt aber auf erhebliche datenschutzrechtliche Bedenken. Der Bundesgesetzgeber nimmt damit nämlich in Kauf, daß auch Daten von Auszubildenden, die kein BAföG erhalten und die Ausbildung abbrechen, an die Ämter für Ausbildungsförderung übermittelt werden.

13.2.2 Einsichtsrecht von Hochschulmitarbeitern in Evaluierungsunterlagen

Zwischen den LfD der neuen Bundesländer wurde über Fragebögen diskutiert, die für das Verfahren zur Prüfung der persönlichen Eignung von Bewerbern für wissenschaftliche und künstlerische Stellen an Hochschulen zur Anwendung kommen. Manche Fragebögen gehen dabei im Umfang über die der sonst allgemein üblichen Form für den öffentlichen Dienst hinaus. Eine Anfrage des TLfD beim TMWK ergab, daß von den Hochschulen ausschließlich der Fragebogen

aufgrund des Runderlasses der Thüringer Landesregierung über die Prüfung der persönlichen Eignung für den öffentlichen Dienst (vgl. auch ThürStAnz 1992 S. 1122 ff.) Anwendung findet. Dieser Fragebogen löste das bis dahin gültige Verfahren zur Feststellung der persönlichen Eignung von Hochschullehrern und wissenschaftlichen bzw. künstlerischen Mitarbeitern durch Evaluierung ab.

Gemäß § 1 Abs. 1 Satz 3 Evaluationsordnung (EvalO) für Thüringer Hochschulen erfolgte bis zum 02.10.1992 eine Überprüfung der persönlichen Eignung von Hochschullehrern und wissenschaftlichen bzw. künstlerischen Mitarbeitern. Zur Feststellung der persönlichen Eignung wurden Einzelfallprüfungen von Personalkommissionen durchgeführt. Die Personalkommissionen bestanden aus acht Mitgliedern, und zwar vier Vertretern des öffentlichen Lebens und vier Vertretern der Hochschule. Die von Amts wegen tätig gewordenen Personalkommissionen gaben in den von ihr geprüften Fällen gegenüber dem Minister für Wissenschaft und Kunst eine zu begründende Empfehlung ab, ob die persönliche Eignung zum Verbleib an der Hochschule vorlag oder nicht.

In einer Eingabe wurde an den TLfD die Frage herangetragen, inwieweit die Auffassung des TMWK richtig sei, daß für Hochschulmitarbeiter kein Einsichtsrecht in ihre Evaluierungsunterlagen bestehe, um berechtigte Interessen Dritter nicht zu verletzten. Der TLfD wandte sich mit dieser Frage an das TMWK. Dieses war der Auffassung, daß zum Schutz der Mitglieder der Personalkommissionen bzw. eventueller Zeitzeugen vor persönlichen Angriffen durch betroffene Hochschulmitarbeiter die Akteneinsicht in Evaluierungsunterlagen stark eingeschränkt wäre. Die Akteneinsicht setzt prinzipiell einen Antrag des Betroffenen voraus. Eine Einsicht wurde aber nur gewährt, sofern die Entscheidung des Ministers über die persönliche Eignung bereits vorlag und aus diesem Grund eine Kündigung ausgesprochen wurde sowie ein Arbeitsrechtsstreit anhängig war. Weiterhin waren vor einem Akteneinsichtsrecht die Evaluierungsunterlagen zu kopieren und alle darin befindlichen Namen der Mitglieder der Personalkommission sowie eventueller Zeitzeugen in den Kopien unkenntlich zu machen. In Fällen, in denen sich aus dem Text Hinweise auf die Identität der vorgenannten Person ergeben könnte, waren auch zusätzlich Textpassagen unkenntlich zu machen. Die Zuordnung einer Aussage zu einer bestimmten Person war in jedem Fall unmöglich zu machen. Erst danach war eine Akteneinsicht in die fotokopierte Unterlage zu gestatten. Außerdem teilte das TMWK mit, nach Abschluß aller arbeitsrechtlicher Verfahren die Akten “endgültig” schließen zu wollen.

Abweichend vom Erlaß des TMWK vom 23.02.1993 ist der TLfD der Meinung, daß der Auskunftsanspruch des Betroffenen nicht von Bedingungen abhängig gemacht werden kann, wie etwa von der Entscheidung des Ministers über die persönliche Eignung oder von der Frage, ob ein Arbeitsrechtsstreit gegenwärtig geführt wird. Die Auffassung des TMWK, wonach die Auskunftserteilung unterbleibt, weil die Kommissionsmitglieder Dritte seien, die wegen den überwiegenden berechtigten Interessen geheimgehalten werden müßten, wird vom TLfD nicht geteilt. Die Mitglieder der Personalkommission können nicht als Dritte i. S. v. § 13 Abs. 5 Nr. 3 ThürDSG angesehen werden, da sie an der Überprüfung ausschließlich und an der Entscheidung maßgeblich beteiligt waren. Die Mitglieder der Evaluierungskommission sind von ihrer Interessenlage mit Behördenbediensteten im Sinne der Ziffer 13.4 Satz 2 VVThürDSG vergleichbar. Gemäß dieser Verwaltungsvorschrift ist das Interesse von Behördenbediensteten gegen das Bekanntwerden ihrer dienstlichen Tätigkeit (z. B. in der Form von Stellungnahmen oder Gutachten) nicht als berechtigtes Interesse im Sinne von § 13 Abs. 5 Nr. 3 ThürDSG anzusehen und steht einer Auskunft nicht entgegen. Nach § 2 Abs. 4 EvalO wurden die Mitglieder der Kommission auf ihr Amt vom Thüringer Minister für Wissenschaft und Kunst verpflichtet und sind somit als Amtsträger anzusehen. Das TMWFK kann sich bei der Auskunftserteilung nicht auf andere Interessen derjenigen Personen berufen, durch die es handelt. Ob die Tätigkeit dienstlich oder ehrenamtlich ausgeübt wurde, ist insoweit ebenfalls unerheblich. Die Entscheidung der Kommission muß für den Betroffenen zugänglich sein, um nicht den Eindruck zu erwecken, nicht nachvollziehbare Entscheidungen getroffen zu haben. Die Empfehlung des TLfD, den o. g. Erlaß zu ändern, blieb bislang ohne Reaktion.

13.3 Forschung

13.3.1 Die Forschung hat auch den Datenschutz einzuhalten

Im Berichtszeitraum gingen zahlreiche Anfragen von öffentlichen und nicht-öffentlichen Forschungseinrichtungen ein, die Auskunft über die datenschutzrechtliche Zulässigkeit beabsichtigter Studien begehrten. Nicht selten dürfte die Motivation für derartige Anfragen darin liegen, bei der Frage an die Probanden um Mitwirkung auf eine “Unbedenklichkeitsbescheinigung” des TLfD verweisen zu können, um so auf eine größere Akzeptanz zur Beteiligung an den jeweiligen Forschungsvorhaben zu stoßen.

Positiv hervorzuheben ist in diesem Zusammenhang allerdings, daß sich Forschungseinrichtungen bereits im Vorfeld um die datenschutzgerechte Konzeption ihrer Studien bemühen. Zu den vorgelegten Forschungsvorhaben konnten

vielfach Verbesserungsvorschläge gemacht werden, die auch bereitwillig aufgenommen wurden. Ob die jeweils geplanten Studien tatsächlich durchgeführt worden sind, ist dem TLfD nicht in allen Fällen bekanntgeworden. Anhand dieser Fälle erscheint es jedoch angebracht, einige grundlegende Ausführungen zu den rechtlichen Voraussetzungen und den Hauptproblemen bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten in Forschungseinrichtungen zu machen, um so eine mögliche Hilfestellung für diejenigen zu geben, die entsprechende Vorhaben vorbereiten.

Die Forschungsfreiheit wird in Artikel 5 Abs. 3 GG sowie in Artikel 27 Abs. 1 Satz 2 VerfThür garantiert. Diese Verfassungsnormen werden von den Wissenschaftlern häufig verabsolutiert und der Datenschutz, der seine verfassungsrechtliche Grundlage im Grundrecht auf informationelle Selbstbestimmung (Artikel 1 Abs. 1 in Verbindung mit Artikel 2 Abs. 1 GG; und Artikel 6 VerfThür) hat, als Hindernis für die Ausübung der Forschungsfreiheit angesehen. Obwohl das Grundrecht der Forschungsfreiheit ohne Gesetzesvorbehalt gewährleistet ist, gilt dieses nicht schrankenlos. Treten Konstellationen auf, bei denen die Wirkungen von Grundrechten sich gegeneinander richten, so müssen nach dem Grundsatz der "praktischen Konkordanz" Regelungen getroffen werden, die den schonendsten Ausgleich zwischen den widerstreitenden Grundrechten in jedem Einzelfall gewährleisten. Solche Regelungen haben der Bundes- und Landesgesetzgeber in den allgemeinen Datenschutzgesetzen in Form von Forschungsklauseln (§ 40 BDSG bzw. § 25 ThürDSG) geschaffen. Darüber hinaus sind in einigen Spezialgesetzen eigene Forschungsregelungen enthalten (z. B. § 75 SGB X für Sozialdaten, § 27 ThürKHG für Patientendaten in Krankenhäusern, § 16 ThürArchivG für Archivdaten). Diese Forschungsklauseln sehen im wesentlichen eine strenge Zweckbindung der erhobenen Daten, die Pflicht zur frühestmöglichen Anonymisierung sowie eine Trennung von Identitätsdaten von sonstigen erhobenen Merkmalen vor. Um den Eingriff in das Grundrecht auf informationelle Selbstbestimmung des Betroffenen so gering wie möglich zu halten, hat der Wissenschaftler in allen Phasen eines Forschungsprojektes die Frage der Erforderlichkeit des Grundrechtseingriffs für seine Forschungszwecke zu prüfen. Kann er mit milderen Mitteln (z. B. ohne Verwendung personenbezogener Daten oder sofortiger Vernichtung von Identitätsdaten) den angestrebten wissenschaftlichen Zweck ebenfalls erreichen, so sind intensivere Grundrechtseingriffe unzulässig. Jeder einzelne Eingriffsschritt ist also auf seine Verhältnismäßigkeit hin zu überprüfen, das heißt, die Geeignetheit, Erforderlichkeit und Angemessenheit der Datenerhebung, -verarbeitung und -nutzung im Verhältnis zum Untersuchungszweck muß gewährleistet sein.

Alle dem TLfD zur Prüfung vorgelegten Projekte sahen vor, daß die Datenbeschaffung der Forschungseinrichtung entweder durch Übermittlung von bereits gespeicherten Informationen oder aber Befragung bzw. Untersuchung der Probanden - jedenfalls immer mit einer schriftlicher Einwilligungserklärung - erfolgen sollte. Dies ist nach § 4 Abs. 1 ThürDSG ein zulässiger Weg zur Informationsgewinnung. Eine wirksame Einwilligung setzt jedoch nach § 4 Abs. 2 ThürDSG voraus, daß der Betroffene ausreichend über den Zweck der Datenverarbeitung aufgeklärt wird und daß diese Einwilligungserklärung schriftlich abgegeben wird. Eine solche "informierte" Einwilligung liegt vor, wenn die Betroffenen ausdrücklich darüber aufgeklärt worden sind, daß die Erhebung freiwillig ist, die Verweigerung der Teilnahme an einer Untersuchung keine Maßnahmen gegen den Betroffenen zur Folge hat und die erhobenen Daten ausschließlich für Zwecke wissenschaftlicher Forschung verarbeitet werden. Außerdem ist er darüber zu informieren, was der Zweck und Gegenstand des Forschungsprojektes ist sowie durch wen und für wen die Daten gesammelt werden. Der Hinweis auf die Freiwilligkeit muß sich aus dem Informationstext besonders hervorheben, so daß ein "Übersehen" durch den Betroffenen ausgeschlossen werden kann.

Ein weiterer zentraler Punkt bei der Sicherung des Rechts auf informationelle Selbstbestimmung im Rahmen von Forschungsvorhaben ist die Pflicht zur frühestmöglichen Anonymisierung, die in der Forschungsklausel des § 25 Abs. 3 ThürDSG niedergelegt ist. Ist aufgrund des Forschungszweckes eine Anonymisierung nicht sofort möglich, so ist zumindest dafür zu sorgen, daß die Identitätsdaten von den übrigen Einzelangaben gesondert gespeichert werden. Anonyme Daten sind nach § 3 Abs. 9 ThürDSG Einzelangaben über persönliche oder sachliche Verhältnisse, die einer bestimmten oder bestimmbaren natürlichen Person nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand zugeordnet werden können. In der Praxis tauchen hier allerdings Abgrenzungsschwierigkeiten auf. So spricht man von nur "formal" anonymisierten Daten, wenn lediglich der Name und ggf. die Adresse vom sonstigem Datensatz abgetrennt werden. In diesen Fällen kann die Person aufgrund der vorliegenden Einzelangaben bereits mit geringem Zusatzwissen identifiziert werden. Es ist daher im Einzelfall zu prüfen, wie die Wiederherstellung des Personenbezugs verhindert werden kann. Daran anknüpfend sind die geeigneten Anonymisierungsverfahren anzuwenden.

Bedient sich eine öffentliche Forschungseinrichtung anderer Personen zur Durchführung des Forschungsprojektes, so sind diese Personen zur Verschwiegenheit zu verpflichten. In einem dem TLfD zur Prüfung vorgelegten Forschungsprojekt beabsichtigte eine Universitätsklinik im Rahmen von zwei Promotionsarbeiten ca. 200 Infarktpatienten zu Lebensgewohnheiten zu befragen, um Rückschlüsse auf familiäre, soziale und arbeitsbedingte Einflüsse auf die Ausbildung einer Herzkrankheit mit Endpunkt Infarkt ziehen zu können. Zur Durchführung der Studie sollten zwei nicht

in der Klinik beschäftigte Mitarbeiter mit Hilfe von Krankenhausakten ehemalige Patienten zur Mitarbeit an dem Projekt gewinnen. Bei diesem Projekt war zu beachten, daß nach § 27 Abs. 4 Satz 3 ThürKHG als bereichsspezifischer Sonderregelung die Nutzung von Patientendaten zu Forschungszwecken anderen Personen gestattet werden darf, wenn dies zur Durchführung des Forschungsvorhabens erforderlich ist und die Patientendaten im Gewahrsam des Krankenhauses verbleiben. In Satz 4 ist ausdrücklich geregelt, daß diese Personen zur Verschwiegenheit zu verpflichten sind. Dies erfolgt aufgrund von § 1 Abs. 1 Nr. 1 des Verpflichtungsgesetzes vom 02.03.1974 (BGBL. I S.547), wobei die Verpflichtung mündlich mit dem Hinweis auf die strafrechtlichen Folgen vorgenommen wird, zu der eine Niederschrift anzufertigen ist, die der Verpflichtete unterzeichnet.

Häufig läßt der Forschungszweck eine sofortige Anonymisierung samt Vernichtung der Identitätsdaten nicht zu, weil z. B. nach einer ersten Auswertung bestimmte Rückfragen an den Probanden gestellt werden müssen. In diesen Fällen bestimmt die Forschungsklausel des § 25 ThürDSG, daß die Identitätsdaten von den sonstigen Merkmalen getrennt gespeichert werden und nur dann zusammengeführt werden dürfen, wenn dies der Forschungszweck erfordert. Erfolgt diese Trennung innerhalb einer öffentlichen Stelle, kann dieser Grundrechtseingriff dadurch abgemildert werden, daß eine Vertrauensstelle als Datentreuhänder die Anonymisierung durchführt und lediglich die anonymisierten Angaben an den Träger des Forschungsprojektes weitergibt. Dieses Verfahren war in einem anderen, dem TLfD zur Prüfung vorgelegten Forschungsprojekt gewählt worden. Ein städtisches Gesundheitsamt hatte 100 Probanden mit empfindlichen Atemwegen, deren Adressen dort aus einer Untersuchung aus dem Jahr 1991/92 vorlagen, im Auftrag einer privaten Forschungseinrichtung angeschrieben, um deren Einwilligung zu einer von der Forschungseinrichtung durchzuführenden medizinischen Untersuchung der Atemwege zwecks Erstellung einer Studie zu Atemwegserkrankungen zu erhalten. Nach Vorliegen der Untersuchungsergebnisse sollten die Adressen mit einer laufenden Nummer im städtischen Gesundheitsamt gespeichert werden. Die epidemiologischen Daten, die zuvor anonymisiert wurden, sollten dagegen der Forschungseinrichtung übermittelt werden. Zur späteren Befundmitteilung sowie zweier weiterer Untersuchungen im Abstand von je drei Jahren kann die Forschungseinrichtung über den Datentreuhänder (städtisches Gesundheitsamt) die Verbindung zu den Probanden wieder herstellen. Diese Verfahrensweise war nicht zu beanstanden.

Häufig besteht bei Forschungsvorhaben das Problem, daß schon für das Einholen der Einwilligung eine Nutzung der Adresse, die bei öffentlichen Stellen gespeichert ist, zwingende Voraussetzung ist. Oftmals reicht hierzu eine Melderegisterauskunft (Gruppenauskunft oder Zufallsstichprobe) nicht aus, da bestimmte Probanden gezielt angesprochen werden sollen. Fehlt eine spezielle Regelung, so ist die Übermittlung der Adresse mangels Einwilligung des Betroffenen bereits unzulässig. Dieser Konflikt kann durch das sogenannte Adreßmittlungsverfahren gelöst werden. Dabei werden den öffentlichen Stellen frankierte, aber noch nicht adressierte Briefumschläge sowie das zu versendende Material übergeben. Die speichernde Stelle adressiert die Umschläge aufgrund der ihr vorliegenden Adressen und gibt sie zur Post. Dabei sollte der Angeschriebene in dem Begleitschreiben über das gewählte Verfahren aufgeklärt werden. Durch dieses Verfahren wird sichergestellt, daß der Forschungseinrichtung die Adressen von Probanden nur dann zur Kenntnis gebracht werden, wenn diese bereits eingewilligt haben, sich an dem Forschungsprojekt zu beteiligen.

13.3.2 Gemeinsames Krebsregister der neuen Länder in Berlin

Das zentrale Krebsregister der ehemaligen DDR soll durch die fünf neuen Länder und Berlin weitergeführt werden. Grundlage hierfür ist das Gesetz über Krebsregister (Krebsregistergesetz - KRG) des Bundes, das nach zähen Verhandlungen - insbesondere hinsichtlich der Gesetzgebungskompetenz des Bundes - durch einen Kompromiß im Vermittlungsausschuß zum 01.01.1995 in Kraft getreten ist. Dieses Gesetz hat allerdings nur eine Geltungsdauer von fünf Jahren und verpflichtet alle Bundesländer bis zum 01.01.1999, flächendeckend bevölkerungsbezogene Krebsregister einzurichten und zu führen. Neben dem zentralen Krebsregister der ehemaligen DDR, an das die Ärzte Daten über Krebserkrankungen ohne Kenntnis der Patienten gemeldet haben, gab es in den alten Bundesländern bisher nur in Hamburg und im Saarland landesweite Krebsregister, so daß mit dem KRG praktischer Handlungsbedarf vor allem in den alten Bundesländern besteht. Allerdings bedarf es zur Fortführung des zentralen Krebsregisters der ehemaligen DDR ebenfalls landesrechtlicher Regelungen.

Die Ärzte sind nach dem neuen KRG berechtigt, jedoch nicht verpflichtet, dem jeweiligen Krebsregister patientenbezogene Daten zu übermitteln. Der Arzt hat die Pflicht, den Patienten von einer beabsichtigten oder erfolgten Mitteilung zum frühestmöglichen Zeitpunkt zu unterrichten. Dies darf nur solange unterbleiben, als zu erwarten ist, daß dem Patienten dadurch gesundheitliche Nachteile entstehen könnten. Ist der Patient unterrichtet, so kann er der Meldung widersprechen. Auf dieses Widerspruchsrecht ist er vom Arzt hinzuweisen. Nach bereits erfolgter Meldung hat ein Widerspruch des Patienten zur Folge, daß schon gemeldete Daten wieder gelöscht werden müssen. Im Krebsregister selbst werden die Meldungen in einem zweistufigen Verfahren verarbeitet. Zunächst werden die gemeldeten Daten in den unter ärztlicher Leitung stehenden Vertrauensstellen auf Schlüssigkeit und Vollständigkeit überprüft und gegebe-

nenfalls nach Rückfrage bei der meldenden Stelle berichtigt. Im Anschluß daran erfolgt die Übernahme von Identitätsdaten und epidemiologischen Daten auf jeweils getrennte Datenträger. Die Vertrauensstellen verschlüsseln die Identitätsdaten und übermitteln diese sowie die epidemiologischen Daten an die Registerstelle. Danach werden alle bei der Vertrauensstelle noch vorhandenen patientenbezogenen Daten gelöscht. Eine Reidentifikation ist möglich und für Forschungszwecke, die einer Genehmigung bedürfen, erlaubt. Durch dieses - zugegebenermaßen etwas komplizierte - Verfahren ist es gelungen, die Interessen der Patienten an der Geheimhaltung ihrer Krankheitsdaten mit den Erfordernissen der Forschung zu vereinbaren.

Schon 1993 haben sich die neuen Länder und Berlin geeinigt, das zentrale Krebsregister der ehemaligen DDR als gemeinsames Krebsregister fortzuführen. Da das hierfür erlassene Krebsregistersicherungsgesetz zum 31.12.1994 auslief, bedurfte es einer Regelung, um dieses Register bis zum Inkrafttreten einer landesrechtlichen Regelung fortführen zu können. Hierzu haben die beteiligten Länder am 23.12.1994 ein Verwaltungsabkommen geschlossen, wonach das gemeinsame Krebsregister als nicht rechtsfähige Anstalt des öffentlichen Rechts des Landes Berlin geführt wird. Die zuständigen Ministerien der beteiligten Länder haben einen gemeinsamen Entwurf eines Krebsregisterausführungsgesetzes erarbeitet, zu dem die jeweiligen LfD Gelegenheit bekamen, Stellung zu nehmen. Der Hauptkritikpunkt der DSB an diesem Entwurf besteht darin, daß er in wesentlichen, auch grundrechtsrelevanten Bereichen auf das Verwaltungsabkommen verweist, dem kein Gesetzesrang zukommt. Daher haben die DSB der neuen Länder und Berlins angeregt, über solche Regelungen bzgl. der Errichtung und Führung des gemeinsamen, großen Krebsregisters einen Staatsvertrag als landesrechtliche Rechtsgrundlage nach § 1 Abs. 1 und 4 KRG abzuschließen, die grundrechtsrelevante Wirkung entfalten. Ob die betroffenen Länder hierauf eingehen werden, war bei der Berichtsabfassung noch nicht absehbar. Hierzu werden aber noch weitere Beratungen zwischen den zuständigen Ministerien und den LfD stattfinden.

Das gemeinsame Krebsregister wird möglicherweise auch auf europäischer Ebene Aufgaben im Rahmen der Krebsursachenforschung erhalten. Die Gremien der EU beraten seit 26.04.1993 den Entwurf eines Dritten Aktionsplans zur Krebsbekämpfung für die Jahre 1996 bis 2000, das Anfang 1996 mit einem Finanzierungsvolumen von 24 Mio. ECU verabschiedet werden soll. Als einer der zentralen Punkte wird die Unterstützung des Austausches von Informationen und Erfahrungen auf dem Gebiet der Sammlung und Weitergabe von zuverlässigen vergleichbaren Daten für Krebsregister gefordert. Daher sollen im Rahmen prioritärer Aktionen Einrichtungen wie das Europäische Netz der Krebsregister weiter unterstützt werden, um für eine bessere Berichterstattung über die Krebstrends genauere Erhebungen und eine schnellere Aktualisierung der Daten über Krebsmortalität und -morbidität zu erhalten. Es wird darauf zu achten sein, daß der Datenschutzstandard entsprechend dem KRG auch im Rahmen des Austausches innerhalb der EU gewährleistet bleibt.

13.3.3 Nutzung von Totenscheinen für wissenschaftliche Forschungsvorhaben

Der TLfD wird häufig um Auskunft und Unterstützung gebeten, wenn es darum geht, medizinische Daten für die Durchführung wissenschaftlicher Forschungsaufgaben zu nutzen. Dies trifft in besonderem Maße auch auf die Einsichtnahme in Totenscheine zu. Diesbezüglich besteht in Thüringen mitunter eine erhebliche Rechtsunsicherheit bei den Beteiligten, da eine entsprechende Rechtsvorschrift zum Umgang mit Totenscheinen nicht existiert und die Vorschriften der ehemaligen DDR als fortgeltendes Recht auf diese Frage keine Antwort geben. Da die Daten auf den Totenscheinen aufgrund ihres Inhaltes der ärztlichen Schweigepflicht unterliegen und eine unbefugte Offenbarung unter Strafe steht, bedarf es dringend einer gesetzlichen Regelung. Darauf wurde das zuständige TMSG bereits mehrmals hingewiesen. Der Gemeinsame Runderlaß des TMSG und des TIM zur Verwendung, Auskunftserteilung und Aufbewahrung von Totenscheinen vom Juni 1994 stellt dafür keine ausreichende Rechtsgrundlage dar und konnte bestenfalls als Übergangslösung verstanden werden. Der TLfD erwartet deshalb im Interesse der Forschung, aber insbesondere auch zum Schutz der Ärzte, daß hier baldmöglichst durch die Verabschiedung eines Leichenschaugesetzes die notwendige Rechtssicherheit hergestellt wird.

13.4 Archivwesen

Das öffentliche Archivwesen hat unter anderem die Aufgabe, Unterlagen öffentlicher Stellen, soweit sie archivwürdig sind, auf Dauer zu Zwecken der Geschichtsforschung oder anderer gesetzlich festgelegter Zwecke sicher aufzubewahren, und eine zweckentsprechende Nutzung zu ermöglichen. Rechtsgrundlage hierfür ist das Thüringer Archivgesetz (ThürArchivG) vom 23. April 1992. Das ThürArchivG ist eine bedeutsame bereichsspezifische Datenschutznorm, die das ThürDSG insoweit ergänzt, als u. a. der Umgang mit solchen personenbezogenen Daten geregelt wird, die eigentlich gelöscht werden müßten, weil sie z. B. nicht mehr erforderlich sind, jedoch nach § 16 Abs. 3 ThürDSG dem zuständigen Archiv zur Übernahme anzubieten wären. Mit dem Inkrafttreten des ThürArchivG am 1. Mai 1992 ist § 33 ThürDSG

überholt, der verhindern sollte, daß wichtige Unterlagen aus ehemaligen Einrichtungen der DDR (z. B. für Rehabilitierungszwecke) nur deshalb gelöscht werden, weil keine Regelungen für eine mögliche Archivierung bestanden. Der Schutz des Grundrechtes auf informationelle Selbstbestimmung der Betroffenen wird einerseits durch technische und organisatorische Maßnahmen sowie der Verweisung auf die Vorschriften des ThürDSG (§ 15 ThürArchivG) und andererseits durch die Festlegung von sogenannten Schutzfristen (§ 17 ThürArchivG) gewährleistet. Danach darf personenbezogenes Archivgut grundsätzlich erst zehn Jahre nach dem Tod und soweit das Todesjahr nicht zu ermitteln ist, erst 90 Jahre nach Geburt der betreffenden Person genutzt werden. Ausnahmen hiervon sind nur in den vom Gesetz ausdrücklich vorgesehenen Fällen (z. B. Suche von Vermißten) möglich.

13.4.1 Einführung des landeseinheitlichen Bibliotheksautomatisierungssystems

Aufgrund des Abschlusses einer Vereinbarung mit dem Land Niedersachsen über die Zusammenarbeit auf dem Gebiet der Bibliotheksautomation, insbesondere an der Beteiligung der staatlichen wissenschaftlichen Bibliotheken des Freistaates Thüringen am Bibliotheksverbund Niedersachsen - Sachsen-Anhalt, hatte das TMWK den TLfD über die Einführung eines landeseinheitlichen Bibliotheksautomatisierungssystems in Kenntnis gesetzt und hinsichtlich der vorgesehenen Richtlinie um seine Stellungnahme gebeten. Ziel des Systems ist es, die Literaturversorgung, die Benutzungsbedingungen und die Arbeitsbedingungen der Bibliotheksmitarbeiter zu verbessern und Voraussetzungen für eine enge Zusammenarbeit der Thüringer Bibliotheken mit in- und ausländischen Bibliotheksverbünden und Einzelbibliotheken zu schaffen. Der Entwurf der Richtlinie enthielt bereits eine Vielzahl datenschutzrechtlicher Regelungen hinsichtlich der Registratur von Nutzern der wissenschaftlichen Bibliotheken. Änderungsvorschläge des TLfD hinsichtlich des Verbotes, personenbezogene Daten für mögliche “Leistungskontrollen” zu nutzen und den zuständigen Personalrat einzubeziehen, wurden vom TMWK aufgegriffen.

13.4.2 Nutzung von Archivunterlagen zum Anlegen einer Datei über Berufsurkunden in medizinischen Fachberufen

Einer Anfrage des LVwA zufolge war dort beabsichtigt zur Erleichterung der täglichen Arbeit eine Datei anzulegen, in der alle Personen erfaßt werden sollten, die über Berufsurkunden in medizinischen Fachberufen verfügen. Dafür sollten neben den vorhandenen Unterlagen über die Erteilung von Berufserlaubnissen zur Vervollständigung der Übersicht auch Unterlagen aus Archiven (einschließlich Personalunterlagen) über bereits praktizierende Personen genutzt werden. In der Antwort des TLfD wurde darauf hingewiesen, daß sich aufgrund der fehlenden Rechtsgrundlage für die Erhebung aller in Thüringen lebenden und praktizierenden Personen mit Berufsurkunden in medizinischen Fachberufen eine Datei nur auf Personen beziehen kann, die ihre Berufserlaubnis in einem medizinischen Fachberuf vom LVwA erhalten oder einen entsprechenden Antrag gestellt haben. Ansonsten besteht nur die Möglichkeit, die Daten auf freiwilliger Grundlage zu erheben. Eine Nutzung von archivierten Personalunterlagen für die gewünschte Datei schließt das ThürArchivG aus, da gemäß § 17 ThürArchivG die Nutzung personenbezogenen Archivgutes nur im Einzelfall für die im Gesetz ausdrücklich benannten Zwecke, wie Forschungsvorhaben, Strafverfolgung, Rehabilitierung, Wiedergutmachung, Aufklärung vor Ablauf der bestehenden Schutzfristen, zulässig ist.

13.4.3 Fälschung von SED-Archivunterlagen

Für öffentliches Aufsehen sorgte im Frühjahr 1995 der Archivar einer Stadt, der Akten aus dem Bestand der Universitätsparteileitung der SED einer Landesuniversität, die im Thüringischen Staatsarchiv lagern, gefälscht hat. Dabei machte er sich die internen Kenntnisse als Stadtarchivar bei der Benutzung von Archivmaterialien zunutze, tauschte die zuvor gefälschten Aktenseiten bei seiner Einsichtnahme im Staatsarchiv aus und ließ sich später vom Thüringer Staatsarchiv diese Seiten kopieren und mit dem Stempel des Staatsarchivs zusenden. Dadurch wurde der Eindruck erweckt, bei den Unterlagen handele es sich um Kopien der Originale aus den Beständen des Staatsarchivs.

Eine Nachfrage beim Thüringer Staatsarchiv zu den datenschutzrechtlichen Vorkehrungen bei der Benutzung der Archive ergab, daß sich nach der Benutzungsordnung alle Benutzer vor Einsichtnahme nach Angabe des Zwecks der Benutzung in einer schriftlichen Erklärung dazu verpflichten müssen, bei Veröffentlichungen den Personenbezug von Daten unkenntlich zu machen oder zu anonymisieren. Die Sachakten werden allerdings vor der Einsichtnahme im Staatsarchiv wegen des unverhältnismäßigen Verwaltungsaufwandes nicht auf personenbezogene Daten hin überprüft. Diese Vorschriften wurden beachtet. So sind die Kopien aus den Akten mit Schwärzungen von Personenangaben mit Ausnahme von Persönlichkeiten der Zeitgeschichte versehen worden.

Die Schutzvorkehrungen bzgl. der Verwertung von Archivunterlagen wurden im vorliegenden Fall beachtet. Die Besonderheit lag jedoch darin, daß während der Einsicht im Staatsarchiv die Akten durch Austauschen von Blättern verändert wurden. Ob man durch eine vom Thüringer Archivarverband geforderte Einführung einer Kameraüberwa-

chung der Leseräume dieses Fälschungsrisiko ausschließen kann, ist fraglich. Sollte allerdings eine solche Überwachung eingeführt werden, so müßten zum Schutz des Persönlichkeitsrechts der Nutzer Videoaufnahmen - falls solche überhaupt erstellt werden - nach der Auswertung zeitnah gelöscht werden.

14. Wirtschaft, Verkehr, Wohnungswesen, Umwelt

14.1 Wirtschaft

14.1.1 Nutzung von Daten von Antragstellern zu Förderzwecken

Im Berichtszeitraum gab es mehrere Anfragen zur Zulässigkeit der Übermittlung von Einzeldaten aus Anträgen zur Wirtschaftsförderung bzw. aus Erhebungsbögen für die Statistik im produzierenden Gewerbe an öffentliche und nicht-öffentliche Stellen. Soweit dies nicht durch spezielle Rechtsvorschriften geregelt ist, gelten auch hierbei für personenbezogene Daten die allgemeinen Datenschutzbestimmungen. Danach ist unter Beachtung der Zweckbindung der Daten im Einzelfall zu prüfen, ob dies bei öffentlichen Stellen zur Aufgabenerfüllung des Übermittelnden oder des Empfängers erforderlich ist bzw. der Empfänger ein berechtigtes Interesse glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Ausschluß der Übermittlung hat.
In diesem Zusammenhang ergab sich die Frage, warum im Wirtschaftsausschuß des Landtags zur Vergabe der Fördermittel nicht die Namen der jeweiligen Antragsteller bekanntgegeben werden. Nach Prüfung des Sachverhaltes war festzustellen, daß der Ausschuß für Wirtschaft und Verkehr des Thüringer Landtags keine Entscheidungskompetenz hinsichtlich der Vergabe von Fördermitteln hat. Seine Aufgaben sind in § 74 der Geschäftsordnung des Thüringer Landtags abschließend geregelt. Ein Mitentscheidungsrecht bei der Vergabe von Fördermitteln widerspräche zudem dem in der Verfassung des Freistaats Thüringen verankerten Prinzips der Gewaltenteilung zwischen Exekutive und Legislative. Dementsprechend können betriebswirtschaftliche Daten von Antragstellern, soweit das Unternehmen nicht zugestimmt hat, nicht übermittelt werden. Aufgrund spezialgesetzlicher Rechtsvorschriften gilt § 30 ThürVwVG, wonach die Antragsteller Anspruch darauf haben, daß ihre Betriebs- und Geschäftsgeheimnisse nicht unbefugt offenbart werden.
Eine weitere Anfrage bezog sich auf die Zulässigkeit der Übermittlung statistischer Daten an das TMWI, da eine Übermittlung von Daten aus Erhebungsunterlagen der amtlichen Statistik an andere Stellen zur Wahrung des Statistikgeheimnisses regelmäßig unzulässig ist. Hierzu enthält jedoch das Gesetz über die Statistik im produzierenden Gewerbe eine spezielle Ausnahmeregelung, die bestimmt, daß in Einzelfällen auf Anforderung Einzelangaben aus dieser Statistik unter Nennung des Namens und der Anschrift der erfaßten Unternehmen und Betriebe sowie der Auskunftspflichtigen an die für die Wirtschaft zuständige oberste Bundes- oder Landesbehörde übermittelt werden dürfen. Gefordert wird in diesen Fällen eine unverzügliche Unterrichtung des betroffenen Auskunftspflichtigen über die Weiterleitung der Einzelangaben unter Angabe des Zwecks der Anforderung. Ein Einverständnis des Betroffenen ist dafür nicht erforderlich. Selbstverständlich kann daraus keine Generalvollmacht zur Nutzung von Einzelangaben für eine Erfolgskontrolle abgeleitet werden. Dies ist aufgrund der Zweckbindung der statistischen Daten unzulässig und wird auch wie eine Rückfrage beim zuständigen Ministerium sowie im TLS ergab, in der Praxis ausgeschlossen.

14.1.2 Erhebung und Übermittlung von personenbezogenen Daten durch IHK

Ende 1992 wurde das Gesetz zur Änderung von Gesetzen auf dem Gebiet des Rechts der Wirtschaft verabschiedet. Nach Artikel 2 Nr. 2 sind die Industrie- und Handelskammern berechtigt, zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken Daten über Anschriften, Wirtschaftszweig und Firma ihrer kammerzugehörigen Unternehmen an nicht-öffentliche Stellen zu übermitteln. Soweit der Betroffene keinen Widerspruch eingelegt hat, können zusätzlich der Name des Betriebsinhabers, die Telefonnummer, die angebotenen Waren- und Dienstleistungen sowie die Betriebsgrößenklasse übermittelt werden. Auf die Möglichkeit, der Übermittlung der Daten an nicht-öffentliche Stellen zu widersprechen, sind die kammerzugehörigen Unternehmen vor der ersten Übermittlung schriftlich hinzuweisen.
Im Rahmen der praktische Umsetzung dieser Regelungen hatte sich die Industrie und Handelskammer Südthüringen (IHK) mit der Bitte um Prüfung des vorgesehenen Verfahrens an den TLfD gewandt. Im Ergebnis dessen konnte festgestellt werden, daß aus datenschutzrechtlicher Sicht gegen die von der IHK vorgesehenen Form der Umsetzung dieser Neuregelung keine Bedenken bestanden, da die IHK den vom Gesetzgeber vorgesehenen Ermessungsspielraum unter Berücksichtigung datenschutzrechtlicher Aspekte künftig dahingehend ausschöpfen wird, daß grundsätzlich nur Daten übermittelt werden sollen, wenn der Betroffene nicht widersprochen hat. In diesem Sinne wurden auch die Kammerangehörigen informiert.

14.1.3 Auskunfts- und Einsichtsrechte der IHK gegenüber Fahrschulen

Der TLfD wurde vom Thüringer Fahrlehrerverband gebeten, zu überprüfen, ob alle Fahrschulen in Thüringen zur Feststellung ihrer Kammerzugehörigkeit eine Kopie der Fahrschul- und Fahrlehrererlaubnisurkunden bei der IHK zur Einsichtnahme vorlegen müssen. Dem Fahrlehrerverband wurde mitgeteilt, daß sich aus dem Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHK-G) weitgehende Auskunfts- und Einsichtsrechte der IHK gegenüber den Gewerbetreibenden ergeben. Die Adressen der Gewerbetreibenden erhält die IHK vom Gewerbeamt und aus dem Handelsregister. Wer die in diesem Gesetz näher bestimmte Bedingungen erfüllt, wird automatisch Pflichtmitglied. Kammerzugehörige sind der Kammer gegenüber zur Auskunft verpflichtet, um die zur Festsetzung der Beiträge erforderlichen Sachverhalte festzustellen. Gegebenenfalls darf die Kammer in sich hierauf beziehende Geschäftsunterlagen einsehen. Ebenfalls ist in § 9 IHK-G abschließend geregelt, welche Daten die IHK erheben darf.

14.1.4 Mitteilung von Prüfungsergebnissen an Ausbildungsbetriebe

Im Rahmen des Erfahrungsaustausches zwischen den LfD wurde festgestellt, daß in anderen Bundesländern das Ergebnis der Abschlußprüfung derjenigen Stelle mitgeteilt wird, die den Auszubildenden angemeldet hat. Nach Auskunft der IHK war diese Verfahrensweise auch gültige Praxis in Thüringen. Der TLfD hatte die IHK Nordthüringen darauf hingewiesen, daß § 45 Abs. 1 Berufsbildungsgesetz als Rechtsgrundlage ausscheidet. Der einzige mögliche Weg ist deshalb das Einholen einer Einwilligungserklärung bei dem Auszubildenden bezüglich einer Übermittlung des Ergebnisses an den Ausbildungsbetrieb. Im Ergebnis konnte erreicht werden, daß die IHK Nordthüringen ihr Verfahren umgestellt hat. Seit der abgelaufenen Sommerprüfung 1995 werden alle Prüfungsergebnisse ausschließlich an die Auszubildenden weitergeleitet. Der Ausbildungsbetrieb erhält lediglich die Mitteilung über die zugesandten Unterlagen. Damit ist für den Auszubildenden gewährleistet, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

14.1.5 Entwurf der Verwaltungsvorschrift zum Vollzug der §§ 14, 15 und 55 c der Gewerbeordnung

Das TMWI bat den TLfD um eine datenschutzrechtliche Stellungnahme zum Entwurf einer Allgemeinen Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55 c GewO. Dieser bundeseinheitliche Entwurf konkretisiert die Erfordernisse bei der Anzeige eines Gewerbes und deren Bescheinigung.
In seiner Stellungnahme wies der TLfD zunächst darauf hin, daß auf den zur Anwendung kommenden Anzeigeformblättern gemäß § 19 Abs. 3 ThürDSG der Erhebungszweck und dessen Rechtsgrundlage gegenüber dem Betroffenen angegeben werden muß. Weiterhin hielt der TLfD die generelle gegenseitige Unterrichtung bei einer Betriebsverlegung für problematisch, da die GewO selbst keine Kontrollmitteilung vorsieht und nach § 19 Abs. 2 ThürDSG personenbezogene Daten beim Betroffenen zu erheben sind. Da dem Gewerbetreibenden nicht unterstellt werden darf, er würde seiner Anzeigepflicht nicht nachkommen, wurde vorgeschlagen, diesen Teil der Vorschrift zu streichen. Außerdem hielt der TLfD es für geboten, deutlich herauszustellen, daß die Vorlage eines Führungszeugnisses gemäß § 31 BZRG nur dann direkt an die Behörde erfolgen darf, wenn eine solche Aufforderung an den Betroffenen nicht sachgerecht ist oder erfolglos bleibt. Dem Betroffenen darf nicht die Möglichkeit genommen werden, die Gewerbeanzeige aufrechtzuerhalten oder aber zurückzunehmen. Es ist zu begrüßen, daß alle diese datenschutzrechtlichen Bedenken beim Erlaß der Verwaltungsvorschrift berücksichtigt wurden.

14.1.6 Sind Handwerksmeisterdaten geschützt?

Eine Thüringer Handwerkskammer richtete an den TLfD die Anfrage, ob es aus datenschutzrechtlicher Sicht zulässig sei, anläßlich der Meisterfreisprechung alle Namen der angehenden Meister einer Tageszeitung zu übermitteln, die diese Namen veröffentlichen wollte.
Bei der Handwerkskammer handelt es sich um eine öffentliche Stelle, die personenbezogene Daten (also auch die Namen der Meister) nur dann an Private übermitteln darf, wenn der Betroffene hierzu eingewilligt hat oder eine Rechtsvorschrift dies erlaubt (§ 4 Abs. 1 ThürDSG). Das Handwerksrecht enthält für diesen Fall keine bereichsspezifischen Regelungen. Daher ist dies nach § 22 Abs. 1 ThürDSG zu beurteilen. Nach dessen Nummer 1 müßte die Weitergabe der Namen an die Zeitung zur Erfüllung der in der Zuständigkeit der Handwerkskammer liegenden Aufgaben erforderlich sein. Es war jedoch nicht erkennbar, daß zur Abnahme der Meisterprüfung eine listenmäßige Übermittlung aller Namen von freizusprechenden Meistern erforderlich sein sollte. Auch die Voraussetzungen der Nummer 2 waren nicht gegeben, da zwar ein berechtigtes Publikationsinteresse angenommen werden kann, dieses jedoch schutzwürdige Interessen der Betroffenen am Ausschluß der Übermittlung nicht überwogen hat. Das schutzwürdige Interesse der betroffenen Meister kann nur aufgrund einer hypothetischen Einschätzung ermittelt werden, da die Betroffenen keine Gelegenheit hatten, sich zuvor zu äußern. In diesem Fall war zu berücksichtigen, daß mit der

Übermittlung zum Zweck der Veröffentlichung jede weitere Zweckbindung der Daten unmöglich war, da durch die Zeitung die Daten an eine unbestimmte Anzahl von Personen weitergegeben wurde. Deshalb war es durchaus wahrscheinlich, daß zumindest bei einzelnen der über 600 Betroffenen überwiegende, schutzwürdige Interessen (beispielsweise nicht mit Werbematerial belästigt zu werden oder Vertreterbesuche zu bekommen) einer Übermittlung entgegenstanden.

Diese Einschätzung wurde der Handwerkskammer mitgeteilt, die sich bei einer entsprechenden Anfrage der Zeitung dieser Meinung auch anschloß. Dabei überzeugte die Redakteure der betreffenden Zeitung diese Auffassung auch nach einer entsprechenden Anfrage beim TLfD offensichtlich nicht. Aus Zeitgründen (die Veröffentlichung sollte bereits am nächsten Tag stattfinden) konnte auch keine Einwilligung der Betroffenen mehr eingeholt werden. Daraufhin veröffentlichte die Zeitung die Namen von 77 freigesprochenen Meistern, die sie von der Handwerkskammer bekommen hatte, bevor diese aufgrund ihrer datenschutzrechtlichen Zweifel den TLfD konsultiert hatte. Gleichzeitig wurde die Rechtsauskunft des TLfD, an die sich die Handwerkskammer größtenteils gehalten hatte, als "kleinkariert" und als "Unterdrückung kreativen Engagements durch Bürokraten" kritisiert. Datenschutz ist nach Auffassung des TLfD jedoch nicht so zu verstehen, daß man sich auf ihn nur berufen kann, wenn er sich als vorteilhaft auswirkt, sondern auch dann, wenn er einmal dazu führt, daß gewünschte Informationen nicht weitergegeben werden können.

Um den nachvollziehbaren Wunsch der Öffentlichkeit an der Information über den Leistungsstand des Thüringer Handwerks wie auch dem Recht auf informationelle Selbstbestimmung der Handwerksmeister Rechnung zu tragen, hat der TLfD der Handwerkskammer folgendes Verfahren vorgeschlagen: Ein überwiegendes schutzwürdiges Interesse der Meister könnte im Rahmen der Abwägung des § 22 Abs. 1 Nr. 2 ThürDSG dann ausgeschlossen werden, wenn die Prüflinge vor der geplanten Veröffentlichung auf die Möglichkeit eines Widerspruches hiergegen schriftlich hingewiesen worden sind und von diesem Widerspruchsrecht keinen Gebrauch gemacht haben. Daneben bestünde auch die Möglichkeit der Einholung der schriftlichen Einwilligung zur Veröffentlichung beispielsweise bei der Anmeldung zur Prüfung. Welches Verfahren die Handwerkskammer hierbei zukünftig anwenden will, hat sie bisher noch nicht mitgeteilt.

