THÜRINGER LANDTAG
3. Wahlperiode

Drucksache 3/2268
11.03.2002

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

durch die Präsidentin des Landtags

Vierter Bericht über die Tätigkeit des Thüringer Landesbeauftragten für den Datenschutz

Der Thüringer Landesbeauftragte für den Datenschutz hat den oben genannten Bericht mit folgendem Schreiben vom 11. März 2002 zugeleitet:

"Anliegend übergebe ich Ihnen meinen 4. Tätigkeitsbericht gemäß § 40 Abs. 1 des Thüringer Datenschutzgesetzes (ThürDSG) zur Kenntnisnahme und zur weiteren Verwendung.

Der Bericht wurde gemäß § 40 Abs. 4 ThürDSG abschließend im Beirat vorberaten."

Lieberknecht
Präsidentin des Landtags

Hinweis der Landtagsverwaltung:
Der Bericht wird nach Auskunft der Landesbeauftragten Ende März/Anfang April 2002 als Broschüre herausgegeben und dann auch an die Mitglieder des Landtags verteilt.
Ein Exemplar des Berichts wurde vorab jeder Fraktion zur Verfügung gestellt. Der Bericht kann auch in der Landtagsbibliothek und im Landtagsinformationssystem unter obiger Drucksachennummer eingesehen werden.
Gemäß § 52 Abs. 5 GO wurde der Bericht sowie die gemäß § 40 Abs. 2 des Thüringer Datenschutzgesetzes zu erwartende Stellungnahme der Landesregierung zum Bericht an den Innenausschuss überwiesen.

Druck: Thüringer Landtag, 12. März 2002

Vorwort

Der vorliegende 4. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz umfasst den Berichtszeitraum vom 1. Januar 2000 bis zum 31. Dezember 2001.

Er beinhaltet einen Überblick über aktuelle Themen und rechtliche Regelungen auf dem Gebiet des Datenschutzes und der Datensicherheit sowie wesentliche Feststellungen und Bewertungen aus der Kontroll- und Beratungstätigkeit einschließlich von Anregungen und Empfehlungen zu Verbesserungen des Datenschutzes. Über durchgeführte Kontrollen, die im Berichtszeitraum noch nicht abgeschlossen wurden, werde ich in meinem nächsten, 5. Tätigkeitsbericht, weiter berichten.

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

Dieser Bericht steht wie auch die vorangegangenen Tätigkeitsberichte im Internet unter www.datenschutz.thueringen.de zur Verfügung.

Erfurt, im Dezember 2001

Silvia Liebaug
Landesbeauftragte für den Datenschutz

4. Tätigkeitsbericht des TLfD
Berichtszeitraum vom 01.01.2000 bis 31.12.2001

Inhaltsverzeichnis
Abkürzungsverzeichnis

Anlagen

Entschließungen der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 14./15. März 2000 in Hannover

Entschließungen zwischen den Konferenzen 2000

Entschließungen der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 12./13. Oktober 2000 in Braunschweig

Entschließungen der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09. März 2001 in Düsseldorf

Entschließungen zwischen den Konferenzen 2001

Entschließungen der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. - 26. Oktober 2001 in Münster

Abkürzungsverzeichnis

Abkürz.	**Bedeutung**
3. VwVfÄndG	Drittes Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften
4. StVollzGÄndG	4. Gesetz zur Änderung des Strafvollzugsgesetzes
ABl.	Amtsblatt
ACCESS	Datenbanksystem von Microsoft
AG	Arbeitsgruppe
AK	Arbeitskreis
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
APC	Arbeitsplatz-Computer
Art.	Artikel
ATG	Aktionsforum Telematik im Gesundheitswesen
AuslG-VwV	Allgemeine Verwaltungsvorschrift zum Ausländergesetz
BAföG	Bundesausbildungsförderungsgesetz
BAT-O	Bundes-Angestelltentarif-Ost
BDO	Bundesdisziplinarordnung
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMBF	Bundesministerium für Bildung und Forschung
BMF	Bundesfinanzministerium
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMV-Ä	Bundesmantelverträge-Ärzte
BND	Bundesnachrichtendienst
BNotO	Bundesnotarordnung
BR-Drs.	Bundesratsdrucksache
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informations-

	technik
bspw.	beispielsweise
BStBl.	Bundessteuerblatt
BT	Bundestag
BVerfG	Bundesverfassungsgericht
BVerfSchG	Bundesverfassungsschutzgesetz
bzw.	beziehungsweise
CA	Certification Authority (Zertifizierungsdienste-anbieter)
CC	Common Criteria
CN	Corporate Network
DES	Data Encryption Standard (symmetrischer Verschlüsselungsalgorithmus)
DIN	Deutsches Institut für Normung
DNA-Analyse	Genetischer Fingerabdruck
DRG	Diagnosis Related Groups
DSB	Datenschutzbeauftragter/Datenschutzbeauftragte
DSRL	Datenschutzrichtlinie
DV	Datenverarbeitung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGG	Elektronischer Geschäftsverkehr-Gesetz
E-Government	Elektronische Verwaltung
ELSTER	Elektronische Steuererklärung
E-Mail	Elektronic-Mail (elektronische Post)
EMRK	Europäische Menschenrechtskonvention
ENFOPOL	Enforcement Police (polizeiliche Zusammenarbeit)
ERJuKOG	Gesetz über Elektronische Register und Justizkosten für Telekommunikation
EStG	Einkommenssteuergesetz
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EUROJUST	Gemeinsame Stelle zur justiziellen Zusammenarbeit
EUROPOL	Europäisches Polizeiamt
FAG	Fernmeldeanlagengesetz
FeV	Verordnung über die Zulassung von Personen

	zum Straßenverkehr (Fahrerlaubnisverordnung)
FISCUS	Förderales Integriertes Standardisiertes Computerunterstütztes Steuersystem
G 10 Gesetz	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel-10-Gesetz)
GBO	Grundbuchordnung
GBV	Grundbuchverfügung
GdB	Grad der Behinderung
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GO	Geschäftsordnung
GPS	Global Positioning System
GVBl.	Gesetz- und Verordnungsblatt
HeimG	Heimgesetz
i. d. R.	in der Regel
i. V. m.	in Verbindung mit
IABV	Integriertes Automatisches Besteuerungsverfahren
IFG	Informationsfreiheitsgesetz
IGLU	Internationale-Grundschul-Lese-Untersuchung
IMA-IT	Interministerieller Ausschuss für Informationstechnik
INPOL	Informationssystem der Polizei
InsO	Insolvenzordnung
IP	Internet Protokoll
IT	Informationstechnik
ITSEC	Information Technologie Security Evaluation Criteria
IuK	Informations- und Kommunikationstechnik
IuKDG	Informations- und Kommunikationsdienste-Gesetz
JMBl.	Justiz-Ministerialblatt
JuMiKo	Konferenz der Justizministerinnen und -minister
JVA	Justizvollzugsanstalt
KAN	Kriminalaktennachweis
Kfz	Kraftfahrzeug
KoopA-ADV	Kooperationsausschuss Automatisierte Datenver-

	arbeitung Bund, Länder, Kommunaler Bereich
KV	Kassenärztliche Vereinigung
LAN	Local Area Network
LfD	Landesbeauftragter für den Datenschutz
LfV	Landesamt für Verfassungsschutz
LKA	Landeskriminalamt
LVA	Landesversicherungsanstalt
MDK	Medizinischer Dienst der Krankenkasse
MDStV	Mediendienste-Staatsvertrag
MiStra	Anordnung über Mitteilungen in Strafsachen
o. ä.	oder ähnliches
o. g.	oben genannt
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
P3P	Platform for Privacy Preferences Projekt
PAG	Polizeiaufgabengesetz
PAuswG	Personalausweisgesetz
PC	Personal Computer
PD	Polizeidirektion
PISA	internationale Schülerleistungsstudie (Programme for International Students Assessment)
PKI	Public Key Infrastructure
PStG	Personenstandsgesetz
RA	Registration Authority (Registrierungsstellen)
RegTP	Regulierungsbehörde für Post und Telekommunikation
RiStBV	Richtlinie für das Straf- und Bußgeldverfahren
RNS oder RNA	Ribonukleinsäure
SAM	Strukturanpassungsmaßnahmen
SchwbG	Schwerbehindertengesetz
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SIJUS-Straf	Staatsanwaltschaftliches Informationssystem Geschäftsstellenautomation in Strafsachen bei Staatsanwaltschaften
SIS	Schengener Informationssystem

sog.	Sogenannte(n)
SSO	Single-Sign-On
StARoV	Staatliches Amt zur Regelung offener Vermögensfragen
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVÄG	Strafverfahrensänderungesetz
TB	Tätigkeitsbericht
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikationsdienstunternehmen-Datenschutzverordnung/Telekommunikations-Datenschutzverordnung
TESTA	Trans European Services für Telematics between Administrations
TFM	Thüringer Finanzministerium
ThürArchivG	Thüringer Archivgesetz
ThürBG	Thüringer Beamtengesetz
ThürBVVG	Thüringer Gesetz über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid
ThürDSG	Thüringer Datenschutzgesetz
ThürHortkBVO	Thüringer Hortkostenbeteiligungsverordnung
ThürKAG	Thüringer Kommunalabgabengesetz
ThürKHG	Thüringer Krankenhausgesetz
ThürKO	Thüringer Kommunalordnung
ThürMeldeG	Thüringer Meldegesetz
ThürPersVG	Thüringer Personalvertretungsgesetz
ThürPsychKG	Thüringer Gesetz zur Hilfe und Unterbringung psychisch Kranker
ThürSchulG	Thüringer Schulgesetz
ThürStAnz	Thüringer Staatsanzeiger
ThürZustVBezüge	Thüringer Verordnung über Zuständigkeiten für die Feststellung, Berechnung und Anordnung der Zahlung der Bezüge von Bediensteten
TIM	Thüringer Innenministerium
TJM	Thüringer Justizministerium
TJM	Thüringer Justizministerium
TK	Telekommunikation

TKG	Telekommunikationsgesetz
TKM	Thüringer Kultusministerium
TKÜV	Telekommunikationsüberwachungsverordnung
TLfD	Thüringer Landesbeauftragter für den Datenschutz
TLfV	Thüringer Landesamt für Verfassungsschutz
TLRZ	Thüringer Landesrechenzentrum
TLS	Thüringer Landesamt für Statistik
TLVwA	Thüringer Landesverwaltungsamt
TMSFG	Thüringer Ministerium für Soziales, Familie und Gesundheit
TMWAI	Thüringer Ministerium für Wirtschaft, Arbeit und Infrastruktur
TMWFK	Thüringer Ministerium für Wissenschaft, Forschung und Kunst
u. a.	unter anderem (und andere)
u. ä.	und ähnliches
UMTS	Universal Mobile Telecommunications System
Urt.	Urteil
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
WPflG	Wehrpflichtgesetz
WWW	World Wide Web
z. Z.	zur Zeit
z. B.	zum Beispiel
ZBS	Zentrale Bußgeldstelle
ZG	Zentrale Gehaltsstelle Thüringen
ZIV	Zentrum für Informationsverarbeitung

1. Vorbemerkung

1.1 Festveranstaltung - 10 Jahre Datenschutz in Thüringen

Der Freistaat Thüringen hat als erstes der neuen Bundesländer im Oktober 1991 sein Landesdatenschutzgesetz im Thüringer Landtag verabschiedet.
Anlässlich des 10 jährigen Jubiläums des Inkrafttreten des Thüringer Datenschutzgesetzes haben die Landtagspräsidentin, Frau Christine Lieberknecht, und die Landesbeauftragte für den Datenschutz zu einem Festakt in den Thüringer Landtag eingeladen. In ihren Grußworten hob die Landtagspräsidentin den Schutz der Persönlichkeitsrechte eines jeden Bürgers als eine der wesentlichsten Aufgaben des Rechtsstaates hervor.
Der Thüringer Innenminister betonte in seinem Redebeitrag, dass ein Jahrzehnt Datenschutz in Thüringen guten Grund biete, einen Rückblick und auch Ausblick in die Zukunft zu halten. Bezogen auf die Entstehungsgeschichte des Landesdatenschutzgesetzes erwähnte der Innenminister, dass Erfahrungen der alten Bundesländer, insbesondere der Nachbarländer Thüringens genutzt worden seien. Datenschutz sei mehr als eine technische Frage, er sei auch eine Frage des Menschenbildes. Im Hinblick auf die Novellierung des Thüringer Datenschutzgesetzes (ThürDSG) im September 2001 betonte der Innenminister, dass dies im Wesentlichen eine notwendige Anpassung an das Datenschutzrecht der Europäischen Union war.
Bei der Weiterentwicklung des Datenschutzrechts ist seiner Auffassung nach auch zukünftig das Verhältnismäßigkeitsprinzip zu beachten. Bei den erhöhten berechtigten Anforderungen an die Sicherheit darf es seiner Auffassung nach keinen Ausnahmezustand für den Datenschutz geben. Datenschutz, stellte er fest, ist kein Verwaltungshindernis, sondern Teil der Verwaltung. Bei einigen Forderungen für die Zukunft des Datenschutzrechts brachte er zum Ausdruck, dass es effektiver, verständlicher und vor allem übersichtlicher werden sollte.
Ein besonderer Höhepunkt der Veranstaltung war die Festrede von Herrn Prof. Dr. Dr. hc. Spiros Simitis. Prof. Simitis war 16 Jahre lang Datenschutzbeauftragter im Nachbarland Hessen und ist heute Hochschullehrer an der Universität Frankfurt am Main. Seit Ende der 80er Jahre ist er als Berater der Europäischen Kommission in Daten-

schutzfragen tätig und hat darüber hinaus die wichtige Aufgabe als Vorsitzender des Nationalen Ethikrates inne. In seiner Festrede ging Prof. Simitis auf die Wurzeln des ThürDSG ein. Er sieht in diesem Zusammenhang eine ostdeutsche und eine westdeutsche Wurzel.
In seinen Ausführungen zur ostdeutschen Wurzel schilderte er persönliche Erfahrungen der Wendezeit, als er damals in einem Anruf vom Bürgerkomitee gebeten wurde, nach Erfurt zu kommen. Damals ging es um die Stasi-Akten. Man wollte von ihm in seiner Funktion als Hessischer Datenschutzbeauftragter wissen, wie man mit diesen Akten umgehen soll. Prof. Simitis äußerte seine persönliche Überzeugung, dass bei einer Offenbarung der Akten zugleich der Schutz des Einzelnen zu gewährleisten und sein Entscheidungsrecht beim Umgang mit seinen Daten zu berücksichtigen sei. Für eine ostdeutsche Komponente des Datenschutzes in Thüringen sah er auch die Entscheidung an, den Datenschutz entsprechend seiner Bedeutung und der Erfahrungen der Vergangenheit, in die Verfassung aufzunehmen.
Bei der zweiten, der westdeutschen Wurzel des ThürDSG sprach Prof. Simitis die westdeutschen Landesdatenschutzgesetze an, die bei den ostdeutschen Gesetzen als Vorbild zugrunde lagen.
Nachdem Prof. Simitis auch die Novellierung des ThürDSG in Anpassung an die EU-Datenschutzrichtlinie ansprach, wies er auch auf die 2. Phase, die eigentliche Modernisierungsphase des Datenschutzrechts hin. Er regte an, dass bei der nächsten Novellierung des ThürDSG besonderes Augenmerk auf eine völlige Unabhängigkeit der Kontrollbehörde im Hinblick auf die bisherige Beibehaltung der Aufsichtsbehörden für den nicht öffentlichen Bereich gerichtet werden sollte. Ein weiterer Punkt, auf den das Augenmerk seiner Meinung nach gerichtet werden sollte, ist das Widerspruchsrecht der Betroffenen bei bestimmten Akten gegen Kontrollen des Datenschutzbeauftragten.
Unter den aktuellen Datenschutzthemen ging Prof. Simitis auch auf die vorgesehenen Sicherheitsmaßnahmen in den Gesetzentwürfen des Bundesinnenministeriums ein und machte die Notwendigkeit der Normenklarheit der Regelungen deutlich. Dazu bedarf es präziser Aussagen, warum was geändert werden soll. Bei Situationen, in denen es Datenverarbeitung geben muss, die das informationelle Selbstbestimmungsrecht einschränken, muss dies genau definiert werden. Dies fehlt jedoch teilweise bei den derzeitigen Entwürfen.

Abschließend vertrat Prof. Simitis die Auffassung, dass Maßnahmen in einer Europäischen Union, die eine gemeinsame Innen- und Sicherheitspolitik verfolgt, international und europäisch angelegt sein müssen, wenn sie greifen sollen.

1.2 Schwerpunkte des Datenschutzes

Im Berichtszeitraum wurden neben Kontroll- und Informationsbesuchen in den öffentlichen Stellen des Freistaats Thüringen auch zahlreiche Beratungsgespräche zu Fragen des Datenschutzes und der Datensicherheit durchgeführt.
Einen Schwerpunkt der Arbeit bildeten auch die Anfragen der Bürger. In vielen Fällen konnten Hinweise im Zusammenhang mit der Wahrnehmung des Grundrechts auf Datenschutz gegeben werden. Es ist festzustellen, dass ein zunehmendes Interesse der Bürger an der Aufklärung zu Schutzmöglichkeiten und über Datensicherheit beim Umgang mit Computern sowie beim Surfen im Internet besteht.
Aufgrund festgestellter Mängel beim Umgang mit personenbezogenen Daten wurden im Berichtszeitraum insgesamt 13 Beanstandungen ausgesprochen.
Da die Fragen und Probleme zur IT-Sicherheit zunehmen, wurde bereits seit längerem eine weitere Stelle für das Referat Technik beantragt. Diese wurde bislang nicht bewilligt. Ich halte die Stellenaufstockung nach wie vor für dringend erforderlich, um den Kontroll- und Beratungsauftrag des TLfD angemessen wahrnehmen zu können.