14.2 Verkehr

14.2.1 Änderung straßenverkehrsrechtlicher Vorschriften

Die Bundesregierung hat einen Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze mit Stand vom 20. Oktober 1995 vorgelegt. Begründet wird die Änderung mit der Umsetzung der zweiten EG-Führerscheinrichtlinie sowie anderer notwendiger Neuregelung im Straßenverkehrsbereich. Die DSB des Bundes und verschiedener Länder halten den Entwurf in großen Bereichen für datenschutzrechtlich nicht vertretbar. Aus diesem Grund fanden bisher mehrere Diskussionsrunden statt, in denen alle datenschutzrechtlich bedeutsamen Fragen des Gesetzentwurfs erörtert wurden.
Als zentraler Kritikpunkt ist dabei die geplante Erstellung eines zentralen Fahrerlaubnisregisters zu nennen. Dieses beim Kraftfahrtbundesamt einzurichtende Register wäre mit ca. 50 Mio. Datensätzen die größte personenbezogene behördliche Datensammlung in der Bundesrepublik. Es soll sowohl inländischen wie auch ausländischen Behörden zur Einsicht zur Verfügung stehen. Gründe für ein überwiegendes Allgemeininteresse an der Einrichtung eines solchen Registers, die eine zweifellos bestehende Mißbrauchsgefahr rechtfertigen könnten, werden dabei aus Sicht des Datenschutzes nicht gesehen. Darüber hinaus bestehen auch gegen die geplante Einführung eines zentralen Fahrlehrer- und eines zentralen Kraftfahrsachverständigenregisters datenschutzrechtliche Bedenken, da auch hieran ein überwiegendes Allgemeininteresse nicht erkennbar ist. Außerdem enthält der Entwurf des Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze eine Reihe von zu unbestimmten Formulierungen sowie Begriffe, die in der Terminologie des Datenschutzrechts eine andere Bedeutung haben, als die hier bezweckte. Schließlich wurde von einigen DSB auch darauf hingewiesen, daß verschiedene Begründungen einzelner Paragraphen unzutreffend sind.
Der TLfD wird die weitere Entwicklung des Entwurftextes aufmerksam verfolgen.

14.2.2 Speicherung von Parksündern unzulässig

Im Rahmen des Erfahrungsaustausches der LfD erhielt der TLfD Kenntnis davon, daß in anderen Bundesländern Wiederholungsfälle bei Verstößen im ruhenden Straßenverkehr regelmäßig gespeichert werden. In Ermangelung einer Rechtsgrundlage ist dies unzulässig. Zur Beantwortung der Frage, ob in Thüringen bei anstehenden Verwarnungs- und Bußgeldverfahren eine Überprüfung von früheren, bereits abgeschlossenen Verkehrsordnungswidrigkeitenverfahren zum Zweck der Mehrfachtäterahndung unter Zuhilfenahme von automatisierten Verfahren oder der Auswertung von Hand erfolgt, wandte sich der TLfD an das TIM. Es wurde mitgeteilt, daß in der Zentralen Bußgeldstelle keine örtlichen Karteien oder Dateien geführt werden, in denen personenbezogene Daten zur Erkennung von Mehrfachtätern

gespeichert werden. Die Nachfrage bei verschiedenen Ordnungsämtern ergab, daß in Thüringen die Daten aus Ordnungswidrigkeitenverfahren und die entsprechenden Akten ausschließlich zu Rechnungsprüfungszwecken archiviert werden. Ein Rückgriff auf die Akten oder eine Nutzung der Daten durch die Mitarbeiter erfolge nicht und sei technisch auch nicht möglich. Der TLfD wird im Zuge der datenschutzrechtlichen Kontrollen bei Ordnungsämtern die Richtigkeit der Darstellungen verstärkt überprüfen. Zur Zeit besteht allerdings kein Anlaß anzunehmen, daß Wiederholungsfälle in Thüringer Kommunen gespeichert und genutzt werden.

14.2.3 Dürfen Verfehlungen Führerscheinbewerbern für immer vorgehalten werden?

In Thüringen nutzt der größte Teil der Fahrerlaubnisbehörden die nach § 52 Abs. 2 BZRG gegebene Möglichkeit, strafrechtliche Verurteilungen, die sowohl im BZR als auch im Verkehrszentralregister gelöscht sind, im Verfahren der Wiedererteilung/Entziehung der Fahrerlaubnis zu verwenden. So sind in anderen Bundesländern Fälle bekannt, in denen bei der Urteilsfindung über 30 Jahre alte Eintragungen herangezogen wurden. Der TLfD hält die aus der Vorschrift des § 52 Abs. 2 BZRG hergeleitete, zeitlich unbegrenzte Verwertungsmöglichkeit früherer strafrechtlicher Verurteilung für unverhältnismäßig und datenschutzrechtlich bedenklich. In begründeten Einzelfällen ist das Einbeziehen auch länger zurück liegender Straftaten zur Beurteilung der charakterlichen Eignung der Gesamtpersönlichkeit des Fahrerlaubnisinhabers sicherlich angezeigt. Abzulehnen ist dieses Vorgehen aber insbesondere bei mehr als 10 Jahre zurückliegenden Verurteilungen und wenn es sich nicht um Wiederholungstäter handelt.
Der TLfD hat sich mit dem Vorschlag an das TMWI gewandt, einen Runderlaß herauszugeben, in dem die ihm nachgeordneten Verkehrsbehörden aufgefordert werden, die Aufbewahrung und Verwertung bereits getilgter Eintragungen im Regelfall nach Ablauf von 10 Jahren zu unterlassen. Das TMWI will aber an der durch § 52 Abs. 2 BZRG gegebenen Möglichkeit weiterhin festhalten. Der TLfD wird sich deshalb gemeinsam mit den anderen LfD für die baldige Änderung des § 52 Abs. 2 BZRG einsetzen.

14.2.4 Übermittlung personenbezogener Daten an Fahrschulen bei Nachschulungskursen durch Führerscheinstelle

Ein Bürger beschwerte sich über das Schreiben einer Fahrschule, in dem es heißt, er sei nicht zum Nachschulungskurs für Fahranfänger erschienen und man ihn darauf aufmerksam macht, daß bei Nichterscheinen des Nachschulungskurses der Führerschein eingezogen werden würde. Die Fahrschule konnte an die Daten nur durch eine Übermittlung der Führerscheinstelle gelangen, vermutete der TLfD.
Nach Informationen des betreffenden Landratsamtes wurden tatsächlich bis zu diesem Zeitpunkt entsprechende namentliche Listen an die Fahrschulen ausgegeben, und die Betroffenen damit für die Nachschulung auf eine bestimmte Fahrschule festgelegt.
Der TLfD erachtete die Praxis der Thüringer Führerscheinstellen für unzulässig. § 2a Abs. 2 Nr. 1 in Verbindung mit § 2b Straßenverkehrsgesetz (StVG) stellt keine ausreichende Rechtsgrundlage für eine Übermittlung von personenbezogenen Daten an die Fahrschulen dar. Die Anordnung einer Nachschulung kann nicht mit der Auflage verbunden werden, bei einer bestimmten Fahrschule die Nachschulung abzulegen. Vielmehr muß dem Betroffenen freigestellt sein, innerhalb der von der Führerscheinstelle zu benennenden Frist, eine ihm genehme Fahrschule selbst auszusuchen. Die Praxis in anderen Bundesländern beweist, daß dies zu keiner erheblichen Störung führt, insbesondere geht der Hinweis fehl, daß “es nicht dem einzelnen Nachschüler überlassen werden kann, bei welcher Fahrschule er sich meldet, da auf diese Weise vermutlich nie genügend Teilnehmer zusammen kommen würden!” Fehlt es indes an der Erforderlichkeit der Datenübermittlung an die Fahrschulen, so ist diese Datenübermittlung auch unzulässig. Das betreffende Landratsamt erklärte, daß zukünftig keine Namenslisten mehr an die Fahrschulen ausgegeben werden. Vielmehr wird dem Betroffenen nur noch eine Frist zur Beibringung der Teilnahmebescheinigung gesetzt. Auf welche Weise gewährleistet werden kann, daß der gemäß § 2b StVG geforderte Gruppenunterricht zustande kommt, entzieht sich der datenschutzrechtlichen Beurteilung durch den TLfD.

14.2.5 Gutachten der medizinisch-psychologischen Untersuchungsstellen

Die vom TMWI erlassene Eignungsrichtlinie bezüglich der Erfordernis der medizinisch-psychologischen Untersuchung (MPU) bei Bewerbern und Inhabern der Fahrerlaubnis zur Fahrgastbeförderung in Kraftomnibussen (ThürStAnz Nr. 48/1993 S. 2075 und 2076) stößt beim TLfD auf datenschutzrechtliche Bedenken. Die Richtlinie schreibt diesen Inhabern ein solches Gutachten einer MPU ab dem 55. Lebensjahr zur Verlängerung der Geltungsdauer der Fahrerlaubnis zwingend vor.
Die Vermutung einer Nichteignung zur Fahrgastbeförderung ab einem bestimmten Alter und der damit verbundenen Anforderung eines MPU-Gutachtens hielt der TLfD nicht mit dem Verhältnismäßigkeitsgrundsatz für vereinbar, wonach der kleinstmögliche Eingriff in das Persönlichkeitsrecht zu erfolgen hat. Die Vorlage eines ärztlichen Zeugnisses, aus dem lediglich die geistige und körperliche Eignung hervorgeht, ist deshalb als ausreichend anzusehen.

Die Anforderung eines MPU-Gutachtens kann nur im Einzelfall von der Verwaltungsbehörde verlangt werden, etwa wenn aufgrund des Gesundheitszeugnisses noch Zweifel an der Eignung bestehen. Da die Richtlinie nach Auffassung des TLfD einen unzulässigen Eingriff in das Recht auf informationelle Selbstbestimmung des einzelnen darstellt, hält er eine Änderung für dringend erforderlich. Die vom TLfD vertretene Rechtsauffassung wurde durch ein Urteil des Bundesverwaltungsgerichtes vom 17. Mai 1995 nunmehr bestätigt, so daß das TMWI angekündigt hat, es werde die Richtlinie ändern.

14.2.6 Auskunftsverweigerung für Fahrzeugdaten bei der Zulassungsstelle

Ein Bürger wandte sich an den TLfD mit der Frage, ob eine Zulassungsstelle einem Gläubiger, der zur Durchsetzung von Unterhaltsleistungen einen Personenkraftwagen des Schuldners pfänden will, Auskunft aus dem öffentlichen Verkehrsregister erteilen darf. Dem Bürger wurde mitgeteilt, daß die Übermittlung von Halter- und Fahrzeugdaten aus dem Fahrzeugregister zur Verfolgung von Rechtsansprüchen in § 39 StVG geregelt ist. Danach sind unter anderem Art, Hersteller und Typ des Fahrzeuges durch die Zulassungsstelle oder Kraftfahrtbundesamt zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeugidentifizierungsnummer darlegt, daß die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Bei der Vollstreckung in das Vermögen eines Schuldners, in welchem sich zufällig auch ein Kraftfahrzeug befindet, fehlt indessen der Zusammenhang mit der Teilnahme am Straßenverkehr. Eine Datenübermittlung durch die Zulassungsstelle zu solchen Zwecken ist danach nicht zulässig. Ausschließlich bei öffentlich-rechtlichen Ansprüchen, die nicht mit der Teilnahme am Straßenverkehr im Zusammenhang stehen, dürfen dem Empfänger Halterdaten übermittelt werden.

14.2.7 Zustellung eines Schriftstückes ohne Briefumschlag durch Kfz- Zulassungsstelle

In der Eingabe eines Bürgers an den TLfD beschwerte sich dieser darüber, daß ein an ihn gerichtetes Schriftstück einer Kfz-Zulassungsstelle aufgrund seiner Abwesenheit an eine Nachbarin ohne Schutzumschlag abgegeben wurde. Auf dem Formblatt über die Hinterlegung eines Bescheides und der Aufforderung, sich umgehend mit der Zulassungsstelle in Verbindung zu setzen, befanden sich auch handschriftliche Anmerkungen “keine Kfz-Steuern, keine Versicherung und nicht umgemeldet”, aus denen der Inhalt des Schreibens ersichtlich war.
Der Kfz-Zulassungsstelle wurde durch den TLfD zur Kenntnis gegeben, daß der Petent ein berechtigtes, schutzwürdiges Interesse an der Geheimhaltung der in dem Schriftstück aufgeführten sachlichen Verhältnisse hat. Durch die Übergabe des Schriftstückes an eine Nachbarin wurden geheimhaltungsbedürftige Tatsachen gegenüber Dritten unbefugt offenbart. Dabei wurde gegen § 9 Abs. 3 ThürDSG verstoßen. Danach sind beim Transport von Unterlagen mit personenbezogenem Inhalt Maßnahmen zu treffen, die ein unbefugtes Zugreifen auf Daten verhindern. Dienstliche Schriftstücke sind generell in einem verschlossenen Briefumschlag zu übergeben, der nur mit einer nachträglich sichtbaren Beschädigung geöffnet werden kann. Die Mitteilung des Amts für Straßenverkehrsangelegenheiten, der Vollzugsbedienstete hätte dem Irrtum unterlegen, daß die Nachbarin eine Verwandte des Petenten gewesen wäre, ist für die datenschutzrechtliche Bewertung des Vorfalls ohne Bedeutung. Von einer Beanstandung hat der TLfD gemäß § 39 Abs. 3 ThürDSG abgesehen, da es sich offenbar um einen einmaligen Vorgang gehandelt hat und das Amt für Straßenverkehrsangelegenheiten der Vorfall kritisch ausgewertet hat.

14.2.8 Kinderlose Rentnerin soll für “ihren” schwarzfahrenden Sohn erhöhtes Beförderungsgeld bezahlen

In einer Eingabe an den TLfD beschwerte sich eine Bürgerin darüber, daß sie von den Verkehrsbetrieben zur Zahlung eines erhöhten Beförderungsentgelts wegen Schwarzfahren ihres Sohns aufgefordert wurde. Nachweislich hat die entsprechende Bürgerin aber nie einen Sohn gehabt. Sie hatte den TLfD gebeten, zu prüfen, ob der Verdacht der unerlaubten Weitergabe bzw. Verwendung von Personalien gegeben sei.
Auf die Nachfrage des TLfD bei den Verkehrsbetrieben hin, konnte der Ablauf des Vorgangs geklärt werden. Demzufolge wurde ein Jugendlicher in einer Straßenbahn von einem der Kontrolleure ohne gültigen Fahrausweis angetroffen. Er gab einen Namen als eigenen Namen und einen weiteren als den Namen der Erziehungsberechtigten, seiner Mutter, an. Namensangaben können von den Kontrolleuren nicht nachgeprüft werden, da nach geltendem Recht niemand verpflichtet ist, ständig ein Ausweispapier bei sich zu haben, wobei auch nur Personen, die über 16 Jahre alt sind, einen derartigen Ausweis besitzen. In der Regel, das wurde dem TLfD von seiten der Verkehrsbetriebeverwaltung versichert, sind Jugendliche, die ohne Fahrschein in der Straßenbahn angetroffen werden, ehrlich und machen korrekte Angaben. Mitunter werden aber auch unrichtige Namen angegeben, in der Annahme, daß die Straßenbahngesellschaft weder den Schwarzfahrer noch seine Familie auffinden wird. Die Kontrolleure sind verpflichtet, der Verwaltung der Verkehrsbetriebe über die angetroffenen Schwarzfahrer Mitteilung zu machen und ihr die Namen derjenigen Personen zu nennen, die das erhöhte Beförderungsentgelt nicht bezahlt haben. Durch die Verkehrsbetriebeverwaltung werden

diese Personen aufgefordert, das erhöhte Beförderungsentgelt nachträglich zu zahlen. Sie schickt dann die Aufforderung an die Adresse, die der Schwarzfahrer genannt hat.

Im Ergebnis der Prüfung konnte der TLfD keine unerlaubte Verwendung bzw. Weitergabe von seiten der Verkehrsbetriebe feststellen. Die Straßenverkehrsbetriebe sind berechtigt, Kontrollen vorzunehmen oder vornehmen zu lassen. Sie sind auch berechtigt, sich den Namen desjenigen angeben zu lassen, der keinen gültigen Fahrschein vorweisen kann, damit sie das erhöhte Beförderungsentgelt nachträglich einfordern können. Weiterhin sind die Straßenverkehrsbetriebe mit Hilfe ihrer Kontrolleure berechtigt, durch Kontrollen ihre Schuldner festzustellen. Die Kontrolleure, die sich den Namen des Schwarzfahrers nennen lassen, sind entweder Mitarbeiter der Straßenverkehrsbetriebe oder sie handeln in deren Auftrag; sie sind von den Straßenverkehrsbetrieben gerade zu diesem Zweck mit dieser Aufgabe betraut worden. Eine Überprüfung der Adressenangaben durch die Polizei ist nicht realisierbar. Jedes Jahr wird eine so große Anzahl von Schwarzfahrern angetroffen, daß der Freistaat Thüringen und seine Polizei völlig überfordert sein würde, wenn Name und Adresse eines jeden Schwarzfahrers, der sich nicht korrekt ausweist, von der Polizei überprüft werden sollte. Aus diesen Gründen hält der TLfD derartige Versehen für den Bürger im Einzelfall für hinnehmbar. Außerdem hatte sich der Verkehrsbetrieb in aller Form bei der Bürgerin entschuldigt.

14.3 Wohnungswesen

14.3.1 Nutzung von Wohnungskarteikarten

Anfragen in der letzten Zeit lassen vermuten, daß in einer Reihe größerer Gemeinden und Landratsämter, denen aufgrund der zweiten Zuständigkeitsverordnung Aufgaben im Bereich des Wohnungswesens übertragen sind, zur Aufgabenerfüllung Wohnungskarteikarten geführt werden, deren Umfang und Inhalt über das gesetzlich zulässige Maß hinausgehen.
Als Ausgangsdatenbasis wurden dazu überwiegend die Wohnungskarteien, die in der ehemaligen DDR bei den Gemeinden in der Regel im Bereich der Wohnungslenkung zum Zwecke der Wohnungsbestandsfortschreibung geführt wurden, genutzt. Ein Recht oder eine Verpflichtung zur Fortnutzung der gesamten Datenbestände in den gemeindlichen Wohnungskarteien war rechtlich nicht begründet.
Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von Daten zur Führung von Wohnungskarteien bzw. entsprechender automatisierter Dateien ist das Wohnungsbindungsgesetz sowie das Thüringer Belegungsrechtegesetz vom 8. Dezember 1995. Danach haben die gemäß § 19 Zweite Zuständigkeits-VO für das Wohnungswesen zuständigen Stellen im Rahmen der Umsetzung des Wohnungsbindungsgesetzes für alle staatlich geförderten Wohnungen eine Bestandsdatei zu führen. Der Datenumfang dieser Datei ist in der VV WoBindG abschließend geregelt. Nach Außerkrafttreten des Gesetzes über die Gewährleistung von Belegungsrechten im kommunalen und genossenschaftlichen Wohnungswesen zum 31. Dezember 1995 haben nur die im Thüringer Belegungsrechtegesetz benannten kreisfreien Städten sowie die durch die Thüringer Verordnung über Belegungsbindung vom 1. Januar 1996 bestimmten Städte für einen Teil ihrer kommunalen bzw. genossenschaftlichen Wohnungen eine weitere Wohnungsbestandskartei bzw. -datei zu führen. Der Datenumfang der Datei ist in der VV zum Belegungsrechtegesetz ebenfalls abschließend geregelt. Außer diesen Dateien ist jede weitere Speicherung oder Fortschreibung von Daten über Wohnungen oder Wohngebäude unzulässig. Dies trifft im besonderen Maße auf noch teilweise vorhandene Unterlagen des ehemaligen Datenspeichers Wohnungspolitik zu. Gemäß § 11 ThürArchivG sind diese Daten dem zuständigen Archiv anzubieten. Mit Beginn dieses Jahres wird deshalb die Einhaltung der Datenschutzbestimmungen in diesem Bereich einen Kontrollschwerpunkt für den TLfD bilden.

14.3.2 Verwaltungsvorschriften zum Vollzug des Wohnungsbindungsgesetzes

Im April 1994 wurden durch das TIM im Rahmen seiner Zuständigkeit für das Wohnungswesen Verwaltungsvorschriften zum Vollzug des Wohnungsbindungsgesetzes (VVWoBindG) erlassen. Der TLfD erhielt erst über die Veröffentlichung im Thüringer Staatsanzeiger hiervon Kenntnis. Bei Prüfung der Vordrucke war festgestellt worden, daß der Antrag auf Erteilung eines Wohnberechtigungsscheines Fragen enthielt, die zur Bearbeitung nicht erforderlich waren, so daß die Erhebung einiger Daten aufgrund der Rechtsvorschriften sowie der fehlenden Rechtsfolge bei einer entsprechenden Beantwortung nach Auffassung des TLfD nicht als zulässig anzusehen war. Dies betraf insbesondere detaillierte Auskünfte zum Familienstand, die Zuordnung zu einem nicht definierten Personenkreis sowie Fragen hinsichtlich der Dringlichkeit ("Angaben zum sozialen Gewicht"), die ebenso nicht näher erläutert waren. Die Bedenken des TLfD wurden vom zuständigen Ministerium zum Anlaß genommen, die entsprechenden Unterlagen zu überarbeiten, so daß bei der Neuveröffentlichung der Verwaltungsvorschriften im Thüringer Staatsanzeiger Nr. 44/1994 die übergebenen Hinweise und Anregungen voll inhaltlich berücksichtigt wurden. Es zeigte sich auch in diesem Fall, daß eine frühzeitige Information bzw. Anhörung des TLfD bei der Erarbeitung von Landesregelungen mit datenschutzrelevantem Inhalt zweckmäßig ist.

14.3.3 Veröffentlichung personenbezogener Daten aus Prüfberichten einer Wohnungsgesellschaft

Durch Zeitungsberichte sowie eine entsprechende Eingabe erfuhr der TLfD, daß in einer außerordentlichen öffentlichen Gesellschafterversammlung der Wohnungsgesellschaft einer Stadt personenbezogene Daten von Mitarbeitern bekannt gegeben worden waren. Tagesordnungspunkt der außerordentlichen Sitzung war der von zwei Gutachtern vorgelegte Betriebsprüfungsbericht der Wohnungsgesellschaft. Da ein Schwerpunkt des Berichtes die Prüfung der Personalkosten betraf, gab es in der Diskussion mehrere diesbezügliche Anfragen zum Prüfbericht. Trotz der Öffentlichkeit der Sitzung und in Kenntnis des Inhaltes des Prüfberichtes wurden die Gutachter vom Aufsichtsratsvorsitzenden und Bürgermeister der Stadt ausdrücklich von ihrer Verschwiegenheitspflicht befreit. Das hatte zur Folge, daß entsprechend dem Inhalt des Prüfungsauftrages über konkrete Fakten hinsichtlich des erforderlichen Personalbestandes, der Personalkosten und der Einstufungen des Personals diskutiert wurde. Aufgrund der im Prüfbericht enthaltenen Einzelangaben und der damit verbundenen Möglichkeit der Herstellung eines unmittelbaren bzw. mittelbaren Mitarbeiterbezuges wurde der Grundsatz der “internen” Vertraulichkeit von Personaldaten nicht mehr eingehalten. Im Ergebnis der Prüfung des Sachverhaltes wurde deshalb gegenüber der Wohnungsgesellschaft als öffentliche Stelle im Sinne des ThürDSG beanstandet, daß die Vertraulichkeit von Personalakten der Mitarbeiter im Rahmen der außerordentlichen Gesellschafterversammlung verletzt worden war. Gleichzeitig wurde die Stadtverwaltung und das zuständige Landratsamt darüber unterrichtet.

14.3.4 Bonitätsprüfung eines Wohnungsunternehmens anhand von Vermietungslisten

Im Zusammenhang mit der Abwicklung des Altschuldenhilfegesetzes ist das TMWI mit der Frage an den TLfD herangetreten, ob einer Kreditanstalt von Thüringer Wohnungsunternehmen Listen mit Namen der Mieter sowie der Miethöhe übermittelt werden dürfen.

Zur Finanzierung der noch verbliebenen Altschulden waren die Wohnungsunternehmen gezwungen, Kredite aufzunehmen, die mit Grundpfandrechten an den unternehmenseigenen Wohnungen abgesichert werden mußten. Die finanzierende Bank verlangte hierfür jedoch die Einräumung der ersten Rangstelle. An dieser Stelle waren jedoch vielfach Grundpfandrechte der Kreditanstalt eingetragen, die mit der Abwicklung der Wohnungsbauförderung in Thüringen beauftragt ist. Diese Kreditanstalt war im Einvernehmen mit dem TMWI bereit, auf diese erste Rangstelle zugunsten der finanzierenden Bank zu verzichten. Zur Einschätzung des verbleibenden Risikos hielt es die Kreditanstalt jedoch für erforderlich, daß ihr die Wohnungsunternehmen den aktuellen Stand der Vermietung der Objekte in Form einer Liste mitteilen, die die Namen der Mieter, die jeweilige Miethöhe sowie die nicht vermieteten Wohnungen enthält.

Der TLfD hat dem TMWI mitgeteilt, daß eine solche Datenübermittlung erforderlich und angemessen ist, sowie, daß hiergegen keine Bedenken bestehen, soweit sichergestellt ist, daß die übermittelten Daten nur für diesen konkreten Zweck verwendet werden.

14.3.5 Unklare Einwilligungserklärungen auf Bauantragsformularen

Von einem LfD eines benachbarten Bundeslandes wurde der TLfD auf die Praxis der Bauordnungsbehörden im Umgang mit Angaben aus Bauantragsformularen befaßt. In diesen Formularen ist eine Erklärung enthalten, wonach sich der Bauherr und Entwurfsverfasser damit einverstanden erklären, daß Ort und Straße der Baustelle, Art und Größe des Bauvorhabens sowie ihre Namen und Anschriften im Amtsblatt veröffentlicht bzw. einen Bautennachweis zur kostenlosen Veröffentlichung mitgeteilt werden. Der TLfD hat daraufhin die in Thüringen gültigen Formulare dahin gehend überprüft, ob die Anforderungen einer wirksamen Einwilligung nach § 4 Abs. 2 Satz 3 ThürDSG eingehalten werden. Weder die Thüringer Bauordnung noch die zu deren Ausführung erlassenen Vorschriften sehen eine Regelung zur Übermittlung der Bauherrendaten an sogenannte Baustelleninformationsdienste zur Veröffentlichung vor. Daher bleibt es bei dem Grundsatz von § 4 Abs. 1 ThürDSG, wonach die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig sind, soweit der Betroffene eingewilligt hat. Diese Einwilligung ist nach § 4 Abs. 2 ThürDSG vom Betroffenen unter Hinweis auf den Zweck der Speicherung und einer vorgesehenen Übermittlung grundsätzlich schriftlich einzuholen. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Das vom TIM in der Bekanntmachung über den Vollzug der Thüringer Bauordnung und der Verordnung über bautechnische Prüfungen (Thür StAnz 1994 S. 3051 ff.) unter Nr. 1 für verbindlich erklärte Formular wird dieser Pflicht zur Hervorhebung der Einwilligungserklärung im äußeren Erscheinungsbild nicht in ausreichendem Maße gerecht. Unter einer gemeinsamen Überschrift werden zwei voneinander unabhängige Hinweise optisch als ein Block im Formular zusammengefaßt. Es folgt zunächst der Hinweis nach § 19 Abs. 3 ThürDSG, wonach die im Antrag zu machenden Angaben für die Erteilung einer Baugenehmigung bzw. die Bestätigung einer eingereichten Bauanzeige erforderlich sind. Danach folgt die Frage nach dem Einverständnis zur Übermittlung der Bauherrendaten an Baustel-

lenverlage. Dadurch, daß diese beiden Hinweise auf dem Formular in einem Block erscheinen, besteht die Gefahr, daß beide Textpassagen als zusammengehörend aufgefaßt werden könnten. Hierbei könnte der Eindruck entstehen, daß die Einwilligung zur Übermittlung der Bauherrendaten an die Baustelleninformationsdienste zur Erteilung der Baugenehmigung erforderlich sei. Dies ist aber gerade nicht der Fall. Vielmehr ist es dem Bauherren freigestellt, diese Einwilligung zu erteilen.

Daher wurde dem nunmehr zuständigen TMWI empfohlen, beide Hinweise mit separaten Überschriften zu versehen, und so den Anforderungen an eine rechtswirksame Einwilligungserklärung zu genügen. Dabei wurde konzediert, daß die gedruckten Formulare zunächst aufgebraucht werden können, bevor ein entsprechend geändertes Formular verbindlich vorgeschrieben wird. Das TMWI hat daraufhin mitgeteilt, daß die Formularverlage bei der Drucklegung davon ausgegangen sind, daß innerhalb der nächsten zwei Jahre keine Veränderung des Antragsformulars zu erwarten ist. Darüber hinaus wird derzeit eine Novelle des Baugesetzbuches vorbereitet, die ebenfalls in etwa zwei Jahren in Kraft treten wird. Bei der dann vorzunehmenden Überarbeitung der Formulare wurde die Beteiligung des TLfD aus datenschutzrechtlicher Sicht zugesagt.

14.3.6 Datenübermittlung zwischen Wohnungsgesellschaft und Sozialamt

In der Eingabe eines Bürgers an den TLfD beschwerte sich dieser darüber, daß er in einem Schreiben von seinem Vermieter, einer im kommunalen Eigentum befindlichen Wohnungsgesellschaft, aufgefordert wurde, die Betriebskostenrechnung beim Sozialamt einzureichen. Weiterhin wurde er darauf hingewiesen, daß eine Auszahlung des Guthabens, der durch das Sozialamt überbezahlten Betriebskosten, an den Mieter nicht möglich sei. Das zuständige Sozialamt wurde aufgefordert, dem TLfD mitzuteilen, ob, in welchem Umfang und auf welcher Rechtsgrundlage der Wohnungsgesellschaft mitgeteilt wurde, daß der Bürger Sozialhilfeempfänger ist. Das betroffene Sozialamt teilte dem TLfD mit, daß der Bürger Sozialhilfeempfänger sei und seine Mietkosten zu 100 Prozent übernommen würden. Generell hat der Bürger dabei zwei Möglichkeiten der Mietkostenübernahme durch das Sozialamt. Entweder erhält der Mieter direkt vom Sozialamt die Zahlung der Miete oder das Sozialamt zahlt die Miete direkt an den Vermieter. Im vorliegenden Fall hat der Mieter dem Sozialamt gegenüber eine schriftliche Einverständniserklärung erteilt, daß die fällige Miete direkt an den Vermieter überwiesen wird. Es wurde aber kein Schriftwechsel mit der Wohnungsgesellschaft geführt.

Eine Anfrage bei der Wohnungsgesellschaft ergab dann, daß die auf dem Mietüberweisungsträger angegebene Kontonummer der Stadtkasse auch den Mitarbeitern der Wohnungsbaugesellschaft bekannt ist. Aus dieser Tatsache wurde dann leicht geschlossen, daß der entsprechende Mieter Sozialhilfeempfänger ist. Da die Betriebskosten als Bestandteil der Miete ebenfalls durch das Sozialamt übernommen werden, hat dieses auch das Recht, eventuelle Guthaben direkt vom Vermieter zurücküberwiesen zu bekommen. Daß der Vermieter anhand der Bankverbindung entnehmen kann, welche Stelle die Mietzahlungen leistet, ist nach Meinung des TLfD auch aus datenschutzrechtlicher Sicht hinzunehmen. Aufgrund eines Erlasses des TMWI ist lediglich festgelegt, daß auf dem Überweisungsträger nicht die Worte Sozialamt oder Sozialhilfe erscheinen dürfen. Der TLfD konnte im Einvernehmen mit dem Sozialamt erreichen, daß die Einverständniserklärungen in Zukunft nicht nur die Überweisung des monatlichen Mietzins durch das Sozialamt beinhalten, sondern den gesamten Zahlungsverkehr einschließen. Die Wohnungsgesellschaft teilte mit, daß zukünftig bei jeder Betriebskostenabrechnung der Hinweis an alle Mieter gemacht wird, falls die Miete durch das Sozialamt bezahlt wird, eine Auszahlung des Guthabens auch an dieses vorgenommen wird.

In einer weiteren Eingabe an den TLfD beschwerte sich eine Bürgerin über ein an sie gerichtetes Schreiben des Sozialamts, in dem sie aufgefordert wurde, sich wegen bestehender Mietschulden mit "der Außenstelle des Sozialamts" in Verbindung zu setzen. Die Beschwerdeführerin bestritt, überhaupt Mietschulden zu haben und bat um Aufklärung, auf welche Weise eine solche Information an das Sozialamt gelangt war. Der zur Klärung dieses Sachverhaltes durchgeführte Informationsbesuch bei der sich ebenfalls in kommunaler Trägerschaft befindlichen Wohnungsgesellschaft ergab, daß sich die Beschwerdeführerin dort in einem größeren Rückstand mit ihren Mietzahlungen aufgrund einer von ihr selbsttätig vorgenommenen Mietminderung befand. Weiterhin wurde von seiten der Wohnungsgesellschaft erklärt, daß es sich bei der "Außenstelle des Sozialamts" um eine sowohl organisatorisch als auch fachlich der Wohnungsgesellschaft zugeordnete Stelle handle, die bei deren Einrichtung auch vom Sozialamt unterstützt worden wäre. Mit Hilfe dieser Stelle soll mit Mietern, die auf Schriftverkehr nicht reagieren, das persönliche Gespräch gesucht werden. Allerdings konnte bislang weder von der Wohngeldstelle noch vom Sozialamt in Erfahrung gebracht werden, wer für Benutzung des sozialamts-ähnlichen Briefkopfes verantwortlich ist. Dem TLfD wurde zugesichert, daß ab sofort ausschließlich das Logo der Wohnungsgesellschaft benutzt wird. Die betroffene Bürgerin wurde entsprechend unterrichtet.

Im Rahmen der o. a. Prüfung wurde auch festgestellt, daß die Wohnungsgesellschaft ein automatisiertes Mahnsystem zur Anwendung bringt. Ist die Miete nach einem bestimmten Zeitpunkt nicht beglichen, so erfolgt automatisch eine

Mahnung an den säumigen Mieter. Danach folgen verschiedene Erinnerungen und Mahnungen. Ist der Mieter mindestens zwei Monate im Verzug, erhält er die fristlose Kündigung des Mietverhältnisses sowie die Androhung einer Räumungsklage. Aus datenschutzrechtlicher Sicht erläuterungsbedürftig sah der TLfD dabei die Tatsache an, daß die Kündigung generell in Kopie auch an das Sozialamt übermittelt wird. Der Mieter wird in der Kündigung darauf hingewiesen, daß das BDSG die gesetzliche Grundlage für eine solche Übermittlung der personenbezogenen Daten darstellen würde. Der TLfD anerkennt dabei durchaus die Vorteile des Verfahrens für alle Beteiligten. Die Wohnungsgesellschaft hat ein geschäftsmäßiges Interesse an der pünktlichen Zahlung der Miete, die ggf. dann durch das Sozialamt übernommen wird. Der Mieter selbst kann vor einer drohenden Obdachlosigkeit bewahrt werden und das Sozialamt erlangt Informationen über die mögliche Hilfsbedürftigkeit, wonach die Verpflichtung des Sozialhilfeträgers gemäß § 5 BSHG besteht, auch ohne Antrag des Hilfesuchenden von Amts wegen tätig zu werden. Insgesamt erspart das Verfahren der Stadtverwaltung soziale und finanzielle Belastungen, die sich beispielsweise aus dem Räumungsurteil und dessen Vollstreckung durch den Gerichtsvollzieher ergeben. Der TLfD wies aber darauf hin, daß nur diejenigen säumigen Mietschuldner an das Sozialamt übermittelt werden dürfen, bei denen davon auszugehen ist, daß diese hilfsbedürftig sind. Für Mieter, die sich wie im o. a. Fall, in einem Streit über die Miethöhe mit der Wohnungsgesellschaft befinden, muß eine solche Übermittlung ausgeschlossen werden, da es sich hierbei ausschließlich um zivilrechtliche Auseinandersetzungen handelt. Der Schluß, daß nicht (vollständig) beglichene Mietschulden immer auf mangelnder Leistungsfähigkeit des Mieters beruhen und dieser daher hilfsbedürftig ist, darf nicht gezogen werden. Die zunächst vom TLfD vorgeschlagene Einwilligung in die Datenübermittlung an das Sozialamt scheidet aus Praktikabilitätsgründen aus. Mieter, die aus verschiedenen Gründen auf die zahlreichen Mahnungen bis hin zur fristlosen Kündigung nicht reagieren, werden voraussichtlich ebensowenig selbständig eine Einwilligungserklärung abgeben. Deshalb muß in der Kündigung der Mieter wenigstens auf die Möglichkeit eines Widerspruchs gegen die Übermittlung seiner personenbezogenen Daten an das Sozialamt hingewiesen werden.

14.4 Umwelt

14.4.1 Umweltinformationsgesetz

Am 16. Juli 1994 trat das Umweltinformationsgesetz (UIG) in Kraft. Das Gesetz orientiert sich dabei eng an der Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (90/313/EWG). Auch die Verfassung des Freistaats Thüringen gewährt in Artikel 33 jedem "das Recht auf Auskunft über die Daten, welche die natürliche Umwelt in seinem Lebensraum betreffen und die durch den Freistaat erhoben worden sind, soweit gesetzliche Regelungen oder Rechte Dritter nicht entgegenstehen". Gemäß § 2 Abs. 1 UIG hat jeder Anspruch auf freien Zugang zu Informationen über die Umwelt, die bei Behörden oder einer Person des Privatrechts im Sinne des § 2 Nr. 2 vorhanden sind. Aus datenschutzrechtlichen Gründen ist dieser Anspruch gemäß § 8 Abs. 1 ausgeschlossen oder beschränkt, wenn durch das Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden würden. Der TLfD wird aufmerksam verfolgen, wie sich solche allgemein formulierten Einschränkungen zum Schutz des Persönlichkeitsrechts in der Praxis auswirken werden.

14.4.2 Gewährleistung des Datenschutzes bei Beraterverträgen der Gemeinden sowie Wasser-/Abwasserzweckverbänden

Die DSB der neuen Länder hatten sich mit der Tätigkeit von Beratern von Gemeinden sowie Wasser-/Abwasserzweckverbänden in datenschutzrechtlicher Hinsicht zu beschäftigen. Die Gemeinden und Zweckverbände schließen zur Erledigung kommunaler Aufgaben häufig Verträge mit privaten Beratungsunternehmen ab. Diese umfassen neben der Beratung zu Fragen des kommunalen Abgaberechts sowie der Mitwirkung beim Entwurf von Beitrags- und Gebührensatzungen auch Tätigkeiten zur Erfassung der abgabenpflichtigen Grundstücke und Grundstückseigentümer einschließlich der Berechnungsgrundlage (Fläche, Geschoßfläche, Frontlänge usw.) bis hin zur Erstellung versandfertiger Abgabebescheide. Es werden also eine Vielzahl von personenbezogenen Daten durch die privaten Unternehmen im Auftrag der Gemeinden verarbeitet.

Ein dem TLfD vorliegender Vertragsentwurf enthält beispielsweise keinerlei Regelungen, die den Auftragnehmer verpflichten, Datenschutzrecht einzuhalten. So fehlen insbesondere Regelungen, wonach der Auftragnehmer (Berater) die Daten nur im Rahmen der Zweckbestimmung und der Weisungen des Auftraggebers (Gemeinde/ Zweckverband) erheben, verarbeiten oder nutzen darf. Weiter müssen Regelungen über geeignete organisatorische und technische Maßnahmen getroffen werden, um die personenbezogenen Daten vor der unbefugten Einsichtnahme Dritter zu schützen. Schließlich ist durch eine Regelung sicherzustellen, daß sich der Auftragnehmer der Kontrolle durch den TLfD entsprechend der §§ 37 bis 40 ThürDSG unterwirft, wobei der Auftraggeber nach § 8 Abs. 6 Satz 3 ThürDSG den TLfD über eine Auftragserteilung zu unterrichten hat. Dem LVwA als oberer Kommunalaufsicht wurden von seiten des TLfD

diese Anforderungen mitgeteilt. Das LVwA hat in einem Rundschreiben an alle Landratsämter und kreisfreien Städte sowie die Zweckverbände seines Zuständigkeitsbereiches über diese Problematik informiert sowie die unteren Rechtsaufsichtsbehörden angewiesen, bei der Genehmigung nach § 79 ThürKO in künftig abzuschließenden Verträgen die zu beachtenden Minimalanforderungen zur Gewährleistung des Datenschutzes sicherzustellen. Der TLfD geht davon aus, daß bei künftigen Vertragsgestaltungen der Beraterverträge die datenschutzrechtlichen Anforderungen beachtet werden.

Ein Beleg für die Richtigkeit dieser Annahme scheint eine kürzlich von einem solchen Kommunalberater im Auftrag eines Abwasserzweckverbandes vorgelegte Anfrage auf Überprüfung eines Erhebungsbogens zur Erfassung von Erstdaten für die Berechnung von Beiträgen bei Abwasseranlagen zu sein. Entsprechende Anfragen legten aber auch Zweckverbände direkt vor. Zentraler datenschutzrechtlicher Aspekt ist hierbei, daß nur die zur Beitragsfestsetzung erforderlichen Angaben erhoben werden dürfen. Rechtsgrundlage und Maßstab hierfür bildet eine aufgrund des Thüringer Kommunalabgabengesetzes erlassene Beitrags- und Gebührensatzung zur Entwässerungssatzung. Als Orientierungshilfe für den Erlaß derartiger Satzungen hat das TIM Ende 1995 im Thüringer Staatsanzeiger ein Satzungsmuster veröffentlicht. Um die Beiträge möglichst gerecht auf die einzelnen Grundstückseigentümer verteilen zu können, sind nach den jeweiligen Satzungen - wie schon erwähnt - eine Vielzahl von Einzelangaben zur Grundstückssituation als erforderlich anzusehen. Bei der Erhebung sollte auf diese Zusammenhänge ausführlich hingewiesen werden, nicht nur, weil § 19 Abs. 3 ThürDSG verlangt, dem Betroffenen den Erhebungszweck anzugeben, sondern auch, um mehr Akzeptanz bei den Beitragsschuldnern, wenn schon nicht für die Höhe, dann doch wenigstens für den Verteilungsmaßstab der Beiträge zu erreichen.

15. Technischer und organisatorischer Datenschutz

15.1 Neue Technologien - eine Herausforderung für den Datenschutz

Die sich immer mehr beschleunigende Entwicklung auf dem Gebiet der Informations- und Kommunikationstechnik (IuK) stellt in zunehmendem Maße an den Datenschutz erhöhte Anforderungen.
Global zeichnet sich ab, daß Computer, Software, Telekommunikation, Unterhaltungselektronik und Medien zu einem komplexen, digitalen Informationsverbund zusammenwachsen. Das Wort des Jahres 1995 heißt Multimedia. Multimedia-Techniken basieren auf einer computergestützten, interaktiven und medienintegrierenden (Film, laufende Bilder, Texte, Sprachen, Grafiken) Arbeitsweise.
Schon jetzt leben wir im Zeitalter der Informations- und Kommunikationstechnologien. Weltweite Netzwerkdienste bieten ihre Informationsdienste unter Einbeziehung von Satelliten an. Die Wege der Informationsübertragung sind nicht nur für den Laien eine nicht mehr transparente Datenwelt. Zwei Drittel aller deutschen Haushalte verfügen schon über einen nutzungsfähigen Anschluß eines einheitlichen Netzes auf der Basis der Telefonnetze der Telekom und des Kabelfernsehnetzes. Der forcierte Einsatz von Glasfaserkabel als Übertragungsmedium und der Einsatz moderner Übertragungsprotokolle erlauben hohe Übertragungskapazitäten, die auch den Transfer bewegter Bilder erlauben. Man spricht in diesem Zusammenhang von Informations-Highways oder Datenautobahnen. Solche Hochgeschwindigkeitsnetze sind notwendig für Multimedia-Anwendungen. Der überwiegend begrenzte Einsatz von IuK auf den geschäftlichen Bereich gehört der Vergangenheit an.
Die Miniaturisierung und Leistungssteigerung der Informationstechnik führte zu einem eindeutig verbesserten Preis-Leistungsverhältnis und zu einer sprunghaften Zunahme der Anwendung der Informationsverarbeitung in allen Bereichen des gesellschaftlichen Lebens. Für Massensoftware, die sich durch einen wesentlich verbesserten Benutzerkomfort auszeichnet, ist ein Preisverfall zu verzeichnen. Standardsoftware wird immer komplexer und erschließt immer neue Anwendungen, wobei implementierte Sicherheitsfunktionen mit den wachsenden Anforderungen auf diesem Gebiet nicht Schritt halten.
Computer gehören schon zur Standardausrüstung vieler privater Haushalte. Von 100 Einwohnern verfügen allein in den USA 30 über einen PC, in Deutschland sind es zwölf und in Japan erstaunlicherweise erst acht. Daneben kommen tragbare Computer (Laptops), elektronische Notizbücher (Notebooks) und mobile Datenerfassungsgeräte immer mehr zum Einsatz (siehe Punkt 15.8). Die Sicherheit, ordnungsgemäße Verarbeitung und Kontrolle der auf solchen nicht ortsgebundenen Computern gespeicherten personenbezogenen Daten ist datenschutzrechtlich nicht unbedenklich.
Parallel zur zentralen Datenverarbeitung in Rechenzentren hat sich durch den Einsatz von Arbeitsplatzcomputern eine dezentrale Datenverarbeitung entwickelt. Derzeit erfolgt eine zunehmende Vernetzung von Einzel-PC auch unter Einbeziehung öffentlicher Übertragungsmedien. Der Einsatz lokaler Netze (LAN) ist in vielen Bereichen schon vollzogen (siehe Punkt 15.6). Lokale Netze werden über größere Entfernungen zu Weitverkehrsnetzen (WAN) verbunden und können gleichzeitig mit der Großrechnerwelt kommunizieren. Die Nutzung offener weltweiter Netzwerkdienste, wie Internet, Compuserve etc., ist für jedermann möglich.
Mitte 1995 gab es in Deutschland ca. 750.000 Datex-J, 250.000 Internet - sowie 100.000 Compuserve - Anschlüsse.
Zunehmend entwickelt sich eine integrierte Multimedia-Kommunikationsinfrastruktur. Dienste auf der Basis moderner

Kommunikationstechnik prägen immer mehr unseren Alltag. Interaktives Fernsehen, Telebanking, Teleshopping, Teleworking, Telelearning und elektronischer Post- und Dokumentenaustausch sind nur einige Beispiele hierfür. Mit dem dienstintegrierenden Telekommunikationsnetz (ISDN) der Telekom können unter einer einheitlichen Nummer bisher getrennte Dienste wie Sprache, Telefax, Telex und Dokumentenaustausch ausgeführt werden.
Statt analoger Technik wird immer mehr digitale Technik eingesetzt, welche eine computergestützte Verarbeitung der übertragenen Nachrichten ermöglicht. Als ISDN-Telekommunikationsanlagen (siehe Punkt 15.7) bezeichnete Computer übernehmen die Vermittlung und Registrierung von Telefongesprächen.
Überdurchschnittlich wächst der Markt der Mobilkommunikation. Schätzungen besagen, daß ca. 350 Millionen Teilnehmer im Jahr 2000 drahtlose Sprach- und Datenübertragungsdienste nutzen werden. Etwa 10 Prozent der Mobiltelefonteilnehmer in Europa nutzen schon derzeit Datenkommunikations- und Faxdienste. Mit zunehmender Zahl der privaten Netzbetreiber werden auch diese Dienste wachsen.
Allerorten auf dem Vormarsch befinden sich Chipkarten (siehe Punkt 15.10), die sowohl mit Speicherchips als auch mit Prozessorchips ausgestattet sind. Karten mit Speicherchips, welche das Schreiben und Lesen bestimmter Daten auf der Karte ermöglichen, befinden sich schon längere Zeit im Einsatz, z. B. als Telefonkarte und Krankenversichertenkarte. Momentan steht der massenhafte Einsatz von Karten mit einem intelligenten Speicher oder Mikrocontroller an, die auch als SmartCard bezeichnet werden. Diese Karten besitzen einen eigenen Steuerungsprozessor, mit dem sich Routinen für vielfältige Aufgaben - von der Datenverwaltung bis zu Verschlüsselungsalgorithmen - programmieren lassen. Je nach Programmierung kann eine Karte somit ganz bestimmte Funktionen für eine oder, wenn es das Chipkarten-Betriebssystem zuläßt, für mehrere Anwendungen (multifunktional) realisieren. Insbesondere im Zahlungsverkehr und im Gesundheitswesen ist der Einsatz solcher intelligenter Karten in der Diskussion. Entsprechende Pilotprojekte befinden sich schon in der Testphase.
Die beispielhaft aufgezeigten Entwicklungen in der IuK tragen natürlich auch vielfältige Gefahren für einen Mißbrauch von Daten in sich. Risiken ergeben sich für die Absicherung des Rechtes auf informationelle Selbstbestimmung bzw. für den Schutz personenbezogener Daten. Der Datenschutz muß sich diesen neuen Herausforderungen stellen.
Insbesondere die Vertraulichkeit und die Integrität (Schutz vor Manipulationen) personenbezogener Daten sind durch den Einsatz der neuen Technologien gefährdet. Im Internet (siehe Punkt 15.13) z. B. gibt es keinen Datenschutz. Jeder Benutzer hinterläßt hier seine persönlichen Spuren und nationale Datenschutzrechte gelten nur bedingt.
Der vorgesehene Einsatz von Chipkarten im Gesundheitswesen (siehe Punkt 11.10) zum Speichern der kompletten Krankengeschichte einschließlich EKG, Laborbefunden, Röntgenbildern und medikamentösen Daten, wirft zahlreiche datenschutzrechtliche Probleme auf. Im Mittelpunkt stehen auch technische Fragen zum Schutz der Patientendaten vor unbefugter Kenntnisnahme und Manipulation sowie eines Einsatzes der Karte in einer hinreichend gesicherten infrastrukturellen IuK-Umgebung.
Digitale Telekommunikationsanlagen, Sprach- und Datenübermittlungsdienste, Mobilfunk- und Multimedia-Dienste zeichnen sogenannte Verbindungsdaten auf, aus denen Kommunikationsprofile der Benutzer erstellt werden können. Wer, wann mit wem kommunizierte, ist somit problemlos festzustellen. Aber auch Bewegungsprofile, wer sich wann wo aufhielt, können zum Beispiel über Nutzer des Mobilfunks oder über Besitzer von Chipkarten, welche als personenbezogene Buchungskarte für nicht anonymisierte Zahlungsvorgänge eingesetzt werden, angefertigt werden. Eine elektronische Autobahnmaut (siehe Punkt 15.15.1) oder die Einführung elektronischer Geldbörsen (siehe Punkt 15.15.3) sind in diesem Sinne aktuelle Themen mit datenschutzrechtlicher Brisanz.
Eine Minimierung der aufgezeigten Risiken für das Persönlichkeitsrecht Betroffener erfordert zwingend schon bei der Konzeption und der Entwicklung von IuK-Vorhaben datenschutzrechtliche Aspekte zu beachten und umzusetzen. Eine auf das unbedingt notwendige Maß beschränkte transparente Erhebung und Verarbeitung personenbezogener Daten, die Beachtung der Zweckbindung dieser Daten sowie ein technisch integrierter Datenschutz sind diesbezügliche unverzichtbare grundsätzliche Forderungen. Die Sensibilisierung der Bevölkerung bezüglich der Wahrnehmung ihres Rechtes auf informationelle Selbstbestimmung entsprechend dem Volkszählungsurteil zwingt in zunehmendem Maße auch die IuK-Industrie, diese Belange ernst zu nehmen, und intensiver an Lösungen von offenen Problemen in Bereichen von Datenschutz und Datensicherheit zu arbeiten. Teilerfolge sind insoweit zu verzeichnen, als daß Forderungen des Datenschutzes zunehmend nicht mehr als Behinderung angesehen, sondern aufgegriffen, in Produkte integriert und erfolgreich vermarktet werden.

15.2 Grundsätze

Im Berichtszeitraum war festzustellen, daß bei öffentlichen Stellen im Umgang mit EDV teilweise Unsicherheiten bei der Anwendung datenschutzrechtlicher Vorschriften bestehen. Dies ist u. a. damit zu erklären, daß einige grundlegende Begriffe des ThürDSG nicht mit den gebräuchlichen Begriffen der EDV deckungsgleich sind. Daher sollen diese grundlegenden Begriffe in bezug auf die Anwendung in der EDV kurz erläutert werden.
Der Begriff **Verarbeiten** wird datenschutzrechtlich umfassender ausgelegt, als er datenverarbeitungstechnisch gebräuchlich ist. Er umfaßt nach § 3 Abs. 3 ThürDSG das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten und nicht nur das arithmetische und logische Verknüpfen derselben. Zur “Datenverarbei-

tung" gehört nach dem ThürDSG auch der Umgang mit Daten in Karteien und Akten. "Datenverarbeitung" ist somit nicht nur auf die automatisierte Verarbeitung von Daten im Sinne der Informationstechnik beschränkt. Datenschutzrechtliche Grundsätze gelten damit unabhängig von der Art und Weise der Verarbeitung personenbezogener Daten. Allerdings unterscheidet das ThürDSG in einzelnen Vorschriften zwischen einer Verarbeitung personenbezogener Daten in Dateien und einer Verarbeitung in Akten. Der datenschutzrechtliche Begriff "Datei" unterscheidet sich dabei von dem in der Informationsverarbeitung definierten Dateibegriff. Im ThürDSG wird eine Datei als eine Sammlung personenbezogener Daten bestimmt. Neben automatisierten Dateien, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden können, gehören hierzu auch nicht automatisierte Datenbestände, welche gleichartig aufgebaut sind und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden können (z. B. Karteien). Alle in den öffentlichen Stellen geführten automatisierten Dateien mit personenbezogenen Daten müssen dem TLfD zum Datenschutzregister gemeldet werden (siehe Punkt 1.1.6).
Nutzen ist nach § 3 Abs. 4 ThürDSG jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeiten handelt.
Nach dem Grundsatz der Erforderlichkeit ist das Speichern, Verändern und Nutzen personenbezogener Daten nur zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist (§ 20 Abs. 1 ThürDSG). Dies bedeutet aber auch, daß der einzelne Mitarbeiter nur auf die Daten zugreifen und diese verarbeiten darf, welche er für die Erfüllung seiner Aufgaben benötigt.
Der Grundsatz der Zweckbindung besagt, daß personenbezogene Daten nur für die Zwecke geändert oder genutzt werden, für die sie erhoben oder gespeichert worden sind (§ 20 Abs. 1 ThürDSG). Für das Verarbeiten und Nutzen personenbezogener Daten sind nach dem ThürDSG die Grundsätze der Erforderlichkeit, der Zweckbindung und der Verhältnismäßigkeit zu beachten.
§ 9 ThürDSG bestimmt, daß öffentliche Stellen, die personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen haben, die erforderlich sind, um die Ausführung des Gesetzes zu gewährleisten. Diese Verpflichtung zur Durchführung von Datensicherungsmaßnahmen gilt für jegliche Verarbeitung personenbezogener Daten, unabhängig davon, ob diese automatisiert oder nichtautomatisiert erfolgt. Nach § 9 Abs. 1 ThürDSG gilt hierfür der Grundsatz der Verhältnismäßigkeit: "Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."
Die zu vollziehenden Schutzmaßnahmen sind auf die Aufgaben des Datenschutzes ausgerichtet. Sie zielen auf den gesetzmäßigen Umgang mit personenbezogenen Daten ab, d. h. auf den Schutz von Rechtsgütern für diese Person. Das betreffende Schutzobjekt sind also Personen und nicht ausschließlich nur deren Daten.
Das Spektrum und der Wirkungsbereich der technischen und organisatorischen Maßnahmen zum Datenschutz muß somit umfangreicher sein als die herkömmlichen Maßnahmen einer rein technischen Datensicherung. In der Regel steht bei dieser nur die Absicherung der Integrität und der Reproduzierbarkeit der Daten (bei Verlust) im Vordergrund. Dabei wird nicht unterschieden zwischen befugter und unbefugter Kenntnisnahme personenbezogener Daten entsprechend dem Grundsatz der Erforderlichkeit.
Die Datensicherheit im Sinne des Datenschutzes umfaßt dagegen Anforderungen, die sowohl eine störungsfreie als auch eine gegen den Mißbrauch von personenbezogenen Daten geschützte Datenverarbeitung zum Ziel haben. Technische Maßnahmen beziehen sich auf gebäudespezifische und räumliche Absicherungen sowie auf software- und hardwaretechnische Einrichtungen. Bezüglich der automatisierten Datenverarbeitung kann ein wirksamer technischer Datenschutz nur gewährleistet werden, wenn dem Aspekt der Sicherheit in informationstechnischen Systemen Rechnung getragen wird. Ohne IT (Informationstechnik) -Sicherheit kann die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Verbindlichkeit von Daten nicht sichergestellt werden. In diesem Sinne bedeuten:
- Vertraulichkeit, daß nur Befugte Zugriff auf die Daten besitzen und diese zur Kenntnis nehmen können;
- Integrität, daß nur Befugte die Daten in zulässiger Weise modifizieren (ändern, löschen) dürfen und möglichen Modifikationen der Daten durch technische Funktionsstörungen vorgebeugt wird;
- Verfügbarkeit, daß Befugte entsprechend ihren Rechten auf die Daten zugreifen können und die Funktionalität des IT-Systems nicht beeinträchtigt ist;
- Verbindlichkeit, daß die Daten inhaltlich korrekt sind und von dem angegebenen Urheber stammen.

Schwachstellen (Fehler, Mängel, Defekte) im Design oder bei der Implementierung eines Informationssystems können die IT-Sicherheit gefährden. Auch fehlende oder unzureichende Regelungen bezüglich des Umgangs mit personenbezogenen Daten schaffen einen Freiraum für Bedrohungen. Ein Schutz der Daten vor Mißbrauch, Verfälschung oder physischem Verlust kann somit nicht mehr gewährleistet werden. Eine Gefährdung der IT-Sicherheit hat also unmittelbar negative Auswirkungen auf die Gewährleistung eines wirksamen Datenschutzes.
Eine Bedrohung für die Sicherheit der Daten kann von einer ungenügenden oder nicht geeigneten technischen Ausstattung bezüglich der eingesetzten Hard- und Software oder einer nur mangelhaften räumlichen Abschottung der IT-Geräte ausgehen. Irrtum und Nachlässigkeit beim Anwenden getroffener Datensicherungsmaßnahmen, Fehler bei der Eingabe von Daten und der Bedienung des EDV-Systems sowie gezielter Datenmißbrauch sind einige Beispiele für eine Bedrohung, die seitens der Mitarbeiter bestehen.

Die Risiken bzw. Gefährdungen für eine sichere und sorgsame Verarbeitung von Daten sind vielfältig. Das ThürDSG schreibt deshalb keine einzelnen konkreten Datensicherungsmaßnahmen verbindlich vor, sondern überläßt es der speichernden Stelle, die geeigneten Maßnahmen entsprechend den Gegebenheiten so auszuwählen und aufeinander abzustimmen, daß die vom Gesetz geforderte Gewährleistung erreicht wird. Entscheidend ist immer der von der Gesamtheit der getroffenen Maßnahmen erzielte Schutzeffekt.
In § 9 Abs. 2 ThürDSG werden jedoch im Hinblick auf die automatisierte Datenverarbeitung konkrete Anforderungen definiert, die in einem angemessenen Verhältnis zum Schutzzweck durch geeignete Maßnahmen bzw. Sicherheitsmechanismen zu realisieren sind. Obwohl diese Anforderungen vorrangig auf die automatisierte Datenverarbeitung abzielen, trifft ein Teil von ihnen ebenso für die nicht-automatisierte Datenverarbeitung zu. Hinsichtlich ihrer Zielorientierung können die Anforderungen in drei Gruppen klassifiziert werden.

1. Auf eine vorbeugende Vermeidung datenschutzrechtlicher Risiken zielen die Anforderungen:
   - Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren (Zugangskontrolle),
   - unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verhindern (Datenträgerkontrolle),
   - unbefugte Eingabe, Kenntnisnahme, Veränderung oder Löschung von Daten im Speicher zu verhindern (Speicherkontrolle),
   - unbefugtes Nutzen von EDVA mit Einrichtungen zur Datenübertragung zu verhindern (Benutzerkontrolle),
   - Überschreiten der rechtmäßigen Zugriffsberechtigung zu verhindern (Zugriffskontrolle),
   - unbefugtes Lesen, Kopieren, Verändern und Löschen bei der Übertragung von Daten und bei dem Transport von Datenträgern zu verhindern (Transportkontrolle).
2. Den Einsatz von Kontrollmechanismen bezüglich einer Beweissicherung der durchgeführten Datenverarbeitung verlangen die Anforderungen:
   - Prüfbarkeit der möglichen Empfänger bei Datenübermittlungen (Übermittlungskontrolle) und
   - zeitliche und personelle Prüfbarkeit der Dateneingabe (Eingabekontrolle).
3. Bezug auf organisatorische Regelungen nehmen die Anforderungen:
   - weisungsgemäße Auftragsverarbeitung zu gewährleisten (Auftragskontrolle) und
   - Gestaltung der Organisation der öffentlichen Stellen unter Berücksichtigung der Anforderungen des Datenschutzes (Organisationskontrolle).

Für die nichtautomatisierte Verarbeitung personenbezogener Daten werden gemäß § 9 Abs. 3 ThürDSG gleichfalls entsprechende Datensicherungsmaßnahmen gefordert. Damit weist der Gesetzgeber ausdrücklich darauf hin, daß auch für die nichtautomatisierte Verarbeitung personenbezogener Daten notwendige Schutzmaßnahmen festzulegen sind. Damit soll eine datenschutzrechtliche Abwertung der manuellen Verarbeitung personenbezogener Daten verhindert werden.

Einige grundsätzliche Empfehlungen zum Datenschutz bei Arbeitsplatzrechnern und anderen IT-Geräten sind in der Anlage 35 enthalten.

15.3 Das Schutzstufenkonzept - eine Basis für den technischen Datenschutz

Durchgeführte Prüfungen ergaben, daß Datensicherungsmaßnahmen im Sinne des ThürDSG nicht immer konsequent durchgeführt bzw. umgesetzt werden. Unsicherheiten bestehen z. B. in der Auswahl geeigneter technischer Maßnahmen, die einen angemessenen Schutz der Daten entsprechend ihrer Sensibilität gewährleisten. Es zeigt sich aber mitunter auch eine gewisse Sorglosigkeit beim Umgang mit personenbezogenen Daten. Fehlende oder unzureichende Datenschutz- und Datensicherheitskonzepte offenbaren, daß die Gefahren und Risiken bezüglich des Schutzes der Daten insbesondere beim Einsatz automatisierter Verfahren unterschätzt werden. Intuitiv oder sporadisch festgelegte Sicherheitsmaßnahmen erzeugen eine gefährliche Scheinsicherheit.
Im folgenden sollen einige Grundsätze bei der Auswahl von Datensicherungsmaßnahmen unter Berücksichtigung eines Schutzstufenkonzeptes aufgezeigt werden:
Das Schutzobjekt der Datensicherungsmaßnahmen sind die zu verarbeitenden personenbezogenen Daten. An ihren konkreten Gefährdungen haben sich die technischen und organisatorischen Maßnahmen zu orientieren. Ein wesentlicher Gradmesser für den notwendigen Schutzbedarf der Daten stellt ihre Sensibilität dar. Je sensibler die zu verarbeitenden Daten sind, um so höher ist ihr Schutzbedarf; ein zunehmender Aufwand an Sicherungsmaßnahmen ist erforderlich. Von diesem Grundsatz ausgehend muß auch die Frage beantwortet werden, ob der geplante bzw. realisierte Schutzaufwand im konkreten Fall angemessen ist. Dies erfordert konsequenterweise von jeder speichernden Stelle, die zu schützenden personenbezogenen Daten nach dem Grad ihrer Sensibilität einzustufen, um die in § 9 ThürDSG geforderten angemessenen Datensicherungsmaßnahmen festzulegen. Für eine Einstufung der Daten bezüglich ihrer Sensibilität sind allerdings in den datenschutzrechtlichen Vorschriften keine Kriterien vorgegeben. Nach dem Volkszählungsurteil des Bundesverfassungsgerichtes von 1983 gibt es infolge der automatisierten Datenverarbeitung kein belangloses Datum mehr. Der Gesetzgeber hat im ThürDSG festgelegt, die geforderten technischen und organisatorischen Maßnahmen angemessen an der Schutzwürdigkeit der Daten zu orientieren. Dabei spielen sicher auch die hiermit

verbundenen Aufwendungen, insbesondere finanzieller Art, eine Rolle. Eine Schlußfolgerung hieraus wäre, für jedes IT-Vorhaben ein spezifisches Sicherheitskonzept zu erarbeiten. Dies ist in der Regel mit einem erheblichen Aufwand verbunden und erfordert auch detaillierte Kenntnisse bezüglich der möglichen Gefährdungsrisiken und der Maßnahmen, diese Risiken abzudecken. Personell und finanziell könnten kleinere öffentliche Stellen hiermit überfordert sein. Mit Hilfe eines Schutzstufenkonzeptes lassen sich diese Aufwendungen in der Regel für IT-Anwendungen mit fixierbaren Datenobjekten reduzieren.
Ein Schutzstufenkonzept stellt eine Orientierungshilfe dar, um den Grad der Schutzwürdigkeit der Daten zu ermitteln und davon abgeleitet für diese die erforderlichen Datensicherungsmaßnahmen festzulegen. Die Schutzstufen sind in Abhängigkeit von dem Grad der Beeinträchtigung des informationellen Selbstbestimmungsrechts bei einem Mißbrauch der personenbezogenen Daten festgelegt. Der TLfD empfiehlt entsprechend dem derzeitigen Erkenntnis- und Erfahrungsstand hierfür nachfolgende Einstufungskriterien:

Stufe 0: Kein besonderer Schutzbedarf
Personenbezogene Daten aus öffentlich zugänglichen Quellen, deren Verarbeitung keine Beeinträchtigung des informationellen Selbstbestimmungsrechtes erwarten läßt und die gegen Änderungen, Verfälschungen etc. keines besonderen Schutzes bedürfen.
Beispiele: Angaben aus öffentlichen Telefon- und Adreßbüchern, Branchenverzeichnissen, amtliche Bekanntmachungen, Presseveröffentlichungen.

Stufe 1: Grundschutzbedarf
Personenbezogene Daten, deren Verarbeitung eine Beeinträchtigung des informationellen Selbstbestimmungsrechts insofern erwarten läßt, als durch einen Mißbrauch der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
Beispiele: Daten, deren Übermittlung eines berechtigten Interesses bedürfen, z. B. Daten aus öffentlichen Registern (z. B. Grundbuchauskunft, einfache Melderegisterauskunft, sofern keine Auskunftssperre vorliegt).

Stufe 2: Hoher Schutzbedarf
Personenbezogene Daten, deren Verarbeitung eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts insofern erwarten läßt, als der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann oder personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen oder deren unbefugte Kenntnis eine Gefahr für Leib, Leben oder die persönliche Freiheit des Betroffenen befürchten läßt.
Beispiele: Daten, deren Übermittlung eines rechtlichen Interesses bedürfen, Sozialdaten, Gesundheitsdaten, Steuerdaten, Personaldaten, religiöse und politische Anschauungen, Berufs- und Geschäftsgeheimnisse, Fernmeldegeheimnis, personenbezogene Daten von Personen, deren Indentität zu schützen ist (wie Adressen von polizeilichen V-Leuten, Adressen von Zeugen in bestimmten Strafverfahren etc.).

Eine Einstufung der zu verarbeitenden Daten kann nicht schematisch erfolgen. Beachtet werden müssen in jedem Fall die Besonderheiten des jeweiligen Anwendungsfalles. Die zu schützenden personenbezogenen Daten sind immer aus dem Zusammenhang ihrer Verwendung in eine Schutzstufe einzuordnen. Die Eingruppierung kann also nicht anhand eines nur isoliert betrachteten Datums erfolgen.
Für die ausgewählte Schutzstufe sind die erforderlichen technischen und organisatorischen Datensicherungsmaßnahmen nach § 9 ThürDSG festzulegen, die den notwendigen Schutzbedarf für die hier eingeordneten personenbezogenen Daten gewährleisten. Unter Beachtung der eingesetzten DV-Technik und Betriebssysteme könnten als Orientierungshilfe “standardisierte” Datensicherungsmaßnahmen hierfür vorgegeben werden. Solche Standardmaßnahmen können jedoch nicht die konkreten örtlichen Gegebenheiten und die spezifischen Besonderheiten eingesetzter Anwendungssysteme berücksichtigen. Ihr nicht schematischer Einsatz stellt jedoch eine Hilfestellung für den normalen Anwender dar, um zumindest einen Grundschutz mit technischen und organisatorischen Maßnahmen zu gewährleisten.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem IT-Sicherheitshandbuch und dem IT-Grundschutzhandbuch zwei Orientierungshilfen mit dem Ziel herausgegeben, die Sicherheit von IT-Systemen und der zu verarbeitenden Daten zu gewährleisten. Die Absicherung der Verfügbarkeit, der Integrität und der Vertraulichkeit der Daten sind auch datenschutzrechtliche Zielvorgaben.
In beiden Handbüchern stehen Aspekte der IT-Sicherheit im Vordergrund, wobei auf datenschutzrechtliche Gesichtspunkte primär nicht eingegangen wird. Die ausgewiesenen Technologien und Schutzmaßnahmen können jedoch die Basis für einen ausreichenden technischen Datenschutz bilden, wenn sie differenziert unter Beachtung des Grades der Schutzwürdigkeit der abzusichernden personenbezogenen Daten ausgewählt werden.
Nach Erfahrungen des BSI ist für etwa 80 Prozent der IT-Anwendungen ein Grundschutz ausreichend. Die hierfür erforderlichen Sicherungsmaßnahmen und -mechanismen sind im IT-Grundschutzhandbuch aufgeführt. Diese Maß-

nahmen gewährleisten einen angemessenen Schutz für personenbezogene Daten, welche entsprechend dem aufgezeigten Schutzkonzept in die Schutzstufe 1 einzuordnen sind.
Eine solche konfektionierte Sicherheitslösung ist allerdings in der Regel nicht ausreichend für IT-Anwendungen, die personenbezogene Daten verarbeiten, deren Schutzbedarf der Klasse 2 entspricht.
In diesem Fall muß ein spezifisches Sicherheitskonzept erarbeitet werden, das gegenüber dem Grundschutz eine maßgeschneiderte Sicherheitslösung darstellt. Ein solches Konzept ist ausgehend von einer Bedrohungs- und Risikoanalyse zu erstellen. Das IT-Sicherheitshandbuch des BSI bietet hierfür viele hilfreiche Anregungen und Hinweise.
Zur Gewährleistung eines ausreichenden Datenschutzes bei der Verarbeitung personenbezogener Daten wird im Interesse der Betroffenen sowie einer angemessenen Datensicherheit hinsichtlich eines ordnungsgemäßen Datenverarbeitungsbetriebes je nach Behördengröße und Umfang der Datenverarbeitung folgende Sicherheitsstrategie empfohlen:

1. Einrichten eines IT-Sicherheitsmanagements
   Bildung einer Projektgruppe für IT-Sicherheit , in der je nach Sachlage Vertreter folgender Bereiche ihre Kenntnisse und Erfahrungen einbringen sollten:
   EDV/Organisation, Fachabteilungen, Benutzer, Sicherheitsbeauftragter, Datenschutzbeauftragter und Personalrat.
   Aufgabe dieser Projektgruppe wären u. a. das Definieren und Aktualisieren der IT-Sicherheitsziele unter Beachtung auch datenschutzrechtlicher Anforderungen, das Erstellen und Aktualisieren von IT-Sicherheitskonzepten und das Aufstellen eines Realisierungsplanes zur Umsetzung der Maßnahmen.
2. Ermittlung der Schutzbedürftigkeit
   Alle vorhandenen und geplanten IT-Systeme sind mit ihren Anwendungen und zu verarbeitenden Daten in die Ermittlung einzubeziehen.
   Anhand einer Analyse der zu verarbeitenden Daten sind die vorhandenen personenbezogenen Informationen in eine der aufgezeigten Schutzstufen unter Beachtung des Verwendungszusammenhangs einzuordnen (siehe oben).
   Der Schutzbedarf für ein IT-System ergibt sich immer aus dem Schutzbedarf seiner bedürftigsten Anwendung.
3. Bedrohungs- und Risikoanalyse
   Wird nach 2. ein Grundschutz als Schutzbedarf ermittelt (Zuordnung der Daten in Schutzstufe 1), so werden technische und organisatorische Sicherheitsmaßnahmen entsprechend dem IT-Grundschutzhandbuch des BSI als angemessen und ausreichend angesehen. Die möglichen Bedrohungen bzw. Gefährdungen für die IT-Systeme bezüglich der zu verarbeitenden Daten können aus den entsprechenden Katalogen des Grundschutzhandbuches entnommen und zusammenfassend dargestellt werden. Mittels einer Risikoanalyse sind die Risiken zu bestimmen.
   Wird nach 2. ein hoher Schutzbedarf festgestellt (Zuordnung der Daten in Schutzstufe 2), sollte über die Einbeziehung des Grundschutzhandbuches hinaus eine individuelle Bedrohungs- und Risikoanalyse durchgeführt werden. Diese sollte anhand des IT-Sicherheitshandbuches vom BSI erfolgen.
4. Sicherheitskonzept
   Durch die Auswahl und Bewertung von Sicherheitsmechanismen sollen die unter 3. ermittelten Risiken auf ein auch aus datenschutzrechtlicher Sicht akzeptables Niveau reduziert werden. Dazu werden geeignete Mechanismen identifiziert und den Bedrohungen zugeordnet.
   Ein Sicherheitskonzept muß zur Umsetzung der gestellten Sicherheitsanforderungen sowohl organisatorische und technische Maßnahmen vorsehen, wobei diese immer im Zusammenhang zu betrachten sind.
   Die erforderlichen Maßnahmen sind für das konkrete IT-System aus dem Maßnahmekatalog des Grundschutzhandbuches unter Berücksichtigung der unter 3. ermittelten Risiken auszuwählen.
   Falls nach 2. ein hoher Schutzbedarf festgestellt wurde, ist aufbauend auf der durchgeführten individuellen Riskoanalyse ein individuelles Sicherheitskonzept zu erstellen. Hier sind über das Grundschutzhandbuch hinaus zusätzliche Maßnahmen zu realisieren, wie z. B. Verschlüsselung der Daten, digitale Signatur, umfassende Protokollierung, Einschränkung von Datenmasken.
   Nachdem die Maßnahmen festgelegt, ihre Wirkungen verbal beschrieben und mit den technischen, organisatorischen und rechtlichen Gegebenheiten der verarbeitenden Stelle abgestimmt sind, ist das Restrisiko zu analysieren und eine Kosten-Nutzen-Betrachtung anzustellen. Eventuell sind angemessenere oder kostengünstigere Maßnahmen auszuwählen, um die angestrebte Sicherheit zu gewährleisten.

15.4 Kooperative Arbeit im IMA-IT

Im Freistaat Thüringen wird die Koordinierung des Einsatzes von Informationstechnik für die Landesverwaltung durch den interministeriellen Ausschuß für Informationstechnik (IMA-IT) wahrgenommen. Der Ausschuß wurde durch Kabinettsbeschluß vom 22.01.1991 eingerichtet und arbeitet ministerienübergreifend. Im IMA-IT sind die Staatskanzlei und jedes Ressort durch je einen Beauftragten mit Stimmrecht vertreten. Der TLfD, der Thüringer Rechnungshof und der Thüringer Landtag nehmen als beratende Mitglieder an den Sitzungen teil. Alle zwei Jahre wählen die stimmberechtigten Mitglieder einen Vorsitzenden. Diese Funktion wird zur Zeit von dem Vertreter des TIM wahrgenommen.

Der IMA-IT stellt ein wichtiges Gremium für den TLfD dar, um die Entwicklung der Informations- und Kommunikationstechnik in der Landesverwaltung unter datenschutzrechtlichen Aspekten zu beobachten und kritisch zu begleiten (§ 40 Abs. 5 ThürDSG).
Leider gibt es für die Kommunalverwaltungen keinen Ausschuß mit analogen Aufgaben. Hier wäre aus der Sicht des Datenschutzes eine koordinierende Stelle ebenfalls von Vorteil, um alle aktuellen Aufgaben effektiver erfüllen zu können. Eine entsprechende Initiative vom Landkreistag und Gemeinde- und Städtebund für die Einrichtung einer solchen Koordinierungsstelle würde der TLfD begrüßen.
Mit Rundschreiben des TIM vom 25. März 1993 sind in der Thüringer Landesverwaltung Richtlinien für den Einsatz der Informationstechnik (Stand: 14. Mai 1992) verbindlich eingeführt worden. Im Abschnitt 1.3 -rechtliche Rahmenbedingungen- wird hier auf die Beachtung der Datenschutzvorschriften hingewiesen. U. a. ist in den IT-Richtlinien festgelegt, daß die obersten Landesbehörden einen IT-Ressortplan führen, der die IT-Vorhaben und Verfahren, beginnend mit dem jeweiligen Haushaltsjahr, für einen Zeitraum von drei Jahren enthält und jährlich fortzuschreiben ist.
Mit Stand vom 16. Juni 1994 sind vom IMA-IT verbindliche Regelungen für den Aufbau von IT-Ressortplänen beschlossen worden. Hierin sind die Forderungen des TLfD zur Sicherstellung des Datenschutzes aufgegriffen worden und bei den Maßnahmen zur IT-Sicherheit sowohl für die konzeptionelle IT-Gesamtplanung einbezogen als auch bei den einzelnen IT-Vorhaben oder -Verfahren berücksichtigt worden.
Dem IMA-IT sind alle IT-Konzepte und konkrete IT-Vorhaben zur Begutachtung vorzulegen, deren Gesamtwert 100.000 DM überschreiten. Diese IT-Konzepte werden im Umlaufverfahren auch dem TLfD angezeigt.
Im Rahmen der personellen Möglichkeiten prüft der TLfD die IT-Konzepte, in welchen eine Verarbeitung personenbezogener Daten ansteht, auf die vorgesehenen bzw. realisierten Maßnahmen zum Datenschutz. Bisher war allerdings festzustellen, daß etwa die Hälfte der IT-Konzepte unter den verbindlich vorgegebenen Gliederungspunkten vollkommen unzureichend diesbezügliche Aussagen enthalten. So beschränken sich manche auf unverbindliche lapidare Standardaussagen wie “die datenschutzrechtlichen Vorschriften werden eingehalten” oder “den datenschutzrechtlichen Erfordernissen wird Rechnung getragen” als einzigen Hinweis. Der TLfD wird hier weiterhin beim IMA-IT darauf dringen, solche IT-Konzepte erst zu bestätigen, wenn ein Datensicherheitskonzept mit angemessenen Maßnahmen nach § 9 ThürDSG bezüglich der Schutzwürdigkeit der zu verarbeitenden Daten nachgereicht wird.
Ein wirksamer Schutz personenbezogener Daten verlangt schon bei der Planung von IT-Vorhaben, die datenschutzrechtlichen Risiken abzuklären, die erforderlichen technischen und organisatorischen Maßnahmen festzulegen und die hierfür erforderlichen materiellen und finanziellen Aufwendungen für ihre Realisierung als feste Größen einzuplanen.

15.5 Ausgewählte IT-Projekte der Landesverwaltung

15.5.1 Corporate Network

Eine Arbeitsgruppe des interministeriellen Ausschusses für Informationstechnik (IMA-IT) hat eine Konzeption für einen interministeriellen Kommunikationsaustausch für Sprache, Bilder und Daten über ISDN-fähige Festverbindungen erarbeitet. Im Kern geht es darum, die im erweiterten Ortsbereich Erfurt/Weimar in den Landeseinrichtungen vorhandenen digitalen Telekommunikations (TK)-Anlagen und Rechnersysteme bzw. lokale Netze (LAN) zu vernetzen. Als Hauptargument für die Vernetzung werden in dem Konzept wirtschaftliche Gründe angeführt.
Vorgesehen ist eine sternförmige Vernetzung der jeweiligen TK-Anlagen nach dem Nebenstellenprinzip mit einer TK-Hauptanlage und der LAN mit einem zentralen Datenvermittlungsknoten. Dabei soll die Übertragung von Sprache und Daten über gemeinsam genutzte digitale Festverbindungen in Form eines privaten Netzes erfolgen. Ein solches Corporate Network (CN) bietet eine weitgehende Unabhängigkeit von öffentlichen Netzbetreibern.
Eine derartige Vernetzung zur Übertragung von Sprache und Daten ermöglicht einerseits die Einführung effizienterer Arbeitsmethoden, beinhaltet andererseits aus datenschutzrechtlicher Sicht und unter Aspekten der informationstechnischen Sicherheit jedoch auch erhebliche Gefahren.
In seiner Stellungnahme zu dem o. g. Konzept setzte sich der TLfD intensiv mit den hiermit verbundenen Gefahren aus der Sicht des Datenschutzes auseinander und zeigte datenschutzrechtliche Aspekte bzw. Forderungen auf, die beim Aufbau eines solchen Netzes schon in der Planungsphase zwingend zu beachten sind. Aus der Sicht des Datenschutzes kann ein solches ressortübergreifendes Netz mit erheblichen Risiken für das Grundrecht auf informationelle Selbstbestimmung verbunden sein. Die informationelle Trennung zwischen den verschiedenen Aufgaben und den dazu erforderlichen personenbezogenen Daten wird bei einem solchen behördenübergreifenden Netz mit einheitlichen Schnittstellen zumindest hardwaremäßig aufgehoben. Die mit der interministeriellen Vernetzung verbundene Tendenz des Zusammenwachsens der Ressorts zu einem informatorischen Ganzen ist somit datenschutzrechtlich nicht unbedenklich. Hierbei ist generell zu beachten, daß trotz einer vernetzten IuK-Infrastruktur die angeschlossenen Ressorts informationell weiterhin abgeschlossene Einheiten bilden müssen, die wiederum aus informationell abgeschotteten Untereinheiten bestehen. Der Aufbau technischer Schnittstellen zwischen verschiedenen IT-Verfahren in den Ressorts

oder zwischen diesen ist nur dann gerechtfertigt, wenn die wahrzunehmenden Aufgaben einen entsprechenden Informationsfluß gesetzlich zulassen. Diesem Grundsatz muß auch die zukünftige Informations- und Kommunikationsinfrastruktur in und zwischen den öffentlichen Stellen Rechnung tragen.
Mit der Integration von EDV-Technik durch Netze werden die zentral gespeicherten Daten prinzipiell netzweit verfügbar und könnten von Unbefugten genutzt werden. Dies gilt insbesondere angesichts der Tatsache, daß die für Netze verfügbaren Datenschutzmechanismen mit der zunehmenden Funktionalität solcher Systeme bisher nicht Schritt halten konnten.
Die Gewährleistung von Datenschutz und Datensicherheit kann nur durch das Zusammenwirken arbeitsorganisatorischer, personeller und informationstechnischer Maßnahmen erfolgen. Die Kommunikationsteilnehmer müssen deshalb umfassend und verständlich über die ihnen zur Verfügung gestellten Systemfunktionen und die gespeicherten Daten informiert werden.

Das ThürDSG enthält keine ausdrücklichen Regelungen darüber, unter welchen datenschutzrechtlichen Voraussetzungen das konzipierte CN eingerichtet werden kann. Grundsätzlich gilt aber, daß eine Verarbeitung oder Nutzung personenbezogener Daten nur dann zulässig ist, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat (§ 4 Abs. 1 ThürDSG).
Neben der allgemeinen Gültigkeit des ThürDSG sind insbesondere die folgenden Regelungen dieses Gesetzes zu beachten:
- § 6 Datengeheimnis
- § 7 Automatisiertes Abrufverfahren
- § 9 Technische und organisatorische Maßnahmen
- § 10 Anlagen- und Verfahrensverzeichnis
- § 20 Datenspeicherung, -veränderung und -nutzung
- § 21 Datenübermittlung innerhalb des öffentlichen Bereichs
- § 22 Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs

Nach § 3 Abs. 3 ThürDSG gehört definitionsgemäß zum Begriff “Verarbeiten von Daten” auch das “Übermitteln von Daten”. Die rechtliche Zulässigkeit der Übermittlung personenbezogener Daten innerhalb des öffentlichen Bereichs wird in § 21 ThürDSG geregelt, wobei auf die Übertragungswege kein Bezug genommen wird. Spezialgesetzliche Regelungen zum Datenschutz können weitergehende Spezifizierungen enthalten. Nach § 21 ThürDSG ist die Übermittlung zulässig, wenn sie zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und die Zweckbindung der Daten entsprechend den Vorschriften des § 20 ThürDSG beachtet wird. Auch für Datenübermittlungen zwischen öffentlichen Stellen, die miteinander vernetzt sind, ist der Grundsatz der Zweckbindung zu beachten, analog wie bei einer Datennutzung innerhalb einer öffentlichen Stelle. Für die Einhaltung dieses Grundsatzes sind die Ressorts in eigener Verantwortung zuständig. Automatisierte Abrufverfahren dürfen nur unter Beachtung der in § 7 ThürDSG aufgeführten Regelungen eingerichtet werden.
Der Grundsatz der Vernetzung, wonach theoretisch jeder mit jedem kommunizieren kann, ist aus der Sicht des Datenschutzes besonders kritisch zu bewerten. Die Möglichkeit berechtigter Netzteilnehmer, personenbezogene Daten netzweit zur Verfügung zu stellen, darf nicht unterschätzt werden.
Datensicherheitsrisiken, welche das Lesen, das Verändern oder das Einfügen von (personenbezogenen) Daten durch Unbefugte in einem Kommunikationsnetz ermöglichen, sind im Punkt 15.6 aufgeführt.
Die im Konzept für das CN über den neutralen Vermittlungsknoten vorgesehene Punkt-zu-Punkt-Verbindung zwischen dem Absender und dem Empfänger von Daten sowie der Einsatz digitaler Festverbindungen sind Maßnahmen, die der Sicherstellung der Vertraulichkeit dienen. Der Anschluß von lokalen Netzen der Ressorts an das CN kann die Gefahr eines unberechtigten Zugriffs auf diese Netze verstärken. Laut Konzept soll der Anschluß über Router erfolgen. Zur Minimierung des Risikos unberechtigter Zugriffe auf diese Netze sollten die Router über filternde Funktionen verfügen. Der Aufbau der Routingtabellen sollte statisch, d. h. manuell durch den Netzverwalter erfolgen. Zugriffe der System- bzw. Netzverwalter auf personenbezogene oder andere sicherheitsrelevante Daten sind zu unterbinden.
Die Schnittstellen des CN zu öffentlichen Netzen bedürfen der Einführung verstärkter Sicherheitsmechanismen zur Abschottung gegen Angreifer. Geeignete Firewall-Konzepte sollten hierfür zum Einsatz kommen. Rechner und Verfahren, die personenbezogene Daten verarbeiten und entsprechend ihrer Aufgabenstellung keine Daten über das CN übermitteln müssen, sind vor jeglichen Zugriffen aus dem CN sicher abzuschotten. In die Sicherheitsbetrachtungen sollte insbesondere der zentrale Vermittlungsknoten einbezogen werden. Alternativen bei einem Ausfall dieses Knotens sind aufzuzeigen.
Für den Einsatz elektronischer Mitteilungssysteme sind die datenschutzrechtlichen Forderungen und Empfehlungen der DSB des Bundes und der Länder zu beachten (siehe Anlage 22 sowie Punkte 15.5.2 und 15.15.2).
Die Nutzung des geplanten ressortübergreifenden Kommunikations- und Datenverbundes muß somit fallbezogen und restriktiv unter Beachtung obengenannter Vorschriften erfolgen. Nicht das technisch Mögliche, sondern nur das aufgabenbezogene Notwendige darf realisiert werden.

Der Datenschutz in einem Kommunikationssystem bezieht sich im wesentlichen auf den Schutz

- des Persönlichkeitsrechts (Privatsphäre) der Teilnehmer,
- der Nutzdaten und
- der Abrechnungsdaten.

So ist sicherzustellen, daß die in ISDN-Anlagen gespeicherte Daten nur im Rahmen ihrer Zweckbestimmung verwendet werden. Die Verwendung dieser Daten für Leistungs- und Verhaltenskontrollen von Teilnehmern wäre eine unzulässige Zweckdurchbrechung. Bei Privatgesprächen ist die Speicherung von Verbindungsdaten nur in dem Umfang zulässig, in dem sie zur Überprüfung der vom Dienstherrn erstellten Telefonrechnung durch den Bediensteten erforderlich ist und eine entsprechende Dienstvereinbarung vorliegt. Sie sind zu löschen, sobald die Gebühren ohne Vorbehalt gezahlt worden sind.
Bei der Auswahl und bei der Anwendung von ISDN-Leistungsmerkmalen sollten die unter Punkt 15.7.2 aufgeführten datenschutzrechtlichen Empfehlungen zum Schutz des Persönlichkeitsrechts beachtet werden.
Die Einführung des CN stellt einen Schritt in eine neue Dimension der Nutzung moderner Kommunikationstechnologie durch die Landeseinrichtungen dar. Aufgrund der strategischen Bedeutung dieses zentralen Vorhabens wird die Erarbeitung eines Datenschutz- und Datensicherheitskonzeptes (DDK) dringend empfohlen. Vorausgehen sollte eine Risikoanalyse anhand der Kriterien des IT-Sicherheitshandbuches des Bundesamtes für Sicherheit in der Informationstechnik. Diese Risikoanalyse muß die wesentlichen Gefahren und Ansatzpunkte für die Sicherheit des CN aufzeigen und sollte auch die Grundlage für die Erarbeitung des DDK sein.

15.5.2 X.400-Verbund der Thüringer Landesverwaltung

Elektronische Mitteilungssysteme (E-Mail) dienen der Übermittlung von Nachrichten und dem Austausch von Dokumenten zwischen Teilnehmern auf elektronischem Wege. Im Gegensatz zum Telefaxdienst können hier die übertragenen Informationen direkt in digitaler Form weiterverarbeitet werden.
Für die Thüringer Landesverwaltung ist der Einsatz eines ressortübergreifenden elektronischen Mitteilungssystems auf der CCITT-Empfehlung X.400 geplant. X.400 ist ein Standard, der als Teil einer weltweiten Normierung das Übermitteln von digitalen Informationen mit einem weltweit einheitlichen Verfahren und eindeutiger Adreßstruktur ermöglicht, wobei die Integration unterschiedlicher Nachrichtenformate möglich ist.
Der elektronische Nachrichtenverkehr wird über sogenannte elektronische Postämter (Computer) kontrolliert, gesteuert und protokolliert. Ein elektronisches Postamt erfüllt äquivalente Funktionen wie eine bisherige konventionelle Poststelle in einer Verwaltung. Eingehende Nachrichten (Briefe) werden protokolliert, an die Adressaten verteilt, den Mitarbeitern bei Strukturwechsel nachgesandt sowie unkorrekte Adressen korrigiert etc.
Ein Bereich, innerhalb dessen ein bestimmter Betreiber die Verantwortung für den Betrieb seines elektronischen Mitteilungssystems selbst trägt, wird als Domäne (Versorgungsbereich) definiert. Man unterscheidet zwischen öffentlichen Domänen (Administration Management Domains-ADMD) und privaten Domänen (Private Management Domains-PRMD). Das Telebox-System der Deutschen Telekom unterstützt das Versenden von Mitteilungen zwischen unterschiedlichen Domänen, wie z. B. von einer öffentlichen Domäne zu einer privaten Domäne. Laut einer vom TLRZ im Auftrag des IMA-IT erarbeiteten Konzeption ist folgendes vorgesehen:
Die gesamte Thüringer Landesverwaltung bildet eine private Domäne (PRMD) mit dem Namen “thueringen”. Innerhalb dieser PRMD erfolgt die Kommunikation zwischen allen Struktureinheiten der Landesverwaltung über das Landesdatennetz (LDN). Jedes Ressort ist als Subdomäne eingegliedert.
Globale Aufgaben innerhalb der PRMD werden von einer einzurichtenden X.400-Landeskopfstelle übernommen. An diese zentrale Poststelle (zentraler MTA) werden die jeweils in den Ressorts einzurichtenden lokalen Postämter (Kopfstellen-MTA) über das LDN angeschlossen. Der Zugriff sogenannter remote UA (entfernter Zugriff von einem seperaten Rechner) auf die Landeskopfstelle ist für kleinere Ressorts vorgesehen.
Nur der zentrale MTA besitzt einen Zugang zum Telebox-System der Telekom als öffentliche Domäne (ADMD “dbp”). Über diese Telebox erfolgt der Datenaustausch mit anderen PRMD (z. B. Bund und Länder).
Der ressortübergreifende X.400-Verbund wird von einer Vielzahl von Benutzern mit unterschiedlichen Aufgabenprofilen genutzt werden, wobei sich für jeden Benutzer die zu übertragenden Daten von Fall zu Fall unterscheiden können. In der Regel sind diese Daten im voraus nicht bestimmbar. Somit kann eine an der Sensibilität der konkreten Daten orientierte Sicherheitskonzeption, die ansonsten für sachgebietsorientierte Anwendungen mit ihren fest umrissenen Datenobjekten üblich ist, keine geeignete Lösung darstellen, da die zu verarbeitenden Daten vorab nicht immer bekannt sind.
Grundsätzlich ist bei dem Einsatz von elektronischen Mitteilungssystemen davon auszugehen, daß auch sensible personenbezogene Daten übermittelt und gespeichert werden. Die Mindestanforderungen an die Datensicherheit müssen diesem Aspekt Rechnung tragen, selbst wenn anfangs keine sensiblen Daten verarbeitet werden sollen. Offensichtliche Risiken, mit denen ein ungesicherter elektronischer Versand von Nachrichten behaftet ist, sind:

- Die Vertraulichkeit des Inhaltes ist durch mögliche unberechtigte Zugriffe Dritter nicht gewährleistet.