2. Europäischer Datenschutz

2.1 Grundrecht auf Datenschutz in der Charta der Grundrechte der Europäischen Union

Der von dem hierzu eingesetzten Gremium (Konvent) unter Vorsitz des ehemaligen Bundespräsidenten Roman Herzog erarbeitete Entwurf einer Charta der Grundrechte der Europäischen Union ist vom Europäischen Parlament, Rat und Kommission gemeinsam am 7. Dezember 2000 in Nizza feierlich proklamiert worden.
Entsprechend der Forderungen der DSB des Bundes und der Länder (3. TB, 2.2) hat erfreulicherweise das Grundrecht auf Datenschutz in

der Charta der Grundrechte der Europäischen Union Aufnahme gefunden.
Nach Artikel 8 der Charta hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.
Nach den vom Präsidium des Konvents in eigener Verantwortung formulierten und rechtlich unverbindlichen Erläuterungen stützt sich dieser Artikel auf Artikel 286 des Vertrags zur Gründung der Europäischen Gemeinschaft und auf die EU-Datenschutzrichtlinie sowie auf Artikel 8 EMRK und das Übereinkommen des Europarates vom 28.01.1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, das von allen Mitgliedsstaaten ratifiziert wurde. Das Recht auf Schutz der personenbezogenen Daten wird nach Maßgabe der genannten Richtlinien ausgeübt und kann gemäß den Bedingungen nach Artikel 52 der Charta eingeschränkt werden. Zu der für die Kontrolle der Einhaltung dieser Vorschrift bestimmten unabhängigen Stelle ist im Konvent klargestellt worden, dass damit die jeweiligen nationalen DSB gemeint sind.

Damit trägt die Charta der herausgehobenen Bedeutung des Datenschutzes im „Kommunikationszeitalter“ Rechnung. Zwar wird die feierliche Erklärung von Nizza zunächst rechtlich unverbindlich bleiben; im Europäischen Rat wird zu entscheiden sein, ob und wann die Charta in die Verträge aufgenommen und damit verbindlich werden soll.

2.2 EUROJUST

Bereits 1999 hat der europäische Rat in Tampere beschlossen, dass zur Verstärkung der Bekämpfung der schweren organisierten Kriminalität eine Stelle (EUROJUST) mit der Aufgabe eingerichtet werden soll, eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften zu erleichtern und die strafrechtlichen Ermittlungen in Fällen mit Bezug zu organisierter Kriminalität zu unterstützen sowie mit

dem europäischen justiziellen Netz und, soweit dies mit der Aufgabenwahrnehmung von EUROJUST und für die Erreichung seiner Ziele von Belang, mit Europol eng zusammenzuarbeiten. Im Vorgriff auf EUROJUST ist bereits eine vorläufige Stelle zur justiziellen Zusammenarbeit eingerichtet worden, die ihre Arbeit am 1. März 2001 aufgenommen hat.
EUROJUST setzt sich aus je einem Staatsanwalt, Richter oder Polizeibeamten pro Mitgliedsstaat zusammen, dem eine weitere Person zur Unterstützung und Stellvertretung zugeordnet werden kann. Der Zuständigkeitsbereich soll sich auf die Kriminalitätsformen und Straftaten nach Art. 2 des EUROPOL-Übereinkommens (organisierte Kriminalität), Computerkriminalität, Betrug und Korruption, Straftaten gegen die finanziellen Interessen der Europäischen Gemeinschaften, Geldwäsche und Umweltkriminalität erstrecken. Auf Ersuchen einer Ermittlungsbehörde um Unterstützung kann EUROJUST aber auch bei anderen Straftaten tätig werden. Die nationalen Mitglieder unterliegen dabei dem Recht des Herkunftsstaates. Der Informationsaustausch zwischen EUROJUST und den Ermittlungsbehörden der Mitgliedsstaaten findet über das jeweilige nationale Mitglied statt. In der Entschließung der 62. Konferenz der DSB des Bundes und der Länder „EUROJUST – Vorläufer einer künftigen europäischen Staatsanwaltschaft?“ (Anlage 30) haben die DSB des Bundes und der Länder die datenschutzrechtlichen Anforderungen formuliert. Diese betreffen vor allem den Informationsaustausch mit Partnern, die Verarbeitung personenbezogener Daten, das Auskunftsrecht der Betroffenen, Speicherungsfristen, Datensicherheit sowie einer unabhängigen gemeinsamen Kontrollinstanz.
Der Beschluss des Rats der europäischen Union soll bis Ende 2001 verabschiedet werden. Danach bedarf es der Umsetzung in den Mitgliedsstaaten.

3. Datenschutz im Parlament

3.1 Datenschutzregelungen für den Thüringer Landtag

Im 2. TB (3.) habe ich bereits auf die Thematik von Datenschutzregelungen für Parlamente sowie Inhalt und Umfang einer rechtlichen Grundlage hingewiesen. Die von Seiten der DSB des Bundes und der Länder einberufene Arbeitsgruppe hatte dazu inhaltliche und rechtli-

che Fragen ausgearbeitet, die bei der Diskussion eine Rolle spielten. Ich habe dabei bspw. die Auffassung vertreten, dass unter Berücksichtigung der Besonderheiten des jeweiligen Landesrechts einiges dafür spricht, parlamentsspezifisches Datenschutzrecht durch ein formelles Gesetz zu regeln.
Im Zuge der Novellierung des ThürDSG im September 2001 wurde im § 2 Abs. 5 zum Anwendungsbereich des ThürDSG festgelegt, dass die Bestimmungen dieses Gesetzes für den Landtag nur gelten, soweit er in **Verwaltungsangelegenheiten** tätig wird. Verwaltungsangelegenheiten sind insbesondere

1. die wirtschaftlichen Angelegenheiten des Landtags nach Artikel 57 Abs. 4 Satz 1 der Verfassung des Freistaats Thüringen,
2. die Personalverwaltung des Landtags,
3. die Ausübung des Hausrechts und der Ordnungs- und Polizeigewalt nach Artikel 57 Abs. 3 Satz 2 der Verfassung des Freistaats Thüringen und
4. die Ausführung der Gesetze, soweit diese dem Präsidenten des Landtags zugewiesen ist und nicht in unmittelbarem Zusammenhang mit der Wahrnehmung parlamentarischer Aufgaben steht.

Für die Verarbeitung und Nutzung personenbezogener Daten bei der Wahrnehmung **parlamentarischer Aufgaben** durch den Landtag einschließlich der Fraktionen wurden nunmehr erstmalig die Bestimmungen des ThürDSG, unter Berücksichtigung der verfassungsrechtlichen Stellung des Landtags, für entsprechend anwendbar erklärt. Soweit der Landtag in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeitet oder nutzt, wird allerdings die Kontrolle der Einhaltung des Datenschutzes nicht durch den TLfD, sondern durch den Ältestenrat des Landtags wahrgenommen.

3.2 Regelungen in der Geschäftsordnung des Thüringer Landtags zum Datenschutzbeauftragten

In meinem 3. TB (3.3) habe ich angeregt, im § 112 der Geschäftsordnung des Thüringer Landtags eine Regelung aufzunehmen, die der Thüringer Landesbeauftragten für den Datenschutz das Recht einräumt, an Sitzungen der Ausschüsse teilnehmen zu können, wenn datenschutzrechtliche Themen auf der Tagesordnung stehen.

Im Rahmen der Debatte zur Änderung der Geschäftsordnung habe ich mein Anliegen auch an den Justizausschuss herangetragen und dargelegt, dass aus meiner Sicht der Datenschutzbeauftragte gemäß § 40 Abs. 3 Satz 1 ThürDSG nicht nur das Recht, sondern auch die Pflicht hat, den Landtag und seine Organe bei datenschutzrechtlichen Fragen unterstützend zu beraten. Nach § 40 Abs. 6 ThürDSG kann er sich jederzeit an den Landtag wenden. Auch in der Verfassung des Freistaats Thüringen wurde in Artikel 69 bestimmt, dass zur Unterstützung bei der Ausübung der parlamentarischen Kontrolle ein Datenschutzbeauftragter beim Landtag berufen wird.
In der im Berichtszeitraum beschlossenen neuen Geschäftsordnung wurde meinem Anliegen entsprechend nunmehr bestimmt, dass der Datenschutzbeauftragte Zutritt zu allen nicht öffentlichen Sitzungen des Landtags hat. Der Datenschutzbeauftragte kann weiter an den Sitzungen der Ausschüsse des Landtags teilnehmen, soweit es sich nicht um Immunitätsangelegenheiten, nicht-öffentliche Sitzungen von Untersuchungsausschüssen oder vertrauliche Sitzungen handelt. Mit der Mehrheit von zwei Dritteln der Ausschussmitglieder kann der Datenschutzbeauftragte von der Teilnahme an nicht öffentlichen Sitzungen ausgeschlossen werden.

4. Medien/Telekommunikation

4.1 Sicherheit freier Telekommunikation

Schon vor diesem Berichtszeitraum sind immer neue Eingriffsbefugnisse zur staatlichen Kontrolle der Telekommunikation geschaffen worden. Vorschriften, die früher nur das Abhören von Telefonaten betrafen, sollten nunmehr auch für E-Mails und den Abruf von Informationen aus dem Internet gelten. Die DSB des Bundes und der Länder haben daher auf der 59. Konferenz im März 2000 eine Entschließung „Für eine freie Telekommunikation in einer freien Gesellschaft“ gefasst (Anlage 5).
Als Gründe für die Zunahme des Umfangs und der Intensität der Eingriffe in das von Artikel 10 GG geschützte Fernmeldegeheimnis wurde die erhebliche Zunahme der Telekommunikationsvorgänge, der stark angestiegene Umfang und die wesentlich verbesserte Aussagequalität der Daten gesehen. Hinzu kamen die erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten sowie die Entwick-

lung des Internets zum Massenkommunikationsmittel, aber auch die schwer durchschaubare Rechtslage durch die Zersplitterung der Regelungen in einer Vielzahl von Gesetzen. Vor dem Hintergrund eines bereits 1996 erarbeiteten Positionspapiers haben die DSB daher gefordert, die Geltung des Fernmeldegeheimnisses auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen. Eine Datenvorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung von eventueller, noch gar nicht absehbarer zukünftiger Straftaten wurde abgelehnt. Insbesondere wird weiterhin eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben für erforderlich angesehen.

4.2 Telekommunikationsüberwachungsverordnung (TKÜV)

Nach §§ 100a, 100b StPO und anderen Rechtsvorschriften hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die Aufbewahrung und Aufzeichnung der Telekommunikation zu ermöglichen. Die Einzelheiten ergeben sich aus § 88 Abs. 1 TKG, wonach jeder Betreiber einer Telekommunikationsanlage verpflichtet ist, die technischen Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation zu gestalten und vorzuhalten sowie auf einer hierauf beruhenden Rechtsverordnung zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen. Die Bundesregierung hat am 24.10.2001 diese Rechtsverordnung TKÜV beschlossen, die am 29.01.2002 in Kraft getreten ist. Einer der Vorentwürfe gab den DSB des Bundes und der Länder Veranlassung, im Rahmen einer Entschließung (Anlage 21) Kritik daran zu äußern, dass nach dem seinerzeit diskutierten Entwurf gegebenenfalls auch die Internetnutzung über die TKÜV erfassbar war. Die TKÜV begrenzt nunmehr den Kreis derjenigen, die Vorkehrungen für die Umsetzung der Überwachungsmaßnahmen vorzusehen haben, sodass Nebenstellenanlagen, unternehmensinterne Telekommunikationsanlagen und Corporate Networks von der Vorhaltung entsprechender technischer Einrichtungen und organisatorischer Vorkehrungen freigestellt sind. Wichtige Bedeutung wird die nach § 11 zu erstellende technische Richtlinie zur Umsetzung der TKÜV in der Praxis erhalten. Vorgesehen ist

auch, dass zur Umsetzung erstmals vorgeschriebener technischer Einrichtungen längere Übergangsfristen gelten sollen.

4.3 Teledienstedatenschutzgesetz (TDDSG) / Teledienstegesetz (TDG)

Im Berichtszeitraum wurde sowohl das TDDSG als auch das TDG geändert. Dies geschah in Umsetzung der Richtlinie 2000/31/EG des Europäischen Parlamentes und des Rates vom 08. Juni 2000 über den Elektronischen Geschäftsverkehr (ABl. EG Nr. l 178/1 vom 17. Juli 2000) durch das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz – EGG) vom 14.12.2001. Es dient dazu, die Harmonisierung der geltenden innerstaatlichen Regelungen für Dienste der Informationsgesellschaft und die Sicherstellung des freien Dienstleistungsverkehrs in diesem Bereich herbeizuführen. Das TDDSG erhält nunmehr eine Klarstellung, wonach die im Dienst- und Arbeitsverhältnis sowie in Unternehmen und öffentlichen Stellen der Steuerung von Arbeits- und Geschäftsprozessen erfolgenden Teledienste nicht von der Regelung des TDDSG erfasst werden. Neu aufgenommen wurden Regelungen, wonach der Diensteanbieter nach Maßgabe der hierfür geltenden Bestimmungen sowohl zu Bestandsdaten als auch zu Abrechnungsdaten Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung erteilen kann. Die DSB des Bundes und der Länder hatten sich in einer Entschließung (Anlage 18) dagegen gewandt, dass Bestands- und Nutzungsdaten u. a. auch zur Verfolgung von Ordnungswidrigkeiten übermittelt werden und Anbieter zur Speicherung von Nutzungsdaten auf Vorrat für eine mögliche spätere Strafverfolgung verpflichtet werden sollten. Sie hatten darauf hingewiesen, dass durch diese pauschale Registrierung tief in das Persönlichkeitsrecht eingegriffen werde.
Klarer gefasst werden die Pflichten der Diensteanbieter; vereinfacht werden die Voraussetzungen der Erteilung der elektronischen Einwilligung, zu denen jetzt auch eine Regelung gehört, wonach die Auskunft über die zu einer Person oder deren Pseudonym gespeicherten Daten auf Verlangen des Nutzers nunmehr auch elektronisch erteilt werden kann.
Im TDG wird vom Geltungsbereich nun ausdrücklich der Bereich der Besteuerung ausgenommen. Die Begriffsbestimmungen werden in

§ 3 präzisiert und ergänzt. Durch die Neufassung werden auch in der Bundesrepublik Deutschland niedergelassene Diensteanbieter vom Geltungsbereich erfasst, wenn die Teledienste in einem anderen Staat innerhalb der EG geschäftsmäßig angeboten oder erbracht werden, wobei man davon ausgeht, dass der freie Dienstleistungsverkehr von Telediensten nicht eingeschränkt werden soll. Das Gesetz sieht dabei jedoch zahlreiche Ausnahmen vor. Der Kreis der Angaben, zu deren Information oder Bereithaltung die Diensteanbieter verpflichtet werden, wird insgesamt erweitert. Bei kommerzieller Kommunikation werden die Diensteanbieter zudem verpflichtet, diese klar und als solche erkennbar zu machen und auch natürliche und juristische Personen, in deren Auftrag kommerzielle Kommunikationen erfolgen, müssen eindeutig identifizierbar sein. Im Bereich der Verantwortlichkeit der Diensteanbieter für eigene und fremde Informationen sowie für solche, zu denen der Zugang vermittelt wird, präzisiert das Gesetz die bisher bestehende Verantwortlichkeit.

4.4 Telekommunikations-Datenschutzverordnung (TDSV)

Am 21.12.2000 trat die TDSV (BGBl. I, S. 1740 ff) in Kraft, die den Schutz personenbezogener Daten der an der Telekommunikation Beteiligten bei der Verarbeitung durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken, regelt. Bisher galt für Diensteanbieter, dass sie Verbindungsdaten zu Abrechnungszwecken bis zu 80 Tagen speichern konnten. Nunmehr ist diese Frist nach § 7 Abs. 3 TDSV auf höchstens 6 Monate nach Versendung der Rechnung erweitert worden. § 3 TDSV normiert, dass Diensteanbieter personenbezogene Daten der an der Telekommunikation Beteiligten nur erheben, verarbeiten und nutzen dürfen, soweit dies die TDSV erlaubt oder eine Einwilligung nach den Vorschriften des BDSG vorliegt. Zu begrüßen ist die klare Regelung zur Einwilligung im elektronischen Verfahren nach § 4 TDSV, die auch das Recht der Beteiligten klarstellt, die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen zu können. § 9 TDSV ermächtigt den Diensteanbieter, zur Eingrenzung und Beseitigung von technischen Fehlern sowie zur Missbrauchsbekämpfung Bestands- und Verbindungsdaten zu erheben, zu verarbeiten und zu nutzen. Die Verbindungsdaten dürfen hierbei dergestalt

genutzt werden, dass aus dem Gesamtbestand aller Verbindungsdaten, die nicht älter als 6 Monate sind, die Daten derjenigen Verbindungen ermittelt werden, für die tatsächliche Anhaltspunkte über den Verdacht einer rechtswidrigen Inanspruchnahme von Telekommunikationsdiensten begründen. Neu ist auch, dass bei Einrichtungen, die eine anonyme telefonische Beratung gewährleisten, die Regulierungsbehörde für Telekommunikation und Post die Inhaber dieser Anschlüsse in einer Liste aufnimmt und für Diensteanbieter die Verpflichtung besteht, den Inhalt der Liste einem Abrechnungsverfahren zugrunde zu legen, sodass bei Einzelverbindungsnachweisen Verbindungen zu diesen Anschlüssen nicht mehr erkennbar sind.

4.5 Sechster Rundfunkänderungsstaatsvertrag

Mit dem am 20.12.2001 unterzeichneten Sechsten Rundfunkänderungsstaatsvertrag wird unter anderem auch der Mediendienstestaatsvertrag (MDStV) geändert. Die wesentlichen Änderungen beziehen sich auf die Umsetzung der Richtlinie 2000/31/EG des Europäischen Parlamentes und des Rates vom 08. Juni 2000, die zu den Änderungen im TDG und TDDSG geführt haben. Der MDStV übernimmt wortgleich die neugefassten Begriffsbestimmungen sowie die Regelungen zur Informationspflicht und der Verantwortlichkeit des TDG. Auch bezieht er ausdrücklich in der Bundesrepublik Deutschland niedergelassene Diensteanbieter und ihre Mediendienste in den Geltungsbereich ein, wenn die Mediendienste in einem anderen Staat innerhalb des Geltungsbereichs der Richtlinie geschäftsmäßig angeboten oder erbracht werden. Darüber hinaus werden auch die Vorschriften des TDDSG in den MDStV aufgenommen, sodass der Diensteanbieter nun auch nach Maßgabe der hierfür geltenden Bestimmungen Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung erteilen darf.

4.6 Neue Medienordnung

Im Medienbereich ist zunehmend festzustellen, dass die herkömmliche Trennung zwischen Rundfunk, Mediendiensten und Telekommunikation mit den hier bestehenden unterschiedlichen Zuständigkeiten zwischen Bund und Ländern zu Problemen führt, die es angezeigt erscheinen lassen, über eine Neuverteilung der Kompetenzen nach-

zudenken. Gegenwärtig werden hierzu zwischen Bund und Ländern Gespräche geführt, die noch nicht abgeschlossen sind. Die DSB des Bundes und der Länder haben in einer Entschließung zur „Neuen Medienordnung“ (Anlage 26) deutlich gemacht, dass der Schutz der Privatsphäre, der personenbezogenen Daten, der Meinungsfreiheit und der Vertraulichkeit der Kommunikation auch in einer neuen Medienordnung durchgängig gewährleistet bleiben muss und der Grad der Vertraulichkeit nicht davon abhängig sein kann, welchen der vorbezeichneten Medien der Kommunikationsvorgang zugeordnet ist. Sie haben die Forderung erhoben, das Fernmeldegeheimnis nach Art. 10 GG (Art. 7 VerfThür) zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis zu entwickeln und es gesetzlich abzusichern. Dabei wurde auch betont, dass die sehr komplizierten Rechtsvorschriften nicht nur inhaltlich angeglichen, sondern auch klarer strukturiert und verständlicher gestaltet werden sollten.

4.7 Datenschutz im Pressebereich

In Umsetzung der EU-Datenschutzrichtlinie und aufgrund der Novellierung von § 41 BDSG ist eine Verbesserung des Datenschutzes im Pressebereich zu gewährleisten. Der Deutsche Presserat hat zwischenzeitlich allgemeine Datenschutzleitlinien in den Pressekodex aufgenommen, in denen Regeln zur Richtigstellung falscher Berichterstattung sowie deren Dokumentation, zur Auskunft über die der Berichterstattung zugrunde liegenden personenbezogenen Daten und zur Löschung und Archivierung personenbezogener Daten sowie zum Umfang zulässiger Datenübermittlungen getroffen sind. Dieser neue „Pressekodex“ verlangt vom Presserat, dass er im Rahmen der freiwilligen publizistischen Selbstkontrolle Beschwerden über die Erhebung, Speicherung und Veröffentlichung von personenbezogenen Daten zu bearbeiten hat. In diesem Zusammenhang wurde ein Beschwerdeausschuss beim Presserat eingerichtet. Die Grundsätze stellen eine Richtlinie für die Redaktionen dar, sind aber nicht gesetzlich festgeschrieben.
Redaktionen sollen im Rahmen der freiwilligen publizistischen Selbstkontrolle von sich aus gespeicherte falsche und unzulässig erhobene Daten über Personen korrigieren und sperren, um die Gefahr von Fehlern bei Veröffentlichungen zu vermeiden. Allgemeine Datenschutzleitlinien im Pressekodex betreffen weiter Regelungen

zur Auskunft, zur Löschung und Archivierung personenbezogener Daten sowie zum Umfang zulässiger Datenübermittlungen.
Da nicht alle Verlage Mitglieder in den Organisationen sind, die Mitglieder im Trägerverein des Deutschen Presserates sind, kann für diese Verlage das vorgesehene Selbstregulierungsverfahren keine Anwendung finden. § 41 Abs. 1 BDSG verpflichtet die Länder in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.
In Thüringen ist vorgesehen, das Thüringer Pressegesetz um eine entsprechende Vorschrift zu ergänzen. Der mir hierzu zur Stellungnahme zugeleitete Gesetzentwurf begegnet aus meiner Sicht keinen Bedenken.

4.8 Videoüberwachung

Im Berichtszeitraum geriet der Einsatz von Videotechnik und deren Datenschutzaspekt zunehmend ins Blickfeld der öffentlichen Diskussion. War in der Vergangenheit eher zu beobachten, dass sich im privaten Bereich Tankstellen, Banken und Kaufhäuser des Einsatzes der Videotechnik bedienten, um vermeintliche Betrüger oder Ladendiebe ausfindig zu machen, ist nunmehr festzustellen, dass auch im öffentlich zugänglichen Bereich durch öffentliche Stellen zunehmend diese moderne Technik eingesetzt wird. Das Problem beim Einsatz dieser neuen Technik liegt darin, dass völlig unverdächtige Bürger in ihren individuellen Verhaltensweisen von einer Videoüberwachung erfasst werden können. Der Betroffene kann oftmals nicht erkennen, ob er überhaupt beobachtet wird, ob die Beobachtungen gerade aufgezeichnet und für welche Zwecke diese Aufzeichnungen unter Umständen verwendet werden, zumal immer kleinere Kameras, die versteckt installiert werden können, auf den Markt kommen. Nicht abgeschätzt werden kann zudem, welche Möglichkeiten der modernen Technik im Rahmen der Bearbeitung von Videoaufzeichnungen bestehen. Die DSB des Bundes und der Länder haben sich der Thematik zu einem frühen Zeitpunkt in einem eigenen Arbeitskreis ange-

nommen. Es ging darum, aufzuzeigen, in welchen Fällen Videoüberwachung als datenschutzrechtlich zulässig angesehen werden konnte. In einer Entschließung (Anlage 6) haben sie auf die Gefahr hingewiesen, dass der zunehmende Einsatz der Videotechnik zu einer Überwachungsinfrastruktur führen kann. Sie sind der Auffassung, dass es eine strenge Zweckbindung und eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Dateien zu bestimmten Personen geben muss. Dass an Kriminalitätsschwerpunkten sowie für Übersichtsaufnahmen zur Verkehrslenkung und bei Gefahrenlagen zum Schutz öffentlicher Einrichtungen ein Einsatz der Videotechnik in Betracht kommen kann, haben die DSB des Bundes und der Länder für möglich erachtet. Auch im Rahmen des Hausrechts kann diese Technik aus ihrer Sicht eingesetzt werden, wenn der grundsätzlich unbeobachtete Besuch öffentlicher Gebäude nicht unverhältnismäßig eingeschränkt wird und die Videoüberwachung durch entsprechende Hinweise erkennbar gemacht ist.
In der Praxis ist festzustellen, dass Dienststellen zunehmend dazu übergehen, im Rahmen des Hausrechts Videotechnik zur Zugangskontrolle einzusetzen. Ich habe mir hierzu die Verfahrensweise bei der Landtagsverwaltung angesehen. Die Landtagsverwaltung hat durch Hinweisschilder, wie dies auch seitens der DSB für sinnvoll erachtet wird, auf die Videoüberwachung hingewiesen. Mängel habe ich nicht festgestellt. Auf Bundesebene hat der Bundesgesetzgeber mit der Novelle des BDSG in § 6b BDSG nunmehr Regelungen getroffen, die den Intentionen der DSB entsprechen. Im Rahmen der Novelle zum ThürDSG (5.1.1) hatte ich eine der Bundesregelung vergleichbare Norm vorgeschlagen. Eine Aufnahme des Vorschlags im Gesetz erfolgte nicht.

5. Innenverwaltung - Kommunales - Sparkassen

5.1 Innenverwaltung

5.1.1 Novellierung des Thüringer Datenschutzgesetzes (ThürDSG)

In meinem 3. TB (2.1) habe ich darauf verwiesen, dass die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz

natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bereits bis Oktober 1998 in nationales Recht umzusetzen war. Im Hinblick darauf, war eine Anpassung der Regelungen sowohl im BDSG als auch im ThürDSG überfällig.
Im Mai 2001 trat schließlich die Novelle des BDSG in Kraft (BGBl. I, S. 904). Die Änderungen zum ThürDSG, die der Thüringer Landtag am 06. September 2001 beschlossen hat, sind am 27. September 2001 in Kraft getreten (GVBl. S. 276). Die Änderungen des ThürDSG bezogen sich im Wesentlichen auf:

- die Einführung einer Regelung über belastende automatisierte Einzelentscheidungen,
- die Ergänzung der Rechte der Betroffenen im Hinblick auf die automatisierte Verarbeitung der Daten bei mobilen Speichermedien,
- die gesetzliche Normierung des behördeninternen DSB,
- die Einführung einer Regelung über besonders geschützte Daten,
- die Einführung eines besonderen Widerspruchsrechts gegenüber einer an sich rechtmäßigen Datenverarbeitung und
- die Neufassung der Schadenersatzregelung.

Die Änderungsvorschläge, die von Seiten des TLfD im Rahmen der abgegebenen Stellungnahmen gemacht wurden, sind teilweise berücksichtigt worden und fanden Niederschlag im Gesetz. Zu begrüßen ist, dass auch weiterhin die Auskunftserteilung an Betroffene nach § 13 ThürDSG grundsätzlich kostenfrei bleibt. Dies konnte im Rahmen der parlamentarischen Beratung des Gesetzentwurfs erreicht werden. Lediglich bei einem besonderen Verwaltungsaufwand sollen Verwaltungskosten geltend gemacht werden können.
Kritik habe ich an der Änderung der Regelungen zur Auftragsdatenverarbeitung nach § 8 ThürDSG geübt. Danach ist zukünftig nicht mehr der einheitliche Kontrollauftrag des TLfD für sämtliche Auftragsdatenverhältnisse vorgesehen, die von öffentlichen Stellen veranlasst werden. Auch die Informationspflicht an den TLfD über ein solches Auftragsdatenverhältnis ist im Gesetz nicht mehr vorgesehen.
Damit ist die so genannte erste Stufe zur Novellierung des Datenschutzrechts zum Abschluss gekommen.
In der 2. Phase soll eine grundlegende Überarbeitung und Modernisierung des BDSG in Angriff genommen werden, Zielvorstellungen werden diskutiert und wissenschaftliche Gutachten vorgestellt. Krite-

rien dabei sind die zunehmende Bedeutung des technischen Datenschutzes wie auch das Ziel, das Datenschutzrecht insgesamt klar, übersichtlich und für den Bürger verständlich zu regeln. Datenschutz durch Technik und der Einsatz datenschutzfreundlicher Technologien sind präventive Maßnahmen, den Schutz betroffener Personen sicherzustellen.

5.1.2 Novellierung des Melderechtsrahmengesetzes

Von der Bundesregierung wurde Ende 2001 dem Bundestag ein Gesetzentwurf zur Novellierung des Melderechtsrahmengesetzes vorgelegt. Ziel der Änderungen ist es damit vor allem, Rahmenbedingungen für die Nutzung moderner Informations- und Kommunikationstechnologien bei der Verarbeitung von Meldedaten, insbesondere bei Auskunftserteilungen, zu schaffen. Darüber hinaus ist auch die Abschaffung einzelner Melde- und Mitwirkungspflichten vorgesehen. Bereits im Vorfeld hatten die DSB des Bundes und der Länder in einer Entschließung anlässlich der 61. Datenschutzkonferenz (Anlage 13) auf wesentliche datenschutzrechtliche Fragen bei der Novellierung des Melderechts hingewiesen. Wie aus dem Entwurf an den Bundestag zu entnehmen ist, wurden diese nur teilweise berücksichtigt. Zu begrüßen ist, dass der Forderung, bei den künftig geplanten Auskunftserteilungen über das Internet an nicht öffentliche Stellen, den Betroffenen zumindest ein Widerspruchsrecht einzuräumen, Rechnung getragen wurde. Da desweiteren auch Datenübermittlungen an öffentliche Stellen durch Datenübertragungen nach Maßgabe des Landesrechts erlaubt sein sollen, wird es Aufgabe des TLfD sein, hierbei die Vorgabe entsprechenden Datensicherungsmaßnahmen (wie die Pflicht zur Nutzung von Signatur und Verschlüsselungsverfahren), die einen Zugriff Unbefugter auf Meldedaten ausschließen können, einzufordern.

5.1.3 Wahlen – Änderung des Wahlgesetzes

In meinen Tätigkeitsberichten (1. TB, 5.2.6.1; 3. TB, 5.2.4) hatte ich bereits auf datenschutzrechtliche Probleme im Zusammenhang mit der Auslegung von Wählerverzeichnissen hingewiesen. Sie betrafen die nicht auszuschließende Gefahr, dass die im Rahmen der Prüfung des Wahlrechts durch die Einsichtnahme in das Wählerverzeichnis

gewonnenen Informationen über Wohnanschriften von Wahlberechtigten auch zweckwidrig, insbesondere zur Umgehung von Melderegisterauskunftssperren, genutzt werden könnten. In gleicher Angelegenheit hatten die DSB des Bundes und der Länder auf ihrer 49. Konferenz 1995 bereits den Bundesgesetzgeber aufgefordert, durch eine geeignete Neuregelung den möglichen Missbrauch von Daten aus Wählerverzeichnissen auszuschließen. Im fünfzehnten Gesetz zur Änderung des Bundeswahlgesetzes vom 27. April 2001 wurde diesen Hinweisen folgend das Einsichtsrecht in Wählerverzeichnisse neu geregelt. Danach hat jeder Wahlberechtigte - wie bisher - das Recht, die Richtigkeit oder Vollständigkeit der zu seiner Person im Wählerverzeichnis eingetragenen Daten zu überprüfen. Ein Recht auf Einsicht in das Wählerverzeichnis zur Überprüfung der Richtigkeit oder Vollständigkeit der Daten von anderen im Wählerverzeichnis eingetragenen Personen besteht aber nur noch, wenn Tatsachen glaubhaft gemacht werden, aus denen sich eine Unrichtigkeit oder Unvollständigkeit des Wählerverzeichnisses ergeben kann. Eine Einsicht in das Wählerverzeichnis bleibt aber verwehrt, wenn es sich um Daten von Wahlberechtigten handelt, für die im Melderegister ein Sperrvermerk wegen einer unmittelbaren Gefahr für Leben, Gesundheit oder anderer schutzwürdiger Belange entsprechend den Vorschriften der Landesmeldegesetze eingetragen ist. Damit wurde den Forderungen des Datenschutzes auf Bundesebene Rechnung getragen. Auf eine Anfrage im TIM wurde signalisiert, dass man dort der Aufnahme einer gleich lautenden Regelung grundsätzlich aufgeschlossen gegenüber stehen würde.
Im weiteren wurde durch eine Ergänzung im Bundeswahlgesetz dem Anliegen einer Vielzahl von Städten und Gemeinden nach einer gesetzlichen Ermächtigung zur Erhebung und Verarbeitung von Daten Wahlberechtigter zum Zweck ihrer Berufung als Mitglieder von Wahlvorständen entsprochen.

5.1.4 Informationsfreiheitsgesetz (IFG)

Einige Bundesländer haben durch Gesetze die Voraussetzungen dafür geschaffen, dass ein allgemeines Akteneinsichtsrecht auch in Akten, die den Bürger nicht selbst betreffen, besteht. Die DSB des Bundes und der Länder haben in ihrer Entschließung (Anlage 14) betont, dass das Recht auf informationelle Selbstbestimmung des

Einzelnen dem freien Zugang zu internen, amtlichen Informationen nicht entgegensteht, wenn die Privatsphäre der Betroffenen sowie die Betriebsgeheimnisse gesetzlich geschützt bleiben. Auf Bundesebene gibt es einen Entwurf eines Informationsfreiheitsgesetzes. Im Thüringer Landtag wird ein Gesetzentwurf für ein entsprechendes Gesetz derzeit beraten.

5.1.5 Drittes Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften (3. VwVfÄndG)

Im Rahmen der Modernisierung der Verwaltung bedarf auch das Verwaltungsverfahrensrecht insbesondere im Hinblick auf die elektronische Kommunikation, auf die die Vorschriften des Verwaltungsverfahrensrechts bisher nicht angelegt sind, der Anpassung. Auf Bund-Länder-Ebene wird derzeit das 3. VwVfÄndG diskutiert. Ich habe hierzu die Auffassung vertreten, dass eine elektronische Kommunikation zwischen der Behörde und den Bürgern nur dann stattfinden soll, wenn diese sich ausdrücklich damit einverstanden erklärt haben. Aus der Bekanntgabe einer E-Mail-Adresse kann nämlich nicht die Schlussfolgerung gezogen werden, dass der Bürger damit schon seine Einwilligung für eine zukünftig stattfindende Kommunikation auf diesem Wege mit der Behörde erteilt hat. Probleme kann es hier auch mit dem Nachweis des Zugangs eines elektronischen Dokumentes geben, da nicht unbedingt davon ausgegangen werden kann, dass anders als beim Postverkehr das „elektronische Postfach“ täglich geöffnet wird. Entsprechende Änderungen sollen auch im Sozialgesetzbuch und der Abgabenordnung erfolgen. Für das Gesetz sollte eine Vorschrift aufgenommen werden, die die Verwaltung verpflichtet, Verwaltungsakte mit personenbezogenen Daten zu verschlüsseln, damit die Vertraulichkeit gewährleistet ist. Ich werde das Gesetzgebungsvorhaben weiter begleiten.

5.1.6 E-Government

Infolge der zunehmenden elektronischen Kommunikation verändern sich auch die Verwaltungsvorgänge.
Umständliche Behördengänge, eingeschränkte Sprechzeiten und oftmals lange Wartezeiten vor Ort sollen zukünftig weitestgehend vermieden werden, indem z. B. An- und Abmeldungen, Anträge, ja

sogar Verwaltungsakte elektronisch versandt und empfangen werden können. In diesem Zusammenhang wird der Begriff Electronic-Government (E-Government) verwendet. Man spricht aber nicht nur von E-Government, wenn es sich um das Außenverhältnis der Verwaltung handelt, also zur Wirtschaft und zum Bürger, sondern man spricht auch von E-Government, wenn innerhalb der Verwaltung Verfahren der Vorgangsbearbeitung den neuen Kommunikationstechniken angepasst werden, um diese auch sinnvoll zu nutzen. Als Beispiel für das Außenverhältnis der Verwaltung sei stellvertretend für die Beziehung Verwaltung/Wirtschaft die Ausschreibung zur Beschaffung und für die Beziehung Verwaltung/Bürger das Verfahren zur elektronischen Steuererklärung ELSTER (9.2) genannt. Ein Beispiel für das automatisierte Abwickeln von Verwaltungsvorgängen ist ein verwaltungsinterner Workflow oder die Informationbereitstellung über ein Intranet.
Gesetzliche Rahmenbedingungen hierfür wurden u. a. mit dem Telekommunikationsgesetz, Teledienstedatenschutzgesetz, Mediendienstestaatsvertrag, dem neuen Signaturgesetz (15.7) und werden mit dem derzeit in Überarbeitung befindlichen Verwaltungsverfahrensgesetz geschaffen (5.1.5).