- Der Absender ist nicht eindeutig identifizierbar.
- Inhaltliche Manipulationen können nicht zweifelsfrei erkannt werden.

Durch ein elektronisches Mitteilungssystem muß zumindest die gleichwertige Sicherheit erzielt werden wie beim Einsatz des Mediums Papier. Dies erfordert vor allem:

- die Wahrung der Vertraulichkeit aller Arten von Daten im elektronischen Mitteilungssystem (Nachrichten- und Verbindungsdaten),
- die Sicherstellung der Authentizität des Absenders,
- die Gewährleistung der Integrität der Nachrichten,
- die Bereitstellung fälschungssicherer Kommunikationsnachweise (Sende-, Empfangs- und Übertragungsnachweise).

Gefährdungen für das Persönlichkeitsrecht der betroffenen Bürger und Bediensteten können sowohl von einem Mißbrauch der Verbindungsdaten als auch der Inhaltsdaten der elektronischen Post ausgehen.
Gefahren für die inhaltlichen Daten (Nachrichteninhalte) ergeben sich bezüglich ihrer Verfügbarkeit, ihrer Vertraulichkeit, ihrer Integrität und ihrer Authentizität.
Verbindungsdaten ermöglichen das nicht erlaubte Erstellen von Persönlichkeitsprofilen sowie unzulässige Leistungs- und Verhaltenskontrollen. Die Einführung und der Betrieb elektronischer Mitteilungsdienste unterliegt daher der Mitbestimmung des Personalrates (§ 74 Abs. 3 Nr. 18 ThürPersVG).
§ 9 ThürDSG verpflichtet die öffentlichen Stellen, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die rechtmäßige Verarbeitung und Nutzung der Daten sicherzustellen. Dabei umfaßt die Verarbeitung auch das Übermitteln und Speichern solcher Daten (Nachrichten).
Entsprechend § 1 ThürDSG sind Betroffene davor zu schützen, daß sie durch den Umgang mit ihren personenbezogenen Daten durch öffentliche Stellen in ihrem Persönlichkeitsrecht beeinträchtigt werden. Konkretisiert wird dies im ThürDSG mit dem Zweckbindungs- und Erforderlichkeitsprinzip.
Für den Betrieb des E-Mail-Dienstes ist weiterhin das Fernanmeldeanlagengesetz (FAG) zu beachten. Für die von der Deutschen Telekom betriebenen Teile des E-Mail-Dienstes (Telebox System)- und damit auch für die in diesem Bereich übertragenen Daten- sind die Telekommunikationsverordnung (TKV) und die Telekom-Datenschutzverordnung (TDSV) gültig. Die TDSV wird durch die schon im Entwurf vorliegende Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) abgelöst werden.
Von seiten des BfD und der LfD (siehe Punkt 15.15.2 und Anlage 22) sind grundsätzliche Forderungen und Empfehlungen beim Einsatz von elektronischen Mitteilungssystemen aufgemacht worden.
Für den geplanten X.400-Verbund der Landesverwaltung sind daraus aus datenschutzrechtlicher Sicht weiterhin folgende konkrete Forderungen zu beachten:
Ausgehend von einer Bedrohungs- und Risikoanalyse sollte ein Datenschutz- und Datensicherheitskonzept (DDK) erarbeitet werden.
Mit Hilfe einer Bedrohungs- und Risikoanalyse sind für das IT-Vorhaben unter Berücksichtigung seiner Einsatzumgebung die Sicherheitsentscheidungen begründbar bzw. transparent zu machen. Die potentiellen Bedrohungen für die Sicherheit der Daten sind zu analysieren, die Risiken zu identifizieren und zu bewerten. Mit diesen Ergebnissen kann eine Abwägung der verschiedenen Sicherheitsanforderungen an das System und eine geeignete Auswahl der notwendigen Sicherheitsmechanismen erfolgen. In die Analyse sollten neben den Hardware- und Software-Systemkomponenten auch das infrastrukturelle, organisatorische und personelle Umfeld miteinbezogen werden. Dabei sollte auch berücksichtigt werden, daß E-Mail auf der Basis von X.400 in absehbarer Zeit sicher auch landesweit behörden- und länderübergreifend genutzt wird.
Als MTA (Postamtsrechner) sind dedizierte Rechner (Server) einzusetzen, um eine mögliche unzulässige Übernahme von personenbezogenen Daten aus Anwendungen und ihre Versendung mit E-Mail an unberechtigte Empfänger zu verhindern.
Grundsätzlich sind sensible personenbezogene Daten nur verschlüsselt zu übertragen. Empfohlen wird allerdings, nicht zuletzt auch aus Gründen der Praktikabilität, generell personenbezogene Daten verschlüsselt zu übermitteln. Vor Ort erforderliche ad-hoc Einstufungen der Daten bezüglich ihrer Sensibilität (siehe Punkt 15.3) und die damit verbundenen Risiken einer falschen Einstufung aus Unkenntnis werden somit ausgeschlossen. Der Einsatz von E-Mail sollte für personenbezogene Daten, deren Verarbeitung eine Gefahr für Leib und Leben der Betroffenen erwarten läßt, nur im Ausnahmefall erfolgen.
Es sind Möglichkeiten der elektronischen Unterschrift bereitzustellen, um die Integrität und die Authentizität der zu übertragenen Nachrichten zu gewährleisten. Neben der Auswahl eines hinreichend sicheren Verschlüsselungsverfahrens muß ein Schlüsselmanagement zur Erzeugung, Verwaltung und Verteilung der Schlüssel eingerichtet werden.
Weiterhin wird empfohlen, für die Benutzung von X.400 vom TIM eine Rahmendienstanweisung zu erstellen. Auf der Basis dieser Rahmendienstanweisung sollten die einzelnen Ressorts ihre Dienstanweisungen ableiten. Die Regelungen der existierenden Geschäftsordnungen in den Ressorts sind den neuen technischen Gegebenheiten anzupassen.

Vom IMA-IT wurde eine Arbeitsgruppe “X.400-Verbund” einberufen, an dessen Sitzungen in beratender Funktion auch der TLfD teilnimmt. Das Ziel dieser Arbeitsgruppe ist die Erarbeitung eines Realisierungskonzeptes für den X.400-Verbund.

15.5.3 Stellen- und Personalverwaltungssystem PERSOSTH

PERSOS ist ein Stellen- und Personalverwaltungssystem für dienstliche Zwecke der Personalplanung und Personalbetreuung sowie der Stellenbewirtschaftung. In der 32. Sitzung des IMA-IT wurde durch die IMA-IT-Mitglieder die Einführung des IT-Verfahrens PERSOS, welches im Auftrag des Bundesministeriums für Forschung und Technologie entwickelt wurde, in der Thüringer Landesverwaltung empfohlen. Die technische Betreuung von PERSOS und erforderliche problemorientierte Anpassungen zum Erstellen einer Thüringer Version wurden dem TLRZ übertragen. Beim TLRZ liegt inzwischen diese Version von PERSOS für die Installation in den einzelnen Ressorts bereit.
PERSOS arbeitet auf der Basis des Datenbanksystems ACCESS und kann sowohl als Einzelplatzsystem als auch in einem Netzwerk betrieben werden.
Eine Stellungnahme des TLfD entsprechend dem derzeitigen Erkenntnisstand zur Thüringer Version von PERSOS (PERSOSTH) liegt den betreffenden Ressorts vor. Eine abschließende datenschutzrechtliche Einschätzung kann allerdings erst erfolgen, wenn dem TLfD die teilweise noch in Arbeit befindlichen System- und Anwendungsdokumentationen vollständig vorliegen.
Personaldaten sind als sensibel einzustufen und müssen somit der Stufe 2 im Schutzstufenkonzept (siehe Punkt 15.3) zugeordnet werden. Die zu ergreifenden Schutzmaßnahmen sind entsprechend hoch anzusetzen. Erforderlich ist das Erstellen eines Sicherheitskonzeptes sowie dessen Umsetzung. Insbesondere ist ein ausreichender Zugriffsschutz notwendig, um die Vertraulichkeit und die Integrität der Daten abzusichern.
Nach dem derzeitigen Erkenntnisstand des TLfD können die hohen Sicherheitsanforderungen, die an ein Personalverwaltungssystem gestellt werden, durch das verwendete Programmsystem PERSOSTH allein nicht abgedeckt werden. Diesbezügliche Schwachstellen von PERSOSTH müssen durch das eingesetzte Betriebssystem abgedeckt werden. Das TLRZ installiert PERSOSTH nur auf der Basis von Windows NT. Der Einsatz dieses Betriebssystems, sowohl auf dem Server als auch auf den Clients, ermöglicht die Bereitstellung von Sicherheitseigenschaften, die für einen sicheren Einsatz von PERSOSTH von grundlegender Voraussetzung sind.
Für eine Umsetzung der Sicherheitfunktionalitäten von PERSOSTH und dem Betriebssystem bedarf es einer sorgfältigen Administration. Hierzu sind eindeutige Vorgaben für die Festlegung aller Sicherheitsparameter, der Rechtestruktur sowie der Handhabung der für die Installation erforderlichen Paßwörter notwendig. Um einen Zugriff Unbefugter auf PERSOSTH zu erschweren, sollte die Implementierung des Systems in einem Inselnetz erfolgen. Zusätzlich zu den systemtechnischen Sicherheitsmaßnahmen sind auch organisatorische und personelle Maßnahmen für einen sicheren Einsatz zu vollziehen. Regelungen für die Benutzer sind in einer Dienstanweisung festzuhalten. Auf eine eindeutige Funktionstrennung von Benutzer, Datenbankadministrator und bDSB innerhalb von PERSOSTH ist zu achten. Die Rolle des Systemadministrators (Verwaltung des Betriebssystems) und des Datenbankadministrators (Verwaltung PERSOSTH) dürfen nicht derselben Person zugewiesen werden.

15.6 Lokale Netze - Risiken und Schutz

Der zunehmende Einsatz von vernetzten Arbeitsplatzrechnern in der öffentlichen Verwaltung Thüringens erfordert auch seitens des Datenschutzes, dem Thema Netzwerksicherheit große Beachtung beizumessen. Die durchgeführten Kontrollen offenbarten, daß die mit einer Vernetzung verbundenen Risiken bei der Verarbeitung personenbezogener Daten den Verantwortlichen nicht immer im erforderlichen Maße bewußt waren bzw. oftmals in ihren Auswirkungen auf die schutzwürdigen Belange der Betroffenen unterschätzt wurden.
Aus der Sicht des Datenschutzes ist die zunehmende Vernetzung von Arbeitsplatzrechnern bei der Verarbeitung personenbezogener Daten nicht unbedenklich. Es ist nicht zu verkennen, daß bei der Planung und dem Betreiben von Netzen vorwiegend die technischen Möglichkeiten ausgenutzt werden. Das technisch Machbare wird versucht umzusetzen, wobei datenschutzrechtliche Aspekte nicht immer in dem erforderlichen Maße schon in die konzeptionellen Überlegungen einbezogen werden. Vernetzungen von PC werden auch vorgenommen, ohne daß zwingend die fachlichen Aufgaben, deren Ablauforganisation oder die eingesetzten programmtechnischen Verfahren dies erfordern würden. Die somit geschaffenen technischen Möglichkeiten für einen unbeschränkten Austausch von oder einen Zugriff auf personenbezogene Daten unabhängig von einer konkreten Erforderlichkeit im Einzelfall können zu einem unkontrollierbaren Datenmißbrauch führen.
Aus datenschutzrechtlicher Sicht sollte eine Vernetzung nur dann erfolgen, wenn die Arbeitsaufgaben dies erfordern und schutzwürdige Rechte der Betroffenen nicht verletzt werden. Der notwendige Zugriff auf den gleichen Datenbestand durch mehrere Benutzer oder ein erforderlicher Datenaustausch zwischen diesen wäre hier beispielhaft zu nennen. In zahlreichen öffentlichen Stellen Thüringens sind schon PC örtlich begrenzt auf das jeweilige Verwaltungsgelände

zu einem sogenannten lokalen Netz (LAN-Local Arta Network) verbunden. Der jeweilige PC-Arbeitsplatz ist somit aus seiner reinen Isolierung herausgelöst und in die Gesamtorganisation der jeweiligen Struktureinheit eingebunden. Damit wird nicht nur eine (ökonomische) Nutzung teurer peripherer Geräte von jedem vernetzten PC ermöglicht, sondern unter anderem auch die zentrale Bereithaltung und Verwaltung von mehrfach genutzten Datenbeständen, das gemeinsame Nutzen zentral bereitgestellter Software und ein interaktiver Austausch von Informationen zwischen den vernetzten Arbeitsplätzen.
Diese verstärkte Einbindung der PC-Arbeitsplätze in Netze sollte aber auch gezielt von den betroffenen Stellen genutzt werden, die bisher teilweise unkontrollierbaren Freiräume der PC-Benutzer auf das notwendige Maß einzuschränken.
Das LAN ist ein Kommunikationsnetz auf File-Server-Basis. Im Gegensatz zu öffentlichen Netzen steht es ausschließlich unter der rechtlichen Kontrolle seines Betreibers. Die Daten und Programme werden auf einem als Server bezeichneten Rechner, mit dem alle PC des LAN verbunden sind, zentral vorgehalten.
Im Einsatz befinden sich sogenannte Client-Server-Systeme als auch Peer-to-Peer-Systeme. Bei einer Peer-to-Peer-Netzstruktur sind alle PC gleichberechtigt miteinander vernetzt. Jeder PC kann je nach Bedarf sowohl als Server seine Daten und Programme anderen PC zur Verfügung stellen oder als Arbeitsplatzrechner Anwendungsprogramme abarbeiten. Im Gegensatz hierzu sind bei einem Client-Server-System alle PC als sogenannte Clients an einen zentralen und leistungsfähigen Rechner (Server) angeschlossen. Dieser Server verwaltet zentral für alle Clients die Daten und Programmdateien. Auf dem Client erfolgt die Abarbeitung der Anwendungssoftware, wobei bei einem echten Client-Server-Prinzip die Anwendungsprogramme so entworfen sind, daß sie teils auf dem Server und teils auf dem Client abgearbeitet werden.
In der Öffentlichkeit werden immer wieder Fälle bekannt, die belegen, daß Computernetze ein bevorzugter Tummelplatz für Angreifer sind. Nach Meinung von Experten stellen die bekannten Fälle nur die Spitze des Eisberges dar. Aus Imagegründen werden erkannte Angriffe von den betreffenden Stellen zumeist nicht publiziert. Verhängnisvoller sind jedoch unbemerkt gebliebene Angriffe, weil sich hier ein Zustand der trügerischen Scheinsicherheit manifestiert. Schon allein durch ihre räumliche Ausdehnung ist die Gewährleistung von Sicherheit in Netzen schwieriger handhabbar als bei zentralisierten Hostsystemen oder bei Einzelplatz-PC. Unter Sicherheit wird hier der Schutz vor unerlaubten Angriffen auf die Daten bei ihrer Übertragung im Netz oder Speicherung auf dem Server oder Client verstanden. Angriffe stellen immer eine bewußte und zielgerichtete Bedrohung für die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Verbindlichkeit der zu verarbeitenden Daten dar (siehe Punkt 15.2). Das Risikopotential erhöht sich, wenn das eigene LAN mit öffentlichen Netzen gekoppelt ist. Interne oder externe Angreifer nutzen vorhandene sicherheitstechnische Schwachstellen in Netzen aus, um getroffene Sicherheitsmaßnahmen zu umgehen. Solche Schwachstellen können personeller, organisatorischer und technischer Natur sein.
Wesentliche Sicherheitsrisiken für die Verarbeitung personenbezogener Daten in Netzen sind:

- Maskeraden
  Ein Angreifer täuscht die Identität eines berechtigten Benutzers vor, um dessen Rechte sich anzueignen. Der Angreifer kann somit alle Privilegien für sich in Anspruch nehmen, über die ansonsten nur der berechtigte Benutzer verfügen soll.
- Manipulationen
  Ein Angreifer kann sowohl über das Netz übertragene Daten als auch im Vermittlungsknoten gespeicherte Daten manipulieren. Durch unbefugtes Ändern, Löschen und Einfügen von Daten wird die Integrität der Daten verletzt und der Empfänger kann zu einem falschen Verhalten veranlaßt werden.
- Verzögern oder Wiederholen von Daten
  Während der Datenübertragung werden durch einen Angreifer gezielt Daten aufgezeichnet und zeitlich verzögert oder wiederholt zum Ziel übertragen. Auch hier kann der Empfänger zu falschen Aktionen veranlaßt werden.
- Fehlleiten
  Daten werden durch Adreßmanipulationen nicht dem regulären Empfänger zugestellt.
- Boykottieren des Kommunikationsnetzes
  Ein Angreifer verhindert oder unterbricht den Datenstrom durch Manipulationen an den Netzelementen.
- Leugnen einer Kommunikationsbeziehung
  Der Sender oder der Empfänger von Daten streitet ab, an einer Kommunikation teilgenommen zu haben. Dies kann eine rechtliche Relevanz haben.

Die aufgezeigten Gefährdungen stellen, bis auf den letzten Anstrich, aktive Angriffe auf die Kommunikation in Netzen dar. Im Gegensatz zu den aktiven Angriffen, welche im wesentlichen den Datenstrom verfälschen, stellen passive Angriffe eine Bedrohung für die Vertraulichkeit der Datenkommunikation dar. Solche Angriffe können z. B. mit Klemmen oder Induktionsschleifen an den Übertragungsleitungen durchgeführt werden. Sofern die Daten unverschlüsselt übertragen werden, können diese somit abgehört werden. Neben Inhalts- und Verbindungsinformationen können während einer Login-Prozedur auch die Benutzerkennung und das Paßwort des Teilnehmers ausgespäht werden.

Erhöhte datenschutzrechtliche Risiken für im Netz zu verarbeitende personenbezogene Daten bestehen weiterhin durch:

- Unkontrollierte Datenübertragung
  Durch eine unzureichende Trennung von lokaler PC-Verarbeitung und Netzanwendung können leseberechtigte Benutzer über das Netz unkontrolliert Daten auf die lokale Festplatte oder Diskette bzw. über eine ungesicherte Netzstelle unbefugt kopieren.
- Manipulation von Netzwerkadressen
  Jeder am Netz angeschlossene PC besitzt eine eigene Netzadresse. Die im Netz transportierten Datenpakete enthalten u. a. die Adresse des jeweiligen Zielrechners. Bei den sogenannten broadcast-orientierten Netzsystemen (Bus- oder Ring-Topologie) wird die Zieladresse von den Netzrechnern überprüft und bei Übereinstimmung mit der eigenen Adresse wird das Datenpaket von diesem Rechner übernommen. Durch eine Manipulation der eigenen Netzadresse ist es somit möglich, einen unbefugten Zugriff auf Daten zu erlangen.
- Einsatz von Netzanalyse- oder Fernsteuerungsprogrammen
  Netzanalyseprogramme gestatten das inhaltliche Lesen der im Netz übertragenen Datenpakete. Fernsteuerungsprogramme ermöglichen, den aktuellen Bildschirminhalt eines Netzteilnehmers auf den eigenen PC aufzubauen. Die Möglichkeiten eines Datenmißbrauches bei einem Einsatz solcher Programme sind offensichtlich.
- Unzureichende Kontrolle des Netzverwalters
  Der Netzverwalter verfügt entsprechend seiner Funktion über umfassende Rechte, die einen Datenmißbrauch jederzeit ermöglichen. Werden seine Aktivitäten nicht protokolliert, so ist ein Mißbrauch nachträglich kaum feststellbar.
- Netzweites Versenden von Daten
  Zugriffsberechtigte Benutzer stellen ihre Daten unbefugt anderen Netzteilnehmern zur Verfügung.
- Gemeinsame Nutzung der Netzdrucker
  Alle technischen Sicherungsmaßnahmen greifen ins Leere, wenn bei der Datenausgabe auf Netzdruckern durch organisatorische Maßnahmen die Einsichtnahme durch Unbefugte nicht verhindert wird.

Schon bei der Konzeption von Netzen muß ein hoher Sicherheitsstandard angesetzt werden. Auch wenn zum derzeitigen Erkenntnisstand gegebenenfalls noch keine Verarbeitung personenbezogener Daten ansteht. Aufgesetzte Sicherungsmaßnahmen, die nachträglich realisiert werden, sind oftmals kostspieliger und gewährleisten nicht immer einen umfassenden Datenschutz. So wird zum Beispiel die Datensicherheit in einem Netz schon grundlegend durch dessen Topologie (Netzstruktur) und das eingesetzte Übertragungsmedium beeinflußt. Die Festlegungen hierfür erfolgen schon bei der Konzeption des Netzes.
Es gibt drei topologische Grundformen (Stern, Bus, Ring) für LAN mit unterschiedlichen Sicherheitsrisiken.
Bei einem Sternnetz ist jede Arbeitsstation über eine eigene Leitung mit der Zentrale (Server) verbunden. Der Datenverkehr eines Netzteilnehmers erfolgt beim Einsatz intelligenter Sternkoppler mit entsprechenden Filterfunktionen nur über seine eigene Leitung und nicht durch das gesamte Netz, wodurch das Abhörrisiko vermindert wird. Von einem Ausfall der Zentrale sind allerdings alle Netzteilnehmer betroffen, weil der gesamte Datenverkehr über den zentralen Knoten des Netzwerkes läuft.
Bei einem Busnetz sind alle Arbeitsstationen und der Server an ein gemeinsam zugängliches Übertragungsmedium, dem sogenannten Datenbus, angeschlossen. Alle Arbeitsstationen können direkt zu jeder anderen Arbeitsstation in Kontakt treten. Arbeitsstationen können jederzeit ohne Unterbrechung des Netzwerkbetriebes neu installiert oder abgebaut werden. Der gesamte Datenverkehr läuft über den Datenbus. Das Abhörrisiko ist hier hoch, da ein technisch versierter Angreifer sich problemlos an den Datenbus anschließen kann. Da über den Bus die Daten aller Netzteilnehmer übertragen werden, können die Auswirkungen gravierender sein als bei einem Sternnetz.
Bei einem Ringnetz sind die Arbeitsstationen ringförmig miteinander verbunden. Im Gegensatz zu einem Busnetz, bei dem alle angeschlossenen Arbeitsplätze die ausgesandten Daten gleichzeitig empfangen können, werden im Ringnetz alle Daten von Station zu Station weitergeleitet. Das Abhörrisiko ist hoch, da jeder Teilnehmer prinzipiell die Möglichkeit hat, die über das Netz übertragenen Daten zu lesen.
Die Übertragung der Daten im Netz kann leitungsgebunden oder drahtlos erfolgen. Als Leiter können Koaxialkabel, Kupferkabel (Twisted-Pair-Kabel) und Glasfaserkabel eingesetzt werden.
Mit Hilfe von Spezialwerkzeugen kann der Innenleiter des Koaxialkabels angezapft und somit die übertragenen Daten abgehört werden. Ein solcher Angriff ist schwer erkennbar, da beim Anzapfen der Netzbetrieb nicht unterbrochen wird und er nachträglich nicht feststellbar ist. Für die Übertragung unverschlüsselter Daten sollte deshalb auf den Einsatz von Koaxialkabel verzichtet werden.
Twisted-Pair-Kabel bestehen aus paarweise miteinander verdrillten Kupferadern. Insbesondere durch das Auftrennen der Ummantelung kann die Abstrahlung des Kabels aufgefangen werden. Ein Abhören ist aber auch durch das Auftrennen des Kabels möglich. Beide Angriffsarten sind optisch erkennbar. Bei einer gebäudeübergreifenden Verkabelung sollte auf den Einsatz von Twisted-Pair-Kabeln verzichtet werden.

Lichtwellenleiter (Glasfaserkabel) sind abstrahlarm. Um Lichtwellenleiter abzuhören, müssen sie aufgetrennt werden. Sowohl das Auftrennen als auch das Zusammenfügen der Lichtwellenleiter erfordern Spezialwerkzeuge. Obwohl Lichtwellenleiter ebenfalls nicht völlig abhörsicher sind, bieten sie immer noch eine hohe Abhörsicherheit und sollten zumindestens für die externe Verkabelung von Gebäuden eingesetzt werden.
Eine kabellose Datenübertragung kann durch Funk bzw. Infrarotlicht erfolgen. Aufgrund der Streuung der Strahlen ist die Abhörsicherheit nicht gegeben. Deshalb sollten beim Einsatz drahtloser Übertragungsmedien sensible Daten verschlüsselt übertragen werden.

Ein wichtiges Ziel der Datenschutzmaßnahmen ist, die in Netzen rechtmäßig verarbeiteten personenbezogenen Daten vor unberechtigter Kenntnisnahme zu schützen. Die Maßnahmen müssen so ausgerichtet sein, daß jeder befugte Netzteilnehmer nur die Funktionen ausführen darf, die genau seinem Verantwortungsbereich entsprechen (siehe auch Punkt 15.14.2).

Wichtige Sicherheitsfunktionen für das Betreiben von Netzen sind die:
- Identifizierung und Authentisierung
  Die Identifizierung und Authentisierung bilden die wichtigsten Mechanismen zur Zugangskontrolle. Gängige Praxis ist derzeit die Identifizierung mittels Benutzerkennung und die Authentisierung mittels Paßwort. Ein höheres Sicherheitsniveau läßt sich durch den Einsatz von Chipkarte und Paßwort erzielen.
- Rechteverwaltung und Rechteprüfung
  Durch die Rechteverwaltung und Rechteprüfung wird eine wirksame Zugriffskontrolle realisiert. Hiermit werden die Zugriffsrechte bezüglich der Ressourcen wie Laufwerke, Dateien und Drucker für den jeweiligen Benutzer oder für Benutzergruppen festgelegt. Die Zugriffsrechte werden über das jeweilige Netzwerkbetriebssystem verwaltet und kontrolliert.
- Beweissicherung
  Die Beweissicherung umfaßt die Protokollierung von Benutzer- und Netzverwalteraktivitäten. Das Aufzeichnen von sicherheitsrelevanten Netzwerkaktivitäten wird als Auditing bezeichnet. In einer vom Netzwerkbetriebssystem geführten Datei kann protokolliert werden, wer wann im System aktiv war, ob Zugangs- und Zugriffsverletzungen begangen wurden etc. (siehe Punkt 15.12).
- Vertraulichkeit
  Die Maßnahmen zur Gewährleistung der Vertraulichkeit müssen in Abhängigkeit des Schutzbedarfs der zu verarbeitenden personenbezogenen Daten festgelegt werden. Als Orientierungshilfe kann hierfür das in Punkt 15.3 dargestellte Schutzstufenkonzept herangezogen werden. Neben Mechanismen zur Zugangs- und Zugriffskontrolle kommen zur Realisierung der Vertraulichkeit auch Mechanismen zur Verschlüsselung zum Einsatz. Eine Verschlüsselung der Daten kann sowohl bei ihrer Speicherung auf der Festplatte vom Arbeitsplatz-PC als auch vom Server zum Einsatz kommen.
- Datenübertragungssicherung
  Im Vordergrund der Datenübertragungssicherung stehen Maßnahmen zur Gewährleistung der Datenintegrität, der Vertraulichkeit und des Kommunikationsnachweises (Nachweis über Ursprung und Empfang von Daten). Wesentliche Sicherheitsmechanismen hierfür sind die Verschlüsselung der Daten sowie der Einsatz der elektronischen Unterschrift.
- Datensicherung
  Für die physische Sicherung der Datenbestände konzentrieren sich die Anforderungen auf das Sicherungsmedium (z. B. Streamer) und ihre Ablauforganisation (Frequenz der Sicherung, Anzahl der Generationen, Löschfristen, sichere Aufbewahrung). Eine automatisierte Datensicherung ist anzustreben.

Die grundsätzlichen Sicherheitsanforderungen, die durch die oben beschriebenen Sicherheitsfunktionen zum Ausdruck kommen, sind sowohl durch technische als auch durch organisatorische Maßnahmen zu realisieren. Für den jeweiligen Anwendungsfall sind, eventuell auf der Grundlage einer Risikoanalyse, die konkreten Sicherheitsanforderungen und aufgedeckten Risiken durch im einzeln festzulegende Sicherheitsmaßnahmen abzudecken. Die Gesamtheit der festgelegten Maßnahmen bildet das Sicherheitskonzept. Aus datenschutzrechtlicher Sicht sollte dieses Sicherheitskonzept einen angemessenen und wirksamen Schutz der im Netz zu verarbeitenden personenbezogenen Daten gewährleisten.
Die Sicherheitsmaßnahmen beziehen sich auf die Netzelemente (Server, Arbeitsplatzrechner, Übertragungsleitung) und lassen sich in physische, organisatorische und DV-technische Maßnahmen untergliedern. Sie müssen immer im Zusammenhang betrachtet werden. Nachfolgend sind beispielhaft mögliche Sicherheitsmaßnahmen aufgeführt:

Technische Maßnahmen

Server
- Aufstellen in einem separaten Raum mit besonderer Zutrittssicherung,
- Brandschutzvorkehrungen (Kohlensäure- bzw. Kohlendioxidhandfeuerlöscher, eventuell Brandmelder),
- Anschluß an unterbrechungsfreie Stromversorgung (Verhinderung von Datenverlusten bei Netzschwankung oder Stromausfall),
- keine Nutzung als zusätzlicher Arbeitsplatzrechner,
- Zugangssicherung durch Identifizierung/ Authentisierung,
- Begrenzung der Zahl der Anmeldeversuche,
- Zugang nur mit Systempaßwort,
- Benutzerzugriffssteuerung in Form einer Rechteverwaltung bis auf einzelne Dateien und Verzeichnisse hinunter,
- Protokollierung aller Zugriffe bzw. abgewiesenen Zugriffsversuche,
- Zentrale Systemverwaltung aller Clients,
- Einsatz eines hinreichend sicheren Betriebssystems,
- Verschlüsselung sensibler Daten auf der Festplatte,
- Verzicht auf Fernwartung,
- Sperrung der Serverkonsole,
- Nutzung eines Gehäuseschlosses,
- Plattenspiegelung zur Ausfallsicherheit,
- Protokollierung der Aktivitäten des Netzwerkmanagements,
- regelmäßige Datensicherung der Festplatten,
- Einsatz eines Virensuchprogramms,
- Abweisung nicht autorisierter Rechner,
- obligatorische Menüführung der Benutzer im Netzwerk,
- Verhinderung des Zugriffs auf die Netzbetriebssystemebene,
- benutzerbezogene zeitliche Eingrenzung des Netzzugriffs,
- automatischer Entzug der Benutzerberechtigung bei mehrmaliger Falschanmeldung, eventuelle Sperrung des Zugriffsgerätes,
- Zugriffskontrolle der Netzdrucker.

Arbeitsplatzrechner
- Lokale Identifizierung/ Authentisierung,
- Boot-/Setup-Paßwortschutz,
- keine Diskettenlaufwerke bzw. Verschluß vorhandener Diskettenlaufwerke,
- Sperrung serieller und paralleler Schnittstellen,
- bei Arbeitsunterbrechung Bildschirmverdunkelung, Aufhebung durch Paßworteingabe,
- keine Speicherung sensibler Daten auf der lokalen Festplatte, ansonsten Verschlüsselung der Daten,
- Versiegeln der Gehäuse, um Manipulationen der Hardware auszuschließen,
- Einsatz von Sicherheitssoftware bzw. von Betriebssystemen mit hinreichenden Sicherheitsmechanismen,
- Verhinderung des Zugriffs auf die Betriebssystemebene,
- Zugriff der Benutzer nur auf die zugewiesenen Anwendungen.

Netze
- Schutz der Leitungen in gesicherten Kabelschächten,
- räumliche Absicherung der Netzverteiler,
- Auswahl abhörsicherer Übertragungsmedien (Lichtwellenleiter),
- abkoppeln physikalisch nicht benutzter Anschlußdosen,
- verschlüsselte Übertragung sensibler Daten,
- Einsatz der Stern-Topologie.

Organisatorische Maßnahmen
- Technische Dokumentation des Netzwerkes bezüglich Verkabelung, Installation und Konfiguration,
- Dokumentation des IT-Sicherheitskonzeptes durch Festlegung verbindlicher Sicherheitsrichtlinien (angestrebte Sicherheitsanforderungen, getroffene Sicherheitsmaßnahmen, festgelegte Benutzer- und Zugriffsrechte, Aufgaben der Netzadministration, physische Datensicherung, Behandlung von Sicherheitskonflikten, Konsequenzen bei Sicherheitsverletzungen, Kontrolltätigkeit, Virenschutz, Absicherung zwingender Fernwartung),

- klare Regelung der Verantwortlichkeiten,
- regelmäßige Auswertung der Protokolle nach dem Vier-Augen-Prinzip,
- Erarbeitung eines Katastrophenplanes mit Wiederanlaufkonzept.

Personelle Maßnahmen
- Als Netz- und Systemverwalter sollten nur entsprechend qualifizierte Mitarbeiter eingesetzt werden,
- Durchführung ausreichender Weiterbildungs- und Schulungsmaßnahmen für alle Netzteilnehmer,
- Sensibilisierung der Mitarbeiter hinsichtlich des Datenschutzes und der IT-Sicherheit.

Bei der Verarbeitung sensibler Daten empfiehlt sich eine strikte Funktionstrennung von Administration der Sicherheitsmaßnahmen und Kontrolle der getroffenen Maßnahmen. Die Kontrollfunktion sollte nicht vom Netzverwalter wahrgenommen werden.

15.7 Betrieb von Telekommunikationsanlagen (TK-Anlagen)

15.7.1 Grundsätzliches

In zunehmendem Maße werden in den öffentlichen Stellen des Freistaats Thüringen neue Telefonanlagen mit digitaler Technik eingesetzt. Solche internen Telekommunikationsanlagen werden auch ISDN-Nebenstellenanlagen genannt. Sie ermöglichen die Übertragung und Speicherung von Sprache, Texten, Daten und Bildern. In den digitalen Telekommunikationsanlagen (TK-Anlagen) werden personenbezogene Daten automatisiert verarbeitet. Gefahren für das Persönlichkeitsrecht der Telefonbenutzer ergeben sich durch die Leistungsmerkmale (Komfortfunktionen) solcher Anlagen (siehe Punkt 15.7.2).
In den TK-Anlagen werden u. a. sogenannte Verbindungsdaten (Rufnummer des Anrufers und des Angerufenen, Zeitpunkt und Dauer des Gespräches, Art der Verbindung) gespeichert. Diese Daten werden in der Regel mit einem Gebührencomputer, der an die TK-Anlage angeschlossen ist, ausgewertet. Sowohl für die TK-Anlage als auch für den Gebührencomputer sind zur Gewährleistung eines datenschutzrechtlich ordnungsgemäßen Betriebs die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 ThürDSG zu treffen. Diese Maßnahmen dienen dem Schutz der gespeicherten personenbezogenen Daten und des gesprochenen Wortes sowie vor Installation unerlaubter Leistungsmerkmale.
Die Verbindungsdaten, die in einer TK-Anlage gespeichert werden, sind geeignet, Verhaltens- oder Leistungskontrollen der Mitarbeiter durchzuführen. Der Einsatz von TK-Anlagen unterliegt daher nach § 74 Abs. 3 Nr. 18 und 19 ThürPersVG der Mitbestimmung des Personalrates.
Der erstmalige Einsatz automatisierter Verfahren, mit denen Telefongesprächsdaten verarbeitet werden, ist nach § 34 Abs. 2 ThürDSG hinsichtlich der Datenarten und der regelmäßigen Übermittlungen datenschutzrechtlich schriftlich von den in § 34 Abs. 1 ThürDSG genannten Stellen freizugeben.

15.7.2 Datenschutzrechtlich relevante Leistungsmerkmale einer TK-Anlage

Beim Kauf und Einsatz einer TK-Anlage sind auch datenschutzrechtliche Aspekte zu beachten. Neben der Übertragung von Daten, Texten und Bildern stellt die Sprachübermittlung mittels einer TK-Anlage eine der am häufigsten genutzten Dienste dar und soll deshalb näher betrachtet werden.
Die TK-Anlagen bieten hierfür eine Vielzahl von Funktionen, die aus datenschutzrechtlicher Sicht bedenklich sein können. Diese Funktionen sind nicht immer in den Gebrauchsanleitungen detailliert beschrieben. Es ist deshalb darauf zu achten, daß eine vollständige Auflistung aller möglichen Funktionen der TK-Anlage vorliegt.
Wesentliche Leistungsmerkmale einer TK-Anlage, die aus datenschutzrechtlicher Sicht zu beachten sind:

Rufnummernanzeige
Viele öffentliche Stellen verfügen bereits über Telefone bei denen während des Verbindungsaufbaus im Anzeigedisplay die Telefonnummer des Gesprächspartners und bei manchen internen Anlagen auch dessen Name angezeigt und teilweise abgespeichert werden kann. Einerseits kann die Annahme des Gespräches davon abhängig gemacht werden, andererseits können unbeteiligte Dritte über die Anzeige erfahren, mit wem telefoniert wird. Übertragen werden Ortsnetzkennzahl, Teilnehmerrufnummer bzw. Durchwahl- und Nebenstellennummer.
Eine ständige Unterdrückung der Rufnummernanzeige wird auf Wunsch in der entsprechenden Nebenstellenanlage durchgeführt.
Um die Anonymität des Anrufers zu gewährleisten, bietet die Telekom seit Frühjahr 1995 den Erwerb von Telefonen mit wahlweiser Abschaltungsmöglichkeit der Anzeige der Telefonnummer des Anrufenden bei dem Angerufenen an.

Aufschalten
Teilnehmer können sich in eine bestehende Verbindung "Aufschalten" und dadurch aktiv in die Verbindung eingreifen. Das Aufschalten wird durch einen Signalton, manchmal aber auch nur durch eine Displayanzeige mitgeteilt. Für die Teilnehmer des Gespräches besteht die Gefahr, daß gegen ihren Willen die Vertraulichkeit ihrer Verbindung durch das Aufschalten gestört wird. Deshalb ist sicherzustellen, daß die betroffenen Teilnehmer durch ein deutliches Signal von dem Aufschalten Kenntnis erhalten.

Konferenzschaltung
Teilnehmer können in eine bestehende Verbindung zugeschaltet werden, wobei im Gegensatz zur Aufschaltung hier der Konferenzleiter bestimmt, wer wann zugeschaltet wird. Die Anzahl der Teilnehmer und deren Identität ist nicht immer für jeden Teilnehmer feststellbar. Deshalb sollte eine Konferenzschaltung immer angekündigt werden.

Aufzeichnungen
Mit automatischen Aufzeichnungsgeräten ist es technisch möglich, Gesprächsinhalte aufzunehmen. Eine solche Aufnahme stellt, wenn sie unbefugt erfolgt, eine Verletzung der Vertraulichkeit des Wortes nach § 201 Abs. 1 StGB dar. Eine Befugnis zur Aufnahme liegt in den Fällen vor, in denen der Betroffene eingewilligt hat oder wenn die Voraussetzungen eines rechtfertigenden Notstands nach § 34 StGB gegeben sind. Letzteres kann z. B. zur rechtzeitigen Ermittlung des Täters bei telefonischen Bombendrohungen vorliegen. So erfolgen in der Praxis z. B. Aufzeichnungen an bestimmten funktions- und aufgebenbezogenen Stellen der Polizei bzw. in den integrierten Leitstellen für Rettungsdienst sowie für Brand- und Katastrophenschutz.

Automatischer Rückruf
Die Funktion "automatischer Rückruf" kann aktiviert werden, um bei einem nicht erfolgreichen Verbindungsaufbau einen automatischen Rückruf zu erzwingen. Im Freifall wird die Verbindung hergestellt, sobald der Angerufene nach seiner Abwesenheit das Telefon wieder benutzt hat. Im Besetztfall, d. h. wenn gerade ein Telefongespräch geführt wurde, wird der Verbindungsaufbau automatisch eingeleitet, sobald das vorherige Gespräch beendet wird.
Diese Funktion begünstigt eine Anwesenheitskontrolle am Arbeitsplatz.
Ein automatischer Rückruf sollte so installiert sein, daß die Initiative, ob die Verbindung zustande kommt, vom Angerufenen ausgehen muß. Aus datenschutzrechtlicher Sicht wird die Trennung zwischen Rückruf im Frei- und Besetztfall empfohlen. Der Rückruf im Freifall sollte nur mit Einverständnis des Teilnehmers geschaltet werden. Eine akzeptable Alternative zum automatischen Rückruf stellt die Anrufliste dar, in die der Anrufer auf Wunsch eingetragen werden kann.

Lauthören / Freisprechen / Durchsagen
Lauthören/ Freisprechen/ Durchsagen kann man nur mit einem Telefon, das über einen Lautsprecher und ein Mikrofon verfügt. Ohne Wissen des Anrufers, kann der Angerufene diese Funktionen aktivieren und andere Personen in dem selben Raum oder Flur bewußt oder unbewußt Mithörer werden lassen. Die Gesprächspartner sollten deshalb vor jeder Nutzung dieser Funktionen hierzu gefragt bzw. zumindest durch einen Signalton darauf aufmerksam gemacht werden.

Bei den beschriebenen Möglichkeiten zeigt sich, daß die Entwicklung im Fernsprechbereich und die ständige Erweiterung der technischen Möglichkeiten Datenschutzrisiken mit sich bringen, deren sich die Anwender beim Einsatz bewußt sein müssen. Wird sich für den Einsatz entschieden, sind geeignete technisch-organisatorische Maßnahmen einzuleiten, die mögliche Datenschutzrisiken berücksichtigen. Ohne den technischen Fortschritt und Arbeitserleichterungen durch technische Lösungen aus Datenschutzgesichtspunkten von vornherein zu verhindern, ist zu beachten, daß verantwortungsbewußter und vertrauensvoller Umgang grundlegende Voraussetzung für die Handhabung der technischen Möglichkeiten ist. Es kommt stets auf die Gesamtheit der Umstände und Bedingungen an, unter denen eine Anwendung stattfindet. Vor dem Hintergrund, daß das Recht am eigenen Wort die Befugnisse des Sprechenden schützt, den Kreis der Adressaten seiner Worte selbst zu bestimmen, kann z. B. beim "Freisprechen" oder beim Nutzen der Funktion "Durchsage" und beim "Aufschalten" eine Verletzung des Persönlichkeitsrechtes eines Teilnehmers vorliegen. Dies ist in jedem Falle zu bejahen, wenn ein Teilnehmer einen Dritten mithören läßt und dies auf einer Täuschung beruht, wenn der Inhalt des Gespräches vertraulichen Charakter hat oder der andere Gesprächspartner ausdrücklich erklärt, daß er Wert auf Vertraulichkeit legt.

15.7.3 Erhebung von Telefongesprächsdaten

Im Berichtszeitraum wurde der TLfD wiederholt um die datenschutzrechtliche Bewertung von Dienstvereinbarungen für die Datenerfassung und Erhebung von Telefongesprächsdaten gebeten.
Hinweise wurden insbesondere bezüglich der Mitbestimmungspflicht durch den Personalrat nach § 74 Abs. 3 Nr. 19 ThürPersVG, der Notwendigkeit einer datenschutzrechtlichen Freigabe des erstmaligen Einsatzes automatisierter

Verfahren und der Meldung zum Datenschutzregister gemäß § 3 ThürDSRegVO gegeben. Fragen bestanden aber z. B. auch hinsichtlich der Führung privater Ferngespräche und der Speicherung der Telefondaten zur Abrechnung.
Es wurde weiter darauf hingewiesen, daß bei Behördenbediensteten, die einer besonderen Schweigepflicht unterliegen, eine Auswertung und Speicherung der Verbindungs- und Abrechnungsdaten nur summarisch (Summe der Gebühreneinheiten je Nebenstelle) vorgenommen werden darf.
In einem konkreten Fall hatte eine Behörde unzulässige Telefondatenlisten erstellt. Die Listen wurden auf Hinweis des TLfD vernichtet.

Auch die Frauenbeauftragte der Landesregierung bat den TLfD um Meinungsäußerung aus datenschutzrechtlicher Sicht zu folgendem Problem:
Ein Träger von Frauenhäusern hat bei der Telekom den Antrag, gemäß § 6 Abs. 9 Satz 7 der Verordnung über den Datenschutz, bei Dienstleistungen der Deutschen Bundespost Telekom (TDSV) gestellt, durch technische Vorrichtungen sicherzustellen, daß Anrufe aus Einzelentgeltnachweisen nicht ersichtlich sind. Der Antrag wurde dadurch begründet, daß die Adressen von den Frauenhäusern zum Schutze von Frauen und Kindern anonym bleiben müssen. Die Möglichkeit, die Zielrufnummer auf den Einzelentgeltnachweisen um drei Stellen verkürzt auszudrucken, garantiere die Anonymität nicht. Aus den verbleibenden Nummern könne immer noch entnommen werden, in welchem Bezirk sich das Frauenhaus befindet, so daß eine Lokalisierung ermöglicht werde. § 6 Abs. 9 Satz 5 und 7 TDSV läßt zu, daß der Anruf bei Personen, Behörden und Organisationen, die einer besonderen Verschwiegenheitsverpflichtung unterliegen und die Beratungsaufgaben im sozialen oder kirchlichen Bereich ganz oder überwiegend über Telefon abwickeln, aus dem Einzelentgeltnachweis der Telekom nicht ersichtlich sein darf. Aufgrund der Aufgabenwahrnehmung von Frauenhäusern sollten diese hier gleichgestellt werden, auch wenn die Beratungsaufgaben nicht ganz oder überwiegend über Telefon abgewickelt werden. Die Gleichbehandlung rechtfertigt sich aus der besonderen Schutzwürdigkeit der anrufenden Betroffenen. Frauenhäuser haben auch ein besonderes Interesse daran, Ihre Adresse zum Schutz der Frauen und Kinder nicht bekannt werden zu lassen. Um einen ersten Kontakt herstellen zu können, bleibt für Hilfesuchende lediglich die Möglichkeit eines Anrufes. Wenn der Aufenthalt einer Zeugin in einem bestimmten Frauenhaus durch die Angaben im Einzelentgeltnachweis der Telekom doch lokalisiert werden kann, obwohl sie im Strafverfahren wegen Gefährdung ihren Wohnsitz nicht angeben muß, ginge das Geheimhaltungsinteresse des Aufenthaltes ins Leere. So sollte auch hier die Möglichkeit der Unsichtbarkeit der entsprechenden Telefonnummern im Einzelentgeltnachweis der Telekom möglich sein.