Die Bundesregierung plant im Rahmen der Initiative BundOnline2005 bis zum Jahr 2005 alle ca. 1200 internetfähigen Dienstleistungen der Bundesverwaltung auch über das Internet bereitzustellen. Zur Förderung der Initiative BundOnline2005 wurde von Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein E-Government-Handbuch erarbeitet, welches erstmalig öffentlich auf der CeBit 2001 vorgestellt wurde. Dieses Handbuch wird modular im Internet (www.bsi.bund.de) veröffentlicht und aktualisiert. Es enthält sowohl methodische Hinweise für planmäßiges Vorgehen als auch praktische Lösungsansätze. Desweiteren soll eine weitere Initiative der Bundesregierung MEDIA@KOMM diese Entwicklung in den Städten und Gemeinden gezielt unterstützen und die Anwendungen beschleunigen.
In Thüringen stellen inzwischen zahlreiche Kommunen ein Internetangebot bereit, u. a. zum Abrufen von Formularen und der Möglichkeit, per E-Mail zu korrespondieren.
Im Februar 2001 hat die Thüringer Landesregierung den Entwurf eines Leitbildes zur „Weiterentwicklung der Verwaltungsreform und

der Organisation der Landesverwaltung“ entwickelt. Der Entwurf wurde vom Kabinett bestätigt und zur öffentlichen Anhörung freigegeben. In diesem Leitbild heißt es bspw.: „Gleichgültig, ob Bürger, Wirtschaftsvertreter oder Verwaltungsmitarbeiter - alle Nutzer erhalten über ein einziges Portal Zugang zur virtuellen Gemeinschaft Freistaat Thüringen und je nach registrierter Anspruchsberechtigung Zugang zu den virtuellen Anwendungen und Leistungen.“ Vorschläge für die zur Umsetzung des Leitbildes erforderlichen Maßnahmen werden z. Z. in fünf themenspezifischen Arbeitsgruppen erarbeitet. Dabei soll auch der Datenschutzbeauftragte im Rahmen der vertrauensvollen Zusammenarbeit unterrichtet und beratend einbezogen werden.

Die Arbeitsgruppe „Electronic Government“, welche vom TIM geleitet wird, führte im Juni 2001 ein Forum „Bürgernähe und Verwaltungseffizienz“ durch. Dieses Forum gab einen Überblick über die für Thüringen geplante Kommunikationsinfrastruktur und -sicherheit sowie über die z. Z. möglichen E-Government-Applikationen wie Elektronische Beschaffung, Ausschreibung, E-Learning, Thüringer Wasser- und Abwasserkataster, Formular Transaktionen, Lottomittelverwaltung und Kfz-Zulassung.

Die DSB des Bundes und der Länder verabschiedeten im Oktober 2000 die Entschließung „Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung“ (Anlage 10). In dieser Entschließung erklären sie ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Die 61. Konferenz der DSB des Bundes und der Länder beschloss am 8. und 9. März 2001 eine Arbeitsgruppe „Electronic Government“ einzurichten, dessen Federführung Niedersachsen übernahm und an der sich auch der TLfD aktiv beteiligt. Aus der Sicht des Datenschutzes sind bei E-Government-Anwendungen folgende Aspekte zu beachten:

- Datenvermeidung, Datensparsamkeit (z. B. Pseudonymisierung),
- Sichere Transaktionen über das öffentliche Netz,
- Transparenz der Verfahren (Datenschutzinformationen, elektronische Auskunft, Berichtigung, Löschung),
- Beachtung der Zweckbindung und anderer datenschutzrechtlicher Vorschriften sowie
- Datenschutzgerechte Internetangebote (nur zulässige Daten ins Internet, rechtzeitige Löschung von Verbindungsdaten, Anbie-

terkennzeichnung, Reduzierung von Cookies, Anonymität von Statistiken).

Die Anbindung der Verwaltung an das Medium Internet erfordert insbesondere eine sichere und vertrauliche Kommunikation sowie einen angemessenen Schutz personenbezogener Daten. Aus datenschutzrechtlicher Sicht muss gewährleistet sein, dass keine Unberechtigten personenbezogene Daten erlangen oder gar verfälschen können. Hier gilt es, geeignete Sicherheitsmaßnahmen wie Verschlüsselung und elektronische Signatur einzusetzen. Überall da, wo es auf die Integrität und Authentizität einer Willenserklärung ankommt, bietet sich der Einsatz der elektronischen Signatur an. Eine vertrauliche Kommunikation erfordert die Verschlüsselung der zu übertragenden Informationen. Ohne hinreichende Sicherheit werden die Anwender den neuen technischen Möglichkeiten nur bedingt vertrauen und diese nutzen.

5.1.7 Aufbewahrung und Archivierung personenbezogener Daten

Gemäß § 16 ThürDSG sind personenbezogene Daten regelmäßig zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist. In der Praxis, so kann bei Kontrollen immer wieder festgestellt werden, sind in öffentlichen Stellen häufig keine verbindlichen Vorgaben für Aufbewahrungsfristen bekannt oder soweit sie in eigener Kompetenz festgelegt werden können, fehlen mitunter entsprechende Vorgaben. Aufgrund dessen wurde die Initiative des TIM zum Erlass der „Richtlinie über die Aufbewahrung von Akten und sonstigem Schriftgut in der Verwaltung des Freistaates“ vom 25.05.2001 (ThürStAnz. Nr. 27, S. 1492 ff.) nachdrücklich unterstützt. Für den kommunalen Bereich liegen „Empfehlungen der Archivberatungsstelle Thüringen zu Aufbewahrungsfristen für die kommunale Schriftgutverwaltung in Thüringen“ vor.

Gemäß § 16 Abs. 3 ThürDSG sind die Verwaltungsunterlagen nach Ablauf der Aufbewahrungsfrist vor ihrer gesetzlich vorgeschriebenen Löschung oder Vernichtung dem zuständigen Archiv zur Übernahme anzubieten. Das Verfahren hierzu ist in den §§ 11 und 12 ThürArchivG geregelt. Danach sind mit Ausnahme von unzulässig erhobenen Daten grundsätzlich alle Unterlagen anzubieten, auch die, die

besonderen Rechtsvorschriften über die Geheimhaltung oder über den Datenschutz unterworfen sind. Eine Vernichtung oder Löschung der Daten ist nur zulässig, wenn das zuständige öffentliche Archiv die Übernahme abgelehnt oder nicht innerhalb eines Jahres über die Archivwürdigkeit angebotener Unterlagen entschieden hat. Von dem Anbieten und Vorlegen von Unterlagen kann nur im Einvernehmen mit dem zuständigen Archiv abgesehen werden, wenn diese wegen ihres offensichtlich geringen Quellenwertes als nicht archivwürdig zu bewerten sind. Über die Archivwürdigkeit entscheidet ausnahmslos das zuständige Archiv im Benehmen mit der anbietenden Stelle.
Der Umgang mit diesen Unterlagen orientiert sich aber dann allein an archivrechtlichen Bestimmungen, was im kommunalen Bereich zum Beispiel die Existenz entsprechender Archivsatzungen und Benutzungsordnungen voraussetzt.

5.1.8 Umgang mit Behördenpost

Wie bereits in der Vergangenheit hat sich auch im Berichtszeitraum der TLfD mit datenschutzrechtlichen Problemen beim Umgang mit Behördenpost beschäftigt. Neben entsprechenden Anfragen und Beschwerden zeigt sich auch bei Kontrollen, dass fehlende technische und organisatorische Regelungen zum Umgang mit Behördenpost mitunter dazu führen, dass ein nicht erforderlicher Kreis der Beschäftigten Kenntnis von personenbezogenen Daten erhält. Im Rahmen des Direktionsrechts entscheidet der Behördenleiter über den Umgang mit der Behördenpost. Darüber hinaus ist auch der fachlich zuständige Vorgesetzte im Rahmen der Aufgabenstellung befugt, in Unterlagen einsehen zu können. Gemäß § 9 ThürDSG haben die öffentlichen Stellen durch technische und organisatorische Maßnahmen sicherzustellen, dass nur jeweils zuständige Beschäftigte Zugriff auf personenbezogene Daten erhalten. Befugt sind die Beschäftigten, die zuständig sind für die jeweilige Aufgabenerfüllung. Zu diesem Zweck ist es angeraten, die Absender in geeigneter Weise (z. B. durch die konkrete Eintragung der zuständigen Stelle auf Vordrucken) darauf hinzuweisen, dass sie ihre Anfragen und Mitteilungen eindeutig mit der sachbearbeitenden Stelle (z. B. Meldeamt, Standesamt, Personalamt, Sozialamt, Vollstreckungsstelle u. a.) adressieren sollten. Innerhalb der öffentlichen Stelle ist durch Dienstanweisungen, Postordnung u. ä. zu regeln, wer zum Öffnen

welcher Post berechtigt ist bzw. welche Personen bzw. Verwaltungsbereiche die Post zur Kenntnisnahme und weiteren Bearbeitung erhalten. Dabei ist zu berücksichtigen, dass aufgrund spezialgesetzlicher Regelungen in einigen Bereichen eine Kenntnisnahme von personenbezogenen Daten ausdrücklich nur den für die Bearbeitung Zuständigen (Personenstandsgesetz, SGB, Beamtengesetz) erlaubt ist. Auch für die öffentliche Stelle gilt das Brief- bzw. Postgeheimnis gemäß Art. 10 GG. Aus diesem Grund verbietet sich zwangsläufig die Öffnung von Briefsendungen an einen erkennbar privaten Adressaten (insbesondere beim Zusatzvermerk: persönlich oder privat) sowie an gewählte Gremien, die zur öffentlichen Stelle gehören oder ihr unmittelbar zugeordnet sind und aufgrund ihrer Aufgabenstellungen eine besonders vertrauenswürdige Stellung einnehmen (wie z. B. Personalräte, Schwerbehinderten-, Studenten-, Eltern- oder Schülervertretungen). Wie entsprechende Eingaben zeigen, sollten in den Vorschriften zum Umgang mit Behördenpost auch Regelungen zur Verfahrensweise beim Eingang unrichtig adressierter oder irrtümlich geöffneter Postsendungen getroffenen werden. So hatte man z. B. in einem Fall Sitzungsunterlagen für ein Kreistagsmitglied über den Behördenkurierdienst an die Gemeindeverwaltung weitergeleitet, in der das Mitglied beschäftigt war. Dort erfolgte, da die Beschriftung des Umschlags nicht eindeutig war, die Öffnung des Briefes in der Poststelle. In einer anderen Gemeinde führte die mehrmalige Nutzung von Briefumschlägen, ohne dass die nicht mehr zutreffenden Adressen vollständig geschwärzt waren zu einer unbeabsichtigten Kenntnisnahme des Inhalts durch Unbefugte. Unkenntnis und fehlende Regelungen zum Postumgang waren in einem anderen Fall die Ursache dafür, dass in einigen kommunalen Kindertagesstätten von der Leitung unzulässigerweise Briefsendungen an die jeweiligen Elternvertretungen geöffnet wurden. Im Ergebnis der Prüfung des jeweiligen Sachverhaltes wurden in allen vorgenannten Fällen die betreffenden Stellen vom TLfD aufgefordert durch geeignete organisatorische Maßnahmen, insbesondere durch die Schaffung und Überarbeitung von verbindlichen Regelungen zum Umgang mit Behördenpost künftig eine unbefugte Kenntnisnahme personenbezogener Daten auszuschließen.

5.1.9 Datenschutz im Ausländerwesen

Im Berichtszeitraum ist durch die Veröffentlichung im Bundesanzeiger die Allgemeine Verwaltungsvorschrift zum Ausländergesetz (AuslG-VwV) vom 28. Juni 2000 zwischenzeitlich in Kraft getreten. Sie enthält Regelungen, Hinweise und Erläuterungen zur Ausführung des Ausländergesetzes und der aufgrund dieses Gesetzes erlassenen Rechtsverordnungen. Die im 3. TB (5.1.1) aufgeführten vom Bundesrat beschlossenen Änderungsanträge sind eingearbeitet.
Zur Änderung der ausländerrechtlichen Vorschriften lagen mehrere Entwürfe, insbesondere auch im Rahmen des Gesetzes zur Bekämpfung des internationalen Terrorismus, vor. Das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I, S. 361), enthält Änderungen des Ausländergesetzes hinsichtlich der Möglichkeit der Verwendung weiterer biometrischer Merkmale von Fingern oder Händen oder Gesicht und für das automatische Lesen in Aufenthaltsgenehmigungen und im Ausweisersatz. Auch werden die Voraussetzungen zur Feststellung und Sicherung der Identität von Ausländern ergänzt, künftig können hierzu auch Sprachaufzeichnungen gefertigt werden.
Mit dem Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern“ (Zuwanderungsgesetz, BR-Drs. 921/01 vom 08.11.2001), das derzeit noch beraten wird, ist eine Neuregelung des Ausländerrechts vorgesehen.

Im 3. TB (5.1.4) sind die Voraussetzungen der Ausschreibung zur Einreiseverweigerung nach Art. 96 Schengener Durchführungsübereinkommen (SDÜ) dargestellt worden. Auch in diesem Berichtszeitraum erreichten mich über den Bundesbeauftragten für den Datenschutz mehrere Ersuchen von ausländischen Staatsbürgern um Auskunft und Löschung ihrer Daten im Schengener Informationssystem (SIS). Enthält das SIS eine Ausschreibung zur Einreiseverweigerung, wird dem Betroffenen die Einreise in alle Schengen-Staaten verweigert. Diese Anfragen habe ich zum Teil auch zum Anlass datenschutzrechtlicher Kontrollen in den ausschreibenden Ausländerbehörden genommen. Bei der Bearbeitung der Anfragen stellte sich in einigen Fällen heraus, dass keine Gründe zur Ausschreibung zur Einreiseverweigerung bestanden. Die erfolgten Einreisesperren waren teilweise darauf zurückzuführen, dass bei Inbetriebnahme des SIS eine automatische Übernahme der Daten von INPOL- Ausschreibun-

gen erfolgt waren und nach Ablauf der Prüffristen von den zuständigen Ausländerbehörden die gebotenen Überprüfungen auf die Rechtsgrundlage und Löschungen nicht vorgenommen wurden. Die betroffenen Ausländerbehörden habe ich aufgefordert, die Ausschreibungen zur Einreiseverweigerung zu überprüfen und die Daten ggf. zu löschen. Bei der Bearbeitung der Anfragen ist mir von Ausländerbehörden teilweise mitgeteilt worden, dass eine Ausschreibung zur Einreiseverweigerung gemäß Art. 96 SDÜ ohne Befristung erfolge. Das TLVwA hat zwischenzeitlich die Ausländerbehörden auf die einschlägigen Prüf- und Löschfristen hingewiesen. Nach Ablauf der Prüffristen muss geprüft werden, ob Gründe für die Aufrechterhaltung einer internationalen Ausschreibung zur Einreiseverweigerung noch bestehen. Ist dies nicht der Fall, kann eine nationale entsprechende Ausschreibung ausreichen.

Eine weitere datenschutzrechtliche Kontrolle habe ich aufgrund einer Eingabe wegen der Übermittlung personenbezogener Daten durch eine Ausländerbehörde an das Bundesamt zur Anerkennung ausländischer Flüchtlinge durchgeführt. Dabei handelte es sich um Angaben und Vermutungen zu politischer Tätigkeit des Betroffenen, die Zeiten des Aufenthalts im Wohnheim und Verbindungen zu einer deutschen Staatsangehörigen. Ausländerbehörden sind grundsätzlich nicht daran gehindert, zulässigerweise anhand von beweiskräftigen Unterlagen beispielsweise Verstöße gegen die räumliche Beschränkungen (Verlassen des Landkreises ohne Genehmigung) dem im Asylverfahren zuständigen Bundesamt für die Anerkennung ausländischer Flüchtlinge mitzuteilen. Die geschilderten Vermutungen und Sachverhalte durften aber nicht mitgeteilt werden. Die Ausländerbehörde hat infolgedessen geeignete Maßnahmen getroffen, um zukünftig unzulässige Datenübermittlungen auszuschließen.

Eine weitere Eingabe richtete sich gegen die Praxis in einigen Asylbewerberunterkünften, Asylbewerbern die Aufenthaltsgestattungen abzufordern und im Gegenzug einen Hausausweis auszuhändigen. Besucher in Asylbewerberunterkünften sollten ihre Originalpersonalausweise abgeben, um ihn erst bei Verlassen des Asylbewerberheimes wieder zu erhalten. Für beide Verfahrensweisen habe ich keine Erforderlichkeit gesehen. Das TLVwA als Aufsichtsbehörde hat meine Auffassung zu der Einbehaltung von Originalpapieren der Bewohner der Landesgemeinschaftsunterkünfte geteilt. Eine Aufbewahrung dieser Originaldokumente darf nur auf ausdrücklichen

Wunsch der Betroffenen erfolgen. Darüber hinaus hat die Aufsichtsbehörde ebenfalls meine Auffassung, dass das Einbehalten von Ausweisdokumenten von Besuchern nicht zulässig ist, aufgegriffen. Die kommunalen Träger, die von der zulässigen Verfahrensweise abgewichen waren, wurden aufgefordert, ihre Verhaltensweise zu ändern oder eine begründete Stellungnahme mit der Darlegung der Notwendigkeit und den dazu herangezogenen Rechtsnormen vorzulegen.
Soweit eine Erhebung weniger personenbezogener Daten von Besuchern aus Gründen der Sicherheit und Ordnung in einer Asylbewerberunterkunft erforderlich ist und dies durch Mitarbeiter von privaten Wachdiensten geschieht, bedarf dies einer konkreten vertraglichen Vereinbarung.