15.8 Sicherheit für Laptops, Notebooks

Der Einsatz mobiler Computer (Laptops/Notebooks u. ä. Computer) in den öffentlichen Stellen nimmt ständig zu. Deshalb erscheint es wichtig, auf grundlegende Aspekte zum Einsatz dieser IT-Geräte aus der Sicht des Datenschutzes hinzuweisen.
Laptops sind transportable Computer im Aktentaschenformat, welche die gleichen Funktionen und Speicherkapazitäten bieten wie große Desktop-PC. Notebooks sind transportable Computer in DIN-A4 Größe, nur wenige Zentimeter dick und unter 3 Kilogramm schwer. Sie können in der Regel wie die Laptops an Monitore, Drucker, Modem, Fax-Geräte und an Computernetzen angeschlossen werden.
Bei dem Einsatz von mobilen Computern können sich folgende zusätzliche Sicherheitsrisiken im Vergleich zu Desktop-PC ergeben:
- Diebstahl bzw. Verlust des Laptops/Notebooks,
- unzulässige Vermischung dienstlicher und privater Nutzung,
- unkontrollierbarer Datentransfer auf Disketten,
- Nutzung der Laptops/Notebooks durch mehrere Bediener.

Deshalb empfiehlt der TLfD, für die Verarbeitung schutzwürdiger Daten auf mobilen PC, folgende Mindestanforderungen an technischen Sicherheitsmaßnahmen zu realisieren:
- aktivieren des Boot-/Setup-Paßwortes,
- manuelle und automatische Bildschirmdunkelschaltung, die nur mittels Paßwort aufgehoben werden kann,
- Identifikation und Authentisierung des Benutzers, verschlüsselte Abspeicherung des Paßwortes und Möglichkeit der Paßwortänderung durch den Benutzer,
- Verplombung der Rechnergehäuse,
- Sperren des Diskettenlaufwerkes,
- Verschluß der Schnittstellen für periphere Geräte,
- Einsatz von Antivirenprogrammen.

Für mobile PC, auf die mehrere Benutzer zugreifen, sind zusätzlich zu realisieren:
- Differenzierung bei der Zugangsberechtigung durch Paßwortvergabe für jeden einzelnen Benutzer,
- Differenzierung von Zugriffsrechten bezüglich Verzeichnisse, Datendateien, Laufwerke etc..

Die Verarbeitung sensibler personenbezogener Daten erfordert grundsätzlich
- eine verschlüsselte Speicherung dieser Daten,
- eine Protokollierung der Benutzeraktivitäten,
- Nutzung DFÜ und E-Mail mit Verschlüsselungsverfahren.

Je nach eingesetztem Betriebssystem sind die erforderlichen Sicherheitsfunktionen durch den Einsatz zusätzlicher Schutzsoftware zu gewährleisten.

Für den Einsatz von mobilen PC sind auch organisatorische Maßnahmen zu realisieren, z. B.:
- Es ist eine verbindliche Richtlinie für ihren Einsatz zu erlassen.
- Die Beschaffung sollte nach einheitlichen Gesichtspunkten durchgeführt werden.
- In der Regel sollte möglichst eine eindeutige Zuordnung von den Geräten zu den Benutzern erfolgen.
- Eine zentral organisierte System-, Geräte- und Datenträgerverwaltung wird empfohlen.
- Nach § 10 ThürDSG sind auch alle tragbaren Computer in das Anlagen- und Verfahrensverzeichnis aufzunehmen.
- Nach Dienstschluß bzw. bei Nichtgebrauch sind die Geräte sicher aufzubewahren.
- Für jedes Gerät sollte nachweislich eine Freigabe unter Beachtung der obengenannten Maßnahmen erfolgen.
- Nach § 16 ThürDSG sind personenbezogene Daten in Dateien unverzüglich physisch zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist.

15.9 Datenschutzgerechtes Löschen, Entsorgen von (defekten) Festplatten

Die folgenden grundsätzlichen Ausführungen zum Löschen, Reparieren bzw. Entsorgen von magnetischen Datenträgern nehmen Bezug auf entsprechende Anfragen öffentlicher Stellen an den TLfD. Nach § 9 Abs. 2 Nr. 2 ThürDSG sind Maßnahmen zu treffen, die geeignet sind zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle). Auch bei der Weitergabe, dem Austausch, der Reparatur oder der Entsorgung von magnetischen Datenträgern muß einem solchen Mißbrauch vorgebeugt werden.
Es ist grundsätzlich zu verhindern, daß möglicherweise noch gespeicherte schutzwürdige Daten Unbefugten zur Kenntnis gelangen. In der Regel werden hierzu Datenträger inhaltlich gelöscht. Das ThürDSG definiert in § 3 Abs. 3 Nr. 5 das Löschen als das Unkenntlichmachen gespeicherter personenbezogener Daten. Der Begriff "Unkenntlichmachen" besitzt kein technisches Äquivalent. Das sogenannte "logische" Löschen genügt dieser Definition nicht. Denn hier sind Daten noch gespeichert; sie sind lediglich als gelöscht gekennzeichnet und somit zum Überschreiben freigegeben. Solange die Daten nicht überschrieben wurden, besteht die Möglichkeit, den Zugriff wieder herzustellen.
Im Ergebnis wirksamer ist das "physische" Löschen durch Entmagnetisieren des Datenträgers oder durch Überschreiben der gespeicherten Daten. Beim Überschreiben bleiben in der Regel Restinformationen über die vorher gespeicherten Daten erhalten. Diese Datenreste können durch mehrmaliges Überschreiben so minimiert werden, daß eine Rekonstruktion ausgeschlossen werden kann. Ein datenschutzgerechtes Löschen stellt für magnetisierbare Datenträger das sogenannte Entmagnetisieren durch eigens dafür konzipierte Löschgeräte dar. Wenn die Entmagnetisierung korrekt erfolgt, d. h. mit einer ausreichenden Dämpfung, kann eine Rekonstruktion der Daten ausgeschlossen werden. Dieses Verfahren bietet sich insbesondere an, wenn die Festplatte defekt ist. In der Regel wird eine defekte Festplatte, die vor Ort von der Vertragsfirma nicht mehr repariert werden kann, gegen eine andere Festplatte ausgetauscht. Die defekte Festplatte wird normalerweise von der Vertragsfirma zurückgenommen. In einer Vielzahl von Fällen lassen sich solche Festplatten wieder reparieren. Mit einigem Aufwand können dann auch die auf ihr gespeicherten personenbezogenen Daten wieder rekonstruiert werden. Ein Zugriff auf die Daten durch Unbefugte ist somit also möglich bzw. kann nicht ausgeschlossen werden. Um eine solche mißbräuchliche Nutzung gespeicherter personenbezogener Daten in jedem Fall zu verhindern, sollten diesbezügliche Daten auf defekten Festplatten magnetisch "gelöscht" werden. Entsprechende (magnetische) Löschgeräte sind im Handel erhältlich. Ist eine solche Löschung vor Ort nicht möglich (z. B. aus wirtschaftlichen Gründen), so ist hierfür ein geeigneter Auftragnehmer auszuwählen. Dabei sind die in § 8 ThürDSG aufgeführten Vorschriften zu beachten. Der Auftrag ist in jedem Fall schriftlich zu erteilen, und seine Durchführung zu kontrollieren. In jedem Fall bleibt der Auftraggeber für den ordnungsgemäßen Ablauf der unwiderruflichen Datenlöschung verantwortlich. Erst nach einem "physischen" Löschen der personenbezogenen Daten dürfen Festplatten an eine Servicefirma zurückgegeben bzw. einer Entsorgungsfirma zur Vernichtung übergeben werden.

15.10 Technische und datenschutzrechtliche Aspekte bei Chipkarten

In der modernen Informationstechnik werden immer mehr Chipkarten eingesetzt (siehe Punkt 11.10 und 15.1) und weiterentwickelt.
Als Beispiel sei der Einsatz von unterschiedlichen Chipkarten im Kommunikationsbereich genannt. Die bekannteste Anwendung ist hier die Chipkarte als Telefonkarte, welche keine Sicherheitsfunktionen besitzt. Die im Bereich des

Mobilfunks eingesetzten Chipkarten enthalten bereits eine Überprüfung der PIN (Personen-Identifikations-Nummer) sowie Authentisierungsalgorithmen.
Die Chipkarte ist eine Plastikkarte im Scheckkartenformat, in die ein Microchip eingebettet ist, welcher ein oder mehrere Speicher, Kontakte (z. B. für den Datenaustausch) und auch einen Microprozessor enthalten kann. Sie ist wesentlich komplexer und vielfältiger nutzbar als Karten mit Magnetstreifen, die "nur" etwa 150 Zeichen aufnehmen und durch Hitze oder mechanische bzw. magnetische Beschädigungen unbrauchbar werden können.

15.10.1 Unterscheidungsmerkmale bei Chipkarten

Chipkarten können nach der Art des Chips, der Art der Datenübertragung und nach zusätzlichen Merkmalen unterschieden werden.

15.10.1.1 Unterscheidung nach Art des Chips

In der Chipkartentechnik werden unterschiedliche Speicherelemente eingesetzt, deren Kombination unter anderem die Leistungsfähigkeit eines Chips charakterisiert. Folgende Speicherelemente kommen wahlweise zum Einsatz:

ROM - Ist ein Speicher, aus dem Informationen nur gelesen werden können. Die Informationen sind eingebrannt, permanent vorhanden und fälschungssicher.
EPROM - Ist ein elektrisch programmierbarer Speicher, dessen Inhalt durch Bestrahlung mit ultraviolettem Licht gelöscht werden kann. Durch das Einbetten des Chips in die Plastikkarte ist ein Löschen mit dem notwendigen UV-Licht allerdings nicht mehr möglich.
Auf den ROM/EPROM einer Chipkarte können z. B. Grundfunktionen, Übertragungsprotokolle und Kryptoalgorithmen gespeichert werden.
EEPROM - Ist ein Speicher, der elektrisch programmierbar und löschbar ist. Auf den EEPROM einer Chipkarte können z. B. Karteninhaber, Kartenherausgeber, Schlüssel, Zustandsgraph (welcher die Ablaufreihenfolge von Prozeduren vorgibt), PIN-Prüfung, ausgewählte Telefonnummern gespeichert werden. Eine Zugriffskontrolle, wann und wie auf Daten zugegriffen werden darf, kann ebenfalls über ein Kontrollfeld im EEPROM durchgeführt werden.
RAM - Ist ein "flüchtiger" Arbeitsspeicher, bei dem die Informationen im spannungslosen Zustand verloren gehen. Auf den RAM einer Chipkarte kann z. B. der augenblickliche Abarbeitungsstand einer Zustandsleiste gespeichert werden, in der vermerkt wird, welche sicherheitsrelevanten Prozeduren bereits abgearbeitet wurden.

Aufgrund der Kombination dieser Speicherelemente werden die Chipkarten nach Art des Chips unterschieden:
- **Einfache Speicherchipkarten** enthalten im allgemeinen nur einen Datenspeicher zur Speicherung anwendungsindividueller Daten, die einmal oder mehrmals beschrieben und beliebig ausgelesen werden können.
  Die Karte enthält keine vorgeschaltete Sicherheitslogik.
  Beispiele:
  - einfache Telefonkarte
  - Krankenversichertenkarte
- **Intelligente Speicherchipkarten** enthalten eine festverdrahtete Sicherheitslogik, die allerdings nur einen bedingten Schutz (PIN-Prüfung) bezüglich der Vertraulichkeit und Integrität der gespeicherten Daten bietet.
  Beispiel:
  - Zugangsberechtigungskarte
- **Prozessorchipkarten** enthalten zusätzlich zu den Speichern einen eigenen Mikroprozessor. Der Mikroprozessor, mit einem eigenen Betriebssystem versehen, übernimmt dabei die Koordinierung der Abläufe, die Verwaltung der Systemressourcen und die Abschottung von Speicherbereichen. Neben der hohen Speicherkapazität bietet die Prozessorchipkarte die Möglichkeit, Daten im Chip der Karte zu verarbeiten.
  Prozessorchipkarten, ergänzt um einen Kryptocoprozessor, werden auch als Krypthographische Karten bezeichnet und können zur Absicherung der Daten zur "Verschlüsselung" eingesetzt werden.
  Die Prozessorchipkarte bietet unter anderem die Möglichkeiten, daß der Benutzer der Karte sein eigenes Paßwort selbst ändern kann und daß Berechnungen für kryptographische Protokolle ausgeführt werden können.
  Beispiele:
  - österreichische EC-Karte
  - geplante deutsche EC-Karte
  - multifunktionale Mitarbeiterkarte (Zutrittsberechtigung, Gleitzeiterfassung, Inanspruchnahme von Dienstleistungen)
  - geplante Gesundheitskarte/Patientenkarte
  - Zugang zu Online-Diensten und Netzwerken

15.10.1.2 Unterscheidung nach Art der Datenübertragung

Bei der Datenübertragung wird zwischen kontaktbehafteten und kontaktlosen Chipkarten unterschieden.
Die **kontaktbehaftete** Chipkarte muß in ein Lesegerät eingeführt werden. Die Fühler in dem Lesegerät greifen auf die Kontaktfläche der Chipkarte und stellen eine Verbindung her. Die kontaktbehaftete Chipkarte beinhaltet Kontakte unter anderem für den Input (Eingabe)/ Output (Ausgabe) und die Versorgungsspannung.
Bei der **kontaktlosen** Chipkarte wird die Chipkarte kontaktlos an dem jeweiligen Lesegerät im vorgeschriebenen Abstand vorbeigeführt.

15.10.1.3 Unterscheidung nach zusätzlichen Merkmalen

Zur Zeit unterscheidet man nach Hybridkarten, hybride Opto-Chipkarten und Superchipkarten.
Hybridkarten verfügen zusätzlich zum Chip über einen Magnetstreifen.
Die hybriden Opto-Chipkarten - enthalten wie normale Hybridkarten - einen Chip und einen Magnetstreifen und zusätzlich für große Datenmengen einen optischen Speicher.
Sogenannte Superchipkarten können neben dem Chip über Anzeige, Tastatur, Batterie oder vereinfachte Terminals verfügen.

15.10.2 Sicherheitszertifikat für Chipkarten

Durch die technische Entwicklung der Chipkarte in den letzten Jahren, hat sich die Chipkarte (Microprozessorchipkarte) als kleiner Minicomputer und somit als wesentliche Komponente komplexer IT-Systeme entwickelt.
Um den vom Hersteller zugesagten Sicherheitseigenschaften vertrauen zu können, erteilt das BSI auf Antrag des Herstellers ein Sicherheitszertifikat für deren entwickelte Chipkarte. Diesem Zertifikat geht eine technische Prüfung (Evaluierung) nach einheitlichen Sicherheitskriterien voraus.
Das BSI führt ständig eine aktuelle Liste über zertifizierte Produkte, die es Anwendern und Nutzern ermöglicht, sich über “sichere” Produkte zu informieren.

15.10.3 Datenschutz bei Chipkarten

Informationen, die auf einer Chipkarte gespeichert sind, können nur mit Hilfe von technischen Geräten (Lesegeräte, Kartenterminals) gelesen, geändert und kopiert werden. Fälschungen von Chipkarten und Manipulationen von Daten sind bei einfachen Speicherchipkarten, die über keine Sicherheitsfunktionen verfügen, möglich. Bei dem Einsatz von Chipkarten, einschließlich der infrastrukturellen Umgebung, können sich weitere Gefahren durch das Abhören und Manipulieren unverschlüsselter Daten auf dem Übertragungsweg (Chipkarte-Lesegerät-Rechner) durch Dritte ergeben.
Zur Zeit wird nur die kontaktbehaftete Prozessorchipkarte mit der ihr zur Verfügung stehenden “Intelligenz” hohen Sicherheitsanforderungen gerecht, z. B. durch den Einsatz von kryptographischen Verfahren und durch die Kontrollmöglichkeiten von Speicherbereichen.
Datenschutzrechtlich nicht unbedenklich ist für den Benutzer auch die nicht transparente Bearbeitung der Chipkarte im Lesegerät. So ist dem Nutzer eine Kontrolle, inwieweit nur die gewünschten Abarbeitungsprogramme aktiv sind, nicht möglich. Zum Beispiel können unerlaubte Hintergrundprogramme und Datenweiterleitungen nicht festgestellt werden.
Eine weitere Gefahr aus Sicht des Datenschutzes ist auch der mögliche Einsatz von Chipkarten für ursprünglich nicht vorgesehene Anwendungen.
Hier zeigt sich, daß nicht nur technisch bessere Voraussetzungen zur Sicherheit der Chipkarten wichtig sind, sondern auch gesetzliche Maßnahmen notwendig sind, um eine entsprechende Zweckentfremdung der Karte zu unterbinden.
Um datenschutzrechtlichen Gefahren begegnen zu können, sollten folgende technische Sicherheitsmaßnahmen auf der Chipkarte vollzogen werden:
- Authentisierung/Echtheitsprüfung des Benutzers,
- Authentisierung des Dialogpartners,
- digitales Signieren sensibler personenbezogener Daten, um die Sicherstellung der Datenintegrität und des Ursprungs der Daten zu gewährleisten,
- Verschlüsselung der zu übertragenden Daten, wobei die Daten bereits auf dem Chip verschlüsselt werden sollten.

Für die Nutzer einer Chipkarte empfiehlt es sich, in jedem Fall die Vorteile, die ohne Zweifel existieren, mit den Nachteilen abzuwägen. Bei einer freiwilligen Entscheidung für den Einsatz einer Chipkarte sollte jedoch darauf geachtet werden, daß der Rückweg zur konventionellen Methode weiterhin offen steht.

Deshalb sollte sich jeder Nutzer vor dem Einsatz der Chipkarte fragen:
- Ist der Einsatz der Chipkarte unbedingt notwendig?
- Sind die Vorgänge auf der Chipkarte nachvollziehbar?
- Entstehen Nachteile bei Nichtvorzeigen der Karte an Dritte?
- Welcher Schaden tritt bei Verlust der Karte ein?

15.11 Optische Datenspeicher - datenschutzrechtliche Aspekte

Die optische Datenspeicherung entwickelt sich in zunehmenden Maße zu einer Alternative für herkömmliche magnetische Datenträger. Der Begriff optische Datenspeicherung ist abgeleitet vom zugrundeliegenden Aufzeichnungsverfahren mit Hilfe eines Laserstrahles. Anders als bei herkömmlichen Festplatten, deren Schreib-Leseköpfe auf rein magnetischer Basis arbeiten, ist bei den optischen Laufwerken der Laserstrahl zentraler Bestandteil des Gerätes. Durch die Lasertechnologie sind optische Speichersysteme äußerst robust und verfügen über sehr hohe Speicherkapazitäten. Im Gegensatz zu magnetischen Datenträgern gehen hier die Informationen auch bei sehr langen Aufbewahrungszeiten nicht verloren.
Bei einer CD-ROM handelt es sich um einen Nur-Lese-Speicher. Der Anwender kann keinerlei Daten auf die CD schreiben. Die digitalen Daten werden beim Preßvorgang durch einen Laser in Form von Vertiefungen oder Erhöhungen, je nach Intensität des Laserstrahles, fest in das Plastiksubstrat der Oberfläche eingebrannt. Beim Lesen interpretiert die Laufwerkselektronik aus dem unterschiedlichen Reflexionsverhalten des Laserstrahls (bedingt durch die Erhebungen oder Vertiefungen) wieder digitale Daten.
Bei den WORM-Laufwerken handelt es sich im Grunde um CD-ROM-Laufwerke, die nicht nur lesen, sondern auch spezielle CD-ROM-Rohlinge beschreiben können. Die zu speichernden Informationen werden über einen Schreiblaser in die Oberfläche des Speichermediums eingebrannt. Die Oberflächenstruktur ist der CD identisch. An denjenigen Stellen, an denen eine Vertiefung entstehen muß, brennt der Laser das darüberliegende Material weg. Die einmal aufgebrachte Datenstruktur ist nicht mehr zu verändern. WORM-Laufwerke eignen sich daher für die dauerhafte Archivierung von Datenbeständen. Das Lesen erfolgt wie bei der CD durch einen Leselaser.
Magneto-optische (MO)-Laufwerke gewährleisten die Wiederbeschreibbarkeit des Speichermediums. Hier kommen Speichermedien mit hartmagnetischem Material zum Einsatz. Im Zusammenspiel von Laser und Magnetismus werden die Daten auf die magnetische Oberfläche der MO-Scheibe geschrieben. Ein kleiner Hitzelaser erwärmt gezielt das Speichermedium im zu beschreibenden Bereich und die Ausrichtung der Magnetpartikel wird durch den internen Magnetkopf der MO-Laufwerke verändert. Das Lesen erfolgt mit Hilfe eines polarisierten Laserstrahls, wobei sich die Drehrichtung des reflektierten Lichtes je nach der Ausrichtung der Magnetpartikel verändert. Anhand der unterschiedlichen Drehrichtung werden wieder die digitalen Daten erzeugt. Die MO-Laufwerke vereinen die hohen Speicherkapazitäten der optischen Speichermedien und die unbegrenzte Wiederbeschreibbarkeit der magnetischen Medien.
Bei der Auswahl von in der Praxis einzusetzenden Datenträgern müssen bei einer Speicherung personenbezogener Daten auch datenschutzrechtliche Gesichtspunkte beachtet werden. Der AK Technik der Konferenz der DSB des Bundes und der Länder hat deshalb auch eine Empfehlung für einen datenschutzgerechten Einsatz dieser optischen Medien erarbeitet (siehe Anlage 32).
Unter den Voraussetzungen der §§ 14 bis 16 ThürDSG haben Betroffene Anspruch auf Berichtigung, Sperrung und auf Löschung ihrer personenbezogenen Daten. Mit herkömmlichen magnetischen Datenträgern (Magnetplatte, Diskette) können diese Forderungen problemlos realisiert werden. Im Gegensatz dazu können diese datenschutzrechtlichen Anforderungen bei CD-ROM und WORM-Platte nur bedingt realisiert werden.
Der Begriff “Löschen” wird in § 3 Abs. 3 Nr. 3 ThürDSG als das Unkenntlichmachen gespeicherter personenbezogener Daten definiert. In Ziffer 3.6 VVThürDSG wird weiterhin dazu aufgeführt: “Können Daten nur unter Zuhilfenahme technischer Mittel zur Kenntnis genommen werden (z. B.: auf Magnetbändern durch Datenverarbeitungsanlagen), dann sind sie unkenntlich, wenn durch technische oder organisatorische Mittel sichergestellt ist, daß sie von niemanden zur Kenntnis genommen werden können.” Ein Löschen gemäß § 3 ThürDSG ist weder bei CD-ROM noch bei WORM-Platten technisch möglich. Die aufgezeichneten Daten können nur logisch gelöscht werden. Dieses wird durch die Verwaltungssoftware über entsprechende Verweisdaten gesteuert und für deren Einsatzbereich abgesichert. Mittels spezieller Software ist es jedoch möglich, auf die physisch noch vorhandenen personenbezogenen Daten unbefugt Zugriff zu nehmen.
Um die gesetzlichen Löschungsfristen zu gewährleisten, müssen somit innerhalb kürzester Zeit die Datenbestände ohne die zu löschenden Daten auf einen neuen Datenträger kopiert werden. Der ursprüngliche Datenträger ist dann unverzüglich physisch zu vernichten.
Auch das Berichtigen von Daten durch Überschreiben der Ursprungsdaten ist bei beiden optischen Speicherformen nicht möglich. Bei einer WORM-Platte kann jede unbeschriebene Stelle aufgrund der eingesetzten Aufzeichnungstechnik nur ein einziges Mal mit Daten beschrieben werden.

Sperren ist nach § 3 Abs. 3 Nr. 4 ThürDSG das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken. Das Sperren bestimmter Daten oder logischer Datensätze ist bei einer WORM-Platte möglich. Entsprechende Kennzeichen werden durch die Verwaltungssoftware in den Verweisdaten gesetzt und bei der Verarbeitung entsprechend berücksichtigt.
Das nach § 3 ThürDSG erforderliche Löschen der Daten kann nach § 15 Abs. 1 Nr. 2 ThürDSG durch eine Sperrung ersetzt werden, falls eine Löschung aus den in § 16 Abs. 4 ThürDSG genannten Gründen unterbleibt. So kann z. B. nach § 16 Abs. 4 Nr. 2 ThürDSG eine Löschung unterbleiben, wenn wegen der besonderen Art der Speicherung eine Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Damit sind die Voraussetzungen für Punkt 2 der Empfehlung (siehe Anlage 32) im Freistaat Thüringen gegeben.

15.12 Protokollierung, Protokolldateien

Das Aufzeichnen sicherheitsrelevanter Vorgänge stellt eine wichtige Maßnahme im Sinne des technischen und organisatorischen Datenschutzes dar. Gemäß § 9 Abs. 2 Nr. 7 ThürDSG ist zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind. Für den Einsatz von Protokollierungsfunktionen gilt der Grundsatz der Angemessenheit bzw. Verhältnismäßigkeit. Nach § 9 Abs. 1 ThürDSG ist eine solche Maßnahme nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebtem Schutzzweck steht.
Eine wahllose Protokollierung aller Aktivitäten eines Benutzers ist datenschutzrechtlich bedenklich. Für Anwendungen, die bezüglich der zu verarbeitenden personenbezogenen Daten einen hohen Schutzbedarf erfordern, sollte eine umfassende Registrierung der Benutzeraktivitäten erfolgen. Auch die Endgeräte (Terminals, PC) sind hier in die Protokollierung mit einzubeziehen.
Protokolldateien enthalten personenbezogene Daten. Sie unterliegen nach § 20 Abs. 4 ThürDSG dem Grundsatz der Zweckbindung, d. h. sie dürfen ausschließlich nur zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert oder nur für diese Zwecke verwendet werden. Der geplante Einsatz von Protokolldateien sollte dem Personalrat rechtzeitig angezeigt werden, weil Protokolldateien unzulässigerweise zu Verhaltens- und Leistungskontrollen herangezogen werden können. Ihr Einsatz unterliegt demzufolge der Mitbestimmung des Personalrates gemäß § 74 Abs. 3 Nr. 18 und 19 ThürPersVG. Es empfiehlt sich, in einer Vereinbarung mit dem Personalrat den Protokollierungsumfang, die zu protokollierenden Daten, die Löschungsfristen sowie die Modalitäten der zulässigen Auswertung der Dateien festzulegen. Hierbei ist der bDSB zu beteiligen.
Protokolldateien sind nach einer angemessenen Zeit zu löschen. Eine Speicherungsdauer von einem Jahr für Zwecke der Datenschutzkontrolle wird als ausreichend angesehen. Die Protokollierung ist kein Selbstzweck, sondern sinnvoll und datenschutzrechtlich vertretbar, wenn die Protokolldaten auch tatsächlich ausgewertet werden. Zur Beseitigung bestehender Unklarheiten bei den Anwendern, ob und wieweit die Protokollierung notwendig und möglich ist, hat der AK Technik der Konferenz der DSB des Bundes und der Länder eine Arbeitshilfe zur Protokollierung erarbeitet. Diese Orientierungshilfe wurde unter Beachtung der datenschutzrechtlichen Vorschriften des Freistaats Thüringen überarbeitet und sollte grundsätzlich beim Einsatz von Protokolldateien beachtet werden (siehe Anlage 31).

15.13 Internet - die Mutter der Netze

Das Internet ist das älteste und zur Zeit größte globale Computernetzwerk der Welt. Es wird von geschätzten 35 - 40 Millionen Teilnehmern als internationales Informations- und Kommunikationsforum genutzt. Das ursprünglich gesetzte Ziel, einen Datenaustausch und einen Zugriff auf Rechnerleistungen zu realisieren, nutzten immer mehr Universitäten als elektronischen Wissenschaftsverbund. Charakteristisch für das Internet ist seine fast im Selbstlauf erfolgte Entwicklung. Zur Zeit vollzieht das Internet wieder eine Wandlung, und zwar vom reinen Wissenschaftsnetz zum kommerziellen Kommunikationsmedium.
Heute besteht das Internet aus nationalen und lokalen Netzwerken, die weltweit ca. drei Millionen Rechner zusammenschließen. Davon befinden sich allein in den USA ca. zwei Millionen Rechner. Das Internet ist also kein homogenes Gebilde, sondern ein heterogener Verbund lokaler Rechnernetze, die alle über die Protokollfamilie TCP/IP kommunizieren und durch die nationalen Network Information Centers (NIC) logistisch verwaltet werden. Es ist ein reines Transportnetz, über das andere Netze und Dienste verbreitet werden. Jeder lokale Betreiber kann hierbei das Angebot selbst bestimmen.
Wesentliche im Internet angebotene Dienste sind:
- E-Mail (elektronische Post, digitaler Nachrichtenaustausch),
- Usenet-News (öffentliche Teilnahme an weltweiten Diskussionsforen),
- FTP-File Transfer Protocol (Übertragen von Dateien),
- Telnet (Aufbau einer Terminalsitzung zu einem entfernten Rechner, z. B. um dessen Rechenleistung zu nutzen),

- WAIS - Wide Area Information Server (unkomplizierte Textrecherche in zur Zeit ca. 600 Datenbanken),
- Gopher (Menügesteuerte Recherche von Informationen in Dokumenten, die zu bestimmten Fachthemen auf den sogenannten Gopher-Server abgelegt sind),
- WWW - World Wide Web (Zusammenfassung der Dienste FTP, WAIS und Gopher unter einer komfortablen grafischen Hypertextoberfläche, wobei zusätzlich die integrierte Übertragung von Grafik und Ton möglich ist. Die aktuellen Informationen werden auf WWW-Servern bereitgestellt).

Mit WWW wird das multimediale Zeitalter auch im Internet eingeleitet. Durch die einfache Bedienung wird somit das Internet zunehmend auch für kommerzielle Anbieter und gelegentliche Nutzer immer attraktiver.

Den vielfältigen Möglichkeiten der vereinfachten Kommunikation und Beschaffung von Informationen durch das Internet stehen allerdings auch schwer zu lösende Sicherheitsprobleme gegenüber. Derzeit stellt es ein offenes Kommunikationsnetz dar, das nicht kontrollierbar ist. Sicherheitsaspekte spielten bisher eine untergeordnete Rolle. Sicherheitsprobleme ergeben sich insbesondere aus den zur Datenübertragung verwendeten Protokollen, den im Internet benutzten Diensten und den eingesetzten Rechnersystemen. Der Verlust der Vertraulichkeit durch ein Mitlesen der Daten und der Verlust der Integrität durch das Manipulieren von Daten stellen eine potentielle Gefahr dar.
Die im Internet verwendeten Protokolle besitzen keine sicheren Mechanismen zur Identifikation und Authentisierung im Netz. Aber auch fehlerhafte Protokoll-Implementierungen auf vielen Systemen schaffen zusätzliche Sicherheitslükken. Die Mehrzahl der im Internet verwendeten Dienste überträgt Benutzernamen und Paßwörter unverschlüsselt. Ohne die Installation geeigneter Schutzmaßnahmen kann ein Angreifer unter Ausnutzung der Sicherheitslücken in die am Internet angeschlossenen Netze einbrechen, sich unberechtigten Zugang auf Netzrechner verschaffen und sich sogar Systemverwalterrechte aneignen. Hat der Angreifer Systemverwalterrechte erlangt, können Daten im lokalen Netz aufgespürt, manipuliert, abgezweigt oder zerstört werden. Ständig werden neue Wege und Methoden bekannt, mit denen aus dem Internet Angriffe auf die angeschlossenen lokalen Netze und Rechnersysteme erfolgen. Da das Internet selbst über keine Schutzvorkehrungen verfügt, muß jeder Anwender selbst für die Sicherheit seiner angeschlossenen Systeme Sorge tragen. Das Ziel ist, nur Berechtigten den Zugang auf das eigene Netz zu ermöglichen, sowie Angreifer als solche zu identifizieren und abzuwehren.
Die entwickelten und auf dem Markt angebotenen Schutzkonzepte basieren in der Regel auf speziell konfigurierten Rechnern, welche die Kommunikation zwischen dem Internet und einem an diesem angeschlossenen System, wie z. B. ein internes Netz, überwachen und kontrollieren. Solche als Firewall-Systeme bezeichnete Konzepte stellen durch technische und administrative Maßnahmen sicher, daß eine Kommunikation zwischen Netzen nur noch über eine solche zwischengeschaltete Firewall geführt werden. Eine unkontrollierte Kommunikation wird somit verhindert.
Die Firewall-Konzepte unterscheiden sich bezüglich ihrer Funktionalität, des erzielbaren Schutzes und der Transparenz der Internet-Dienste für den Benutzer. Einfache Konzepte ermöglichen eine Beschränkung der Kommunikation auf bestimmte Richtungen, auf bestimmte im Internet benutzte Dienste und auf ausgewählte Rechner. Benutzerbezogene Festlegungen sind hier nicht möglich. Angreifer werden nicht oder zu spät erkannt, da keine System- und Ablaufprotokollierung (Audit) erfolgt. Weiterhin sind keine starken Authentisierungsverfahren zur Überprüfung von Berechtigungen integriert. Solche Firewall-Typen werden als Screening Router oder Packet-Screen bezeichnet. Zum Einsatz kommen in der Regel Router mit entsprechenden Schutzfunktionen, die auf einem Prüfen der ein- und ausgehenden Datenpakete basieren. Sie erlauben eine einfache Installation und Administration des Systems. Weiterhin sind die Internet-Dienste für die Benutzer transparent, das heißt, für ihre Nutzung sind keine Anpassungen vorzunehmen.
Durch die Erweiterung dieses einfachen Konzeptes um einen zusätzlichen Rechner (Bastion-Host), der zwischen das zu schützende eigene Netz und das Internet installiert ist, können die aufgezeigten Nachteile vermieden werden. Der Router wird in diesem Fall so konfiguriert, daß jeglicher Datenverkehr über die Bastion erfolgt, in der die Kontrolle der Kommunikation auf der Anwendungsebene vollzogen wird. Dadurch kann ein weitergehender und flexiblerer Schutz implementiert werden als beim einfachen Konzept. Erweiterte Konzepte verfügen über Zugriffskontroll- und Auditmechanismen und gestatten eine nutzerspezifische Funktionalität. Angriffe können durch ein erweitertes Audit schnell erkannt werden. Eine Identifikation und Authentisierung der Benutzer ist möglich. Allerdings erfordert ein transparentes Nutzen der Internet-Dienste zusätzliche Aufwendungen. Durch den alleinigen Einsatz eines Bastion-Host mit zwei Netzanschlüssen (Dual Home Gateway) kann eine physikalische Netztrennung erzielt werden, die wirksamer ist, als die durch das Routen erfolgte logische Trennung. Der Anschluß öffentlicher Stellen an das Internet bzw. an öffentliche (globale) Netze ist angesichts der aufgezeigten Gefahren aus der Sicht des Datenschutzes nur vertretbar, wenn ihr Kommunikationsbedarf dies zwingend erfordert und zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und entsprechende Gegenmaßnahmen ergriffen werden.
Eine Orientierungshilfe zum Anschluß öffentlicher Stellen an das Internet ist in der Anlage 30 enthalten.

15.14 Kontrolltätigkeit - Schwerpunkte und Empfehlungen

Bei der Beratungs- und Kontrolltätigkeit des TLfD war mehrfach festzustellen, daß Datensicherungsmaßnahmen fehlten und vorhandene Sicherheitsmechanismen nicht ausreichend genutzt wurden.
So fehlten z. B. aus finanziellen Gründen Aktensicherungsschränke, Aktenvernichtungsgeräte und sichere Aufbewahrungsmöglichkeiten für Datensicherungen und Programmquellen. Die dienstlichen Regelungen zur Vernichtung von Schriftgut und Datenträgern sowie Schlüsselordnungen konnten nicht immer vorgelegt werden.

15.14.1 PC - Sicherheit

Auf Grund von durchgeführten Kontrollen wird auf folgende Sicherheitsmechanismen hingewiesen, die zu beachten sind:
- Es ist ein BIOS-Paßwort einzurichten, welches beim Booten des PC automatisch abgefragt wird.
- Um den unerlaubten Zugriff auf PC zu verhindern, sind alle Diskettenschächte und Laufwerke verschlossen zu halten.
- Ein Zugriff auf die Betriebssystemebene sollte für den normalen Nutzer ausgeschlossen sein. Hierzu ist eine lückenlose Menütechnik anzustreben.
- Programme und Daten sind in unterschiedlichen Verzeichnissen zu speichern.
- Regelmäßig muß eine Kontrolle auf Virenprogramme durchgeführt werden.
- Eine Verarbeitung personenbezogener Daten (siehe auch Punkt 15.3) z. B. unter dem Betriebssystem MS-DOS sollte in der Regel nur mit zusätzlicher Sicherheitssoftware durchgeführt werden, die entsprechend dem Grad der Schutzwürdigkeit der Daten eine Benutzeridentifikation und -authentisierung, Verwaltung und Prüfung der Zugriffsberechtigungen, Verschlüsselung der Daten sowie eine Protokollierung (siehe Punkt 15.12) ermöglicht. Die Anzahl der fehlerhaften Login-Versuche ist zu begrenzen (z. B. nur fünf fehlerhafte Anmeldeversuche erlauben).
- Bei sehr sensiblen personenbezogenen Daten ist auch eine Protokollierung über den Zugriff auf die Daten (wer, wann, wie auf welche Daten zugegriffen hat) durch das Anwenderprogramm zu gewährleisten (siehe Punkt 15.12).

15.14.2 Einsatz von Netzwerkbetriebssystemen

Schon bei der Planung eines Netzwerkes sind in jedem Fall Vorüberlegungen zum Schutz der zu verarbeitenden Daten zu treffen (siehe Punkt 15. 6).
Aufgrund der durchgeführten Kontrolltätigkeit erscheint es notwendig, auf bestimmte Sicherheitsmaßnahmen bei der Verarbeitung von personenbezogenen Daten in Netzwerken einzugehen:
- Die jeweilige Servertastatur ist zu sperren.
- Ein Zugriff auf bzw. eine unberechtigte Einsichtnahme in schutzwürdige Daten durch den Netzwerkverwalter muß verhindert werden. Wenn dieses nicht im Netzwerk eingerichtet werden kann, ist eine Verschlüsselung dieser Daten vorzunehmen.
- Für jeden Nutzer sollte eine Kontoführung (Account) eingerichtet werden, um so alle Login- und Logout-Vorgänge, die Dauer des Logins eines Nutzers und die Anzahl der gelesenen Datenblöcke verfolgen zu können.
- Eine Protokollierung, wer zu welcher Zeit mit welchen Mitteln zu welchem Zweck auf welche Dateien zugegriffen hat, ist bei einigen Netzwerksystemen nur unter Verwendung von Zusatzprodukten, welche die wichtigsten Aktivitäten der Benutzer, wie Öffnen, Lesen, Schreiben, Umbenennen und Löschen von Dateien auf einem Server protokollieren, möglich.
- Logisch gelöschte Dateien mit personenbezogenen Daten sind auch physisch zu löschen, um so die Rekonstruierbarkeit der Dateien zu verhindern. Bei sehr sensiblen personenbezogenen Daten muß beim Löschen der Dateien (bei Betätigung der Del-Taste oder Entf-Taste) das sofortige physische Löschen automatisch erzwungen werden.
- Die Informationen, die für die Benutzer definiert wurden und der Zugangssicherheit dienen, müssen in regelmäßigen Abständen kontrolliert werden, um mögliche Sicherheitsverletzungen aufzudecken. Für viele Netzwerke gibt es zusätzliche Sicherheitssoftware, die z. B. komplexe Übersichten erstellen über:
  - Verzeichnisstruktur,
  - Anzahl der definierten Nutzer,
  - Gruppenübersicht einschließlich Rechte,
  - für jeden Nutzer aufgeschlüsselt: Einstellungen zur Kontoführung und zur Paßwortregelung, Zugehörigkeit zu Gruppen, Gleichstellung zu anderen Nutzern, Nutzer Login Script, vergebene Zugriffsrechte.

Login-Ebene:
Für jeden Nutzer ist eine individuelle Benutzerkennung zu vergeben, wonach die Bereitstellung bestimmter Ressourcen erfolgt. Sollte ein Nutzer mehrere streng getrennte Aufgabengebiete bearbeiten, so sind für ihn mehrere Benutzerken-

nungen zu vergeben (z. B. bei EDV-Verantwortlichen, die noch andere Fachgebiete bearbeiten).
Um einer unbefugten Kenntnisnahme des Paßwortes vorzubeugen, sollte bei Netzwerken, die eine Verschlüsselung des Paßwortes anbieten, dieses auch aktiviert werden.
Bei den Kontrollen mußte oft die fehlende bzw. nicht konsequent geführte Paßwortregelung bemängelt werden. Besonders häufig wurde dem TLfD gegenüber die Meinung vertreten, daß das jeweilige Gebäude ausreichend gesichert sei und nur zuverlässige Mitarbeiter eingestellt würden.
Zum anderen besteht teilweise die Auffassung, daß bei gekaufter Anwendersoftware mit integrierter Paßwortregelung, auf die Paßwortsicherheit des Netzwerksystemes verzichtet werden kann. Aus datenschutzrechtlicher Sicht ist eine Vergabe von Paßwörtern auf der Netzwerkebene unbedingt zu aktivieren, um so einen unerlaubten Zugriff auf personenbezogene Daten z. B. über die Betriebssystemebene zu verhindern.
Bei der Bildung von Nutzer-Paßwörtern sind die allgemeinen Regeln zu beachten:
- das Paßwort muß für jede Benutzerkennung eingerichtet werden,
- es muß aus mindestens fünf alphanumerischen Zeichen (einschließlich Sonderzeichen) bestehen,
- der Paßwortwechsel muß mindestens alle drei Monate automatisch erzwungen werden,
- unabhängig von der Forderung, in festgelegten Zeitabständen, z. B. alle drei Monate, automatisch den Paßwortwechsel zu erzwingen, sollte den Benutzern die Möglichkeit eingeräumt werden, jederzeit einen Paßwortwechsel durchzuführen,
- das Paßwort selbst darf nicht zu trivial sein.

Eine vom Netzwerksystem angebotene Zeiteinschränkung für den Benutzer muß spezifiziert werden, wenn Nutzer sich nur an bestimmten Tagen und/oder zu bestimmten Stunden einloggen dürfen.
Eine notwendige Stationseinschränkung macht sich erforderlich, wenn bestimmte Arbeitsstationen nur von bestimmten Nutzern oder bei bestimmten Anwendungen genutzt werden dürfen.

Rechte-Ebene:
Bei Kontrollen wurde weiterhin festgestellt, daß eine gewisse Unsicherheit in der Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse besteht. Empfehlenswert ist eine getrennte Ablage von Programm- und Datendateien in unterschiedlichen Verzeichnissen.
Wenn mehrere Benutzer in einem Verzeichnis Dateien je nach Aufgabenstellung unterschiedlich nutzen, so sind nicht nur für das Verzeichnis die jeweiligen Benutzer-Zugriffsrechte, sondern auch für die darin enthaltenen Dateien entsprechende Zugriffsrechte für die einzelnen Benutzer einzurichten.
In einigen Behörden wurden den Sachbereichen von dem Netzwerkverwalter zu weitreichende Zugriffsrechte eingeräumt. Den Sachbereichen war es dadurch technisch möglich, eigenständig die Rechtevergabe zu ändern und Rechte an andere User zu erteilen, ohne selbst darüber zu verfügen.
Hier zeigt sich deutlich, wie berechtigt die Forderung ist, mindestens bei der Verarbeitung sensibler personenbezogener Daten eine vom Netzwerkverwalter unabhängige Kontrollperson mit für die Vergabe von Zugriffsrechten zu benennen und somit nach dem Vier-Augen-Prinzip zu verfahren.

Attribut-Ebene:
Netzwerke bieten zum Teil die Möglichkeit, Attribute für Verzeichnisse und/oder Dateien zu vergeben, die unabhängig von den Zugriffsrechten vergeben werden können, und darüber zu entscheiden, ob ein Verzeichnis oder eine Datei gelöscht, aufgelistet oder beschrieben werden darf. Diese Sicherheitsmechanismen sollten unbedingt eingesetzt werden, wenn die Anwendungen einen solchen Schutz hierfür erfordern.

15.14.3 Kontrolle eines Rechenzentrums

Die Kontrolle der Zentralen Gehaltsstelle Thüringen (ZGT) durch den TLfD (siehe Punkt 6.3) bezog auch eine Prüfung des Sachbereichs Rechentechnik hinsichtlich der Realisierung und Einhaltung der nach § 9 ThürDSG erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz ein.
Das komplexe integrierte Bezügeverfahren (Besoldung, Versorgung, Bezüge, Lohn) wird auf der Grundlage eines spezifischen Softwareeinsatzes abgearbeitet. Die Neben- und Außenstellen sind über Standleitungen bzw. Vorrechner mittels Terminal oder PC (Emulation) im Dialog mit dem Host-Rechner verbunden.
Ein integratives Sicherheitssystem ermöglicht einen dem derzeitigen Stand der Technik entsprechenden beispielhaften Objekt- und Raumschutz.
Bei der Prüfung wurden, obwohl insgesamt umfangreiche Sicherungsmaßnahmen nach § 9 ThürDSG realisiert waren, u. a. folgende Schwachstellen bzw. Mängel festgestellt:
- Die Identifikation auf der Betriebssystemebene erfolgte nur durch die Eingabe einer Gruppenkennung. Ein revisionsicherer Nachweis der Aktivitäten der jeweiligen Benutzer einschließlich der Systemverwalter auf der Betriebssystemebene war somit nicht möglich. Weiterhin war ein automatisch erzwingbarer Paßwortwechsel, z. B.

nach Ablauf einer vorgegeben Zeitdauer, nicht vorgesehen. Auch eine Limitierung der Anzahl abgewiesener Anmeldevorgänge erfolgte nicht.
Der TLfD forderte deshalb, daß der Paßwortwechsel automatisch vom System nach einer vorgegeben Zeitspanne erzwungen werden muß, die Anzahl der abgewiesenen aufeinanderfolgenden Anmeldungen zu begrenzen ist und die verwendeten Gruppenkennungen durch eine eindeutige Identifikation und Authentifikation jedes einzelnen Benutzers und der Systemverwalter für das Betriebssystem zu ersetzen ist.
Hierfür wurde der Einsatz spezieller Sicherheitssoftware empfohlen.
Weiterhin sind die protokollierten abgewiesenen Anmeldeversuche kontinuierlich zu kontrollieren und festgestellte diesbezügliche Unregelmäßigkeiten auszuwerten.
- Die Funktionsabschottung, daß jeder Benutzer im Bezügeverfahren nur Zugriff auf die ihm aufgabenbezogen zugeordneten Daten haben darf, war nicht durchgängig realisiert.
  Die Vergabe der Zugriffsrechte muß konsequent unter Berücksichtigung einer Vertretungsregelung anhand einer vorgegeben Berechtigungsstruktur, welche den geforderten restriktiven Zugriff vorgibt, erfolgen.
- Bezüglich der durchzuführenden Datenübermittlungen ist eine Dienstanweisung zu erarbeiten.