5.2 Kommunales

5.2.1 Wahrung des Adoptionsgeheimnisses im Meldeamt

Bei der Datenverarbeitung, insbesondere bei Auskunftserteilungen durch Meldebehörden ist die Wahrung des Adoptionsgeheimnisses gemäß § 32 Abs. 8 ThürMeldeG zu gewährleisten. Im Berichtszeitraum wurde der TLfD auf die Problematik im Zuge einer Bürgeranfrage aufmerksam. Im konkreten Fall hatte eine Mutter in Anwesenheit ihres adoptierten schulpflichtigen Kindes im Meldeamt einen Kinderausweis beantragt. Zu diesem Zweck war ihr ein mit Hilfe des automatisierten Melderegisters erstellter, bereits mit den Kindsdaten „vorausgefüllter“ Antrag übergeben worden, der von ihr als Sorgeberechtigte lediglich nach Prüfung der Richtigkeit der Angaben nur noch unterzeichnet werden sollte. Mit Verwunderung stellte dabei die Mutter fest, dass auf dem Antrag neben der aktuellen auch noch die vor der Adoption geltende frühere Anschrift des Kindes ausgedruckt war. Obwohl man den Vordruck mit diesen Angaben nur der Sorgeberechtigten übergeben hatte und insoweit keine unmittelbare Übermittlung der Daten an Unbefugte erfolgt war, war die Verfahrensweise unter Berücksichtigung der besonderen Umstände durchaus geeignet, dass die vom Adoptionsgeheimnis geschützten Daten Unbefugten (z. B. dem adoptierten Kind unter 16 Jahren) zur Kenntnis gelangen können. Die Ursachen hierfür lagen nicht nur an einer fehlerhaften Einstellung im automatisierten Meldeverfahren durch das Meldeamt, indem ohne ein Erfordernis die frühere Anschrift im Antrag auf

einen Kinderausweis aufgenommen worden war, sondern insbesondere auch an einem fehlenden Hinweis im Melderegister (Eintragung einer Auskunftssperre) zur Verhinderung der Offenbarung von Adoptionen. Im Ergebnis der Prüfung wurde deshalb veranlasst, dass neben der Eintragung einer Auskunftssperre beim Ausdruck von Kinderausausweisanträgen nur noch die aktuellen Daten aufgenommen werden. Desweiteren wurden die festgestellten Probleme im Zusammenhang mit der Erhebung und Verarbeitung personenbezogener Daten bei Adoptionen in den Meldebehörden sowie deren Datenaustausch mit den Standes- und Jugendämtern zum Anlass genommen, das TIM in Zusammenarbeit mit dem Landesjugendamt um landeseinheitliche Vorgaben für die Erhebung, Speicherung, Übermittlung und Löschung von Daten bei Adoptionen in den Meldebehörden zu bitten, um künftig jegliche Offenbarung über Adoptionen gegenüber Unbefugten bei den Meldebehörden auszuschließen. Nach vorliegenden Informationen soll eine entsprechende Verwaltungsvorschrift den betreffenden Behörden in Kürze zur Verfügung gestellt werden.

5.2.2 Unterschriftsprüfung durch Meldebehörden bei Volksbegehren

Im Rahmen eines Volksbegehrens in Thüringen hatten die Initiatoren erfahren, dass in einigen Fällen Meldebehörden bei der Prüfung der Unterschriftslisten aufgrund von Zweifeln an der Identität bzw. Wahlberechtigung der Unterzeichner (z.B. bei abweichend zum Melderegister eingetragenen Wohnanschriften) die betreffenden Einwohner zur Klärung in die Meldebehörden gebeten worden seien. Da man dies für unzulässig ansah, wurde der TLfD um eine entsprechende Prüfung gebeten.
Gemäß § 30 des Thüringer Gesetzes über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid (ThürBVVG) dürfen die im Rahmen eines Bürgerantrags, Volksbegehren und Volksentscheides erhoben Daten nur für die Durchführung des jeweiligen Bürgerantrags, Volksbegehrens oder -entscheides genutzt werden. Dabei dienen die Angaben in den Unterschriftslisten allein zur Feststellung der Identität bzw. Wahlberechtigung der Unterzeichner, was von den Meldebehörden durch einen Vergleich mit den Eintragungen im Melderegister in jedem Einzelfall zu prüfen und bei Überein-

stimmung zu bestätigen ist. Eine Nutzung der dabei gewonnenen Informationen für andere Zwecke (z. B. zur Aktualisierung der Melderegister) ist den Meldebehörden nicht erlaubt. Soweit eine eindeutige Zuordnung der Person bei der Prüfung des Stimmrechts durch fehlende, unleserliche oder falsche (d. h. von den im Melderegister abweichende) Angaben nicht möglich ist, sind diese nach den Vorschriften des § 5 ThürBVVG als ungültig zu betrachten. Eine Notwendigkeit für Rückfragen bei den Unterzeichnern zur Klärung ihres Stimmrechts besteht somit nicht. Da diese Rechtsauffassung auch vom TIM geteilt wird, wurden die Meldebehörden in einem Rundschreiben nochmals ausdrücklich darüber informiert.

5.2.3 Nutzung von Meldedaten zur Unterstützung eines Forschungsprojekts

Durch die Anfrage einer Meldebehörde erfuhr ich, dass eine Hochschule zur Durchführung eines Forschungsprojektes über die soziale Situation Alleinerziehender Übersichten von einer Vielzahl Thüringer Meldebehörden mit den Anschriften aller im jeweiligen Zuständigkeitsbereich wohnenden Alleinerziehenden anfordern würde. Diese Listen sollten für eine repräsentative Stichprobenbefragung bei ausgewählten Alleinerziehenden genutzt werden. Auf Rückfrage bei der Projektleitung wurde erläutert, dass die angeforderten Daten zur Durchführung des Projekts unabdingbar seien und sie auf keine andere Art und Weise gewonnen werden könnten. Darüber hinaus habe auch schon die für das Meldewesen zuständige oberste Aufsichtsbehörde, das TIM, die Möglichkeit und Zulässigkeit einer Bereitstellung und Nutzung von Meldedaten für diese Zwecke bestätigt. Diese Auffassung wurde vom TLfD grundsätzlich geteilt. Im konkreten Fall war aber die Erhebung der Namen und Anschriften aller Alleinerziehenden an die Hochschule beabsichtigt, obwohl eine Nutzung der Daten nur für einen Bruchteil zur Durchführung der Stichprobenerhebung vorgesehen war. Dies widersprach dem im Datenschutzrecht maßgeblichen Verhältnismäßigkeitsgrundsatz und hätte zu einer nicht erforderlichen Datenvorratshaltung geführt. Aus diesem Grund wurde die Hochschule aufgefordert, ihre Anforderungen an die Meldebehörden zu präzisieren und auf den für die Aufgabenerfüllung zwingend notwendigen Datenumfang zu beschränken. Da die Hochschule jegliche subjektive Einflussnahme auf die Stichprobenauswahl

ausschließen wollte, eine Ziehung der Stichprobe in den Meldebehörden durch Mitarbeiter der Hochschule aber aus personellen Gründen ausschied und darüber hinaus ohnehin auch eine statistische Übersicht über die Zahl der jeweils im Gemeindegebiet wohnenden Alleinerziehenden benötigte wurde, verständigte man sich im weiteren Gespräche darauf, dass die Meldebehörden der Hochschule zunächst eine (anonymisierte) Auflistung aller Alleinerziehenden unter Angabe der jeweiligen Ordnungszahl im Melderegisters, dem Geschlecht und dem Familienstand übergeben sollte. Auf deren Grundlage konnte dann die Ziehung der gewünschte Stichprobe an der Hochschule erfolgen. Entsprechend den dabei ausgewählten Ordnungszahlen wurden dann die Meldebehörden um Übermittlung der dazugehörigen Namen und Anschriften gebeten.
Durch diese Verfahrensweise war es letztlich möglich, nicht nur den zu übermittelnden Datenbestand sondern auch den Arbeitsaufwand in den Meldebehörden auf das für die Aufgabenerfüllung erforderliche Maß zu beschränken.

5.2.4 Zugang zu personenbezogenen Daten im Rahmen der Dienst- und Fachaufsicht

Nicht nur im Rahmen von Kontrollen sondern auch bei anderen Gelegenheiten wird die Frage an den TLfD gerichtet, ob und in welchem Umfang bei der Wahrnehmung einer Dienst- und Fachaufsicht Einsicht in Arbeitsunterlagen mit personenbezogenen Daten genommen werden darf. Hierzu ist zunächst festzustellen, dass eine in diesem Zusammenhang erfolgte Kenntnisnahme aus der Sicht des Datenschutzes keine Verarbeitung oder Nutzung für andere Zwecke darstellt. Insoweit bestehen grundsätzlich keine Bedenken gegen entsprechende Einsichtnahmen, soweit diesbezüglich keine besonderen gesetzlichen Regelungen vorliegen und es zur Wahrnehmung der Aufsichts- und Kontrollaufgaben erforderlich ist. Es bedeutet aber nicht, dass die Aufsichtsbehörden dauerhaft Kopien von Unterlagen bzw. automatisiert gespeicherter Daten nachgeordneter Einrichtungen vorhalten dürfen, um ggf. bei Bedarf die Rechtmäßigkeit von Entscheidungen überprüfen zu können. Dies wäre ebenso, wie die Einrichtung ständiger Abrufverfahren allein zur Wahrnehmung der Fachaufsicht, eine unzulässige Datenvorratshaltung.

Soweit nur eine Dienstaufsicht vorliegt, besteht überwiegend keine Erforderlichkeit zur Kenntnisnahme von personenbezogenen Daten, die in dem nachgeordneten Bereich zur Aufgabenerfüllung gespeichert sind. Unter diesen Aspekten war im Berichtszeitraum vom TLfD zu prüfen, ob ein Bürgermeister im Rahmen seiner Dienstaufsicht Kenntnis von den im Standesamt der Gemeinde gespeicherten Personenstandsdaten nehmen darf. Ausgehend von den Bestimmungen des § 51 PStG handelt es sich bei den den Standesbeamten obliegenden Aufgaben nicht um Selbstverwaltungsangelegenheiten der Gemeinden sondern um Angelegenheiten des Staates, die den Gemeinden zur Erfüllung nach Weisung übertragen sind. Die Fachaufsicht über die Standesämter obliegt gemäß § 11 der Zweiten Verordnung zur Änderung der Zweiten Thüringer Verordnung zur Bestimmung von Zuständigkeiten im Geschäftsbereich des Thüringer Innenministeriums vom 5. Mai 2000 den Landkreisen und kreisfreien Städte im übertragenen Wirkungskreis als untere Aufsichtsbehörden, dem Landesverwaltungsamt als obere Aufsichtsbehörde und dem für das Personenstandswesen zuständige Innenministerium als oberste Aufsichtsbehörde. Desweiteren wird in § 56 PStG bestimmt, dass im Notfall (z. B. Arbeitsunfähigkeit des Standesbeamten) die zuständige Verwaltungsbehörde die Wahrnehmung der Geschäfte des Standesbeamten vorübergehend einem anderen Standesbeamten eines anderen Standesamtsbezirks übertragen kann. Damit wird unmissverständlich zum Ausdruck gebracht, dass bei einer notwendigen Vertretung die Aufgaben im Personenstandswesen ausschließlich von Standesbeamten wahrgenommen werden dürfen. Es besteht demzufolge, soweit dies nicht besonders geregelt ist (z. B. im Rahmen der Mitteilungspflichten von Standesbeamten an Meldebehörden) keine Aufgabe, die es erfordern und erlauben würde, dass innerhalb einer Gemeinde „Nichtstandesbeamte“ (einschließlich des Bürgermeisters, wenn dieser nicht gleichzeitig als Standesbeamter bestellt ist) Zugang zu Personenstandsdaten erhalten. Aufgrund dessen wäre z. B. die Bekanntgaben der Namen von Brautleuten (seit der Abschaffung des öffentlichen Aufgebotes) - auch gegenüber dem Bürgermeister - ein Verstoß gegen die dem Standesbeamten obliegende besondere Schweigepflicht. Zur Gewährleistung des Datenschutzes und der Datensicherheit haben die Standesämter in Umsetzung der Forderungen des § 9 ThürDSG Maßnahmen zu treffen haben, die verhindern, dass Unbefugte bei der Verarbeitung, Aufbewahrung dem Transport

oder der Vernichtung auf Personenstandsdaten zugreifen können. Dies bedeutet insbesondere, dass ein Zugang zu den Räumen des Standesamtes nicht nur durch Dritte bei Reinigungs- oder Reparaturarbeiten sondern auch durch Bedienstete der Gemeindeverwaltung nur erlaubt ist, wenn durch geeignete verschlusssichere Behältnisse jeglicher Zugang auf personenbezogenen Daten (Unterlagen oder PC u. a.) verwehrt wird.

5.2.5 Veröffentlichung von Geburtsdaten im Amtsblatt

Während einige unserer Mitmenschen aus den verschiedensten Gründen stolz auf ihr erreichtes Alter sind und sich auch über Geburtstagsglückwünsche in der Presse freuen, bevorzugen andere die diesbezügliche Wahrung ihres „Geheimnisses“. Die unterschiedlichen individuellen Auffassungen dazu sind hinreichend aus Diskussionen für und gegen die umstrittenen Geburtstagslisten in Betrieben und Einrichtungen bekannt. Unter Berücksichtigung der unterschiedlichen Interessenslagen hat der Gesetzgeber zunächst grundsätzlich die Möglichkeit geschaffen, dass es nach § 33 Abs. 2 ThürMeldeG den Meldebehörden erlaubt ist, Mitgliedern parlamentarischer Körperschaften (und seit Ende 2001 auch Mitgliedern kommunaler Vertretungskörperschaften), der Presse oder dem Rundfunk Melderegisterauskünfte über Alters- oder Ehejubiläen von Einwohnern zu erteilen, wobei diese aber nur den Vor- und Familiennamen, den Doktorgrad und die Anschrift des Betroffenen sowie den Tag und die Art des Jubiläums umfassen darf. Gleichzeitig wird aber den Betroffenen nach § 33 Abs. 4 ThürMeldeG auch das Recht eingeräumt, der Weitergabe ihrer Daten zu widersprechen. Auf dieses Widerspruchsrecht muss der Betroffene in Thüringen bei der Anmeldung und einmal jährlich durch öffentliche Bekanntmachungen hingewiesen werden. Der Widerspruch kann bei der Meldebehörde formlos geltend gemacht und auch jederzeit zurückgenommen werden. Personen, die in einer Pflegeeinrichtung oder sonstigen Einrichtung, die der Betreuung pflegebedürftiger oder behinderter Menschen, der Rehabilitation oder der Heimerziehung dienen oder in einer Haftanstalt gemeldet sind, müssen vor der Übermittlung ihrer Daten gehört werden, während die Übermittlung immer unzulässig ist, wenn für die betreffende Person im Melderegister eine Auskunftssperre wegen einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche

schutzwürdige Belange des Betroffenen eingetragen ist. Die immer wiederkehrenden Anfragen und Beschwerden beim TLfD zeigen, dass die Veröffentlichung von Alters- und Ehejubiläen in der Bevölkerung nicht unumstritten ist. Die Gründe dafür liegen in der Regel darin, dass die Betroffenen – Bürger in hohem Lebensalter – häufig über ihr Widerspruchsrecht aus objektiven oder subjektiven Gründen nicht ausreichend informiert sind und der Begriff des „Alters- und Ehejubiläums“ bisher unterschiedlich interpretiert wurde. So war es in einigen Gemeinden Praxis, insbesondere alle Geburtstage ab dem 60. einschließlich der „unrunden“ (z. B. 61.) in ihren Amtsblättern zu veröffentlichen, was wohl eher einer regelmäßigen Information der Einwohner (insbesondere in kleinen Gemeinden) über die Geburtstage ihrer Mitbürger im höheren Lebensalter sowie über die demzufolge anstehenden „Familienfeiern“ in der Gemeinde als der vom Gesetzgeber vorgesehenen Ehrung von Jubilaren diente. Es ist zu begrüßen, dass auch vom Thüringer Gesetzgeber in entsprechender Weise (wie in vielen anderen Bundesländern) von der Möglichkeit einer einheitlichen Vorgabe für Alters- und Ehejubiläen Gebrauch gemacht wurde. Mit der Neufassung des § 33 Abs. 2 ThürMeldeG im Ersten Gesetz zur Änderung des Thüringer Meldegesetzes wurde im Gesetzestext der Begriff des Alters- und Ehejubiläums für alle Meldebehörden verbindlich definiert. Danach gelten als Altersjubiläen im Sinne des Thüringer Meldegesetzes nur noch der 65., 70., 75., 80., 85., 90. und jeder spätere Geburtstag und als Ehejubiläum die Goldene Hochzeit und jedes spätere Ehejubiläum.

5.2.6 Auskünfte aus dem Melderegister zur Erstellung einer Ortschronik

In vielen Gemeinden Thüringens werden Ortschroniken geführt, die in unterschiedlichem Umfang personenbezogene Daten enthalten. In diesem Zusammenhang wurde der TLfD um Auskunft gebeten, ob und in welchem Umfang personenbezogene Daten aus dem Melderegister in Ortschroniken übernommen werden können. In meiner Antwort habe ich darauf hingewiesen, dass mangels einer entsprechenden Rechtsnorm, die die Verarbeitung und Nutzung von Meldedaten zur Führung von Ortschroniken ausdrücklich erlaubt, im Hinblick auf die Zielstellung der Datenverarbeitung (Veröffentlichung einer Ortschronik) die diesbezügliche Nutzung von Meldedaten ohne Einwil-

ligung der Betroffenen nicht zulässig ist. Entsprechendes gilt selbstverständlich auch für sonstige in der Verwaltung vorliegende personenbezogenen Daten (z. B. Daten aus dem Gewerberegister), soweit diese nicht aus öffentlich zugänglichen Quellen (wie Zeitungen, Telefon- oder Branchenverzeichnissen, Bekanntmachungen, Beschlüsse öffentlicher Gemeinderatssitzungen) entnommen werden können. Datenschutzrechtlich unproblematisch ist statt dessen die Aufnahme von statistischen Übersichten, so genannten Geschäftsstatistiken, zur natürlichen und räumlichen Bevölkerungsbewegung (Zahl der Geburten, Todesfälle bzw. Zu- und Wegzüge) in Ortschroniken. Darüber hinaus ist es Aufgabe des Archivars gemäß § 12 ThürArchivG festzustellen, welche Unterlagen wegen ihres rechtlichen, politischen, wirtschaftlichen, sozialen und kulturellen Wertes für die Erforschung und das Verständnis der Geschichte und der Gegenwart als Archivgut dauerhaft aufzubewahren sind. Zu diesem Zweck besteht letztlich für alle Verwaltungsstellen die Verpflichtung, die von ihnen nicht mehr benötigten Unterlagen vor ihrer Vernichtung dem zuständigen Archiv zur Übernahme anzubieten. Nach Ablauf der gesetzlichen Schutzfristen (§ 17 ThürArchivG) besteht dann ggf. auch noch die Möglichkeit der Nutzung von personenbezogenen Archivgut für wissenschaftliche Arbeiten (wie z. B. auch für notwendige Ergänzungen in der betreffenden Ortschronik).

5.2.7 Nutzung automatisierter Abrufverfahren von Meldedaten innerhalb von Gemeindeverwaltungen

Aufgrund einer Eingabe hatte sich der TLfD im Berichtszeitraum auch mit der Zulässigkeit und den dabei notwendigen technischen und organisatorischen Anforderungen für die Einrichtung und Nutzung automatisierter Abrufverfahren von Meldedaten innerhalb von Gemeindeverwaltungen zu beschäftigen. Hintergrund war dabei der Vorwurf, dass sich Mitarbeiter einer Stadtverwaltung für private Zwecke Informationen aus dem Melderegister beschafft haben sollen. Gemäß § 29 Abs. 7 ThürMeldeG dürfen Meldedaten, soweit deren Kenntnis zur Aufgabenerfüllung bei einer anderen Stelle erforderlich ist, innerhalb der Gemeinde weitergegeben werden. Obwohl automatisierte Abrufverfahren als regelmäßige Datenübermittlungen anzusehen sind, deren Zulässigkeit bei Meldedaten gemäß § 29 Abs. 5 ThürMeldeG stets an eine besondere gesetzliche Ermächtigung ge-

bunden ist, handelt es sich bei der Weitergabe von Meldedaten innerhalb der Gemeinde lediglich um ein Verfahren zur Datennutzung. Auf dieser Grundlage hatten auch zwei Städte zur Verwaltungsvereinfachung automatisierte Abrufverfahren für verschiedene Ämter eingerichtet, durch die einige wenige, konkret benannte Mitarbeiter zur Erfüllung ihrer dienstlichen Aufgaben den Zugriff auf einen „eingeschränkten Meldedatensatz“ (wie Name, Vorname, Geburtsdatum, Titel, letzte bzw. aktuelle Anschrift) erhielten. Der Zugang zu den Daten war mitarbeiterbezogen passwortgeschützt, sodass ein Zugriff Unbefugter ausgeschlossen werden konnte. Protokollierungen der Zugriffe erfolgten nicht. Insoweit ließ sich im konkreten Fall auch der Vorwurf, dass von für dienstliche Aufgaben befugten Mitarbeitern unzulässigerweise Zugriffe auf Meldedaten für private Zwecke erfolgt waren, anhand von Protokollierungen nicht überprüfen. Mit Inkrafttreten des novellierten ThürDSG gelten nunmehr die bisherigen Vorgaben für die Einrichtung automatisierter Abrufverfahren auch dann, wenn das automatisierte Abrufverfahren nur innerhalb einer Daten verarbeitenden Stelle eingerichtet wird (§ 7 Abs. 6 ThürDSG). Demzufolge muss jede speichernde Stelle gewährleisten, dass die Zulässigkeit der Weitergabe oder Übermittlung personenbezogener Daten mittels eines automatisierten Abrufverfahrens zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Im Ergebnis der Prüfung des TLfD wurden deshalb auch die betreffenden Kommunen aufgefordert, ihre automatisierten Abrufverfahren den neuen gesetzlichen Erfordernissen anzupassen.

5.2.8 Antragsformular zur Freistellung vom Wehrdienst

In der Verwaltung ist es bei standardisierten Verfahren zur Erhebung von erforderlichen Daten zweckmäßig und üblich, Formulare zu verwenden. Dazu werden überwiegend die von einschlägigen Verlagen angebotenen Vordrucke genutzt. Häufig wird dabei gerade die föderale Struktur der Bundesrepublik vergessen, die bei einer Gesetzgebungskompetenz der Länder unterschiedliche Regelungen für die Zulässigkeit der Erhebung personenbezogener Daten erlaubt. Wird zu spät festgestellt, dass der mit den Formularen erhobene Datenumfang das zur Aufgabenerfüllung zwingend erforderliche Maß übersteigt oder die gesetzlich geforderten Hinweise über die

Rechtsgrundlagen für die Datenverarbeitung, die Zweckbestimmung der Daten sowie mögliche Angaben über vorgesehene Datenübermittlungen auf dem Vordruck fehlen, bedarf es in der Regel eines zusätzlichen Aufwandes bzw. weiterer Kosten, um die Rechtmäßigkeit der Datenerhebung wieder herzustellen (z. B. Vernichtung alter Vordrucke oder Druck zusätzlicher Hinweisblätter). Deshalb wird vom TLfD immer wieder empfohlen, vor der Entwicklung oder dem Kauf von Vordrucken deren Gestaltung und die Rechtmäßigkeit und Zulässigkeit der Datenerhebung gerade auch unter datenschutzrechtlichen Gesichtspunkten gewissenhaft zu prüfen. Selbstverständlich ist hierbei der TLfD auch bereit, die öffentlichen Stellen zu beraten.
So wandte sich in dieser Frage z. B. eine Stadtverwaltung an den TLfD, mit der Bitte um Prüfung eines auf den ersten Blick günstigen Angebotes für einen Vordruck zur Unabkömmlichkeitsstellung von Arbeitnehmern der gewerblichen Wirtschaft. Es handelte sich dabei um einen Antrag gemäß § 13 WPflG, wenn für einen Wehrpflichtigen zum Ausgleich des personellen Kräftebedarfs für die Aufgaben der Bundeswehr und andere Aufgaben im öffentlichen Interesse für den Wehrdienst unabkömmlich gestellt werden soll. Grundlage für die datenschutzrechtliche Prüfung war in diesem Fall ein Rundschreiben des TIM zur Verordnung der Landesregierung zur Durchführung der Verordnung über die Zuständigkeit und das Verfahren bei der Unabkömmlichkeitsstellung aus dem Jahr 1998. In einer Anlage zum Rundschreiben hatte man für die Landratsämter und kreisfreien Städte auch einen mit den Kreiswehrersatzämtern und dem Bundesamt für Zivildienst, der Wehrbereichsverwaltung VII und dem Thüringer Wirtschaftsministerium abgestimmten Musterantrag zur Unabkömmlichkeitsstellung von Wehrpflichtigen veröffentlicht. Nach Rücksprache mit dem TIM wurde nochmals bestätigt, dass der in diesem Muster enthaltene Datenkatalog zur ordnungsgemäßen Bearbeitung entsprechender Anträge ausreicht und insoweit als abschließend betrachtet wird. Jede darüber hinaus gehende Datenerhebung wäre somit gemäß § 19 ThürDSG unzulässig. Da der Umfang der Erhebungsmerkmale in dem vom Vordruckverlag angebotenen Formular ein Mehr gegenüber dem Muster des TIM auswies, konnte deshalb nur von einer Bestellung des angebotenen Vordrucks aus datenschutzrechtlichen Gründen abgeraten und statt dessen das Kopieren des vom Innenministerium veröffentlichten Antragsmusters empfohlen werden.

5.2.9 Datenschutz in Kommunalvertretungen

Anfragen aber auch Beschwerden zum Umgang mit personenbezogenen Daten in Kommunalvertretungen beschäftigten auch im Berichtszeitraum den TLfD. Sie betrafen insbesondere die Frage, ob und in welchem Umfang Gemeinderäte befugt oder gar verpflichtet sind, über bestimmte Verwaltungsangelegenheiten mit personenbezogenem Inhalt zu entscheiden. Das Problem bei der Beantwortung liegt dabei meist in der Schwierigkeit der Zuständigkeitsabgrenzung zwischen dem Bürgermeister und dem Gemeinderat. Nach § 22 und § 29 ThürKO ist der Bürgermeister für alle Angelegenheiten des übertragenen Wirkungskreises der Gemeinde zuständig und erledigt die laufenden Angelegenheiten des eigenen Wirkungskreises, während der Gemeinderat über alle Angelegenheiten des eigenen Wirkungskreises, die nicht zu den laufenden Angelegenheiten zu rechnen sind, die Entscheidungen trifft. Aufgrund dieser Regelungen ist eine allgemein gültige Vorgabe von Zuständigkeiten für jeden einzelnen Sachverhalt nicht möglich, da dies im besonderen Maße von der Gemeindegröße abhängig ist. Während in großen Städten die überwiegende Zahl von Anliegen der Bürger z. B. im Bauwesen als so genannte laufende Angelegenheiten ausschließlich von der Verwaltung bearbeitet und entschieden werden, nehmen diese Aufgaben in kleinen Gemeinden aufgrund der wesentlich größeren Auswirkungen einzelner Baumaßnahmen auf das Gemeindegebiet in der Regel die Gemeinderäte wahr. Dies führt aber zwangsläufig zu unterschiedlichen datenschutzrechtlichen Konsequenzen für die betroffenen Bürger. Erfolgt die Bearbeitung eines Anliegens (z. B. bei einem Bauantrag) in einer Stadt ausschließlich durch die Verwaltung, erhält davon regelmäßig nur ein kleiner Kreis zur Verschwiegenheit verpflichteter Mitarbeiter im Rahmen ihrer Aufgabenerfüllung Kenntnis, ggf. noch die unmittelbaren Nachbarn des Antragstellers als Verfahrensbeteiligte. Anders stellt sich dies bei einer Behandlung im Gemeinderat dar. Hier sind in der Regel die Sitzungen ebenso wie bei den Kreistagen gemäß § 40 ThürKO öffentlich, soweit nicht berechtigte Interessen Einzelner dem entgegenstehen. Die nicht öffentliche Sitzung soll somit eine Ausnahme sein, um dem demokratischen Grundsatz nach Transparenz der Tätigkeit und Willensbildung der gewählten Vertreter gegenüber ihren Wählern weitgehend Rechnung zu tragen.

Aufgrund dessen bedarf es stets in jedem Einzelfall einer verantwortungsbewussten Prüfung, d. h. einer umfassenden Abwägung der Interessen des Einzelnen nach Geheimhaltung seiner persönlichen Daten und dem Interesse der Gemeindebürger nach Teilnahme und Transparenz der Arbeit des Gemeinderates im Hinblick auf die Öffentlichkeit oder Nichtöffentlichkeit der Beratung. Entscheidend ist dabei letztlich aber nicht, dass ein überwiegendes öffentliches Interesse vorliegt, sondern, ob vom Betroffenen ein „berechtigtes“ Interesse am Ausschluss der Öffentlichkeit geltend gemacht werden kann. Dies ist keinesfalls nur bei der Behandlung von Personalangelegenheiten gegeben, sondern betrifft auch Anliegen, bei denen insbesondere die soziale oder wirtschaftliche Situation oder andere höchstpersönliche Fragen des Betroffenen zu erörtern sind. Darauf habe ich bei entsprechenden Anfragen hingewiesen. Es empfiehlt sich in diesem Zusammenhang - auch im Interesse der Transparenz und der Gleichbehandlung – zur Gewährleistung des Datenschutzes klare Festlegungen zur Abgrenzung von Zuständigkeiten zwischen Gemeinderat und Bürgermeister zu treffen. Zweckmäßig ist es hierzu konkrete Entscheidungskriterien für die Behandlung von Angelegenheiten in nicht öffentlicher Sitzung in der jeweiligen Hauptsatzung aufzunehmen. Ungeachtet dessen gilt es natürlich gleichzeitig, die in § 12 Abs. 3 ThürKO den Gemeinderats- oder Kreistagsmitgliedern obliegende Verschwiegenheitspflicht über alle Tatsachen, die nicht offenkundig sind oder ihrer Bedeutung nach einer Geheimhaltung bedürfen, was in der Regel auf alle personenbezogenen Daten zutrifft, konsequent und mit Nachdruck durchzusetzen. Dies betrifft nicht nur die unzulässigen Informationen Dritter, sondern auch die unzulässige Nutzung und Offenbarung von Informationen aus nicht öffentlichen Sitzungen in öffentlichen Beratungen.

5.2.10 Prüfung der Erforderlichkeit der Übermittlung von Grundstücks- und Erschließungskosten

Ein Einwohner einer Verwaltungsgemeinschaft erfuhr von seinem Nachbarn, dass dieser im Besitz einer Übersicht der Gemeindeverwaltung sei, die für jedes Grundstück des Wohngebietes die Erschließungskosten, die bisher geleisteten Zahlungen und eingereichte Klagen ausweist. Bei den weiteren Recherchen stellte sich heraus,

dass dieser Mitbürger die Liste als Verfahrensbeteiligter in einem Klageverfahren vom Gericht zur Kenntnis erhalten hatte.
Bei der folgenden Prüfung durch den TLfD zur Klärung des Sachverhaltes in der Verwaltungsgemeinschaft wurde festgestellt, dass dort die betreffende Liste rechtmäßig zur Aufgabenerfüllung erstellt und genutzt wurde. Sie diente dem Haushalt als Übersicht über die Zahlungsverpflichtungen und den Stand der Zahlungseingänge für die Grundstücks- und Erschließungskosten des von der Gemeinde verkauften Gemeindelandes für das neue Wohngebiet. Im Vorfeld der von einem Teil der Käufer der Grundstücke wegen der Höhe der Erschließungskosten angestrebten Gerichtsverfahren war die Verwaltungsgemeinschaft vom Gericht zur Übergabe einer Gesamtübersicht über alle offenen Forderungen, die im Zusammenhang mit dem Verkauf und der Erschließung des ehemaligen Gemeindelandes standen, aufgefordert worden. Nach § 99 VwGO sind Behörden zur Vorlage von Urkunden oder Akten und zu Auskünften gegenüber den Verwaltungsgerichten im Rahmen von Klageverfahren verpflichtet. Aus diesem Grund hatte die Verwaltungsgemeinschaft aus ihren Unterlagen die in Rede stehende Liste in Kopie dem Gericht übergeben, da sie auch die gewünschten Daten enthielt. Dabei war offensichtlich nicht berücksichtigt worden, den Umfang der Datenübermittlung auf das erforderliche (d. h. angeforderte) Maß zu beschränken. Dies umso mehr, da gemäß § 100 VwGO allen Verfahrensbeteiligten das Recht zusteht, in die Gerichtsakten und in die dem Gericht vorgelegten Akten einsehen zu können und sich daraus auch Ausfertigungen, Auszüge oder Abschriften erteilen zu lassen. Aufgrund dieser Vorschrift konnten somit alle Kläger bzw. im konkreten Fall die Nachbarn des Petenten oder deren Anwälte als Prozessbeteiligte bzw. deren Vertreter Kenntnis von dem Inhalt der vorgenannten Übersicht nehmen, die aber auch personenbezogene Daten von Dritten (Unbeteiligten) enthielt.
Während zur datenschutzrechtlichen Beurteilung der Erforderlichkeit für die Vorlage einer Gesamtübersicht beim Gericht und dem Umstand, dass das Gericht diese Übersicht zu den jeweiligen Gerichtsakten genommen hat, festzustellen ist, dass zur Wahrnehmung der richterlichen Unabhängigkeit vom Gesetzgeber ausdrücklich in diesen Fragen dem TLfD keine Zuständigkeiten übertragen worden sind, ist das Verhalten der Verwaltungsgemeinschaft kritisch zu bewerten. Zu prüfen war deshalb, ob vom Gericht eine Liste dieses Datenum-

fangs angefordert worden war bzw. ob von der Verwaltungsgemeinschaft im konkreten Fall bei der Ausübung eines möglichen Ermessensspielraums die Belange des Datenschutzes (Beachtung des Erforderlichkeitsgrundsatzes bzw. Übermaßverbot und Datensparsamkeit bei der Verarbeitung personenbezogener Daten) nicht im notwendigem Umfang berücksichtigt worden waren, da aus der Sicht der Verwaltungsgemeinschaft für den Zweck der Information des Gerichtes über die ausstehenden Gesamtforderungen eine Übersicht, beschränkt auf die Daten der Schuldner oder mit Schwärzungen bzw. Anonymisierungen der Daten der Unbeteiligten, ausreichend gewesen wäre. Dies konnte aber nicht mehr eindeutig geklärt werden, weil das Auskunftsersuchen vom Gericht gegenüber der Verwaltungsgemeinschaft nur mündlich vorgetragen worden war und dies auch dort in keiner Weise dokumentiert wurde.
Um künftig bei ähnlichen Vorgängen jeden Zweifel hinsichtlich eines vorliegenden Auskunftsersuchens auszuschließen, wurde im Ergebnis der Auswertung des Vorganges in der Verwaltungsgemeinschaft festgelegt, dass Auskunftsersuchen in Zukunft stets hinreichend dokumentiert werden und - soweit ein Ermessensspielraum besteht - der Umfang der Auskunftserteilung an Dritte auf das erforderliche Maß zu beschränken ist.