Die aufgezeigten datenschutzrechtlichen Mängel wurden behoben bzw. befinden sich in Realisierung.

15.14.4 Anlaßbezogene Kontrolle einer TK-Anlage

Eine vom TLfD durchgeführte Prüfung der TK-Anlage einer öffentlichen Stelle zeigte wesentliche datenschutzrechtliche Mängel auf:
- Eine datenschutzrechtliche Freigabe des Verfahrens nach § 34 Abs. 2 ThürDSG lag nicht vor.
- Eine Dienstvereinbarung zwischen der Leitung und dem Personalrat war nicht abgeschlossen worden.
- Grundsätzliche Regelungen zum Betreiben der TK-Anlage und Festlegungen zu datenschutzrechtlich relevanten Sachverhalten fehlten. So konnten z. B. keine transparenten Unterlagen vorgelegt werden über installierte und aktivierte Leistungsmerkmale, Art und Umfang der gespeicherten personenbezogenen Daten, Zweckbindung und Löschungsfristen der Daten, Berechtigung zur Aktivierung und Sperrung von Leistungsmerkmalen, revisionssichere Protokollierung des Systemzustandes und Kontrollmaßnahmen.
- Es erfolgte keine Unterscheidung zwischen Dienst- und Privatgesprächen.
- Alle abgehenden Rufnummern wurden vollständig gespeichert, einschließlich der des Personalrates.
- Die Mitarbeiter wurden unzureichend bezüglich des konkreten Einsatztermines der TK-Anlage, der aktivierten Leistungsmerkmale, der eingerichteten Berechtigungsklassen und der gespeicherten Daten informiert. Weiterhin fehlte ein eindeutiger Hinweis darauf, daß bei Privatgesprächen die gleichen Daten wie bei Dienstgesprächen erfaßt werden.
- Es erfolgte keine Protokollierung der systemtechnischen Abläufe, so daß vorgenommene Eingriffe (z. B. durch die Fernwartung der Fremdfirma) nicht nachvollziehbar waren.
- Eine regelmäßige Revision der TK-Anlage (Soll-Ist-Abgleich) war nicht vorgesehen. Somit kann auch nicht festgestellt werden, ob alle nicht vergebenen Rufnummern in der Anlage wirklich gesperrt, verbotene Berechtigungen nirgendwo vergeben und deaktivierte Leistungsmerkmale auch wirklich inaktiv sind.

Die öffentliche Einrichtung hat im konkreten Fall inzwischen die Freigabe des Verfahrens beantragt und mit dem Personalrat eine Dienstvereinbarung abgeschlossen, die alle datenschutzrechtlichen Forderungen berücksichtigt.

15.14.5 Entsorgung von Schriftgut

Überall, wo personenbezogene Daten verarbeitet werden, müssen Datenträger aufbewahrt, transportiert und nach Ablauf der Löschfristen vernichtet werden. Neben magnetischen Datenträgern (Disketten, Magnetbänder, Magnetplatten) und optischen Datenträgern (Mikrofiche, CD-ROM, WORM, MO) ist Papier weiterhin ein wichtiger Datenträger. Auf Datenträgern gespeicherte personenbezogene Daten sind nach § 9 ThürDSG durch technische und organisatorische Maßnahmen zu schützen. Es ist zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle). Insbesondere Schriftgut, das von jedermann unmittelbar gelesen werden kann, sollte vor unbefugter Kenntnisnahme geschützt aufbewahrt werden. Diese datenschutzrechtlichen Forderungen sind in jedem Fall auch bei der Vernichtung bzw. Entsorgung nicht mehr benötigter Datenträger zu beachten.
Durchgeführte Kontrollen offenbarten, daß die Entsorgung von Schriftgut mit personenbezogenen Daten nicht immer korrekt im Sinne der datenschutzrechtlichen Vorschriften erfolgt. So war beispielsweise festzustellen, daß ungesicherte Papierabfallbehälter neben Kopiergeräten aufgestellt waren. Die Kopiergeräte stehen nicht selten an öffentlich zugänglichen Stellen, da sie von vielen Mitarbeitern gemeinsam genutzt werden. Publikumsverkehr ist nicht ausgeschlossen.
Hier liegen Mängel bezüglich o. g. datenschutzrechtlicher Forderungen zur Datenträgerkontrolle vor. Kopiergeräte sollten nicht an öffentlich zugänglichen Stellen aufgestellt werden, wenn auf Ihnen Schriftstücke mit personenbezoge-

nen Daten kopiert werden. Hiervon sollte nur in begründeten Ausnahmefällen abgewichen werden. Eine ordnungsgemäße Entsorgung erfordert auch das Aufstellen von Abfallbehältern, die vor einem unberechtigten Zugriff geschützt sind bzw. statt dieser den Einsatz eines Aktenvernichters oder eines Schredders. So kann vorbeugend ein eventueller Datenmißbrauch durch Unbefugte oder Achtlosigkeit der Mitarbeiter verhindert werden.
Sofern Unterlagen nicht archivwürdig sind, sollten folgende Grundsätze für eine datenschutzrechtliche Entsorgung von Schriftgut mit personenbezogenen Daten beachtet werden:

- Gesetzlich vorgeschriebene Löschungsfristen sind einzuhalten. Falls für den vorliegenden Sachverhalt keine bereichsspezifischen Löschungsvorschriften erlassen sind, sind die Vorschriften in § 16 ThürDSG zu beachten.
- Die Vernichtung von Schriftgut im eigenen Sachbereich mittels eines Aktenvernichters oder eines Schredders ist die einfachste und zugleich sicherste Lösung. Das Sammeln von zu vernichtendem Datenmaterial sollte immer in Behältern erfolgen, die vor unbefugtem Zugriff geschützt sind.
- Die Vernichtung sollte möglichst umgehend erfolgen.
  Wird mit der Entsorgung eine andere Stelle beauftragt, so handelt es sich hierbei um Auftragsdatenverarbeitung gemäß § 8 ThürDSG. Der Auftrag zur Vernichtung der personenbezogenen Daten, die Festlegung zu den technischen und organisatorischen Maßnahmen sowie die Zulassung von Unterauftragsverhältnissen sind schriftlich festzulegen. Der Auftraggeber trägt weiterhin die Verantwortung für eine datenschutzgerechte Vernichtung seiner Daten. Er sollte sich persönlich vor Ort von der sicheren Entsorgung seiner Daten durch den Auftragnehmer überzeugen (siehe Anlage 33).
- Nach § 9 Abs. 2 ThürDSG sind insbesondere drei Maßnahmen bei der Entsorgung von Datenträgern zu beachten. Das betrifft die Datenträger-, Auftrags- und Transportkontrolle (siehe hierzu auch Punkt 15.2).
- Über die Vernichtung sollte ein Protokoll erstellt werden.
- Alle Maßnahmen für eine ordnungsgemäße Entsorgung sollten in einer Dienstanweisung festgelegt werden.
- Die Einhaltung der Maßnahmen ist zu kontrollieren.

Die DIN 32757 beschreibt die Anforderungen an Maschinen und Einrichtungen zur Vernichtung von Informationsträgern (Papier und Mikrofilm). Obwohl sie keine Rechtsnorm ist, liefert sie Anhaltspunkte für das im Einzelfall erforderliche Sicherheitsmaß bei der Vernichtung. Je nach dem Grad der Schutzbedürftigkeit der auf dem Datenträger gespeicherten Informationen werden fünf Sicherheitsstufen definiert. Die Sicherheitsstufe drei (z.B. Streifenbreite max. 2 mm bei beliebiger Länge) sollte eine Mindestanforderung für eine datenschutzgerechte Vernichtung sein. Für sensible personenbezogene Daten sollte eine höhere Sicherheitsstufe gewählt werden. Die Papierdatenträger können in der Regel mit leistungsstarken Aktenvernichtern entsorgt werden. Für Disketten, Streamertapes und Carbonfarbbänder muß allerdings ein Schredder für die Vernichtung unter Beachtung der DIN 33858 eingesetzt werden.

15.15 Länderübergreifende IT-Vorhaben

15.15.1 Automatische Erhebung von Straßenbenutzungsgebühren

Für 1998 ist europaweit die Einführung von elektronischen Mautsystemen vorgesehen. In diesem Zusammenhang ist auch in der Bundesrepublik Deutschland die Benutzung von Autobahngebühren in der Diskussion. Im Auftrag des Bundesministeriums für Verkehr testete der TÜV-Rheinland auf der A 555 verschiedene Systeme auf Ihre Brauchbarkeit und Zuverlässigkeit. In diesem Ergebnisbericht stellte der TÜV Rheinland fest, daß die Funktionsfähigkeit bei keinem automatisierten Kontrollverfahren ausreichte, um die Anforderungen des Datenschutzes zu erfüllen.
Das Problem bei den diskutierten Verfahren besteht darin, daß eine zurückgelegte Strecke auf der Autobahn automatisch gemessen und ein entsprechender Geldbetrag abgezogen werden soll, ohne dabei das Persönlichkeitsrecht des Kraftfahrers zu beeinträchtigen.
Bei der Verrechnung des Geldbetrages gibt es zwei mögliche Verfahren:
Postpaid-Verfahren: Mit optisch-elektronischer Bildauswertung des Nummernschildes wird die Fahrzeugerkennung durchgeführt und eine anschließende Abbuchung von einem Gebührenkonto des betreffenden Fahrzeughalters durchgeführt.
Durch dieses Verfahren können exakte Bewegungsprofile bestimmt und somit konkrete Aussagen getroffen werden, wer, wann, wohin auf der Autobahn gefahren ist.
Bei dem Prepaid-Verfahren wird die veranlaßte Abbuchung des Betrages von einer im Auto befindlichen Chipkarte, die vorher gekauft werden muß, abgebucht. Die geforderte Prepaid-Technologie ermöglicht den Einsatz von Verfahren, welche die Möglichkeit bieten, das Persönlichkeitsrecht des Kfz-Halters/ Fahrers weitgehend zu schützen.
Auf der 49. Konferenz der DSB des Bundes und der Länder wurde eine Entschließung zur automatischen Erhebung von Straßenbenutzungsgebühren verabschiedet, welche eine datenschutzgerechte Ausgestaltung der elektronischen Mautsysteme fordert (siehe Anlage 21). In dieser Entschließung sind die DSB zu dem Ergebnis gekommen, daß das Prepaid-Verfahren nach dem derzeitigen Stand die umfassendste und sicherste Anonymisierung ermöglicht.

15.15.2 Elektronisches Mitteilungssystem auf Basis von X.400

In den öffentlichen Verwaltungen werden neben der derzeit überwiegenden Übertragung von Daten und Dokumenten, z. B. durch Fernschreibdienst, Telex und Fax, in Zukunft vermehrt elektronische Mitteilungssysteme, wie z. B. Electronic-Mail und Message Handling System (MHS/X.400), zum Einsatz kommen. Der elektronische Mitteilungsdienst ermöglicht den Austausch von Nachrichten, die unterschiedliche Informationstypen und -strukturen enthalten können, zwischen den angeschlossenen Einrichtungen und deren Mitarbeitern. X.400 ist ein internationaler Standard, der einen genormten Nachrichtenaustauschdienst definiert.
Am 20. August 1993 faßte die Konferenz der Innenminister und -senatoren der Länder den Beschluß, ab dem 1. Januar 1995 den elektronischen Mitteilungsdienst MHS/X.400 für den Dokumentenaustausch zwischen den Bundesländern zu verwenden und dafür die geeigneten Maßnahmen zu treffen. Inzwischen hat die Innenministerkonferenz wegen der im Probebetrieb aufgetretenen technischen und organisatorischen Schwierigkeiten beschlossen, diesen Dienst erst ab 1996 umfassend einzusetzen.
Auch im Rahmen des Informationsverbundes Berlin-Bonn wird unter anderem ein elektronisches Mitteilungssystem auf der Basis des X.400 Standards eingeführt werden. Zukünftig werden immer mehr öffentliche Stellen in einen solchen Datenaustausch einbezogen werden.
Der wirtschaftliche Vorteil solcher Anwendungen liegt in der schnellen und papierlosen Übermittlung von z. B. Dokumenten, Programmen, Sprache und Bildern in digitalisierter Form und der Möglichkeit des Ausnutzens von Nachttarifen. Weiterhin wird eine neue Qualität der Kommunikation zwischen den öffentlichen Stellen erreicht, in dem die empfangenen Nachrichten in elektronischer Form zwischengespeichert und weiterverarbeitet werden können.
Derzeit wird für die Landesverwaltung in Thüringen durch den Interministeriellen Ausschuß für Informationstechnik (IMA-IT) eine Konzeption für die Einführung von MHS/X.400 erarbeitet (siehe Punkt 15.5.2).

Aus datenschutzrechtlicher Sicht erfordert ein Einsatz von elektronischen Mitteilungssystemen zusätzliche Sicherheitsanforderungen, die der AK-Technik in einer Entschließung “Datenschutz bei elektronischen Mitteilungssystemen” zusammengefaßt hat (siehe Anlage 22).
Diese Entschließung beinhaltet u. a. die folgenden grundlegenden Forderungen an den Einsatz von elektronischen Mitteilungssystemen :

- Authentizität von Benutzern, Nachrichten und Systemmeldungen,
- Vertraulichkeit von übertragenen Daten,
- Integrität von Nachrichten und Meldungen,
- fälschungssichere Kommunikationsnachweise,
- Ausschluß von Kommunikationsprofilen.

Bei der Übertragung von personenbezogenen und vertraulichen Daten ist eine Verschlüsselung vorzunehmen und eine Integritätsabsicherung mittels elektronischer Unterschrift zu gewährleisten. Grundsätzlich sollte ein getrennter Kommunikationsserver für das elektronische Mitteilungssystem eingerichtet werden, der einen Zustellungs- und Empfangsnachweis und einen Sende- Empfangsübergabenachweis führt.

15.15.3 Datenschutz bei elektronischen Geldbörsen und anderen elektronischen Zahlungsmitteln

Aufgrund der voranschreitenden Entwicklung auf dem Gebiet der Chipkartentechnik gewinnt der Einsatz von elektronischen Geldbörsen immer mehr an Bedeutung. Besonders die Zahlungsinstitute und der Handel versprechen sich hiervon erhebliche Vorteile. Neben der wohl verbreitetsten Anwendung der elektronischen Geldbörse als Telefonkarte gibt es bereits an vielen Universitäten den Einsatz von elektronischen Geldbörsen, um den Studenten eine bargeldlose Inanspruchnahme von Dienstleistungen (Mensa, Kopierdienst, Bibliothek etc.) zu ermöglichen. Pilotprojekte in Städten, in denen der Bürger Fahrten mit Bus, Bahn, Taxi, Schwimmbadbesuche, Kinokarten und Parken per elektronischer Geldbörse bezahlen kann, gibt es bereits. In vielen Bereichen wird angestrebt, unter Verwendung der elektronischen Geldbörse, für die Kunden zunehmend Leistungen bereitzustellen. Die Vielzahl der Einsatzmöglichkeiten läßt sich nur annähernd beschreiben.
Damit verbunden sind datenschutzrechtliche Risiken. Die DSB des Bundes und der Länder haben deshalb im Umlaufverfahren eine Entschließung zu dem Thema “Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen” verabschiedet (siehe Anlage 28).
In dieser Entschließung werden die Kartenherausgeber aufgefordert, nur solche elektronischen Geldbörsen zu entwickeln, die möglichst ohne personenbezogene Daten auskommen, um so z. B. einer Registrierung des Kaufverhaltens oder dem Anfertigen von Bewegungsprofilen von Bürgern vorzubeugen.
Dem Prepaid-Verrechnungsverfahren wird dabei der Vorzug gegeben, weil durch die Vorbezahlung von Guthabenkarten eine Erhebung von personenbezogenen Daten nicht notwendig erscheint.

Bei dem Postpaid-Verrechnungsverfahren werden sämtliche Zahlungsvorgänge verbucht und dem Käufer, dessen personenbezogene Daten erfaßt sind, in Rechnung gestellt (z. B. bei Kredit- und Debitkarten).
Die DSB des Bundes und der Länder gehen davon aus, daß im Kleingeldbereich gut auf die Nutzung von Debit- und Kreditkarten verzichtet werden kann und bei größeren Geldbeträgen die Abrechnung über anonyme Konten erfolgen sollte, wobei erst bei Zahlungsunregelmäßigkeiten ein Bezug zum Kontoinhaber erforderlich wird. Eine Beeinträchtigung der Persönlichkeitsrechte Betroffener, wie das Erstellen von Kauf- oder Bewegungsprofilen bis hin zu Persönlichkeitsprofilen, kann somit weitestgehend vermieden werden.

Anlage 1

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

zum

Ausländerzentralregistergesetz

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern , die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben den Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 2. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen, unter denen u. a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

Anlage 2

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

zur

Informationsverarbeitung im Strafverfahren

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz - BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittlungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren - auch mit Zwangsmitteln - erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Insgesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.
In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden - also auch von anderen Staatsanwaltschaften - Auskunft verlangen (§161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit - ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens - von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./ 29. September 1981 zu “Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften”, vom 24./ 25. November 1986 “Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren” und vom 5./6. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 3. November 1988).

Anlage 3

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

zum

Abbau des Sozialdatenschutzes

Der Gesetzgeber hat in den vergangenen Monaten die Möglichkeit der Überprüfung von Sozialleistungsempfängern ohne deren vorherige Befragung oder Kenntnis in drastischem Umfang vermehrt. Insbesondere durch das seit dem 1. Juli 1993 geltende Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms ist das Kontrollinstrumentarium von Sozial- und Arbeitsämtern noch einmal erheblich erweitert worden. Ohne Rücksicht auf konkrete Anhaltspunkte für einen unberechtigten Leistungsbezug im Einzelfall sind künftig automatisierte Datenabgleiche zwischen Sozialhilfeträgern sowie zwischen diesen und der Arbeitsverwaltung bzw. der Kranken-, Unfall- und Rentenversicherung gestattet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sehr besorgt über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und zu immer nachhaltigeren Eingriffen in das Recht auf informationelle Selbstbestimmung aller Betroffenen, d. h. auch und gerade der großen Mehrheit rechtstreuer Antragsteller und Leistungsbezieher, führt.

Mit Nachdruck wenden sich die Datenschutzbeauftragten gegen Versuche von Sozialverwaltungen, bei der Umsetzung der neuen Kontrollregelungen durch extensive Interpretation über den gesetzlich vorgegebenen Rahmen hinauszugehen. So erlaubt beispielsweise der neu gefaßte § 117 Abs. 3 des Bundessozialhilfegesetzes entgegen der Handhabung einzelner Kommunen keinen automatisierten Datenabgleich zwischen Sozialhilfedatei und Kraftfahrzeug-Register, sondern nur den Vergleich von Angaben in Verdachtsfällen.

Die dargestellte Entwicklung macht es erneut notwendig, auf die verfassungsrechtliche Qualität des Grundsatzes der Datenerhebung beim Betroffenen hinzuweisen. An dem Prinzip, daß bei der Überprüfung der Leistungsberechtigung und der Nachweise Auskünfte zunächst beim Antragsteller anzufordern sind und nur aufgrund konkreter Verdachtsmomente Nachfragen bei dritten Stellen oder Datenabgleiche erfolgen dürfen, muß für den Regelfall festgehalten werden, soll der einzelne mündiger Bürger bleiben und nicht zum bloßen Objekt staatlicher Verhaltenskontrolle werden.

Sorge äußert die Konferenz auch über die hartnäckigen Bestrebungen, Datenbestände der Sozialverwaltung für immer neue Zwecke und Adressaten zu öffnen. Beispiele dafür sind die im Gesetzgebungsverfahren zum 2. SGB-Änderungsgesetz im letzten Augenblick gescheiterten Anträge, Polizei und Staatsschutz in unvertretbarem Umfang Zugriff auf Daten Arbeitsloser und sonstiger Sozialleistungsempfänger zu geben. Das Sozialgeheimnis muß ein wirksamer Sonderschutz für die besonders sensiblen Daten in der Sozialverwaltung bleiben. Nur dies entspricht der Abhängigkeit des einzelnen von staatlichen Leistungen und der sich daraus ergebenden speziellen Verletzlichkeit seines Rechts auf informationelle Selbstbestimmung.

Anlage 4

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

zu

Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten von Bund und Ländern verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte “Gesundheitskarten”, etwa “Service-Karten” von Krankenversicherungen und privaten Anbietern, “Notfall-Karten”, “Apo(theken)-Cards” und “Röntgen-Karten” werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen “Gesundheitskarten” über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Antragsteller - etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karteninhabern vorbehält bzw. erleichtert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sogenannten Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die “Möglichkeit einer Beitragsrückerstattung” in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.

- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip - die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.

- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.

- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.

- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.

- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Anlage 5

Entschließung

der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam

zum

Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz -PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der dafür erforderlichen Änderung des Grundgesetzes (BR-Drs. 114/94 = BT-Drs. 12/6717)

I. Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II. Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten insbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer - auch nach dem Wegfall der Monopole - einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kriterien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen , wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III. Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

Anlage 6

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27 September 1994 in Potsdam

zu

Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994(KOM (94) 128 endg. - COD 288)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedsstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.

2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei "berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.

3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.

4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte - wie im ursprünglichen Richtlinienentwurf vorgesehen - untersagt werden.

5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte - wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah - auf Unionsebene garantiert werden.

6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z. B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z. B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedstaaten, diese Anregungen zu unterstützen.

Anlage 7

Entschließung

der Datenschutzbeauftragten des Bundes und der Länder am 25. August 1994 in Potsdam

zum

Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik - EG-Statistikverordnung - (KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings daraufhin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

   Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff “statistische Geheimhaltung” muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert wird. Der Begriff “statistische Geheimhaltung” sollte an einer Stelle in der Verordnung so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgegangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Anlage 8

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam

zu

**Datenschutzrechtliche Anforderungen
an ein Übereinkommen der Mitgliedstaaten der Europäischen Union
über die Errichtung eines europäischen Polizeiamtes (EUROPOL)**

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleibt die Zuständigkeit des BKA als nationale Stelle für EUROPOL unberührt.

- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

Anlage 9

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam

zu

Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministerien vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sogenannte Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht darauf eingegangen werden, ob die Anwendungen, d. h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Anlage 10

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam

zu

Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als zehn Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Statt dessen sind in den letzten Jahren in zunehmenden Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die
- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z. B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz),
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sogenannten Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes entgegenwirken.

Anlage 11

Entschließung

der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam

Art. 12 Verbrechensbekämpfungsgesetz
zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.

- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen.

Anlage 12

Entschließungsvorschlag*

zur 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zur

ASYL-Card

Überlegungen einer "Bund-Länder-Arbeitsgruppe zur Harmonisierung der Verwaltungsabläufe im Asylverfahren" sehen die Einführung einer sogenannten ASYL-Card vor, zu deren Benutzung jeder Asylbewerber verpflichtet werden soll. Auf der Chipkarte sollen neben Fingerabdruck und Lichtbild unter anderem Daten über das Asylverfahren, das Vorliegen einer Arbeitserlaubnis und den Empfang von Sach- und Geldleistungen erfaßt sein. Die Karte soll sowohl Verfahrensdaten für die zuständigen Behörden schnell verfügbar machen (z. B. Asylverfahren, Arbeitserlaubnis) als auch Kontrollzwecken dienen (z. B. Aufenthaltskontrolle, Zutrittskontrolle und anderes) und die Abwicklung fürsorglicher Leistungen unterstützen.

Die Zusammenführung von Daten aus dem Arbeitsbereich verschiedener Stellen stellt einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht dar, das auch für Asylbewerber gilt. Die Datenschutzbeauftragten halten einen solchen Eingriff nicht für vertretbar, zumal die Überlegungen zur ASYL-Card durch Mängel im Vollzug des bisherigen Verfahrens ausgelöst werden. Die Datenschutzbeauftragten sind der Ansicht, daß diese Defizite behoben werden sollten, anstatt ein neues datenschutzrechtlich problematisches Verfahren einzuführen.

Die Datenschutzbeauftragten weisen aus diesem Anlaß auf die allgemeine Gefährlichkeit einer Entwicklung zur multifunktionellen Datenspeicherung auf Chipkarte für Überwachungszwecke hin. Effektivitätsgesichtspunkte, Mißbrauchsbekämpfung, Überwachung auferlegter Pflichten und ähnliches könnten auch für andere Verwaltungsverfahren geltend gemacht werden. Je mehr Bereiche mit Kartenlösungen versehen werden, um so mehr wächst das Bedürfnis, aus praktischen Erwägungen heraus eine Vereinheitlichung oder Zusammenführung der Informationen auf einer Karte anzustreben. Damit wächst die Gefahr der "Rundumerfassung", die mit dem verfassungsrechtlichen Gebot der Verhältnismäßigkeit nicht vereinbar wäre.

Die Einführung der "ASYL-Card" bedürfte im übrigen eines erheblichen technischen und finanziellen Aufwands. Kryptographische Verfahren, Hard- und Software für die mit der ASYL-Card arbeitenden Stellen und Personal- und Arbeitseinsatz für die Herstellung, Verteilung und Verwaltung der Karten würden einen Aufwand erfordern, der zu den von der Arbeitsgruppe erwarteten Vorteilen außer Verhältnis stehen dürfte.

*) Der vorstehende Entschließungsvorschlag wurde in der DSB-Konferenz nicht beschlossen.

Anlage 13

Entschließungsvorschlag*

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zur

Rechtstatsachensammlung zur Überprüfung polizeilicher Befugnisse

Die Datenschutzbeauftragten des Bundes und der Länder hatten in ihrer 48. Konferenz am 26./ 27. September 1994 Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen erarbeitet.
Ziel dieser Vorschläge war es, die Diskussion über die Erforderlichkeit der bestehenden Instrumente zur polizeilichen Datenverarbeitung und deren Ausweitung auf Erkenntnisse zu stützen, die stärker als bisher gesichert sind.
Auch von seiten der Polizei, insbesondere des Bundeskriminalamtes, sind Vorschläge für eine umfassende Rechtstatsachensammlung über die Anzahl besonderer Erhebungsmethoden, den Erfolg dieser Maßnahmen und Durchführungsschwierigkeiten unterbreitet worden. Sie sind jedoch bisher von der Mehrzahl der Länderpolizeien abgelehnt worden. Statt dessen soll eine Bund/Länder-Fallsammlung eingerichtet werden. Hierzu stellen die Datenschutzbeauftragten des Bundes und der Länder fest:
Die Einrichtung einer Rechtstatsachensammlung als objektives Instrument zur Bewertung polizeilicher Eingriffsbefugnisse wäre auch aus datenschutzrechtlicher Sicht zu begrüßen. Diese Sammlung darf jedoch nicht einseitig das Ziel verfolgen, Forderungen der Polizei zur Einführung zusätzlicher Befugnisse argumentativ zu unterstützen. Das Vorhaben geht in die falsche Richtung, wenn es von vornherein aufgrund des angelieferten Datenmaterials auf bestimmte Ergebnisse festgelegt ist. Vielmehr muß die Sammlung ohne rechtspolitische Vorgaben angelegt werden. Sie soll eine objektive Beurteilung des Einsatzes und der Ergebnisse besonderer Methoden zur Datenerhebung ermöglichen.

Das Bundesverfassungsgericht hat im Volkszählungsurteil gefordert, daß der Gesetzgeber ungewissen Auswirkungen eines Gesetzes dadurch Rechnung tragen muß, daß er die ihm zugänglichen Erkenntnisquellen ausschöpft, um die Auswirkungen so zuverlässig wie möglich abschätzen zu können; bei einer sich später zeigenden Fehlprognose ist er zur Korrektur verpflichtet. Der Gesetzgeber kann aufgrund veränderter Umstände zur Nachbesserung einer ursprünglich verfassungsgemäßen Regelung gehalten sein.
Die Datenschutzbeauftragten halten daher ihren Vorschlag einer ergebnisoffenen Überprüfung der bestehenden Befugnisse aufrecht. Sie erwarten, daß sich die Polizeien der Diskussion über die Erforderlichkeit und Angemessenheit weitreichender Befugnisse zu Eingriffen in das Persönlichkeitsrecht nicht entziehen werden. In Betracht kommt auch eine unabhängige Überprüfung der bestehenden polizeilichen Eingriffsbefugnisse durch das kriminalistische Institut beim BKA in enger Kooperation mit einem fachlich qualifizierten unabhängigen Forschungsinstitut. Die Datenschutzbeauftragten des Bundes und der Länder fordern die Innenministerkonferenz auf, die Überlegungen für eine offene und aussagekräftige Rechtstatsachensammlung weiterzuverfolgen und die Datenschutzbeauftragten zu beteiligen.

*) Eine Entschließung wurde nicht gefaßt. Der Vorsitzende des AK Sicherheit wurde gebeten, ein Schreiben mit entsprechendem Inhalt an den Vorsitzenden der Innenministerkonferenz zu richten.

Anlage 14

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zum

Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz)- Bundesrats-Drucksache 94/95

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:

Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind. Hierzu gehören:

- der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sogenannten “Feststellung des Anfangsverdachts”;

- das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;

- Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregeln;

- die Beachtung landesgesetzlicher Löschungsfristen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere:

- für die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;

- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;

- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;

- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahin gehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

Anlage 15

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zum

Maßhalten beim vorbeugenden personellen Sabotageschutz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, bei Sicherheitsüberprüfungen zum personellen Sabotageschutz Augenmaß zu bewahren. Bei diesen Sicherheitsüberprüfungen werden sensible Daten, z. B. über politische Anschauungen oder Alkoholkonsum, vorbeugend erhoben, also ohne daß der Betroffene dazu Anlaß geboten hätte. Polizei und Verfassungsschutz sind routinemäßig beteiligt. Schon wenn der Betroffene im Verlauf der Überprüfung auch nur in den Verdacht der Unzuverlässigkeit gerät, kann dies bereits erheblichen Einfluß zumindest auf das berufliche Fortkommen nehmen.

Gegenwärtig sind solche Überprüfungen spezialgesetzlich für den Atombereich und für Flughäfen vorgesehen. Das Bundesministerium des Innern will jetzt klären, inwieweit Beschäftigte in anderen Einrichtungen überprüft werden sollen.

Unstreitig können solche Überprüfungen unbescholtener Bürger nur zum Schutz von "lebens- und verteidigungswichtigen Einrichtungen" angemessen sein und nur Personen betreffen, die dort an " sicherheitsempfindlichen Stellen" tätig sind. Als "lebenswichtig" sehen die Innenminister und -senatoren aber bereits Stellen an, "die für das Funktionieren des Gemeinwesens unverzichtbar sind". Damit könnten Beschäftigte in weiten Bereichen des öffentlichen Dienstes und der Wirtschaft mit Sicherheitsüberprüfungen überzogen werden.

Die Datenschutzbeauftragten meinen, daß das Persönlichkeitsrecht hier größere Zurückhaltung gebietet. Die Sicherheitsüberprüfungen müssen auf Bereiche beschränkt bleiben, in denen einer erheblichen Bedrohung für das Leben zahlreicher Menschen vorgebeugt werden muß.

Soweit in solchen Bereichen Sicherheitsüberprüfungen durchgeführt werden sollen, bedarf es einer ebenso klaren gesetzlichen Grundlage, wie bisher im Atomgesetz und im Luftverkehrsgesetz. Die zu schützenden Arten lebens- und verteidigungwichtiger Einrichtungen müssen durch Rechtsvorschrift abschließend festgelegt sein. Dabei sind für die jeweiligen Bereiche angemessene Regelungen zu treffen, die mit Rücksicht auf die Interessen Betroffener folgende allgemeine Grundsätze beachten:

- möglichst klare Vorgaben zur "Sicherheitsempfindlichkeit" in der Vorschrift und exakte Festlegung dieser Stellen durch die zuständige Behörde nach Anhörung der Personalvertretung der einzelnen Einrichtung,

- Zustimmung des Betroffenen als Verfahrensvoraussetzung,

- abschließender Katalog der regelmäßig durchzuführenden Maßnahmen, dabei Beschränkung auf vorhandene Erkenntnisse, keine Ausforschungsermittlungen,

- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung, insbesondere Trennung von Personalakte,

- eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung und aktenkundige Gegendarstellung,

- angemessener Auskunftsanspruch, einschließlich Akteneinsicht,

- effektive Datenschutzkontrolle, auch zur Datenverarbeitung in Akten bei nicht-öffentlichen Stellen.

Im Regelfall muß zusätzlich gelten:

- Überprüfung durch die zuständige Aufsichtsbehörde selbst, nicht durch Verfassungsschutzbehörden,

- keine Einbeziehung weiterer Personen (wie Ehegatte usw.).

Ausnahmetatbestände wären - auch zum Verfahren - präzise zu fassen.

Die Praxis der Sicherheitsüberprüfungen zum personellen Sabotageschutz steht in Bund und Ländern vor einer wichtigen Weichenstellung. Sie muß klar und angemessen sein.

Anlage 16

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zu

Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z. B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.

   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.

2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten, sind Verkürzungen vorzunehmen.

3. Die derzeit geltende generelle 30jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.

   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

   Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.

5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.

6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.

7. Für die Daten von Nebenbeteiligten (z. B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.

8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

Anlage 17

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zu

Anforderungen an den Persönlichkeitsschutz im Medienbereich

Die unabhängige und unzensierte Berichterstattung durch Presse, Rundfunk und Film (Art. 5 Abs. 1 Satz 2 GG) dient der freien individuellen und öffentlichen Meinungsbildung. Das Bundesverfassungsgericht hat die freie Meinungsbildung als Voraussetzung sowohl der Persönlichkeitsentfaltung als auch der demokratischen Ordnung bezeichnet. Insofern besteht ein enger Zusammenhang zwischen der Selbstbestimmung des einzelnen und der Medienfreiheit.

Die rasante Entwicklung der Medientechnik, die Zunahme interaktiver Teledienste und die verstärkte kommerzielle Nutzung von Pressedatenbanken eröffnen einerseits neue Informationsmöglichkeiten für den Bürger, verschärfen aber die Gefährdungen des Rechts auf informationelle Selbstbestimmung. Diesen Gefährdungen muß der Datenschutz auf rechtlicher und technisch-organisatorischer Ebene angemessen begegnen.

Electronic Publishing und Medienarchive

Neue Formen der Verbreitung von Informationen über Netze und auf elektronischen Datenträgern führen in bisher unbekanntem Maß zu großen Informationsbeständen, in denen potentiell jedermann gezielt auf personenbezogene Daten zugreifen kann. Zudem öffnen Medienarchive, die bislang ausschließlich für journalistische Zwecke genutzt wurden, riesige Datensammlungen für medienfremde Nutzer. In Persönlichkeitsrechte wird dann besonders tief eingegriffen, wenn auch lange zurückliegende Publikationen praktisch von jedermann recherchiert werden können. Damit droht das in verschiedenen Rechtsbereichen vorgesehene “Recht auf Vergessen” wirkungslos zu werden, das z. B. durch die Löschungsvorschriften für das Bundeszentralregister gewährleistet werden soll.

Angesichts dieser Entwicklungen muß die Reichweite der datenschutzrechtlichen Sonderstellung der Medien (“Medienprivileg”) neu bestimmt werden. Es ist zumindest gesetzlich klarzustellen, daß die geschäftsmäßige Verwendung personenbezogener Daten außerhalb des eigenen Medienbereichs, insbesondere durch kommerzielle Pressedatenbanken, nicht unter das “Medienprivileg” fällt.

Interaktive Dienste und Mediennutzungsprofile

Auch beim Ausbau neuer digitaler Kommunikationsformen (interaktive Dienste wie z. B. Video on Demand) müssen die Persönlichkeitsrechte der Nutzer gewahrt werden. Dabei ist stärker als bisher von vornherein Wert darauf zu legen, daß datenschutzfreundliche Techniken entwickelt werden und zum Einsatz kommen, bei denen personenbezogene Verbindungs- und Nutzungsdaten erst gar nicht entstehen. Von besonderer Bedeutung sind hier anonyme Zahlverfahren, z. B. Prepaid-Karten, auf denen Informationen über die Nutzung ausschließlich dezentral gespeichert werden.

Entsprechend den Bestimmungen im Bildschirmtextstaatsvertrag und in den neueren Mediengesetzen ist sicherzustellen, daß sich die Erhebung und die Aufzeichnung von Verbindungs- und Abrechnungsdaten auf das erforderliche Maß beschränken. Dieser strikte Verarbeitungsrahmen darf auch nicht dadurch ausgeweitet werden, daß die Nutzung eines Dienstes von der Einwilligung in eine zweckfremde Verwendung der Daten abhängig gemacht wird. Die Länder sollten entsprechende einheitliche Regelungen für alle interaktiven Dienste treffen.

Da es sich bei den angesprochenen Diensten um Bestandteile einer entstehenden globalen Infrastruktur handelt, wird die Bundesregierung aufgefordert, sich auf internationaler Ebene für entsprechende Regelungen einzusetzen.

Rechte der Betroffenen gegenüber den Medien

Während die von der Berichterstattung Betroffenen - neben dem für alle Bereiche geltenden Gegendarstellungsrecht - gegenüber den öffentlich-rechtlichen und privaten Rundfunkveranstaltern inzwischen weitere elementare Datenschutzrechte besitzen, gibt es gegenüber der Presse keine vergleichbaren Regelungen.

So kann derjenige, der durch die Berichterstattung der Rundfunkveranstalter in seinem Persönlichkeitsrecht beeinträchtigt wird, in den meisten Fällen nach der Publikation Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Gegenüber der Presse hat er kein entsprechendes Auskunftsrecht. Die meisten Rundfunkveranstalter sind - anders als die Presse - zudem verpflichtet, etwaige Gegendarstellungen zu den gespeicherten Daten zu nehmen, auf die sie sich beziehen (Mitspeicherungspflicht). Ein sachlicher Grund für diese Unterscheidungen ist nicht erkennbar.

Das Presserecht sollte insofern der Rechtslage nach dem Rundfunkrecht (z. B. § 41 Abs. 3 BDSG und Art. 17 Abs. 2 ZDF-Staatsvertrag) angeglichen werden.

Gegenüber Pressedatenbanken, die nicht nur dem eigenen internen Gebrauch dienen, sollte der Betroffene darüber hinaus ein Auskunftsrecht bezüglich des zu seiner Person gespeicherten veröffentlichten Materials haben.

Öffentlichkeitsarbeit der Behörden

Personenbezogene Veröffentlichungen von Behörden können das Recht auf informationelle Selbstbestimmung erheblich beeinträchtigen. Das gilt für Personen, auf die die Aktivitäten der Behörde unmittelbar gerichtet sind, wie auch für andere Verfahrensbeteiligte (wie z. B. Einwender, Opfer von Straftaten, Zeugen) und im besonderen Maße für unbeteiligte Personen aus dem sozialen Umfeld des Betroffenen. Deshalb ist bei der Weitergabe von Daten aus Strafermittlungsverfahren an die Medien besonders zurückhaltend zu verfahren.

Für den Umfang des Anspruchs der Medien auf Weitergabe personenbezogener Daten in Form von Presseerklärungen und Auskünften gibt es keine konkreten gesetzlichen Festlegungen. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für geboten, daß der Gesetzgeber Kriterien für die Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen und der Freiheit der Berichterstattung durch Rundfunk und Presse deutlicher als bisher festgelegt. Dafür kommen die Vorschriften des Landespresserechts, in besonders sensiblen Bereichen aber auch spezialgesetzliche Regelungen wie etwa die Strafprozeßordnung in Betracht.

Gerichtsfernsehen

Die Datenschutzbeauftragten des Bundes und der Länder treten den in jüngster Zeit zunehmend erhobenen Forderungen nach einer Aufhebung des Verbots der Hörfunk- und Fernsehberichterstattung aus Gerichtsverhandlungen entgegen. Insbesondere bei Strafprozessen vor laufenden Mikrofonen und Kameras würde es unweigerlich zu gravierenden Beeinträchtigung des Persönlichkeitsrechts der Angeklagten, der Opfer, der Zeugen und ihrer Angehörigen kommen. Selbst mit Einwilligung aller Prozeßbeteiligten darf die Hörfunk- und Fernsehberichterstattung nicht zugelassen werden.

Die Gerichtsverhandlung darf nicht zu einem massenmedial vermittelten “modernen Pranger” werden.

Anlage 18

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zum

Sozialgesetzbuch VII
Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz - SGB-VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfs berücksichtigt werden müssen:

1. **Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern**

   Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§§ 557 Abs. 2 RVO - § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Bsp.: Handverletzung und Salmonellenvergiftung).

2. **Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte**

   Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbänden der Kassenärzte und der Unfallversicherungsträger geschlossenen "Ärzteabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht des Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. **Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter**

   Im Hinblick auf das Recht des Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund - z. B. wegen möglicher Befangenheit - zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen.

   Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. **Eingriffe der Unfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung**

   Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und -nutzung - einschließlich der Aufbewahrungsfristen - sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt und andererseits Selbstverständlichkeiten wie das Führen von

Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden.

Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und -krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit, nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und -nutzung sowie die Festlegung der jeweils speichernden Stelle.

Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft.

Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

Anlage 19

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zu

Eingeschränkter Zugriff auf Versichertendaten bei landesweiten oder überregionalen gesetzlichen Krankenkassen

Die gesetzlichen Krankenkassen schließen sich zunehmend zu landesweiten oder überregionalen gesetzlichen Krankenkassen zusammen. Es stellt sich daher verstärkt die Frage, welche bzw. wie viele Geschäftsstellen solcher Krankenkassen umfassend auf alle gespeicherten Daten eines Versicherten zugreifen können.

Die Datenschutzbeauftragten halten nur folgendes für vertretbar:

1. Geschäftsstellen einer Krankenkasse können ohne schriftliches Einverständnis des Versicherten nur auf einen "Stammdatensatz" zugreifen. Dieser "Stammdatensatz" darf nur den Namen, das Geburtsdatum, die Anschrift, die Krankenversichertennummer und die betreuende Geschäftsstelle des Versicherten umfassen.

2. Lediglich eine Geschäftsstelle kann umfassend auf den Datensatz eines Versicherten zugreifen, sofern der Versicherte nicht ausdrücklich und eindeutig schriftlich in derartige Zugriffsmöglichkeiten durch weitere Geschäftsstellen eingewilligt hat.

3. Vor der Einwilligung ist der Betroffene umfassend aufzuklären. Die Daten dürfen nur zweckgebunden verwendet werden.

Anlage 20

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zum

Datenschutz bei Wahlen

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z. B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden

- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person angegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:

Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.

Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer, soweit sie nicht ausdrücklich widersprochen haben, in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.

Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig. Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

Anlage 21

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zur

Automatischen Erhebung von Straßenbenutzungsgebühren

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z. B. Verkehrsinformation und -leitung) werden.

Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren wie z. B. die Vignette einzubeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der “datenfreien Fahrt” muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.

- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.

- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme - unabhängig von ihrer Rechtsform - einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

Anlage 22

Entschließung

der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1995 in Bremen

zum

Datenschutz bei elektronischen Mitteilungssystemen

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.

Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. **Authentizität von Benutzern, Nachrichten und Systemmeldungen**

   Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z. B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. **Vertraulichkeit von übertragenen Daten**

   Für alle Arten von Daten in elektronischen Mitteilungssystemen - Nachrichten sowie Verkehrs- und Verbindungsdaten - muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z. B. kryptografische Verfahren, sicherzustellen.

3. **Integrität von Nachrichten und Meldungen**

   Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. **Fälschungssichere Kommunikationsnachweise**

   Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. **Ausschluß von Kommunikationsprofilen**

   Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten:

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme - insbesondere solche, die noch auf Empfehlungen von 1984 basieren -, sollen künftig durch geeignete Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.

2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z. B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.

3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der “elektronischen Unterschrift” zurückgegriffen werden.

4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters - insbesondere der Verwaltung des elektronischen Mitteilungssystems - aus Sicherheitsgründen zu trennen.

5. Es ist grundsätzlich separat administrierbare Hard- oder Software - z. B. in Form eines Kommunikationsservers - für das elektronische Mitteilungssystem vorzusehen.

6. Bei Verwendungen von öffentlichen Übertragungswegen sind die vorhandenen Sicherheitsmechanismen dieser Netze, z. B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch Externe zu nutzen.

7. Zur Beweissicherung einer stattgefundenen Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:

   - Zustellung/Empfangsnachweise
   - Sende-/Empfangsübergabenachweise.

Anlage 23

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. November 1995 in Bremerhaven

zur

Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 08.09.1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehenen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10.02.1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u. a. folgende Aussagen enthält: “Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (...) wird gewährleistet”.

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28.04.1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17.02.1993 und 09./10.03.1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikationsnetze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.
- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.
- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.
- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.

- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich veabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.
- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.
- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.
- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.
- In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.
- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU.
- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z. B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26.05.1994, 08.09.1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25.08.1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Kontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher - unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden - auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Anlage 24

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. November 1995 in Bremerhaven

zu

Planungen für ein Korruptionsbekämpfungsgesetz

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne das Wissen des Betroffenen (§§ 100a, 100c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche - noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben - auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;
- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;
- Trennung von Planung, Überwachung und Ausführung von Ausschreibung und Vergabe;
- Prüfverfahren und Innenrevision;
- Codes of Conduct (formalisierte “Ethikprogramme”) im Bereich der Wirtschaft;
- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den o. g. Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen werden wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100a StPO Veranlassung, den Umfang der darin genannten Straftaten sobald wie möglich grundlegend zu überprüfen.

Anlage 25

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. November 1995 in Bremerhaven

zu

Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.

   Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines “überwiegenden Interesses” der Öffentlichkeit anzulegen.

   Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

4. Grundsätzlich sind in Auskünften und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z. B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

5. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

6. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind, und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

7. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat - auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens - erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

8. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

9. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekanntgemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

10. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienerstattung nicht in Betracht.

Anlage 26

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. November 1995 in Bremerhaven

Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 9./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z. B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)
- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z. B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.
- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.
- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

   Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

   Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

   - ob Daten auf einer Chipkarte gespeichert werden,
   - welche der Gesundheitsdaten auf die Karte aufgenommen werden,
   - welche Daten auf der Karte wieder gelöscht werden,
   - ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
   - welche Daten im Einzelfall zugänglich gemacht werden.

   Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine

wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungs-Nr., gespeichert werden, da andernfalls - zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad - die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzerzwang oder eine Bevorzugung von Karten-Nutzern (z. B. Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z. B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelte Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkarten-vermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte - z. B. mit Hilfe von Schlüsselbegriffen - dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z. B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine “Einwilligung” in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor “billigen Gesundheitskarten” ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

   Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

   Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung,..., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

   Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung des Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten - einschließlich der Sicherungskopien - übertragen oder nicht.

7. Leserecht des Karteninhabers

   Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

   Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 27

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. November 1995 in Bremerhaven

zum

Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)

Mit der Postreform III soll die Neugestaltung des Telekommunikationssektors in Deutschland nach den Vorgaben des Liberalisierungskonzepts der Europäischen Union abgeschlossen werden. Entstehen wird ein riesiger Markt mit einer Vielzahl von großen und kleinen, teilweise auch grenzüberschreitend tätigen Netzbetreibern und Diensteanbietern. Die Akteure auf diesem Telekommunikationsmarkt werden zum größeren Teil als Privatunternehmen operieren, es werden aber auch öffentliche Stellen ihre Leistungen anbieten. Der gesetzgeberische Abschluß der Liberalisierung und der Privatisierung des TK-Sektors wird die rechtliche Grundlage bilden für den endgültigen Eintritt in das Zeitalter von weltweiter Vernetzung, Multimedia und interaktiven Diensten und damit für den rapiden Anstieg des Konsums von Angeboten der Telekommunikation, des interaktiven Rundfunks und der Datenverarbeitung.

Die Konsequenzen sind absehbar: Gegenüber der heutigen Situation werden unvergleichlich mehr personenbezogene Daten durch mehr Stellen registriert und ausgewertet werden. Betroffen sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Dokumente über Datenleitung schicken oder Telebanking oder Teleshopping betreiben. Die Risiken für den einzelnen durch die vermehrten Möglichkeiten der Verhaltens- und Umfeldkontrolle oder der Ausforschung persönlicher Lebensgewohnheiten und Eigenschaften vergrößern sich entsprechend.

Der vom Bundesministerium für Post und Telekommunikation vorgelegte Referentenentwurf für ein Telekommunikationsgesetz (TKG-E, Stand: 06.10.1995) macht es erforderlich, erneut die Realisierung der grundlegenden Rahmenbedingungen für eine datenschutzgerechte Gestaltung der künftigen Telekommunikationslandschaft - soweit die Gesetzgebungskompetenz des Bundes betroffen ist - anzumahnen.

Ein wirksamer Datenschutz muß - wie bereits jetzt gesetzlich fixiert - auch künftig gleichberechtigtes Regulierungsziel neben z. B. der Sicherstellung der flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen bleiben.

Kundenwünsche nach variabler und komfortablerer Nutzung der technischen Möglichkeiten werden zunehmen. Gerade deshalb müssen die Prinzipien der Datenvermeidung und der strikten Begrenzung der Datenverarbeitung auf das erforderliche Ausmaß ihren Vorrang bei der Ausgestaltung der kommunikationstechnischen Infrastruktur behalten. Netzbetreiber und Diensteanbieter sollten verpflichtet werden, überall dort, wo dies technisch möglich ist, auch anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereitzustellen. Für eine sichere Datenübertragung sind ohne prohibitive Zusatzkosten wirksame Verschlüsselungsverfahren bereitzustellen.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z. B. sog. Corporate Networks) einheitlich auf einem hohen Niveau gesichert werden. Der bisherige Schutzstandard darf keinesfalls unter den durch die Postreform II erreichten Stand gesenkt werden. Ein hohes Datenschutzniveau ist als Grundversorgung unabdingbar; seine Gewährleistung sollte deshalb Teil der Universaldienstleistung sein. Die in Grundrechte eingreifenden Regelungen sind im Telekommunikationsgesetz selbst und nicht in Verordnungen zu treffen. Die untergesetzlichen, den Datenschutz betreffenden Normen gehören in eine einzige, nicht verstreut in mehrere Verordnungen.

Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten. Das “Feststellen mißbräuchlicher Inanspruchnahme” oder die “bedarfsgerechte Gestaltung” von TK-Leistungen dürfen nicht als Anlaß für eine umfassende Auswertung dieser Angaben oder sogar der Nachrichteninhalte herangezogen werden.

Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß auch künftig über die Nutzungsrisiken bestimmter Kommunikationstechniken (z. B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des

Betroffenen mißbraucht werden, um bereichsspezifische Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhängige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist wegen deren mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regulierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

Deshalb sollte aufgrund seiner langjährigen fachlichen Erfahrung bei der Kontrolle der TELEKOM und seiner umfassenden Querschnittskenntnisse im TK-Bereich der Bundesbeauftragte für den Datenschutz eine zentrale Funktion für die Kontrolle im Telekommunikationsbereich erhalten. Die Aufgaben, die die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden im Rahmen ihrer Zuständigkeiten erfüllen, sind gesetzlich klar zu regeln.

Die Akzeptanz der Informationsgesellschaft der Zukunft hängt wesentlich ab von der Sicherung des Grundrechts auf unbeobachtete Kommunikation. Das Telekommunikationsgesetz wird einen entsprechenden Baustein für die rechtliche Ausgestaltung der künftigen TK-Infrastruktur bilden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher dazu auf, die von ihr vorgeschlagenen Regelungen im weiteren Gesetzgebungsverfahren zu berücksichtigen und sich für ihre Umsetzung auch auf der europäischen Ebene (z. B. in der ISDN-Richtlinie) einzusetzen.

Anlage 28

Entschließung

der Datenschutzbeauftragten des Bundes und der Länder

zum

Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, daß bei kartengestützten Zahlungssystemen, die zunehmend in Konkurrenz zum Bargeld treten, datenschutzfreundliche Verfahren eingesetzt werden. Dabei bietet es sich an, vor allem Guthabenkarten zu verwenden. Es sollten nur solche Clearingverfahren eingesetzt werden, die weder eine individuelle Kartennummer benutzen noch einen anderen Bezug zum Karteninhaber herstellen.

Sowohl im öffentlichen Personennahverkehr als auch bei der Deutschen Bahn AG können Fahrscheine bargeldlos erworben werden. Auch Autofahrer können auf Bargeld verzichten: Beim Parken, beim Tanken, künftig auch bei der Benutzung von Autobahnen wird verstärkt auf elektronisches Bezahlen zurückgegriffen. Immer mehr Telefone und Warenautomaten werden auf bargeldlose Zahlungsverfahren umgestellt, so daß viele Artikel des täglichen Bedarfs elektronisch bezahlt werden können. Von Kreditinstituten wird die Kombination verschiedener Anwendungen auf einer Karte angestrebt, z.B. mit einer Kombination der Bezahlung für den öffentlichen Nahverkehr, Parkgebühren und Benutzungsentgelte für öffentliche Einrichtungen.

Zum elektronischen Bezahlen werden entweder Kreditkarten, Debitkarten oder Guthabenkarten eingesetzt. Bei Kredit- und Debitkarten werden sämtliche Zahlungsbeträge verbucht, dem Käufer in Rechnung gestellt, auf den Kontoauszügen ausgedruckt und für mindestens 6 Jahre gespeichert. Deswegen wird bei Guthabenkarten im voraus ein Guthaben eingezahlt und bei jeder einzelnen Zahlung das Guthaben entsprechend herabgesetzt; die Zahlungsbeträge müssen keinem Käufer zugeordnet werden.

Beim elektronischen Bezahlen entstehen sehr unterschiedliche Datenschutzrisiken. Bei Kredit- und Debitkarten besteht die Gefahr, daß die aus Abrechnungsgründen gespeicherten personenbezogenen Daten ausgewertet und zweckentfremdet genutzt werden: Informationen über den Kauf von Fahrscheinen oder über die Nutzung von Autobahnen können zu Bewegungsprofilen verdichtet werden. Das Konsumverhalten des einzelnen wird bis ins Detail nachvollziehbar, falls auch Kleineinkäufe am Kiosk nachträglich abgerechnet werden. Durch den Datenverkauf für Werbung und Marketing können sich weitere Risiken ergeben. Demgegenüber kann bei der Verwendung von Guthabenkarten auf das Speichern personen- oder kartenbezogener Daten aus erfolgten Zahlungen verzichtet werden.

Vor allem im Kleingeldbereich ist die Nutzung von Debit- und Kreditkarten entbehrlich, da fälschungssichere Guthabenkarten auf der Basis von Chipkarten mit integriertem Verschlüsselungsbaustein zur Verfügung stehen. Falls größere Geldbeträge nachträglich per Kredit- oder Debitkarte bezahlt werden, ist darauf zu achten, daß die Abrechnung zunächst über Konten erfolgt, deren Inhaber dem Zahlungsempfänger nicht namhaft gemacht wird. Erst bei Zahlungsunregelmäßigkeiten ist es notwendig, den Bezug zum Kontoinhaber herzustellen.

Angesichts der Risiken, aber auch der von Chipkarten ausgehenden Chancen, fordern die Datenschutzbeauftragten die Kartenherausgeber und die Kreditwirtschaft dazu auf, kartengestützte Zahlungssysteme zu entwickeln, die möglichst ohne personenbezogene Daten auskommen, und deren Anwendung so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt. Der Gesetzgeber muß sicherstellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher anonym zu bleiben.

Anlage 29

Entschließung

der Datenschutzbeauftragten des Bundes und der Länder

zum

Entwurf der Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) des Bundesministeriums für Post und Telekommunikation

Das Bundesministerium für Post und Telekommunikation hat den Entwurf einer Telekommunikations- und Informationsdienstunternehmen-Datenschutzverordnung (TIDSV) vorgelegt, der auf der Grundlage des bereits seit Anfang dieses Jahres geltenden Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG) den Schutz personenbezogener Daten der am Fernmeldeverkehr beteiligten Bürger regeln soll. Die Verordnung muß entsprechend der gesetzlichen Vorgabe dem Grundsatz der Verhältnismäßigkeit genügen, insbesondere hat sie die Erhebung, Verarbeitung und Nutzung der Daten auf das Erforderliche zu beschränken und ihre Zweckbindung zu gewährleisten. Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, daß der vorliegende Entwurf diesen aus der Verfassung abgeleiteten gesetzlichen Vorgaben teilweise nicht genügt.

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 8. März 1991 auf die Bedeutung des Grundrechts auf unbeobachtete Kommunikation hingewiesen und gefordert, daß das Telekommunikationsdatenschutzrecht dieses Grundrecht zu sichern hat. Im Zeitalter der elektronischen Information und Kommunikation ist es geboten, die Betreiber zur Bereitstellung anonymer Nutzungsmöglichkeiten zu verpflichten und den Bürger in die Lage zu versetzen, selbst zu entscheiden, ob er seine personenbezogenen Daten preisgeben und sich den damit verbundenen Risiken aussetzen will.

Im einzelnen halten die Datenschutzbeauftragten den vorliegenden Entwurf in folgenden Punkten für verbesserungsbedürftig, auch um eine Absenkung des Datenschutzniveaus gegenüber der gegenwärtigen Rechtslage zu verhindern:

- Die Verarbeitung von Kundendaten muß auch in Zukunft ausdrücklich auf Telekommunikationszwecke und Zwecke der Informationsdienstleistung beschränkt werden; jede Aufweichung des Zweckbindungsgrundsatzes ist abzulehnen.

- Auch im Bereich des Sprachtelefondienstes soll nach dem Entwurf die Speicherung der vollständigen Rufnummer des angerufenen Teilnehmers bis zu 80 Tagen nach Rechnungsversand zur Regel werden. Bislang war dies nur vorgesehen, wenn der Anrufer einen Einzelverbindungsnachweis beantragt hat; dabei sollte es auch in Zukunft bleiben.

- Eine Auswertung der Verbindungsdaten nach Zielrufnummern auch außerhalb des Sprachtelefondienstes ohne Einwilligung des Kunden ist nach § 10 Abs. 2 Nr. 2 PTRegG unzulässig. Hiernach “dürfen Daten des Anrufenden nur mit dessen Einwilligung verwendet und müssen Daten des Angerufenen unverzüglich anonymisiert werden.”

- Die Übermittlung von Verbindungsdaten an Diensteanbieter darf auch für Zwecke des Entgelteinzuges weiterhin nur mit Einwilligung des Kunden zugelassen werden, wenn der Datenempfänger sich vertraglich zur Einhaltung des Fernmeldegeheimnisses verpflichtet hat.

- Ein Einzelverbindungsnachweis sollte auch in Zukunft nur erteilt werden, wenn der Antragsteller das Einverständnis der zum Haushalt gehörenden Mitbenutzer des Anschlusses nachweisen kann.

- Die Anonymität von Anrufern bei Beratungseinrichtungen muß auch dann gewährleistet sein, wenn sie über ein Mobilfunknetz anrufen. Es ist nicht nachzuvollziehen, daß gerade an den dynamischsten und modernsten Teilbereich der Telekommunikation geringere Datenschutzanforderungen gestellt werden sollen als an das traditionelle Festnetz. Ohnehin ist eine Entwicklung absehbar, die Mobilfunk- und Festnetze zusammenwachsen läßt.

- Der Anrufer muß im Sprachtelefondienst die kostenfreie Möglichkeit haben, die Übermittlung seiner Rufnummer an den angerufenen Anschluß dauernd oder fallweise auszuschließen.

- Beim angerufenen Anschluß im Sprachtelefondienst muß auch in Zukunft die Abschaltung der Rufnummernanzeige allgemein und im Einzelfall möglich sein, damit Personen, die sich in räumlicher Nähe zum Angerufenen aufhalten, nicht zwangsläufig Kenntnis vom jeweiligen Anrufer erhalten.

- Die regelmäßige Herausfilterung der Daten solcher Verbindungen, für die tatsächliche Anhaltspunkte den Verdacht eines strafbaren Mißbrauchs von Fernmeldeanlagen oder der mißbräuchlichen Inanspruchnahme von Telekommunikations- oder Informationsdienstleistungen begründen, kommt einer präventiven Rasterfahndung der dem Fernmeldegeheimnis unterliegenden Verbindungsdaten gleich, in die bereits im Vorfeld eines konkreten Verdachts sämtliche Teilnehmer einbezogen werden. Die entsprechende Regelung sollte dieses Verfahren lediglich auf den Einzelfall beschränken.

- Hinsichtlich der Erhebung, Verarbeitung und Nutzung von Nachrichteninhalten sind die strengen Vorgaben von § 10 Abs. 2 Sätze 2 - 5 PTRegG einzuhalten. Insoweit fehlt in dem vorliegenden Entwurf eine Einschränkung auf den Einzelfall und die Verankerung der nach § 10 PTRegG vorgesehenen Informations- und Unterrichtungspflichten.

- Die geplante Umwandlung der bisherigen Telefonauskunft ist datenschutzrechtlich nur vertretbar, wenn der Kunde über die Verwendungsmöglichkeit in der Telefonauskunft und sein Widerspruchsrecht hinreichend informiert wird. So muß er insbesondere wissen, daß nicht nur seine Rufnummern, sondern sämtliche Angaben, die er für die Teilnehmerverzeichnisse freigegeben hat, auch beauskunftet und verwendet werden können, sofern er dem nicht widersprochen hat.

- Die vorgesehenen Regelungen über öffentliche Kundenverzeichnisse und die Telefonauskunft tragen den besonderen Risiken der Verbreitung von Kundendaten in elektronischer Form, etwa auf CD-ROM oder durch Abruf aus Online-Diensten (Adreß-Selektion, bundesweite Recherche, umgekehrte Rufnummernsuche) nicht Rechnung. Der Kunde muß ein differenziertes Widerspruchsrecht erhalten, das ihm ermöglicht, seine Daten zwar in das herkömmliche Telefonbuch aufzunehmen oder von der Telefonauskunft mitteilen zu lassen, eine Aufnahme in elektronische Verzeichnisse mit qualitativ weitergehenden Verarbeitungsmöglichkeiten jedoch zu unterbinden.

- Der Verordnungsentwurf läßt abweichend von der gegenwärtigen Praxis bei der Deutschen Telekom AG die Erstellung von Einzelverbindungsnachweisen mit vollständigen Zielrufnummern ohne Einflußmöglichkeit der angerufenen Kunden zu. Die Anonymität des Angerufenen wird aber auch durch die Verkürzung der Zielrufnummer um die letzten drei Ziffern nicht hinreichend gewährleistet. Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung vom 9./10. März 1994 darauf hingewiesen, daß dem Schutz des informationellen Selbstbestimmungsrechts und des Fernmeldegeheimnisses des Angerufenen am besten dadurch entsprochen würde, wenn jeder inländische Anschlußinhaber selbst entscheiden könnte, ob und gegebenenfalls wie seine Rufnummer auf Einzelverbindungsnachweisen erscheinen soll. Obwohl ein entsprechendes Verfahren in den Niederlanden erfolgreich praktiziert wird, hat der Bundesminister für Post und Telekommunikation diesen Vorschlag bisher nicht aufgegriffen.

- Die Vorschriften für Bildschirmtextdienste sollten, auch im Sinne der Rechtssicherheit, möglichst weitgehend mit denen des Bildschirmtext-Staatsvertrages harmonisiert werden. Insbesondere sollte die Speicherung von Abrechnungsdaten so beschränkt werden, daß Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von den einzelnen Kunden in Anspruch genommener Angebote nicht erkennbar sind, es sei denn, der Kunde beantragt mit Einverständnis der Mitbenutzer einen Einzelverbindungsnachweis. Ferner ist vorzusehen, daß Abrechnungsdaten nicht erst sechs Monate nach Bekanntgabe der Entgeltrechnung gelöscht werden, sondern unverzüglich, wenn sie für Abrechnungszwecke nicht mehr erforderlich sind.

Anlage 30

Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

erstellt vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 1. Dezember 1995

I. Einleitung

Seit einiger Zeit wächst in öffentlichen Stellen der Wunsch nach einem Zugang zu globalen Datennetzen, insbesondere zu dem Internet. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen (zur Beschreibung des Internet und der wichtigsten Internetdienste vgl. Anlage 30a).

Dabei ist der Anschluß an das Internet mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden. Die Risiken resultieren großenteils daraus, daß das Internet nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. So gibt es beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung im Netz. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von z.Zt. mehr als 40 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnutzen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Die vorliegende Orientierungshilfe soll den für den Betrieb von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der "internen" Netze bei einem Anschluß an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Die Frage, ob und ggf. unter welchen Bedingungen Verwaltungen personenbezogene Daten über das Internet austauschen dürfen, ist nicht Gegenstand der Orientierungshilfe und muß jeweils konkret untersucht werden.

Die hier entwickelten Strategien zur Risikobegrenzung bedürfen im Einzelfall einer weiteren Konkretisierung, wobei neben den beschriebenen Firewall-Architekturen ggf. weitere Maßnahmen zu ergreifen sind, um eine Gefährdung personenbezogener Daten zu vermeiden (etwa Einsatz von Verschlüsselungsverfahren). Angesichts einer sich ständig verändernden Gefährdungslage infolge der "Entdeckung" neuer unerwarteter Sicherheitsprobleme bleiben auch bei Einsatz von Firewall-Systemen erhebliche Restrisiken bestehen.

Der Anschluß an das Internet ist angesichts dieser Gefährdungslage aus Datenschutzsicht nur vertretbar, wenn zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und die Gefahren durch technische und organisatorische Maßnahmen sicher beherrscht werden können. Die nachfolgenden Empfehlungen stellen ein Konzentrat aus den weiter unten angestellten eingehenderen Betrachtungen dar.

II. Empfehlungen

- Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und soweit dies erforderlich ist. Die Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muß und ob die Aufgabe mit einem nicht in das Verwaltungsnetz eingebundenen Rechner erfüllt werden kann.
- Voraussetzung für die Anbindung eines Behördennetzes an das Internet ist das Vorliegen eines schlüssigen Sicherheitskonzepts und dessen konsequente Umsetzung. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.
- Die Sicherheit des Verwaltungsnetzes und der Schutz von personenbezogenen Daten, die auf vernetzten Systemen verarbeitet werden, ist durch geeignete Firewall-Systeme sicherzustellen, die eine differenzierte Kommunikationssteuerung und Rechtevergabe unterstützen. Dabei sind die Anforderungen, die von den Firewall-Komponenten zu erfüllen sind, vorab zu definieren, wobei sich die Verwaltung ggf. auch externen Sachverstands bedienen sollte.

- Um der Gefahr von Maskeraden und der Ausforschung der Netzstrukturen des geschützten Netzes entgegenzuwirken, ist eine gesonderte interne Adreßstruktur zu verwenden. Die internen Adressen sind durch die zentrale Firewall auf externe Internet-Adressen umzusetzen.
- Der ausschließliche Einsatz einer zentralen Firewall-Lösung ist nur dann vertretbar, wenn eine Orientierung am höchsten Schutzbedarf erfolgt, auch wenn dies Nachteile für weniger sensible Bereiche mit sich bringt. Die Frage der Kontrolle interner Verbindungen bleibt bei einer solchen Lösung offen. Ferner ist eine ausschließlich zentrale Lösung mit der Maxime der lokalen Haltung und Verwaltung von sicherheitsrelevanten Daten (Pflege von Benutzerprofilen) schwer vereinbar. Werden solche Daten nicht durch diejenigen verwaltet, die den verwalteten Bereich direkt überschauen können, besteht die Gefahr erheblicher Differenzen zwischen Realität und sicherheitstechnischem Abbild.
- Das Konzept gestaffelter Firewalls kommt den Datenschutzanforderungen an Verwaltungsnetze entgegen, die aus einer Vielzahl verschiedener Teilnetze bestehen, in denen Daten unterschiedlicher Sensibilität von unterschiedlichen Stellen für unterschiedliche Aufgaben verarbeitet werden und in denen dementsprechend jeweils unterschiedliche Sicherheitsanforderungen bestehen. Die mit gesonderten Firewalls abgesicherten Subnetze sollten jeweils einen definierten Übergang zu dem Gesamtnetz erhalten. Die Anbindung des Gesamtnetzes an das Internet sollte stets über ein zentrales Gateway erfolgen, das durch eine Firewall geschützt wird.
- Der personelle und sachliche Aufwand für Firewall-Lösungen ist generell hoch. Es ist gleichwohl unverzichtbar, hochspezialisierte Kräfte einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein. Dieser Aufwand ist jedoch stets dann gerechtfertigt, wenn Verwaltungsnetze an das Internet angeschlossen werden sollen, in denen sensible personenbezogene Daten verarbeitet werden.
- Der Betrieb von Firewall-Systemen muß klaren Richtlinien folgen. Diese Richtlinien müssen neben Zuständigkeitsregelungen auch Vorgaben über die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und Sanktionen bei Sicherheitsverstößen enthalten.
- Auch bei Einsatz von Firewalls bleiben Restrisiken bestehen, denen anwendungsbezogen begegnet werden muß. So bleibt es auch beim Einsatz von Firewalls notwendig, sensible Daten nur verschlüsselt zu übertragen; hierzu gehören neben besonders sensiblen personenbezogenen Daten auch Paßwörter und sonstige Authentifikationsdaten.
- Bei einem unvertretbaren Restrisiko muß auf einen Anschluß des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste muß in diesem Fall auf nicht in das Verwaltungsnetz eingebundene Systeme beschränkt werden, auf denen ansonsten keine sensiblen Daten verarbeitet werden.
- Firewall-Konzepte entlasten die dezentralen Verwalter von vernetzten Systemen nicht von ihrer Verantwortung zur Gewährleistung des Datenschutzes; vielmehr erhöhen sich mit der Vernetzung die Anforderungen an die lokale Systemverwaltung, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben könnten als bei stand alone betriebenen Rechnern.

III. Sicherheitsrisiken im Internet

Die nachfolgend dargestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluß wider. Selbst wenn Gegenmaßnahmen gegen die bekannten Gefährdungen getroffen werden, läßt sich ein hundertprozentiger Schutz ohne Verzicht auf die Netzanbindung nicht realisieren. Sobald ein Computer Zugang zu einem Datennetz hat, ist er von anderen angeschlossenen Rechnern aus erreichbar. Damit wird das eigene System der Gefahr eines unberechtigten Gebrauches ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu minimieren.

1. Protokollimmanente Sicherheitsrisiken

Sowohl die Nutzerkennung als auch das Paßwort werden bei den gängigen Diensten im Klartext über das lokale Netz (z.B. Ethernet) und über das Internet übertragen. Mit Programmen, die unter dem Namen Packet Sniffer bekannt sind, kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden. So können diese Abhörprogramme zahlreiche Nutzerkennungen mit den zugehörigen Paßworten ausspähen, mit deren Hilfe sich ein Angreifer einen unberechtigten Zugriff auf andere Rechner verschaffen kann.

Datenpakete können nicht nur abgehört, sondern auch manipuliert werden. Da bei vielen Internet-Diensten die Authentisierung der Rechner lediglich über die IP-Nummer des Nutzers erfolgt, kann sich dies ein Angreifer zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen ans fremde Rechnersystem schickt (IP-Spoofing). Sofern das System die IP-Adresse für vertrauenswürdig hält, wird dem Eindringling ein Zugang, unter Umständen sogar mit Administratorrechten, gewährt. Ferner kann der Übertragungsweg bei dynamischem Routing geändert werden. Pakete können abgefangen werden, so daß sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch

eigene Pakete ersetzen. Weiterhin läßt sich die Kommunikation eines autorisierten Nutzers mitschneiden und später wiedereinspielen, wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers verschafft (z.B. beim Festplattenzugriff über NFS (Network File System)).

2. Dienstspezifische Sicherheitsrisiken

E-Mail und Usenet-News:
Private Nachrichten können mitgelesen werden, sofern sie nicht verschlüsselt sind. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht verändern oder fälschen. Über den elektronischen Postweg können Programme und Textdokumente mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz.
Die Informationen über Datum und Uhrzeit der Erstellung einer Nachricht können zu einem Persönlichkeitsprofil des Absenders ausgewertet werden. Daneben forschen Adreßsammler nach E-Mail- und Post-Adressen, um unaufgefordert Werbung zuzuschicken.
Sendmail, das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post, weist zudem eine ganze Reihe von sicherheitsrelevanten Fehlern auf, die zu einer Zugangsmöglichkeit mit Administratorrechten führen können.
Zudem ist nicht sicherzustellen, daß eine E-Mail den Empfänger überhaupt erreicht und daß der Absender einen Nachweis der Zustellung erhält.

Telnet:
Ist der Telnet-Dienst nicht eingeschränkt, sondern von beliebigen Adressen aus zu beliebigen Ports auf dem eigenen Rechner möglich, wird die Zugangskontrolle gefährdet. Auch einem Angreifer, dem es nicht gelingt, sich einen Zugang mit Administratorrechten zu verschaffen, hat häufig die Möglichkeit, einen nichtprivilegierten Account auf dem Rechner zu nutzen. Dieser Account kann dann als Ausgangsbasis für den Angriff auf weitere Rechner verwendet werden.

FTP:
Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen des FTP-Server-Programms (ftpd) Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Besondere Vorsicht ist geboten, da viele Beschreibungen zur Installation und Konfiguration von Anonymous-FTP-Servern sicherheitsbedenkliche Fehler enthalten. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, die Datei mit den verschlüsselten Paßwörtern aller Benutzer auf seinen Rechner zu laden und dort in aller Ruhe zu entschlüsseln. Läßt man zu, daß Benutzer eines FTP-Servers eigene Dateien in Verzeichnissen ablegen können, wo andere sie sich holen können, kann sich der FTP-Server schnell zu einem Umschlagplatz von Raubkopien entwickeln.

WWW:
Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) läßt sich die Kommunikation abhören. Außerdem weisen CGI (Common Gateway Interface)-Skripte häufig Sicherheitslücken auf. Zur Zeit sind WWW-Browser in der Entwicklung, die das Ablegen von Dateien auf dem Server erlauben. Dies kann zu weiteren Sicherheitsproblemen führen. Beim Nutzen des World Wide Web können zahlreiche Daten über den Anwender und sein Verhalten (was hat wer wann aufgerufen und wie lange gelesen?) protokolliert werden, so daß ein umfassendes Persönlichkeitsprofil erstellt werden kann.

Finger:
Die Daten, die der Finger-Dienst ausgibt, können einem Angreifer Informationen über die Nutzerkennungen auf dem System liefern, die gezielt für einen Angriff verwendet werden können. Berühmt geworden ist dieser Dienst 1988 durch den sogenannten Internet-Wurm. Dabei handelte es sich um ein Angriffsprogramm, das ausnutzte, daß die beim Aufruf von Finger übergebenen Parameter in einen Puffer fester Länge geschrieben wurden. Die Daten, die nicht mehr in den Puffer paßten, überschrieben den Stack im Arbeitsspeicher, wo sie als Programmcode behandelt und ausgeführt wurden. Bei geschickter Wahl der übergebenen Zeichenreihe kann so beliebiger Code zur Ausführung kommen. Ähnliche Programmfehler finden sich auch heute noch in vielen anderen Serverprogrammen. Zum Beispiel ist gerade Ende 1995 ein weiterer solcher Fehler im Programm Sendmail bekannt geworden. Der Protokollierbefehl Syslog und manche WWW-Browser (auch für MS-Windows) enthalten ebenfalls Fehler dieser Art.

IV.Kommunikationsanalyse

Bevor eine öffentliche Stelle Zugang zum Internet bekommt, muß sie eine Analyse des Kommunikationsbedarfs durchführen. Bei der Beurteilung der Erforderlichkeit eines Internet-Anschlusses ist ein strenger Maßstab anzulegen. Auch wenn die Erforderlichkeit bejaht wird, ist zu prüfen, ob der Verwendungszweck nicht schon durch den Anschluß eines isolierten Rechners erreicht werden kann.

Die Art des zu realisierenden Zugangs hängt wesentlich davon ab, welche Dienste des Internet genutzt werden sollen. Dabei ist zu unterscheiden zwischen Diensten, die von lokalen Benutzern im Internet abgerufen werden, und Diensten, die von lokalen Rechnern für Benutzer im Internet erbracht werden. Diese Kommunikationsanforderungen müssen auf Grund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zum Internet als auch für jeden einzelnen Rechner analysiert werden. Es dürfen nur die IP-Pakete weitergeleitet werden, die für den zu nutzenden Dienst bezogen auf den nutzungsberechtigten Rechner notwendig sind.

Wird bei der Analyse des Kommunikationsbedarfs festgestellt, daß die Anbindung an das Internet auf IP-Ebene notwendig ist, das TCP/IP-Protokoll also in seiner vollen Funktionalität genutzt wird, müssen weitere Sicherheitsbetrachtungen durchgeführt werden, die Voraussetzung für die Planung und Realisierung von Sicherheitskonzepten sind. Ausgangspunkte einer derartigen Risikoanalyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle.

In Anlehnung an die Empfehlungen des BSI-Grundschutzhandbuches sind zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Welche Informationen sollen nicht nach außen gelangen?
- Wie können z.B. die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?
- Welche Zugänge werden benötigt (z.B. nur über einen Internet-Service-Provider)?
- Welche Datenmengen werden voraussichtlich übertragen?
- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?
- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?
- Welche Aktivitäten im Netz sollen protokolliert werden? (Dabei werden ggf. Fragen des Arbeitnehmerdatenschutzes tangiert.)
- Welche Dienste sollen auf keinen Fall genutzt werden?
- Wird sichergestellt, daß nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind (was nicht erlaubt ist, ist verboten)?
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?
- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

Um im Rahmen der empfohlenen Kommunikationsanalyse beurteilen zu können, welche Dienste von welchem Nutzer an welchem Rechner tatsächlich benötigt werden, sollten die jeweiligen Stellen zunächst versuchen, genaue Kenntnisse über die Möglichkeiten und Gefährdungen der angebotenen Kommunikationsmöglichkeiten zu erlangen (etwa durch entsprechende Tests mit an das Internet angeschlossenen Einzelplatz-PC).

V. Firewalls

Soll ein Verwaltungsnetz an das Internet angeschlossen werden, so kann dies entweder durch einen zentralen Zugang oder durch mehrere dezentrale erfolgen. Aus Sicherheitsgründen ist ein zentraler Zugang vorzuziehen. Ist das Verwaltungsnetz erst einmal an das Internet angeschlossen, so lassen sich die durch die Anbindung hervorgerufenen Sicherheitsrisiken durch Einsatz einer Firewall reduzieren.

Unter einer Firewall (”Brandschutzmauer”) wird eine Schwelle zwischen zwei Netzen verstanden, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe einer Firewall besteht darin, zu erreichen, daß jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und daß Mißbrauchsversuche frühzeitig erkannt werden. Üblicherweise wird dabei davon ausgegangen, daß die Teilnehmer des internen Netzes (hier: des Verwaltungsnetzes) vertrauenswürdiger sind als die Teilnehmer des externen Netzes (hier: des Internet). Gleich-

wohl sind Firewall-Lösungen auch geeignet, die ”grenzüberschreitenden” Aktivitäten der internen Nutzer, d.h. den Übergang zwischen verschiedenen Teilnetzen (z.B. Ressortnetze) innerhalb eines Verwaltungsnetzes zu begrenzen.

Firewalls weisen die folgenden Charakteristika auf:
- die Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz;
- im internen Netz besteht jeweils ein einheitliches Sicherheitsniveau; eine weitere Differenzierung nach Sicherheitsstufen geschieht - zumindest auf der Ebene des Netzes - nicht;
- die Firewall setzt eine definierte Sicherheitspolitik für das zu schützende Netz voraus; in diese müssen die Anforderungen aller vernetzten Stellen einfließen;
- es besteht die Notwendigkeit einer firewallbezogenen Benutzerverwaltung derjenigen internen Teilnehmer, die mit Rechnern in dem externen Netz kommunizieren dürfen.

Die Stärke der Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab; entscheidend für die Sicherheit sind jedoch auch die Staffelung und die organisatorische Einbindung von Firewalls in die IuK-Infrastruktur.

Von besonderer Relevanz ist der Aspekt, daß für den von einer Firewall geschützten Bereich das erforderliche Schutzniveau definiert wird. Diese Anforderung kann mit drei Lösungsvarianten erfüllt werden:

1. einheitlich hohes Schutzniveau im internen Netz, d.h. Orientierung am höchsten vorhandenen Schutzbedarf;
2. einheitlich niedriges Schutzniveau, d.h. Orientierung am niedrigsten vorhandenen oder einem insgesamt geringen oder mittleren Schutzbedarf;
3. einheitlich niedriges Schutzniveau sowie Durchführung zusätzlicher Maßnahmen zum Schutz von Netz-Komponenten mit höherem Schutzbedarf.

Die Varianten 1 und 2 entsprechen am ehesten zentralen Firewall-Lösungen, wobei angesichts der Sensibilität der in der Verwaltung verarbeiteten Daten allein Variante 1 mit den Anforderungen des Datenschutzrechts vereinbar sein dürfte. Variante 3 führt zur Lösung gestaffelter Firewalls, d.h. zu einer Konstellation, bei der neben einer zentralen, den mittleren Schutzbedarf abdeckenden Firewall (die u.a. die interne Netzstruktur nach außen sichert) bereichsbezogen und bedarfsorientiert Firewall-Anschlüsse mit unterschiedlichem Sicherheitsniveau implementiert werden können. Allerdings können selbst bei einheitlich hohem Schutzniveau im Gesamtnetz gestaffelte Firewalls sinnvoll sein, um den möglichen Schaden, der mit Sicherheitsverletzungen verbunden ist, auf ein Netzsegment zu begrenzen. Dies gilt insbesondere auch für die Abwehr von internem Mißbrauch.

1. Zentrale Firewalls

Rein zentrale Firewall-Lösungen (vgl. Abb. 1) sind durch folgende Aspekte charakterisiert:

- die zentrale Firewall bildet die einzige Schnittstelle zwischen dem kompletten zu schützenden Verwaltungsnetz und dem übrigen Internet;
- innerhalb des Verwaltungsnetzes besteht ein einheitliches Sicherheitsniveau, eine weitere Differenzierung nach Sicherheitsstufen erfolgt nicht;
- eine Kontrolle der internen Verbindungen durch die Firewall ist nicht möglich;
- die zentrale Firewall setzt eine definierte Sicherheitspolitik für das gesamte Verwaltungsnetz voraus; abweichende Sicherheitspolitiken für besonders schützenswerte Bereiche sind auf Netzebene nicht durchsetzbar;
- es besteht die Notwendigkeit einer zentralen Benutzerverwaltung. Für jeden Teilnehmer muß sowohl auf Dienstebene als auch bezogen auf die zugelassenen Adressen die zulässige Kommunikation festgelegt werden.

Da eine zentrale Firewall eine Differenzierung nach Teilnetzen nicht unterstützt und dementsprechend ein einheitliches Sicherheitsniveau für das gesamte Verwaltungsnetz voraussetzt, muß sich der Grad des gewährleisteten Schutzes nach den sensibelsten Daten richten und ist dementsprechend hoch. Dies hat jedoch für Verwaltungsbereiche mit weniger sensiblen Daten den Nachteil, unnötig hohe Schranken zu errichten. Daraus ergibt sich die Gefahr, daß von diesen Stellen zusätzliche Internet-Zugänge mit geringeren Restriktionen geschaffen werden, wodurch der gesamte Zweck der Firewall ad absurdum geführt wird.

Ein weiterer Nachteil zentraler Firewalls besteht in dem - auch aus dem Großrechnerbereich bekannten - Problem, daß eine Benutzerverwaltung, die fernab von dem jeweiligen Fachbereich erfolgt, häufig zu Abweichungen zwischen der Realität von Benutzerrechten und deren Abbildung in Form von Accounts führt.

Da sich Firewall-Lösungen primär zum Schutz gegen Zugriffe von außen eignen, sekundär auch zum Schutz gegen Zugriffe von innen nach außen, jedoch nicht zur Kontrolle der rein internen Zugriffe, besteht bei rein zentralen Lösungen die Gefahr, daß das gesamte Verwaltungsnetz als eine Einheit betrachtet wird und insofern nur die Zugriffe von oder nach außen restringiert werden. Dieser Aspekt ist zwar nur mittelbar Teil des Themas "Internetanbindung", muß bei einer Gesamtbetrachtung von Netzwerksicherheit jedoch unbedingt einbezogen werden.

Der Einsatz einer alleinigen zentralen Firewall ist allenfalls dann vertretbar, wenn alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Mißbrauchs besteht. Davon kann in behördenübergreifenden Verwaltungsnetzen mit einer Vielzahl angeschlossener Rechner jedoch nicht ausgegangen werden.

2. Gestaffelte Firewalls (Voraussetzungen, Einsatzmöglichkeiten, Forderungen)

Gestaffelte Firewall-Lösungen (vgl. Abb.2) sind durch folgende Aspekte charakterisiert:

- es handelt sich um eine Kombination zentraler und dezentraler Komponenten, wobei durch eine zentrale Firewall ein Mindestschutz für das Gesamtnetz gegenüber dem Internet realisiert wird und dezentrale Firewalls in Subnetzen mit besonderem Schutzbedarf ein angemessenes Schutzniveau sicherstellen;
- innerhalb des jeweiligen geschützten Subnetzes besteht jeweils ein einheitliches Sicherheitsniveau;
- eine Kontrolle der verwaltungsinternen Verbindungen ist möglich, sofern die Kommunikation den durch dezentrale Firewalls geschützten Bereich überschreitet;
- auch ein gestaffeltes Firewall-System setzt eine definierte Sicherheitpolitik für das Gesamtnetz voraus; in diese müssen insbesondere die Anforderungen an einen zu garantierenden Grundschutz einfließen; darüber hinaus sind für die Subnetze gesonderte Sicherheitsanforderungen zu definieren;
- die Benutzerverwaltung kann weitgehend dezentralisiert werden. Allerdings sind einheitliche Regeln festzulegen, nach denen Benutzer das Recht haben, über die zentrale Firewall mit Systemen im Internet in Verbindung zu treten.

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Mechanismen wie bei einer zentralen Firewall an. Die Kombination zentraler und dezentraler Schutzmechanismen erlaubt die Realisierung des Prinzips eines autonomen Schutzes; bei sorgfältiger Konfiguration bleiben besonders geschützte Subnetze auch dann gesichert, wenn die zentrale Firewall durch einen Eindringling überwunden wurde.

Mit gestaffelten Firewalls kann - anders als bei zentralen Lösungen - das datenschutzrechtlich bedeutsame Prinzip der informationellen Gewaltenteilung abgebildet werden, mit dem es nicht zu vereinbaren wäre, wenn die Verwaltung als informatorisches Ganzes betrachtet würde. Die Teilnetze können sowohl gegen Angriffe von außen - aus dem Internet - als auch untereinander abgeschottet werden.

Da gestaffelte Lösungen besser als ausschließlich zentrale Firewalls die Anforderungen der Benutzer abbilden können, ist auch die Gefahr der Umgehung der kontrollierten Schnittstellen durch Schaffung "wilder" Internetzugänge geringer. Zudem würden sich die Folgen derartiger Verstöße gegen die festgelegte Sicherheitspolitik besser isolieren lassen.

Auch gestaffelte Firewalls sind mit einem insgesamt hohen Administrations- und Pflegeaufwand verbunden, der jedoch auf die zentrale Firewall und jeweiligen Bereiche verteilt ist. Die Festlegung der individuellen Benutzerrechte kann dabei im wesentlichen den anwendernäheren dezentralen Firewalls zugeordnet werden.

Anlage 30a:

Dienste im Internet

Das Internet ist ein weltumspannender Zusammenschluß vieler lokaler Computernetze. Die Zahl der Benutzer wird auf etwa 40 Millionen geschätzt (Stand: Ende 1995). Bisher wurde das Internet hauptsächlich von wissenschaftlichen Einrichtungen wie Universitäten genutzt. Inzwischen hat sich der Nutzerkreis ausgeweitet, und es ist eine fortschreitende Nutzung für kommerzielle Zwecke zu beobachten. Der Datenübertragung im Internet liegen die einheitlichen TCP/IP-Protokolle (Transmission Control Protocol/Internet Protocol) zugrunde.

Jeder Rechner im Internet erhält eine eindeutige numerische Adresse, die IP-Adresse. Die zu übertragenden Daten werden in Pakete zerlegt, die u.a. mit der Absender- und der Empfänger-IP-Adresse versehen werden. Die Datenpakete werden über zumeist eine Vielzahl von Zwischenstationen weitergeleitet, die den Weg zum Zielrechner aufgrund der Adreßinformationen bestimmen (Routing). Die Zwischenstationen tauschen die Daten über Wähl- oder Standverbindungen im Telefonnetz (per Kabel oder Satellit) aus.

Die wichtigsten Dienste, die das Internet bietet, werden im folgenden beschrieben.

E-Mail: Electronic Mail (kurz E-Mail) ist der am weitesten verbreitete Internet-Dienst. E-Mail ermöglicht das Verschicken von "elektronischen Briefen" zwischen mehreren Computerbenutzern. Die Nachrichten können aus Texten, Programmen, Grafiken oder Tönen bestehen. Sender und Empfänger müssen jeweils eine eindeutige E-Mail-Adresse besitzen (Form: Name@Anschrift), die ähnlich der postalischen Anschrift funktioniert. Um E-Mails in andere Datennetze zu verschicken oder von dort zu empfangen, werden Gateways benötigt, die den Übergang von einem System zum anderen handhaben. E-Mail kann außerdem für eine indirekte Inanspruchnahme von anderen Diensten (z.B. FTP, WWW) genutzt werden.

Usenet-News: Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (Newsgroups) ausgetauscht. Dieser News-Dienst wird auch als Usenet (Kurzform von Users´ Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zur Zeit gibt es etwa 10.000 verschiedene Newsgroups, in denen pro Monat rund 3,2 Millionen Artikel mit einem Datenvolumen von ca. 14 GB geschrieben werden (Stand: August 1995). Die Artikel werden auf zentralen Rechnern (Newsservern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreader-Programme.

Telnet: Mit Hilfe von Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login) und textorientierte Anwendungen zu nutzen. Dazu benötigt man einen Account (Nutzerkennung und Paßwort) oder einen öffentlichen Zugang auf dem entfernten Rechner. Über Telnet sind zum Beispiel Informationssysteme wie Datenbanken oder Bibliotheken zu nutzen. Telnet wird ebenfalls häufig für die Fernwartung von Rechnern eingesetzt.

FTP: FTP steht für File Transfer Protocol und dient dem Übertragen von Dateien zwischen Rechnern mit Hilfe eines normierten Befehlssatzes. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Voraussetzung für die Nutzung sind Accounts auf beiden Rechnern oder eine öffentliche Zugriffsmöglichkeit auf dem FTP-Server durch "Anonymous FTP", wodurch ein eingeschränkter Zugriff auf bestimmte Dateien des entfernten Rechners ermöglicht werden kann. Weltweit gibt es Tausende Anonymous-FTP-Server, die Programme, Texte, Grafiken oder Tondateien bereithalten.

Archie: Archie ist ein mächtiger Dienst für die weltweite Suche nach Dateien auf FTP-Servern. Der Zugriff erfolgt über Telnet, E-Mail oder einen eigenen Archie-Client. Als Suchergebnis liefert Archie entweder Server-, Verzeichnis- und Dateinamen oder eine Kurzbeschreibung zu gesuchten Dateien.

WWW Der jüngste Internet-Dienst WWW (World Wide Web) kann nahezu alle anderen Dienste integrieren. Durch einen multimediafähigen Hypertext-Mechanismus wird eine einfache Bedienbarkeit erreicht. Der Kommunikation zwischen dem WWW-Client und dem WWW-Server, der

die multimedialen Daten anbietet, liegt das Protokoll HTTP (Hyper Text Transport Protocol) zugrunde. Die WWW-Dokumente werden mit der Definitionssprache HTML (HyperText Markup Language) erstellt. Für die Generierung interaktiver WWW-Seiten können CGI (Common Gateway Interface)-Skripte installiert werden.

Gopher: Gopher ist ein menü-orientiertes Werkzeug zur Recherche, das unabhängig davon eingesetzt werden kann, auf welchem Rechner die gesuchten Informationen zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkeiten (FTP, Telnet, WAIS usw.) existieren. Jeder Gopher-Server ist öffentlich zugänglich. Benutzer können mit ihrem Gopher-Client nur lesend auf die angebotenen Daten zugreifen. Gopher ist im WWW integriert.