5.2.11 Web-Cam und Internetpräsentationen von Kommunen

Zunehmend wird das Internet als modernes Medium für Präsentationszwecke genutzt. Soweit dabei auch personenbezogene Daten veröffentlicht werden, sind die einschlägigen datenschutzrechtlichen Bestimmungen zu beachten. Hierbei gilt es besonders zu berücksichtigen, dass eine Internetpräsentation gegenüber bisherigen Formen von Veröffentlichungen einen permanenten, weltweiten und in seinen Dimensionen nicht abschätzbaren Zugriff auf die automatisiert recherchierbaren und im weiteren uneingeschränkt nutzbaren und diesbezüglich nicht mehr kontrollierbaren Daten ermöglicht. Darauf und auf die damit verbundenen besonderen Gefahren haben die DSB des Bundes und der Länder mehrfach in Publikationen (z. B. „Vom Bürgerbüro zum Internet“) hingewiesen. Um unzulässige Eingriffe in das informationelle Selbstbestimmungsrechts auszuschließen, bedarf es deshalb vor jeder Veröffentlichung personenbezogener Daten im

Internet einer gründlichen Prüfung hinsichtlich der Zulässigkeit und den sich aus der Offenbarung ergebenden möglichen negativen Folgen für die Betroffenen. Dies gilt auch dann, wenn die Daten ansonsten bereits oder zusätzlich in anderer Form öffentlich zugänglich gemacht wurden bzw. werden (z. B. in Amtsblättern, amtlichen Bekanntmachungen, durch Aushänge oder auch nur als Diskussionsbeitrag in einer öffentlichen Sitzung). Anfragen aus allen Bereichen zeigen aber nicht nur bestehende Unsicherheiten sondern insbesondere auch das große Interesse an dieser Problematik.
Eine Fragestellung von Kommunen beschäftigt sich in diesem Zusammenhang mit der Zulässigkeit der Nutzung von Web-Cams für Präsentationszwecke, da offensichtlich ein wachsendes Interesse von Gemeinden besteht, sich im Internet nicht nur durch statische Bilder sondern auch durch die Übertragung ständiger aktueller Ansichten aus dem Stadtgebiet oder von touristischen Anziehungspunkten mit Hilfe von Web-Cams weltweit bekannt zu machen. Beim Einsatz von Web-Cams zur Übertragung von Stadtansichten im Internet sollen lediglich Eindrücke der Stadt, insbesondere zur Werbung und Förderung des Tourismus vermittelt werden. Diesem Ziel entsprechend, besteht somit bei Präsentationszwecken keine Notwendigkeit für die Erhebung und Übermittlung personenbezogener Daten. Gemäß §§ 19 und 20 ThürDSG dürfen personenbezogene Daten von öffentlichen Stellen oder in deren Auftrag aber nur dann erhoben und verarbeitet (bzw. übermittelt) werden, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. Aufgrund dessen sind die Kommunen verpflichtet, bei der Bestimmung der Standorte für Web-Cams und deren Benutzung das Auflösungsvermögen und die Reichweite der Kameras, die Aufnahmezeiten und Bildfolgen sowie die Möglichkeit der Einflussnahme von Internetbenutzern auf den Inhalt von Aufnahmen zu berücksichtigen, um nicht erforderliche und somit unzulässige Eingriffe in das informationelle Selbstbestimmungsrecht durch die Übertragung personenbezogener Daten ohne Einwilligung der Betroffenen auszuschließen. Personenbeziehbar sind in diesem Zusammenhang letztlich alle Aufnahmen auf denen identifizierbare Personen oder ihnen aufgrund von Zusatzwissen eindeutig zuordenbare bewegliche Sachwerte (z. B. Fahrzeugkennzeichen, -beschriftung, Verkaufstand u. a.) abgebildet werden, aus denen man u.a. auch ableiten kann, ob und wann sich eine bestimmte Person an einem konkreten Ort aufgehalten hat. Ungeachtet der fehlenden Voraussetzungen für die Da-

tenerhebung ist in diesem Zusammenhang ansonsten auch zu berücksichtigen, dass selbst unter der Voraussetzung, dass die Videoaufnahmen zur Aufgabenerfüllung der Stadt benötigt und somit zulässigerweise erhoben würden, ihre Veröffentlichung im Internet mit personenbezogenem Inhalt nur unter den in § 23 Abs. 2 ThürDSG genannten Voraussetzungen erlaubt ist, da es sich um die weitreichendste Form einer Datenübermittlung (Veröffentlichung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes) handelt. Dies würde aber, soweit eine Einstellung im Internet lediglich zu Präsentationszwecken erfolgen soll, entsprechende Einwilligungen von den Betroffenen voraussetzen, was praktisch unmöglich sein dürfte.
Kompliziert wird es aus datenschutzrechtlicher Sicht mitunter auch, wenn sich mehrere Stellen gemeinsam im Internet präsentieren wollen. So bat mich z. B. im Berichtszeitraum ein Verein um Auskunft, welche Daten der Gemeindeverwaltung vom Verein gemeinsam mit der Gemeindeverwaltung im Internet präsentiert werden können. Hierzu habe ich mitgeteilt, dass zunächst die Frage zu klären wäre, wer künftig die Verantwortung für die Veröffentlichungen im Internet übernimmt, da letztlich für den Umgang mit personenbezogenen Daten für öffentliche und nicht-öffentliche Stellen unterschiedliche Rechtsvorschriften gelten. Ungeachtet dessen ist es in jedem Fall angeraten vor einer Veröffentlichung personenbezogener Daten die Einwilligung der Betroffenen einzuholen. Darüber hinaus ist zu berücksichtigen, dass Daten auch einen mittelbaren Personenbezug haben können, z. B. Angaben und Anschriften von Betrieben, die einzelnen Personen zuzuordnen sind (z. B. Handwerksbetrieb) deren Erhebung, Verarbeitung und Nutzung ebenso den Vorschriften des Datenschutzes unterliegen.

5.2.12 Erheben von Einkommensdaten zur Festlegung von Zuschüssen für einen Kindergartenplatz

Sowohl in der Vergangenheit als auch in der aktuellen Diskussion um das Heranziehen der Erziehungsberechtigten zu den Betriebskosten für Kinderkrippen, Kindergärten und Horte tauchen bei den Betroffenen Unsicherheiten über die Verhältnismäßigkeit der zur Beitragsveranlagung erforderlichen Unterlagen auf. Sofern eine soziale Staffelung vorgenommen werden soll, bedarf es sicherlich zur Überprüfung der Voraussetzungen für die Beitragseinstufung entsprechender

Nachweise. Allerdings ist damit auch ein Eingriff in das informationelle Selbstbestimmungsrecht der Erziehungsberechtigten verbunden, welcher normenklar zu regeln ist. Dies kann nicht ohne Weiteres allein durch den Landesgesetzgeber erfolgen, da die kommunalen Träger die soziale Staffelung sowie den zugrunde liegenden Einkommensbegriff in einer Satzung eigenverantwortlich regeln.

Im Falle des mir zugeleiteten Entwurfs einer Thüringer Hortkostenbeteiligungsverordnung (ThürHortkBVO) hatte ich darauf hingewiesen, dass hierin alle zur Aufgabenerfüllung benötigten Unterlagen konkret benannt und insbesondere auch die kommunalen Träger verpflichtet werden sollen, in ihren Satzungen genau festzulegen, welche personenbezogenen Daten zur Beitragsfestsetzung erhoben, verarbeitet und genutzt werden und welche Nachweise in welcher Form hierfür vorzulegen sind. In der ThürHortkBVO vom 12.02.2001 (GVBl. Nr. 2, S. 16-17) sind meine Vorschläge und Hinweise berücksichtigt worden, sodass Eltern und Träger darüber informiert sind, welche Daten erforderlich und welche Nachweise zu erbringen sind.

In dem o. g. Sinne nahm ich ebenfalls zum Entwurf einer Änderung des Kindertageseinrichtungsgesetzes Stellung und schlug konkret vor, in diesem Gesetz die kommunalen Träger hier ebenfalls zu verpflichten, in den Satzungen oder den vertraglichen Regelungen mit den Erziehungsberechtigten vorzugeben, welche personenbezogenen Daten zur Beitragsfestsetzung erhoben, verarbeitet und genutzt werden sollen und welche Nachweise dafür in welcher Form vorzulegen sind. Das TMSFG hat in diesem Zusammenhang eine Empfehlung über die Beteiligung der Eltern an den Kosten für die Betreuung von Kindern in Tageseinrichtungen veröffentlicht (ThürStAnz. Nr. 39/2001, S. 2012-2015), in dem die Träger auch beispielhaft darüber informiert werden, welche Unterlagen von den Erziehungsberechtigten in der Regel zum Nachweis des Einkommens vorzulegen sind, wobei auf die ThürHortkBVO Bezug genommen wird. Ob aus datenschutzrechtlicher Sicht die Träger in deren Satzungen diese Empfehlung zufrieden stellend umsetzen, wird die Praxis zeigen.

In einer Eingabe wurde ich darüber informiert, dass eine Gemeinde eine Richtlinie erlassen hatte, in der zur Festlegung des Zuschusses

für einen Kindertagesstättenplatz die hiervon betroffenen Erziehungsberechtigten verpflichtet worden waren, die Höhe ihres Einkommens durch Vorlage geeigneter Unterlagen zu belegen. Da aus datenschutzrechtlicher Sicht das Erheben personenbezogener Daten gemäß § 19 Abs. 1 ThürDSG nur zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist, muss der Stelle diese Aufgabe durch eine Rechtsvorschrift übertragen sein. Die vorliegende Richtlinie enthielt aber als Verwaltungsvorschrift keine Rechtsnorm, ist kein Gesetz im materiellen Sinne und für den außerhalb der Verwaltung stehenden Bürger nicht verbindlich. Eine soziale Staffelung nach dem Einkommen von Erziehungsberechtigten ist daher gemäß §§ 19, 20 Abs. 2, 21 ThürKO in einer kommunalen Satzung zu regeln.

5.2.13 Einbruch und Computerdiebstahl - Vorsorgemaßnahmen für den Datenschutz und zur Datensicherheit -

Gemäß § 9 ThürDSG haben öffentliche Stellen, die personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den Zugang und die Kenntnisnahme durch Unbefugte zu verhindern. Dabei soll der Aufwand für die Maßnahmen in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Dass hierbei stets Grenzbereiche erreicht bzw. festgelegt werden, ist daran zu sehen, dass trotz entsprechender Vorkehrungen Diebstähle von Datenverarbeitungsanlagen nie gänzlich ausgeschlossen werden können. Dennoch ist festzustellen, dass der ideelle Schaden mitunter durch Einhaltung einfacher datenschutzrechtlicher Grundregeln ohne weiteren Aufwand beim Diebstahl von Hardware minimiert werden kann. So stellte sich z. B. nach dem Diebstahl mehrerer Computer aus einem Sozialamt heraus, dass auf diesen noch Datenbestände gespeichert waren, die bereits zum Zeitpunkt des Diebstahls zur Aufgabenerfüllung des Sozialamtes nicht mehr benötigt wurden. Obwohl im Rahmen der Ermittlungen der Polizei keine Erkenntnisse erlangt wurden, dass Mängel bei den technischen Vorkehrungen zur Datensicherheit bestanden, wurden hinsichtlich der organisatorischen Maßnahmen zum Datenschutz nicht alle Möglichkeiten zur Verhinderung einer unbefugten Kenntnisnahme von Sozialdaten ausgeschöpft. Bei der Einhaltung der vom

Gesetzgeber vorgesehenen Speicherdauer wäre der Umfang der Sozialdaten, die Unbefugten zugänglich wurden, weitaus geringer gewesen, da gemäß § 67 SGB X das Speichern von Sozialdaten im Sozialamt nur zulässig ist, wenn diese zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgabe erforderlich sind. Für die überwiegende Zahl der gespeicherten Textdateien (Bescheide u. ä.) war aufgrund des bereits erfolgten Ausdrucks bzw. der Ablage der Unterlage in den jeweiligen Sachakten eine Erforderlichkeit für die weitere automatisierte Speicherung nicht mehr gegeben. Dies war nicht ausreichend berücksichtigt worden. Im Ergebnis des Vorfalls wurde deshalb eine entsprechende Regelung erarbeitet, wonach künftig die Speicherung der Daten aufgrund der Vernetzung nur noch - bis auf genehmigte Ausnahmefälle - auf dem zentralen und besonders gesicherten Server erfolgt. Durch die Einrichtung entsprechender Unterverzeichnisse auf dem Server wird dabei gewährleistet, dass nur dem jeweiligen Mitarbeiter die Daten zugänglich sind. Darüber hinaus wurde angewiesen, dass in der Regel Textdateien, die bereits ausgedruckt sind, mangels einer weiteren Erforderlichkeit für die Speicherung, zu löschen sind. Soweit Texte als Textbausteine oder Vorlagen noch genutzt werden sollen, ist zuvor jeglicher Personenbezug zu löschen.

Bei einem weiteren Fall wurde ebenso der Diebstahl zum Anlass genommen, die vorhandenen technischen und organisatorischen Regelungen zum Datenschutz und zur Datensicherheit zu überprüfen und im Ergebnis hier insbesondere neben dem künftigen Einsatz eines Wachdienstes die technischen Vorkehrungen für die Gewährleistung der Verschlusssicherheit weiter zu verbessern. Da die betreffende Stelle, die im Zusammenhang mit der durchgeführten datenschutzrechtlichen Kontrolle erbetenen Auskünfte und Stellungnahmen nur unzureichend bzw. erst nach mehrfachen Erinnerungen gab, sah ich mich veranlasst, dieses Verhalten wegen mangelnder Unterstützung des TLfD gemäß § 39 Abs. 1 ThürDSG zu beanstanden.

5.2.14 Unberechtigte Verweigerung der Auskünfte nach § 83 SGB X

Über einen längeren Zeitraum hatte eine Petentin vergeblich versucht, bei einem Sozialamt Einsicht in den über ihre Person erstellten

Sozialbericht des Allgemeinen Sozialen Dienstes zu erhalten. Begründet wurde diese Verweigerung vom Sozialamt mit § 25 Abs. 1 Satz 2 SGB X, wonach in Entwürfe zu Entscheidungen sowie in die Arbeiten zu ihrer unmittelbaren Vorbereitung kein Akteneinsicht durch den Verfahrensbeteiligten bestehe. Da es sich bei der Anfertigung von Sozialberichten durch den Allgemeinen Sozialen Dienst regelmäßig um solche Vorbereitung handele, sei die Einsichtnahme für den Verfahrensbeteiligten ausgeschlossen. Dabei hat jedoch das Sozialamt das Verhältnis von § 83 SGB X zu § 25 SGB X nicht richtig erkannt. Es ging davon aus, dass es sich bei § 25 SGB X um eine Spezialvorschrift zur Akteneinsicht handelt und im Übrigen wegen des eingeräumten Ermessens zur Auskunftserteilung kein Anspruch der Petentin auf Auskunft aus den beim Sozialamt geführten Akten besteht. Nach § 83 SGB X hat der Betroffene jedoch grundsätzlich einen Anspruch auf Auskunft über die zu seiner Person gespeicherten Sozialdaten, unabhängig davon, ob es sich um elektronisch gespeicherte Daten oder Daten in Akten handelt. Im Gegensatz zu § 25 SGB X kommt es dabei nicht auf die Betroffenheit in einem Verwaltungsverfahren an. Deshalb ist diese Vorschrift wesentlich weiter gefasst, als das Akteneinsichtsrecht nach § 25 SGB X. Eine Auskunftsverweigerung ist nur unter den in § 83 Abs. 4 SGB X dargelegten Gründen zulässig, wobei eine solche Auskunftsverweigerung nach § 83 Abs. 5 SGB X begründet werden muss. Den von der Petentin vorgelegten Unterlagen waren jedoch keine Anhaltspunkte dafür zu entnehmen, dass die Voraussetzungen für eine solche Auskunftsverweigerung vorliegen. Ich habe daraufhin das Sozialamt über meine Rechtsauffassung unterrichtet. Im Anschluss daran hat des Sozialamt der Petentin die begehrte Auskunftserteilung gewährt.

5.2.15 Datenerhebungen des Sozialamts beim Betroffenen haben Vorrang

Ein Petent, der einen Antrag auf Gewährung eines Darlehens zur Stellung einer Mietkaution nach § 15a BSHG bei einem Sozialamt gestellt hatte, wandte sich an mich, weil das Sozialamt sich ohne sein Wissen bei seinem künftigen Vermieter nach der Wohnung erkundigte, was nach seiner Auffassung dazu führte, dass er den Zuschlag für die Wohnung nicht bekommen hat. Bei der daraufhin durchgeführten Kontrolle im betreffenden Sozialamt stellt sich heraus, dass

sich eine Mitarbeiterin des Sozialamtes mit dem künftigen Vermieter telefonisch in Verbindung gesetzt hatte. Dies habe dazu gedient, über den Antrag wegen der besonderen Dringlichkeit rasch entscheiden zu können. Das ist nach meinen Feststellungen auch erfolgt, allerdings mit einem ungünstigen Ausgang für den Petenten. Die Mitarbeiterin des Sozialamts habe den Namen des Petenten nicht genannt, sondern sich lediglich als Mitarbeiterin des Sozialamts der betreffenden Stadt zu erkennen gegeben, dem ein Antrag auf Übernahme der Mietkaution für die vom Vermieter angebotene Wohnung vorliege. Daraufhin habe ein Mitarbeiter des künftigen Vermieters mitgeteilt, dass die Wohnung bereits vermietet worden sei. Dies nahm das Sozialamt zum Anlass, bei der anschließend erfolgten Vorsprache mit dem Petenten, den Kautionsantrag abzulehnen, da ein entsprechendes Mietobjekt offenbar nicht mehr verfügbar sei.