WAIS: WAIS (Wide Area Information Server) ermöglicht eine Volltextsuche in einer Vielzahl von Datenbanken ohne Kenntnis komplizierter Abfragesprachen. WAIS-Abfragen können mit Telnet, E-Mail, einem eigenen WAIS-Client oder über WWW durchgeführt werden.

Finger: Finger ist ein Werkzeug zur Suche nach Informationen über Personen und Rechner, die an der Kommunikation im Internet beteiligt sind. Es können sowohl personenbezogene Daten (Name, E-Mail-Adresse, Telefonnummer, Arbeitszeit, öffentliche Schlüssel usw.) als auch sicherheitsrelevante Informationen über angeschlossene Rechner in Erfahrung gebracht werden.

WhoIs: WhoIs wurde speziell zur Recherche nach personenbezogenen Daten von im Internet registrierten Nutzern entwickelt. Das Vorhaben, eine Datenbank mit weltweit allen Internet-Nutzern aufzubauen, konnte nicht realisiert werden. Zur Zeit existiert eine Vielzahl von einzelnen WhoIs-Servern, auf die mit Telnet oder mit besonderer Client-Software zugegriffen werden kann.

Anlage 30 b

Beispielhafte Darstellung von Firewall-Architekturen

Eine Firewall kann durch verschiedene Konzepte realisiert werden. Im wesentlichen unterscheidet man folgende Grundkonzepte:

- Packet Filter (packet screen, screening router)
- Application Gateway (dual-homed-gateway)

Ein Packet Filter ist ein Router, der IP-Pakete zur Unterscheidung zwischen der erlaubten und unerlaubten Nutzung von Kommunikationsdiensten filtert. Packet Filter können nach Quell- und Zieladresse sowie nach Quell- und Zielport filtern. Damit ist einerseits einschränkbar, welche Rechner an der Kommunikation beteiligt sein dürfen, sowohl im zu schützenden als auch im unsicheren Netz und andererseits, welche Kommunikationsdienste erlaubt sind.

Ein Application Gateway ist ein speziell konfigurierter Rechner, über den die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz stattfindet. Ein Application Gateway arbeitet, anders als ein Packet Filter, auf Anwendungsebene, d.h. die Kontrolle der Kommunikationsbeziehungen findet auf Anwendungsebene statt. Hierbei besteht z.B. die Möglichkeit, ausführliche Protokolle (Audits) zu führen und eine benutzerbezogene Authentisierung für die unterschiedlichen Dienste durchzuführen.

Die Kombination der Grundkonzepte wird als screened Gateway bezeichnet und erhöht die Sicherheit der Firewall erheblich. Die Anordnung der beteiligten Komponenten kann variieren und erlaubt die individuelle Realisierung eines Firewall-Konzeptes.

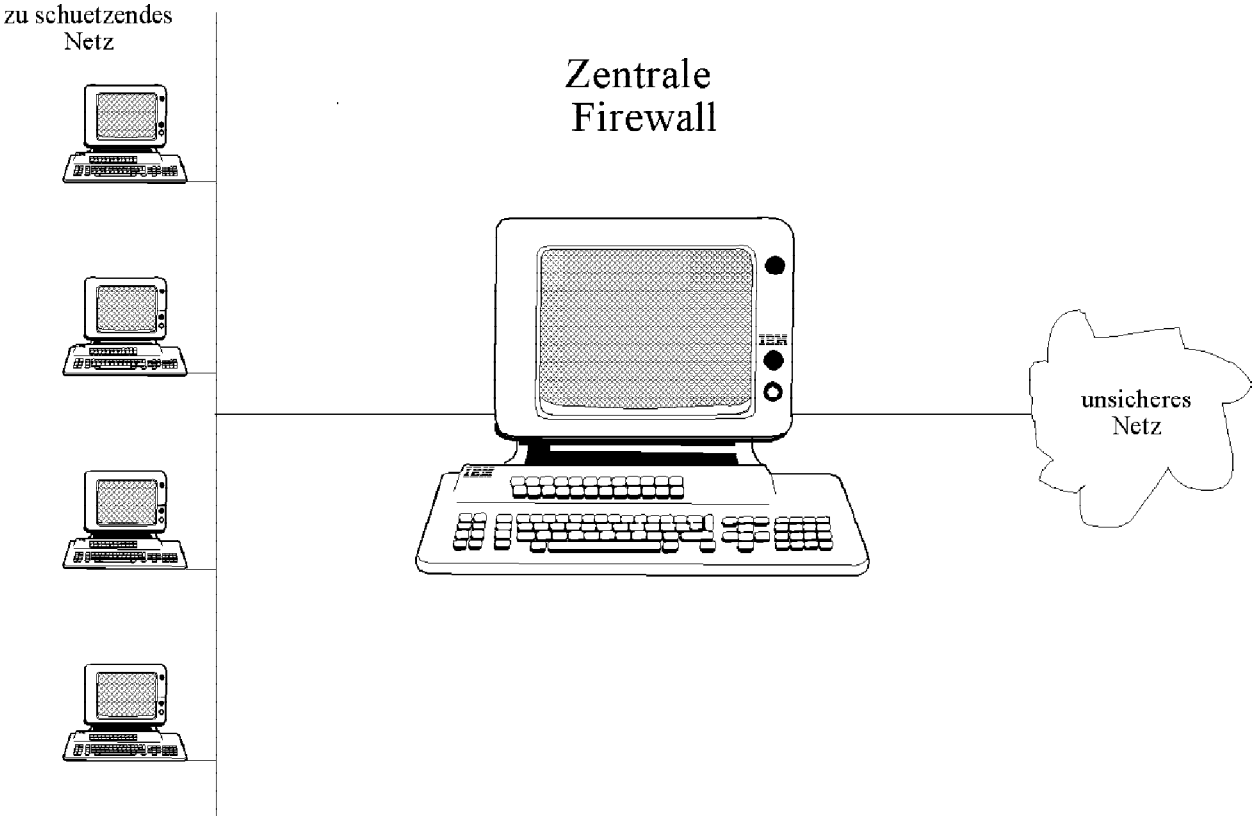


Abbildung 1: Zentrale Firewall-Anordnung

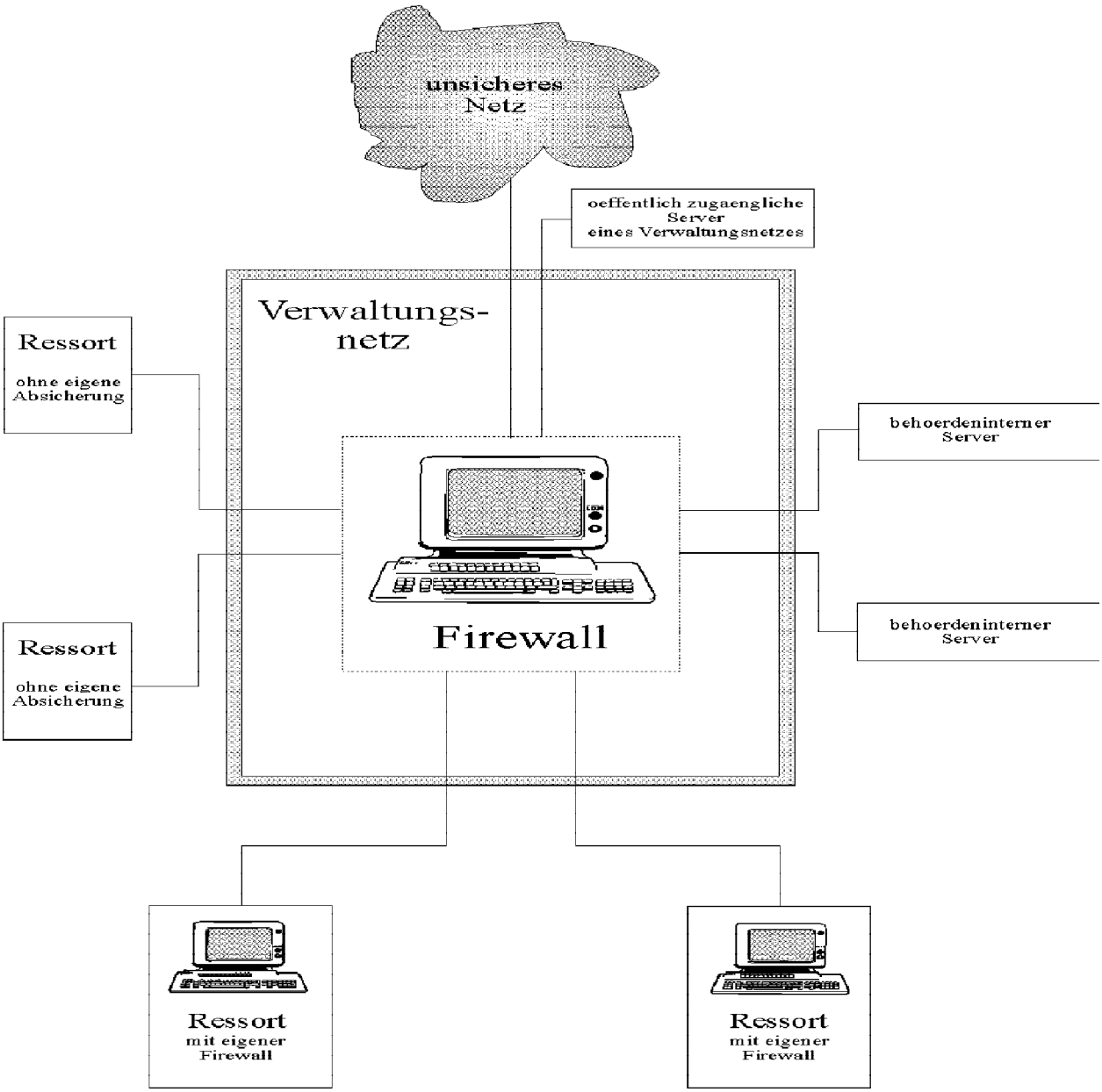


Abb. 2: Gestaffelte Firewall- Anordnung

	VORTEILE	NACHTEILE
PACKET FILTER Router oder Rechner mit spezieller Software	leicht realisierbar: einfache Installation und Administration leicht erweiterbar Router auf dem Markt verfügbar Preis	IP-Spoofing möglich alle Dienste, die erlaubt und erreicht werden können, müssen sicher sein komplexe Filterregeln keine ausreichende Protokollierungsmöglichkeiten es ist nicht möglich, Dienste nur für bestimmte Benutzer zu zulassen
DUAL-HOMED-GATEWAY Applikations-Gateway mit zwei Netz-Interfaces	kein Paket kann ungefiltert passieren umfangreiche Protokollierung möglich interne Netzstruktur wird verborgen	keine Transparenz für den Benutzer Probleme bei neuen Diensten Übernahme des Applikations-Gateway durch einen Angreifer führt zu einen vollständigen Verlust der Sicherheit Preis
SCREENED SUBNET Anordnungen aus Applikation Gateway mit einem oder zwei Packet-Filter bilden Teilnetze	kein direkter Zugang zum Gateway möglich die Struktur der internen Netze wird verdeckt vereinfachte Regeln durch zweiten Filter durch Einsatz mehrerer Gateways läßt sich die Verfügbarkeit steigern umfangreiche Protokollierung möglich	wenn Packet Filter manipuliert werden, ist eine direkte Verbindung unter Umgehung des Gateways möglich keine Transparenz für den Benutzer Preis

Abb. 3: Vorteile und Nachteile von verschiedenen Firewall-Typen

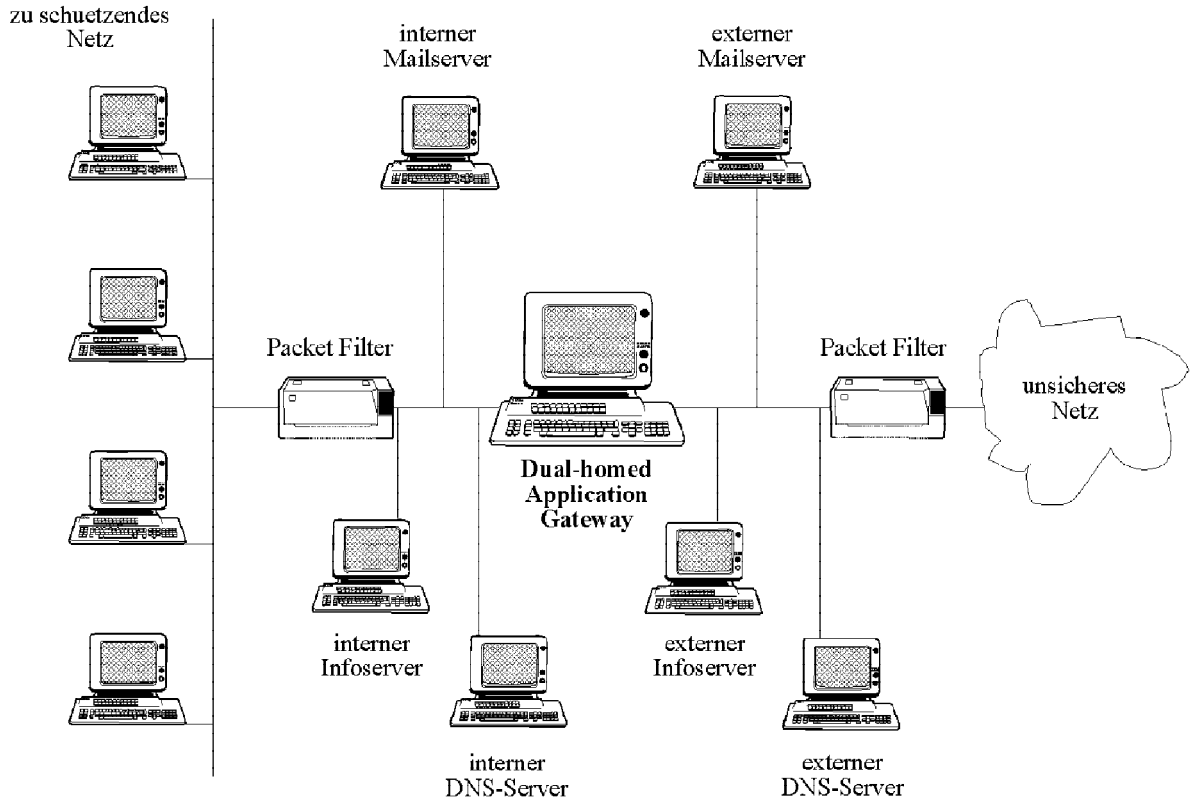


Abb. 4: Screened Subnet mit Dual-homed Gateway

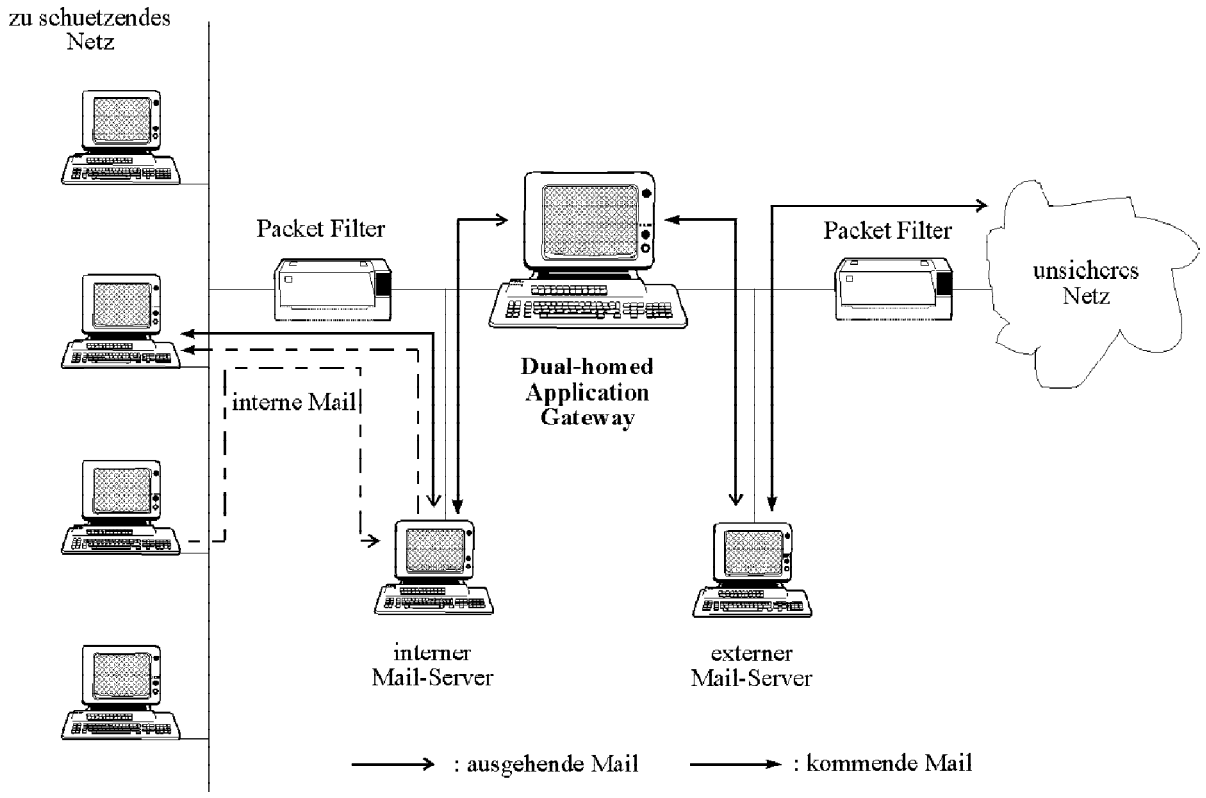


Abb.5: Anordnung der Mail-Server

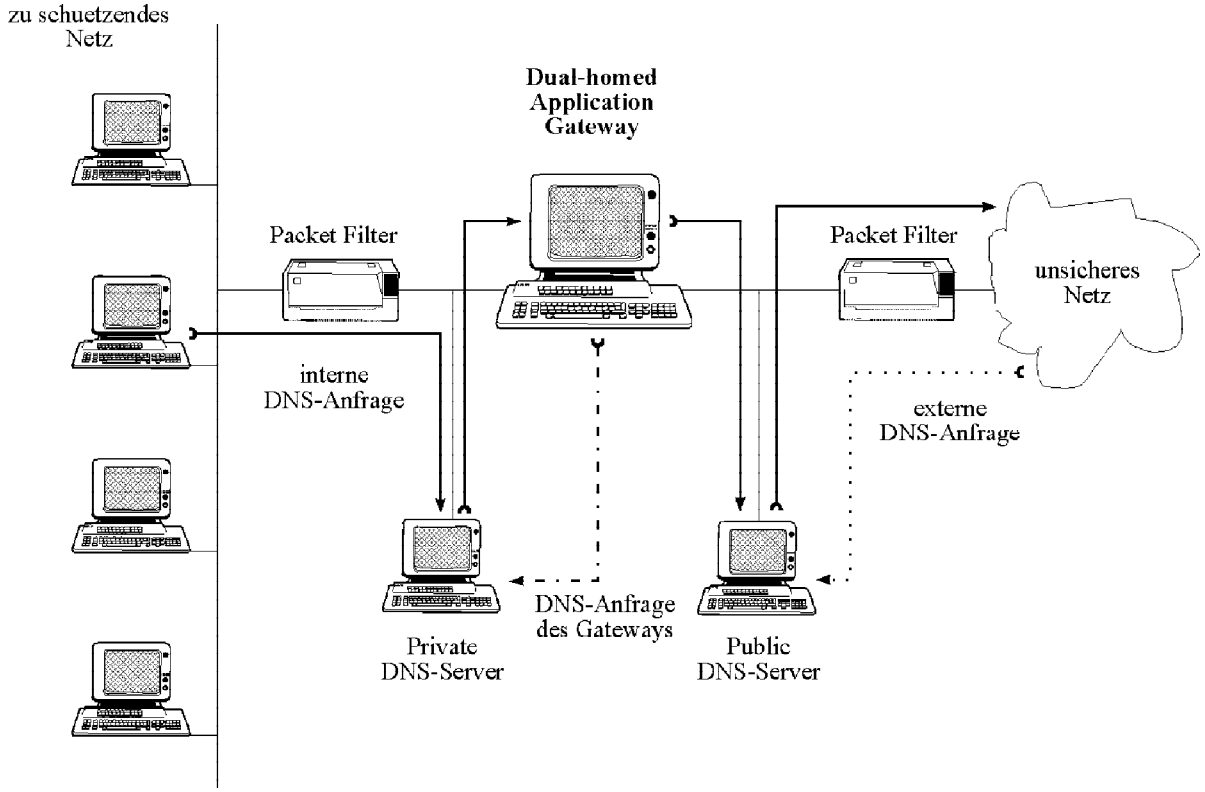


Abb. 6: Anordnung der DNS-Server

Anlage 31

Orientierungshilfe "Datenschutzrechtliche Protokollierung beim Betrieb Informationstechnischer Systeme (IT-Systeme)" vom 17.01.95

1. Begriff

1.1 Unter Protokollierung beim Betrieb von IT-Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen

- über die tatsächlichen Veränderungen an Hardwarekomponenten (z. B. vorübergehendes Entfernen von Sicherheitselementen wie Diskettenschachtverriegelungen o. ä.) und an der Software (Betriebssystemnahe Software, Anwendungssoftware)

sowie

- über die Erhebung, Verarbeitung (Speicherung, Veränderung, Löschung, Sperrung, Übermittlung) und sonstige Nutzung von personenbezogenen Daten

zu verstehen.

1.2 Elemente einer Protokollierung sind:

- Art des Vorganges,
- Zeitpunkt der Aktivität bzw. des Ereignisses,
- Merkmale der Maßnahme (z. B. Eingabewerte),
- ausführende Person.

Aus den Protokollen muß sich mithin die Frage beantworten lassen: "Wer hat wann mit welchen Mitteln was veranlaßt bzw. worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: "Wer hatte von wann bis wann welche Zugriffsrechte?"

2. Rechtsgrundlagen

2.1 Nach § 9 Abs. 1 ThürDSG sind technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.
Die in § 9 Abs. 2 aufgeführten Regelungen erfordern jedoch zur Durchsetzung dieser “10 Gebote der Datenverarbeitung” eine kontrollfähige Organisation darüber, wer, was, wann und wie im Datenbestand eingesehen oder verändert hat.
In den Verwaltungsvorschriften zu § 9 ThürDSG werden deshalb beispielhaft Protokollierungen für die Speicherkontrolle, die Benutzerkontrolle, die Zugriffskontrolle und die Übermittlungskontrolle gefordert.

2.2 Bevor Art und Umfang von Protokollierungen festgelegt werden, haben die datenverarbeitenden Stellen zu ermitteln, welche gesetzlichen Regelungen für ihren Zuständigkeitsbereich welche Rahmenbedingungen definieren. Der Komplex "Protokollierung" stellt sich damit nicht als eine Maßnahme im Rahmen des Ermessens dar, sondern als eine Folge aus den jeweils gültigen gesetzlichen Bestimmungen.

3. Gegenstand der Protokollierung

3.1 Differenzierung zwischen der Administration und der Benutzung von IT-Systemen

3.1.1 Beim Betrieb von IT-Systemen sollte zwischen den Funktionen der Administration und der Benutzung unterschieden werden.

3.1.2 Als "Administration" sind die Maßnahmen zur Installation, Modifikation und Konfiguration von Hard- und Software einschließlich der Abarbeitung von Systemnachrichten zu verstehen. Es handelt sich hierbei im wesentlichen um Basisfunktionen, die die fortdauernde Benutzung des Systems überhaupt erst ermöglichen.

3.1.3 Unter "Benutzung" ist die Inanspruchnahme der vom IT-System bereitgestellten Ressourcen anzusehen. In der Praxis stellt sich dies als der Aufruf von Software dar, die entsprechend den in einem Benutzerprofil festgelegten Zugriffsrechten (in der Regel in einem Menü) zur Verfügung gestellt wird.

3.1.4 Die Protokollierung der Administrationsaktivitäten hat daher den Charakter einer Systemüberwachung, während die Protokollierung der Benutzeraktivitäten im wesentlichen der Verfahrensüberwachung dient.

3.2 Administration von IT-Systemen

Folgende Aktivitäten sind vollständig zu protokollieren:

3.2.1 Systemgenerierung und Modifikation von Systemparametern

Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.

3.2.2 Einrichten von Benutzern

Wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen, ist vollständig zu protokollieren, dies ergibt sich auch aus der Eingabekontrolle. Für diese Protokolle sollten längerfristige Aufbewahrungszeiträume vorgesehen werden, da sie Grundlage praktisch jeder Revisionsmaßnahme sind.

3.2.3 Verwaltung von Befugnistabellen

Im Rahmen der Protokollierung von Befugniszuweisungen kommt es insbesondere auch darauf an, aufzuzeichnen, wer die Anweisung zur Erteilung einer bestimmten Befugnis erteilt hat.

3.2.4 Einspielen und Änderung von Anwendungssoftware

Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.

3.2.5 Änderungen an der Dateiorganisation

Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der "Standard-Dateiverwaltungssysteme" ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu.

3.2.6 Durchführung von Back-up-, Restore- und sonstigen Datensicherungsmaßnahmen

Da derartige Maßnahmen mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in "Ausnahmesituationen" durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.

3.3 Benutzung von IT-Systemen

Folgende Aktivitäten sind in Abhängigkeit von der Sensibilität der Verfahren/Daten vollständig bzw. selektiv zu protokollieren:

3.3.1 Versuche unbefugten Einloggens und Überschreitung von Befugnissen

Geht man von einer wirksamen Authentifizierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller "auffälligen Abnormitäten" beim Einloggen und der Benutzung von Hard- und Softwarekomponenten eine zentrale Bedeutung zu. Benutzer in diesem Sinne ist auch der Systemadministrator.

3.3.2 Eingabe von Daten

Die sogenannte Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, daß Befugnisüberschreitungen anderweitig protokolliert werden, dürfte eine vollständige Protokollierung von Dateneingaben als Regelfall angesehen werden müssen.

3.3.3 Datenübermittlungen

Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, kann eine selektive Protokollierung als ausreichend angesehen werden. In diesem Zusammenhang ist auch die Anfertigung von Dateikopien, Hardcopies usw. relevant. Dabei ist zu beachten, daß der Benutzer die grundsätzliche Befugnis haben muß, derartige Datenübermittlungen zu veranlassen, andernfalls würde es sich um die Überschreitung von Befugnissen handeln (vgl. Tz. 3.3.1).

3.3.4 Benutzung von automatisierten Abrufverfahren

In der Regel dürfte eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich sein, um unbefugte Kenntnisnahmen im Rahmen der grundsätzlich eingeräumten Zugriffsrechte aufdecken zu können.

3.3.5 Löschung von Daten

Eine vollständige Protokollierung ist insbesondere erforderlich, wenn die Daten ausschließlich in automatisierten Dateien gespeichert sind. In Abhängigkeit vom Gegenstand der Datenverarbeitung ist eine Protokollierung der gelöschten Daten oder lediglich die Tatsache der Löschung angezeigt. Ersteres dürfte "kontraproduktiv" sein, wenn Löschungsansprüche der Betroffenen erfüllt werden.

3.3.6 Aufruf von Programmen

Dies kann erforderlich sein bei besonders "sensiblen" Programmen, die z. B. nur zu bestimmten Zeiten oder Anlässen benutzt werden dürfen. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

4. Personenbezug von Protokolldaten

Protokolle, die aus den unter Tz. 3 genannten Gründen erzeugt werden, stellen faktisch alle personenbezogene Dateien dar. In erster Linie besteht ein Personenbezug zu den "veranlassenden Personen oder Stellen" (vgl. Tz. 1.2). In vielen Fällen lassen Protokolle außerdem Rückschlüsse auf Daten von Betroffenen sowie auf das Verhalten der Beschäftigten zu. Die Protokolldaten dürfen nur für Kontrollzwecke verwendet werden (Zweckbindung). Nach § 2 Abs. 2 ThürDSG gelten für die Protokolldateien nur die §§ 6, 9, 20 Abs. 4 sowie in Verbindung damit § 34 Abs. 1 und die §§ 37 bis 40 ThürDSG.

5. Aufbewahrungsdauer für Protokolle

5.1 Die Aufbewahrungsdauer der Protokolle richtet sich, da es sich um personenbezogene Daten handelt, nach § 16 Abs. 1 ThürDSG. Maßstab ist mithin die "Erforderlichkeit zur Aufgabenerfüllung". Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht.

5.2 Eine exakte Bestimmung des Zeitraums der Erforderlichkeit für Protokolle, deren Auswertung zeitlich nicht konkretisiert ist (vgl. z. B. die Protokolle im Zusammenhang mit der Administration, Tz. 3.2), ist nicht möglich. Als Anhaltspunkte können dienen:

- die Wahrscheinlichkeit, daß Unregelmäßigkeiten (noch) offenbar werden können und

- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden.

5.3 Soweit Protokolle zum Zweck gezielter Kontrollen angefertigt werden (vgl. insbesondere Tz. 3.3.1 und 3.3.5), kommen kürzere Speicherungsfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle.

5.4 Eine Begrenzung der Speicherungsdauer von Protokolldaten kann auch dadurch erreicht werden, daß durch eine "Ringspeicherung" nur eine maximale Anzahl von Protokolldatensätzen für die Kontrolle vorgehalten wird.

6. Technische und organisatorische Rahmenbedingungen

Die Effektivität der Protokollierung und ihre Auswertung im Rahmen von Kontrollen hängt im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang sollten folgende Aspekte Berücksichtigung finden:

6.1 Es sollte ein Revisionskonzept erstellt werden, das die Zielrichtung der Protokolle und der Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert.

6.2 Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muß gewährleistet werden.

6.3 Das gleiche gilt für die Manipulationssicherheit der Einträge in Protokolldateien.

6.4 Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden.

6.5 Die Protokolle müssen so gestaltet sein, daß seitens der Revisoren eine effektive Überprüfung möglich ist.

6.6 Die Auswertungsmöglichkeiten sollten vorab mit den Revisoren abgestimmt und festgelegt sein.

6.7 Kontrollen sollten nach dem 4-Augen-Prinzip erfolgen.

6.8 Es sollte vorab definiert werden, welche Konsequenzen sich aus Verstößen ergeben, die durch die Kontrolle von Protokollen aufgedeckt werden.

6.9 Personalräte und Arbeitnehmervertreter(innen) sollten bei der Erarbeitung des Revisionskonzeptes und bei der Auswertung der Protokolle beteiligt werden.

Anlage 32

Empfehlungen zum Einsatz optischer Datenspeicherung

erstellt vom Arbeitskreis Technik
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
Mai 1995

Beim Einsatz der optischen Datenspeicherung ist zu unterscheiden zwischen Datenträgern, die nur einmal beschreibbar, aber beliebig oft lesbar sind (z. B. CD-ROM, WORM, MO als WORM) und anderen Datenträgern, die mehrfach beschreibbar und lesbar sind (z. B. MO).

Aufgrund der fehlenden Löschbarkeit von Daten bei den nur einmal beschreibbaren optischen Datenträgern und unter Berücksichtigung der Löschungs-, Sperrungs- und Berechtigungsvorschriften der Datenschutzgesetze des Bundes und der Länder ist nach folgenden Regeln zu verfahren:

1) Grundsätzlich sind wiederbeschreibbare optische Datenträger einzusetzen. Diese können wie Magnetplatten behandelt werden.

2) Es können optische Datenträger verwendet werden, die nur einmal beschreibbar sind, wenn die gesetzlichen Regelungen es zulassen, daß an Stelle der Berichtigung oder Löschung von Daten eine Sperrung tritt. Die Sperren sind dabei besonders zu kennzeichnen. Spätestens nach dem vollständigen Beschreiben des Datenträgers sind die Datenbestände durch Umkopieren auf einen neuen Datenträger zu bereinigen. Der Ursprungsdatenträger ist unverzüglich und vollständig zu löschen, wozu der Datenträger vernichtet werden muß.

3) Werden Daten gesichert oder langfristig archiviert, können ebenfalls optische Datenträger verwandt werden, die nur einmal beschreibbar sind. Dabei sollten möglichst nur Daten mit gleichen Löschungsfristen auf dem gleichen Datenträger abgelegt werden.

4) Sind Daten auf einem nur einmal beschreibbaren Datenträger zu löschen oder zu berichtigen, muß unter Verwendung des alten Datenträgers ein neuer Datenträger beschrieben werden, der die zu löschenden Daten nicht mehr enthält. Der ursprüngliche Datenträger ist unverzüglich und vollständig zu löschen, wozu der Datenträger vernichtet werden muß.

5) Das vollständige Löschen von Daten auf einem nur einmal beschreibbaren optischen Datenträger (d. h. dessen Vernichtung) ist mit angemessenen technisch-organisatorischen Maßnahmen unter Beachtung der DIN 32757 vorzunehmen. Dazu sind Verfahren wie Ätzen, Einschmelzen, Verbrennen, Zerkratzen oder Schreddern unter Berücksichtigung von Sicherheits- und Umweltverträglichkeitsaspekten anzuwenden.

Erläuterung der Abkürzungen:

- CD-ROM = **C**ompact-**D**isk-**R**ead-**O**nly-**M**emory
  (im Preßverfahren erstellter bzw. einmal beschreibbarer und mehrfach lesbarer optischer Datenträger im CD-Format)
- WORM = **W**rite **O**nce **R**ead **M**any
  (einmal beschreibbarer und mehrfach lesbarer optischer Datenträger)

- MO = **M**agnetic-**O**ptical
  (optischer Datenträger auf der Basis magnetischer Beschichtung),
  als
  - WORM-MO (nur einmal beschreibbar, mehrfach lesbar) und als
  - ROD-MO (**R**ewritable **O**ptical **D**isc, mehrfach wiederbeschreib- und lesbar)

Anlage 33

Rundschreiben Nr. 1

Umsetzung des § 8 Abs. 6 ThürDSG
Löschung / Vernichtung personenbezogener Daten im Auftrag

Aus gegebenem Anlaß möchte ich darauf hinweisen, daß nach § 8 Abs. 6 ThürDSG alle öffentlichen Stellen in Thüringen verpflichtet sind, den Landesbeauftragten für den Datenschutz jede Beauftragung nichtöffentlicher Stellen für die Verarbeitung oder Nutzung personenbezogener Daten zu unterrichten.
Soweit dies den Bereich der Datenverarbeitung (automatisierte Verfahren) umfaßt, ist davon auszugehen, daß mit der Meldung zum Datenschutzregister dieser Forderung Rechnung getragen wird.
Gemäß § 3 Abs. 3 Nr. 5 ThürDSG zählt zur Verarbeitung auch das Löschen (Vernichten) der Daten.

Bei einer Auftragserteilung gemäß § 8 ThürDSG sollte unbedingt eine Sofortkündigungsklausel bei Verstößen gegen den Datenschutz in die Verträge aufgenommen werden. Bei der sorgfältigen Auswahl der Auftragnehmer ist insbesondere darauf zu achten, daß dieser als Dienstleistungsunternehmen in dem entsprechenden Register der zuständigen Aufsichtsbehörde für den nichtöffentlichen Bereich gemäß § 38 Abs. 2 BDSG eingetragen ist.

Anlage 34

Rundschreiben Nr. 2

Meldungen zum Datenschutzregister

Beim Landesbeauftragten für den Datenschutz wird das Datenschutzregister geführt, in welches jedermann Einsicht nehmen kann.
Für die Abgabe der Meldung durch die öffentlichen Stellen des Freistaats Thüringen gilt die Thüringer Datenschutzregisterverordnung - ThürDSRegVO - vom 22.03.1994 und das vom LfD herausgegebene Formblatt im Thüringer Staatsanzeiger Nr. 20/1994, einschließlich dem mitveröffentlichten Merkblatt.

Aus gegebenen Anlaß weise ich nochmals auf die Regelungen des § 3 der ThürDSRegVO hin, wonach die speichernden öffentlichen Stellen über die für sie jeweils zuständige oberste Landesbehörde die Angaben melden. Die obersten Landesbehörden können zulassen, daß bestimmte Stellen die Dateien unmittelbar an den Landesbeauftragten melden. Sollten solche Festlegungen bestehen, bitte ich um eine Information.

Landkreise und kreisfreie Städte melden unmittelbar an den LfD und kreisangehörige Gemeinden und Städte über das Landratsamt an den LfD.

Diese Regelung dient nicht nur dazu, daß die Aufsichtsbehörden Kenntnis über die jeweiligen Meldungen erhalten, sondern auch dazu, daß Hinweise und Unterstützung bei der ordnungsgemäßen Übergabe der Meldung gegeben werden kann.
Bei auftretenden Fragen würde sich der LfD aus diesem Grund auch in erster Linie an die obersten Landesbehörden, Landratsämter und kreisfreien Städte wenden.

Ich bitte entsprechende Festlegungen im Verantwortungsbereich zu treffen.

Anlage 35

Rundschreiben Nr. 3

Empfehlungen zum Datenschutz bei Arbeitsplatzrechnern und anderen IT-Geräten

Öffentliche Stellen, die im Rahmen des ThürDSG personenbezogene Daten verarbeiten, haben die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Ausführung des ThürDSG, insbesondere der Datensicherungsmaßnahmen nach § 9 ThürDSG, zu treffen. Diese Verpflichtung zur Durchführung von Datensicherungsmaßnahmen gilt sowohl für die automatisierte als auch die nicht-automatisierte Datenverarbeitung.

1. Anwendungsbereich

Diese Empfehlungen zum Datenschutz gelten insbesondere für Arbeitsplatzrechner(Einzelplatzrechner/ Personal-Computer (PC)). Der Abschnitt 3 (Allgemeine Datenschutzmaßnahmen bei der Verarbeitung personenbezogener Daten) betrifft auch Anwendungen auf Zentralrechnern bzw. Mehrplatzsystemen.

2. Grundsätzliches

Geräteverzeichnis:
Alle eingesetzten Datenverarbeitungsanlagen und automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, sind in das Anlagen- und Verfahrensverzeichnis der Behörde (§ 10 Abs. 1 ThürDSG) aufzunehmen.

Freigabe von Programmen:
Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf der vorherigen schriftlichen Freigabe durch die Stelle, die den Datenschutz sicherzustellen hat (§ 34 Abs. 2 ThürDSG).
Zugangskontroll- und Zeiterfassungssysteme sind datenschutzrechtlich automatisierte Verfahren und bedürfen neben der Freigabe der Mitbestimmung des Personalrates gem. § 74 Abs. 3 ThürPersVG.

Systemverwalter:
Der für die zentrale Koordinierung verantwortliche Systemverwalter hat in datenschutzrechtlicher Hinsicht u. a. die Aufgabe,
- dafür zu sorgen, daß alle angeordneten oder ohne weiteres realisierbaren technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten eingeführt werden,
- den Verbleib der Geräteschlüssel nachzuweisen,
- Paßwörter sowie Zugangs- und Nutzungsberechtigungen zu vergeben,
- die Einhaltung der Fristen für den nichtautomatisierten Paßwortwechsel und
- die Einhaltung der Fristen für die Datensicherung zu überwachen.

Für Geräte, die ausschließlich zur Verarbeitung nichtpersonenbezogener Daten bestimmt sind, kann die Aufgabe des Systemverwalters dem jeweiligen PC-Bediener übertragen werden.

3. Allgemeine Datenschutzmaßnahmen bei der Verarbeitung personenbezogener Daten

Grundlagen:
Das Thüringer Datenschutzgesetz schützt alle personenbezogenen Daten, differenziert jedoch danach, ob die Daten in Akten, in einer manuellen Datei (Kartei) oder einer automatisierten Datei (§ 3 ThürDSG) gespeichert sind.

Auf PC werden grundsätzlich automatisierte Dateien im Sinne des § 3 Abs. 7 Nr. 1 ThürDSG betrieben. Nach dieser Vorschrift ist eine automatisierte Datei eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann.

Personenbezogen sind alle Einzelangaben, die sich auf die persönlichen oder sachlichen Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person beziehen (§ 3 Abs. 1 ThürDSG).

Auskunft:
Im PC gespeicherte personenbezogene Daten unterliegen der allgemeinen gesetzlichen Auskunftspflicht (§ 13 Abs. 1 ThürDSG).

Löschung personenbezogener Daten:
Personenbezogene Daten sind zu löschen, sobald sie nicht mehr benötigt werden (§ 16 ThürDSG).

4. Technische und organisatorische Datenschutzmaßnahmen

Technische Datenschutzmaßnahmen (§ 9 ThürDSG):
Die durch Hard- und Software selbst zur Verfügung gestellten technischen Datenschutzmaßnahmen, wie auch der Einsatz spezieller Datenschutz-Software bei sensiblen Daten u. ä., sind voll auszunutzen.
Zu berücksichtigen ist dabei, daß die Maßnahme im angemessenen Verhältnis zum angestrebten Schutzzweck ausgewählt werden sollte (Grundsatz der Verhältnismäßigkeit).

Paßwortverfahren:
Paßwörter dürfen nicht leicht zu erraten sein; nicht zu empfehlen sind daher Paßwörter, die ganz oder teilweise aus Angaben zur Organisationseinheit, aus dem Namen des Bedieners oder von dessen Familienangehörigen oder der Personalnummer bestehen.
Sie sollten mindestens fünf Zeichen umfassen, insbesondere sollte auf eine alphanumerische Gestaltung der Paßwörter (einschließlich Sonderzeichen) geachtet werden.
Paßwörter sind jedermann gegenüber geheimzuhalten; die Kontrolle der Einhaltung der Paßwortregeln durch den behördlichen Datenschutzbeauftragten wird dadurch nicht berührt.

Die Paßwörter sind spätestens alle drei Monate, möglichst automatisch gesteuert, zu wechseln. Ein Wechsel ist ferner erforderlich, wenn Grund zur Annahme besteht, daß das Paßwort einem anderen bekannt geworden ist. Die mehrmalige Verwendung derselben Paßwörter ist unzulässig.
Bei Netzbetrieb sollte das Paßwort des Systemverwalters, das nur ihm bekannt ist, für den Vertretungsfall an einem sicheren Ort in einem zumindestens verschlossenen Umschlag aufbewahrt werden.

Protokollierung der PC-Benutzung:
Soweit keine automatisierte Protokollierung erfolgen kann und mehrere Nutzer mit unterschiedlichen Arbeitsaufgaben auf einer Festplatte arbeiten, sollten folgende Angaben festgehalten werden:
- Name des Bedieners,
- Datum und Uhrzeit (Beginn und Ende der Benutzung),
- Art der Anwendung (z. B. Textverarbeitung, Statistik, Datenbank),
- Namen der benutzten personenbezogenen Dateien.

Arbeitsunterbrechungen:
Will sich der Bediener nach Inbetriebnahme des PC auch nur kurzzeitig an einen Ort begeben, von dem aus er nicht in der Lage ist, dessen Bedienung durch andere Personen festzustellen, empfiehlt es sich unter Berücksichtigung der vermutlichen Dauer der Abwesenheit sowie sonstiger Gegebenheiten
- die Anwendung bis zur untersten Paßwortebene zu verlassen,
- den Bildschirm dunkel zu schalten,
- das Gerät abzuschalten oder
- den PC-Raum zu verschließen.

Datenschutz bei Telefax:
Da Faxgeräte nicht immer unmittelbar beim Empfänger stehen, verständigen Sie sich vor der Absendung besonders sensibler Daten mit dem Adressaten über den konkreten Zeitpunkt der Übermittlung.

5. Belehrung der Bediensteten

Alle Bediensteten sollten mit dem Inhalt des Thüringer Datenschutzgesetzes u. a. datenschutzrechtlichen Bestimmungen (s. “Der TLfD informiert” Teil 1 und 2) vertraut gemacht werden.

Anlage 36

Rundschreiben Nr. 4

Zugangskontrolle beim Besuch einer obersten Landesbehörde

Für eine möglichst einheitliche Verfahrensweise bei der Handhabung der Zugangskontrolle unter Berücksichtigung sicherheitsrelevanter Besonderheiten schlage ich die Beachtung nachfolgender datenschutzrechtlicher Gesichtspunkte vor:

1. Der Aufwand für Maßnahmen zur Zugangskontrolle sollte stets in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.

2. Zur Sicherstellung des Datenschutzes (§ 34 Abs. 1 ThürDSG) ist der Zugang Unbefugter an Unterlagen mit personenbezogenen Daten zu verwehren.

3. Im Rahmen der Wahrnehmung des Hausrechts (§ 903 BGB) ist zur Sicherung des Dienstgebäudes die Erfassung des Besucherverkehrs zulässig. Dazu können gemäß § 19 Abs. 1 ThürDSG personenbezogene Daten erhoben werden. Der Umfang der Datenerhebung ist dabei auf das erforderliche Maß zu beschränken.
   Für die Aufklärung etwaiger Vorfälle, die im Zusammenhang mit dem Besucherverkehr stehen können (Zweck der Datenerhebung), erscheinen folgende Daten ausreichend:
   - Name, Vorname des Besuchers
   - Personalausweis- oder Paßnummer oder Dienststelle (bei Vorlage des Dienstausweises)
   - soweit eine Legitimation nicht erforderlich ist, genügt alternativ die Anschrift oder die Firma
   - Datum und Uhrzeiten für das Betreten und Verlassen des Dienstgebäudes
   - besuchte Stelle/Mitarbeiter

4. Die Notwendigkeit zur zeitweisen Abgabe von Personaldokumenten ist datenschutzrechtlich nicht unbedenklich, während gegen eine Übergabe bzw. sichtbare Anbringung von Besucherkarten keine Einwände bestehen.

5. Die Besucherlaufzettel sollten einen Hinweis (z. B. Rückseite) auf die ausschließliche Zweckbestimmung der Datenerhebung enthalten.

6. Die Besucherlaufzettel sind aufgrund ihrer nur kurzzeitigen Erforderlichkeit spätestens 14 Tage nach Datenerhebung zu vernichten. Auswertungen für andere Zwecke als zur Prüfung des Besucherverkehrs aus Anlaß eines besonderen Vorkommnisses sind unzulässig.

7. Soweit private Wachdienste den Besucherverkehr kontrollieren, sind die Bestimmungen des § 9 ThürDSG (Datenverarbeitung im Auftrag) zu beachten.

Ich bitte Sie aus o. g. Gründen um eine Prüfung Ihres Verfahrens bei der Zugangskontrolle unter sicherheitstechnischen und datenschutzrechtlichen Gesichtspunkten und empfehle den Ihnen nachgeordneten Bereich mit einzubeziehen, soweit dies nicht schon geschehen sein sollte.

Sachregister