Aus datenschutzrechtlicher Sicht kann bei dieser Konstellation aber nicht von vornherein, wie vom Sozialamt vorgetragen, davon ausgegangen werden, dass keine Sozialdaten des Petenten unbefugt offenbart wurden. Bei einer Übermittlung ist es nämlich unerheblich, ob gegenüber dem Dritten der Name des Betroffenen genannt wird. Nach § 67 Abs. 1 SGB X sind Sozialdaten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Obwohl der Name des Petenten nicht genannt wurde, sind persönliche oder sachliche Verhältnisse einer bestimmbaren Person übermittelt worden. Die Bestimmbarkeit liegt dann vor, wenn die Person zwar nicht durch Daten allein (eindeutig) identifiziert wird, dies jedoch mit Hilfe anderer Informationen festgestellt werden kann. Hier meldete sich die Mitarbeiterin des Sozialamtes mit „Stadtverwaltung X“ und der Information, dass ein Kautionsantrag vorliegt. Daraus konnte bei verständiger Würdigung aus der Empfängersicht geschlossen werden, dass ein Wohnungsbewerber einen Antrag auf eine Sozialleistung zur Übernahme der Kaution gestellt hat. Dadurch, dass sich nur 4 Personen um die Wohnung beworben hatten und dies in einem anderen Bundesland erfolgte, konnte der künftige Vermieter mit überwiegender Wahrscheinlichkeit den Schluss ziehen, dass es sich um den aus Thüringen stammenden Petenten handelt. Nur wegen der theoretischen, aber wohl äußerst unwahrscheinlichen Möglichkeit, dass der Petent nicht der einzige Bewerber aus Thüringen und der Stadt X war und es mir aufgrund

meiner Zuständigkeit nicht möglich war, beim künftigen Vermieter Ermittlungen anzustellen, konnte letztlich die Bestimmbarkeit des Petenten bei der Anfrage nicht positiv festgestellt werden, obwohl dies überwiegend wahrscheinlich ist.

In jedem Falle lag jedoch ein Verstoß gegen die in § 67a Abs. 2 Satz 2 SGB X vorgeschriebene Pflicht zur Erhebung der Daten beim Betroffenen vor, der von mir beanstandet wurde. Zweck von § 67a Abs. 2 SGB X ist es, die erforderlichen Daten bei der Gewährung von Sozialleistungen grundsätzlich beim Betroffenen oder mit dessen Wissen zu erheben. Dabei werden durch die Mitwirkungspflichten der Empfänger von Sozialleistungen nach den §§ 60 ff SGB I auch die Interessen der Sozialleistungsträger gewahrt, indem der Betroffene verpflichtet ist, ihm zugängliche Informationen in Bezug auf die Gewährung von Sozialhilfe notwendigen Angaben vorzulegen. Das wäre im vorliegenden Fall sehr einfach dadurch möglich gewesen, dass der Petent vom Sozialamt aufgefordert worden wäre, vor Gewährung eines Darlehens einen abgeschlossenen Mietvertrag vorzulegen, was nicht erfolgt ist. Aufgrund meiner Beanstandung hat das Sozialamt seine Mitarbeiter dahingehend belehrt, dass die Antragsteller auf ihre Mitwirkungspflichten hinzuweisen sind und wenn diese nicht im zumutbaren und angemessenen Umfang erfolgen, eine Entscheidung über die Kautionsvergabe bis zur Nachholung der Mitwirkung ausgesetzt werden soll. Damit dürfte sich eine solche Fallkonstellation bei diesem Sozialamt wohl nicht wiederholen.

5.2.16 Speicherung von Kopien von Kontoauszügen der Sozialhilfeantragsteller

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, dass bei einem Sozialamt im Rahmen der Sozialhilfeantragstellung von den Antragstellern regelmäßig zur Überprüfung der wirtschaftlichen Verhältnisse die Kontoauszüge der letzten drei Monate verlangt wurden. Hiervon fertigte das Sozialamt Kopien und nahm sie zu den Sozialhilfeakten. Nach § 60 Abs. 1 SGB I ist derjenige, der Sozialleistungen beantragt, verpflichtet, alle Tatsachen anzugeben, die für die Leistung erheblich sind und auf Verlangen des zuständigen Sozialamts Beweisurkunden vorzulegen. Im Rahmen der Entscheidung über die Gewährung von Sozialhilfe ist auch die finanzielle Lei-

stungsfähigkeit und Bedürftigkeit des Antragstellers vom Sozialamt zu prüfen. Dies bedeutet, dass der Antragsteller geeignete Nachweise zu seiner finanziellen Situation vorzulegen hat. Kommt er diesen Verpflichtungen nicht nach, so kann nach § 66 Abs. 1 SGB I die Leistung ganz oder teilweise bis zur Nachholung der Mitwirkung versagt werden. Mit der Befugnis des Sozialamtes, sich die Kontoauszüge vorlegen zu lassen, ist jedoch nicht automatisch eine Zulässigkeit zur Speicherung dieser Daten durch Aufnahme von Kopien der Kontoauszüge in die Sozialhilfeakte verbunden. Dies wäre nach § 67c Abs. 1 SGB X nur dann zulässig, wenn es für die Erfüllung der jeweiligen Aufgabe erforderlich ist. Da jedoch die Kontoauszüge der letzten drei Monate in der Regel eine Vielzahl von Kontobewegungen enthalten, welche für die Feststellung des Sozialhilfebedarfs nicht relevant sind, ist eine solche Erforderlichkeit nicht von vornherein für alle Daten gegeben. Das betreffende Sozialamt hat mitgeteilt, dass zwar im Regelfall versucht werde, bereits bei der Antragstellung die vorgelegten Kontoauszüge auf deren Relevanz für das Sozialhilfeverfahren zu überprüfen und sich nur Kopien von denjenigen Kontobewegungen zu machen, die hierfür relevant sind, wobei den Antragstellern in diesen Fällen die Originalkontoauszüge sofort wieder mitgegeben werden. Allerdings sei diese Verfahrensweise nicht in allen Fällen möglich, sodass die angefertigten Kopien erst im Rahmen der nachfolgenden Prüfung ausgewertet und im erforderlichen Umfang zu den Sozialhilfeakten genommen werden können. Das Sozialamt hat daraufhin die Praxis dahingehend verändert, dass die Prüfung der Kontoauszüge der letzten drei Monate möglichst am Tag der Antragstellung bzw. am Tag des ersten Beratungsgespräches erfolgt. Weiterhin werden die Originalkontoauszüge dem Antragsteller am gleichen Tag, bei hohen Prüfungsaufwand, innerhalb der nächsten vierzehn Tage zurückgegeben. Neu ist, dass nur die notwendigen Kopien in der Sozialhilfeakte aufgenommen werden sollen, wobei nicht relevante Eintragungen sofort bzw. nach abgeschlossener Prüfung geschwärzt werden. Bei dieser Regelung gehe ich davon aus, dass sowohl dem berechtigten Anliegen des Sozialamtes zur umfassenden Prüfung der wirtschaftlichen Verhältnisse des Antragstellers als auch den datenschutzrechtlichen Gesichtspunkten des Antragstellers ausreichend Rechnung getragen wird.

5.2.17 Sozialdaten auf Überweisungsträgern

Bereits seit längerer Zeit bestanden Gespräche mit dem TMWFK zur Beschriftung von Überweisungsträgern bei Leistungen nach dem BAföG. Da die Betroffenen gemäß § 35 Abs. 1 SGB I Anspruch darauf haben, dass Sozialdaten von den Leistungsträgern als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden, bestand das Problem darin, dass bei einer eindeutigen Deklaration als Leistung zum BAföG die jeweiligen Geldinstitute zwangsläufig über diese Tatsache informiert wurden. Es bestand deshalb die Absicht, dass mit der Antragstellung für Bafög-Leistungen, die Betroffenen auch entscheiden sollten, ob die Überweisungsträger den Hinweis auf Bafög-Leistungen enthalten können. Nach längeren Diskussionen und Prüfungen zur Praktikabilität wurde von den beteiligten Stellen entschieden, dass seit November 2001 auf den Überweisungen von der Staatskasse nur noch ein Kassenzeichen eingetragen wird, aus dem der Betreffende den Grund der Zahlung anhand seiner Unterlagen entnehmen kann.

5.3 Sparkassen

5.3.1 Speicherung vollständiger Testamentskopien durch Sparkassen

In der Eingabe eines Bürgers beschwerte sich dieser darüber, dass die Sparkasse von ihm zur Klärung der Verfügungsberechtigung über das Konto eines Verstorbenen von der vorgelegten Testaments- und der Eröffnungsurkunde jeweils eine Kopie anfertigte und zu ihren Akten nahm. Gegen die Anfertigung einer Ablichtung der vorgelegten Dokumente bestanden meinerseits keine datenschutzrechtlichen Bedenken, ich wandte mich aber an den Sparkassen- und Giroverband Hessen-Thüringen mit dem Vorschlag, alle nicht zur Aufgabenerfüllung der Sparkasse erforderlichen personenbezogenen Daten in den Ablichtungen unkenntlich zu machen. Der Verband hält eine solche Verfahrensweise für nicht praktikabel, da im Vorhinein nicht abzuschätzen sei, welche Angaben im Testament ggf. im Falle von späteren Streitigkeiten hinsichtlich der Nachlassabwicklung bezüglich der Bankverbindung noch von Belang sein könnten. Dieser Argumentation konnte ich mich nicht verschließen, da der Verfügungsberechtigte im Regelfall gemäß Nr. 5 Sparkassen AGB einen Erb-

schein vorzulegen hat, der die zur Erfüllung der Geschäftszwecke der Sparkasse erforderlichen personenbezogenen Daten enthält und die Vorlage der Testaments- und Eröffnungsurkunde lediglich eine Ausnahme darstellt, die dem Verfügungsberechtigten eingeräumt werden kann.

6. Personalwesen

6.1 Personalakten im Justizbereich

Im 2. (6.5) und 3. TB (6.2) habe ich über die beanstandete Verwaltungsvorschrift des TJM zur Führung der Personalakten im Justizbereich zum Stand der Arbeiten berichtet. Inhalt der Beanstandung war, dass die Verwaltungsvorschrift nicht mit dem Thüringer Beamtengesetz (ThürBG) und dem Erforderlichkeitsgrundsatz im Einklang stand und für die Justizbediensteten mehrere vollständige Personalakten bei den jeweiligen Dienststellen im hierarchischen Aufbau vorschrieb. Über jeden Bediensteten darf aber nur eine Personalakte geführt werden. Erforderlichenfalls können Kopien von einzelnen Unterlagen als Nebenakten geführt werden. Mit der Verwaltungsvorschrift des Thüringer Justizministeriums vom 29. Oktober 2000 (3240-3/92) (JMBl. für Thüringen 2000, 50) hat das TJM die Verwaltungsvorschrift des TJM vom 01. Oktober 1992 über die Führung von Personalakten im Justizbereich aufgehoben. Seit 12. Dezember 2000 gibt es daher keine spezifischen Regelungen für den Justizbereich abweichend von der allgemeinen Personalaktenführungsrichtlinie mehr.

Im Rahmen einer durchgeführten Kontrolle aufgrund einer Beschwerde in einer Justizvollzugsanstalt (JVA) wurde Einsicht in die dort geführte Personalnebenakte genommen. Nach § 97 Abs. 2 Satz 3 ThürBG dürfen Personalnebenakten nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerfüllung der betreffenden Behörde erforderlich sind. Die eingesehene Personalnebenakte beinhaltete alle üblichen Unterlagen einer Personalakte, sodass es sich um ein Doppel der Personalakte handelte. Da sich aber die Aufgaben in einer JVA hinsichtlich der Personalverwaltung auf Einzelaufgaben beschränkt, enthielt sie somit Unterlagen, die für die Aufgabenerfüllung nicht erforderlich waren. Nicht erforderlich sind

Unterlagen, die der Behörde auf dem Dienstweg zur Kenntnis gegeben werden oder um deren Aushändigung an den Betroffenen gebeten wird. Nicht erforderlich sind auch Bewerbungsunterlagen die über den Dienstweg eingereicht werden, insbesondere, wenn diese Bewerbungen nicht erfolgreich waren. Begründet wurde die Aufnahme von früheren erfolglosen Bewerbungen damit, solche seien für die Erstellung von Bedarfsbeurteilungen und dem Vorschlagsrecht des Anstaltsleiters notwendig. Aus früheren Bewerbungen sei auch die Bereitschaft, Verantwortung zu übernehmen ersichtlich, sodass sie in die Personalakten aufgenommen werden müssten. Diese Darlegung konnte ich nicht akzeptieren. Zwar ist die Bewerbung Grundlage für die Bedarfsbeurteilung durch den Dienstvorgesetzten, eine Erforderlichkeit zur weiteren Aufgabenerfüllung und damit eine Zulässigkeit zur Abheftung in der Personalnebenakte ist daraus grundsätzlich nicht abzuleiten. Dass erfolglose Bewerbungen nicht zu den Personalakten und somit auch nicht zu Personalnebenakten genommen werden dürfen, wird auch aus der allgemeinen Personalaktenführungsrichtlinie (ThürStAnz. 1998 S. 1812 ff.) deutlich. Auch die Beteiligung des Personalrats nach § 75 ThürPersVG als Teil des Auswahlverfahrens rechtfertigt die Aufnahme der Unterlagen in die Personalakte nicht. Unterlagen über Vorgänge des Auswahlverfahrens gehören nach der Personalaktenführungsrichtlinie gerade nicht in die Personalakte.
Im Ergebnis hat das TJM per Erlass an die Leiter der Justizvollzugsanstalten verfügt, dass die durch erfolglose Bewerbungen entstandenen Unterlagen entsprechend Nr. 9 der Personalaktenführungsrichtlinie jedem Bewerber nach Abschluss des Auswahlverfahrens bzw. rechtskräftigem Abschluss etwaiger Folgeprozesse zurückzugeben sind.

6.2 Personalaktenführung in den Finanzämtern

Die OFD hat mir den Entwurf eines Erlasses zur Personalnebenaktenführung in den Finanzämtern zur Stellungnahme zugeleitet.
Die am 21.09.1998 in Kraft getretene Personalaktenführungsrichtlinie (ThürStAnz. 1998, 1812 ff) bestimmt in Ausführung des § 97 Abs. 2 Satz 3 ThürBG, dass Personalnebenakten nur geführt werden dürfen, wenn dies zu einer reibungslosen Personalverwaltung zwingend notwendig ist, weil mehrere personalverwaltende Behörden

für den Beamten zuständig sind oder weil die personalverwaltende Behörde nicht mit der Beschäftigungsbehörde identisch ist. Die Personalakten der Bediensteten in den Finanzämtern werden bei der OFD geführt. Es versteht sich von selbst, dass auch in den Finanzämtern, in denen die Betroffenen beschäftigt sind, Unterlagen vorhanden sein müssen, um die rechtmäßige Aufgabenerledigung sicherzustellen. In dem Entwurf eines Erlasses zur Führung von Personalnebenakten in den Finanzämtern wird konkret bestimmt, welche Unterlagen in den Personalnebenakten vorhanden sein dürfen. Neben Personalbogen mit Anlageblatt, Ernennungs-, Verwendungs- und Laufbahnvorgängen, Unterlagen zu Nebentätigkeiten, Urlaub, Arbeitszeitregelungen und Lehrgängen sind auch Beurteilungen und Disziplinarverfügungen, missbilligende Äußerungen sowie die Verhängung von Disziplinarmaßnahmen durch das Verwaltungsgericht zur Aufnahme in die Personalnebenakte festgelegt. Seitens der OFD wurde die Erforderlichkeit der Aufnahme von früheren Beurteilungen zur Erstellung von neuen Beurteilungen durch den Finanzamtsvorsteher als Erstbeurteiler sowie für den Personaleinsatz unter Berücksichtigung des Werdegangs und der Entwicklung der Betroffenen dargelegt. Zur Aufnahme von Disziplinarverfügungen, missbilligenden Äußerungen sowie die Verhängung von Disziplinarmaßnahmen durch die Verwaltungsgerichte wurde die Erforderlichkeit aufgrund der Zuständigkeit der Finanzamtsvorsteher in Disziplinarverfahren begründet. Diese Unterlagen sind allerdings nach Ablauf der Fristen nach § 119 BDO wieder zu entfernen. Sofern Bedienstete versetzt werden oder aus dem Dienst ausscheiden, sind konkrete Regelungen zur Übergabe der Unterlagen an die zuständigen Stellen getroffen worden. Der Entwurf stellt darüber hinaus klar, dass die Grundsätze auch für die Personalnebenakten der Angestellten und Arbeiter entsprechend anzuwenden sind.

6.3 Personalverwaltung der Lehrer

Wie bereits im 3. TB (6.3) berichtet, habe ich bei einem Kontrollbesuch im TKM die automatisierte Verarbeitung von Personaldaten der Lehrer überprüft. Im Ergebnis dessen hatte ich vom TKM die Erarbeitung eines Sicherheitskonzepts sowie die Schaffung grundlegender organisatorischer Regelungen zum Datenschutz und zur Datensicherheit gefordert. Dies wurde zwischenzeitlich realisiert, wobei die

von mir gegebenen Hinweise weitgehend Beachtung fanden. Aufgrund des nun im Bereich des TKM vorliegenden Sicherheitskonzepts sowie einer umfassenden Dienstanweisung zur Nutzung der Informationstechnik gehe ich davon aus, dass die zur automatisierten Verarbeitung der Lehrerpersonaldaten im TKM vom Gesetzgeber geforderten erforderlichen Maßnahmen zum Datenschutz und zur Datensicherheit getroffen sind. Unabhängig davon erfordert selbstverständlich der unaufhaltsame technische Fortschritt eine regelmäßige Überprüfung und ggf. Überarbeitung dieser Konzepte und Vorschriften.

Abgeschlossen wurde nunmehr (mit Ausnahme eines Schulamtes) die vorgesehene Übernahme der bisher bei den Landratsämtern aufbewahrten Personalakten der vor dem 03.10.1990 aus dem Schuldienst ausgeschiedenen Lehrer und Erzieher durch die staatlichen Schulämter.

Konkrete Eingaben und Beschwerden veranlassten den TLfD sich im Berichtszeitraum auch mit Fragen der Zulässigkeit eines Zugangs auf Personalunterlagen der Lehrer durch Personen, die nicht zur Personalverwaltung gehören, zu befassen. So hatte z. B. in einem Fall ein Schulamt den Schulleiter einer berufsbildenden Schule um personelle Unterstützung bei der Neuordnung von Personalakten im Schulamt gebeten. Wegen der Kurzfristigkeit des Auftrags und mangels eigener Kräfte hatte der Schulleiter einige „zuverlässige Schüler“ mit obiger Aufgabe betraut. Da einer Kenntnisnahme von Personaldaten bei diesen Arbeiten nicht ausgeschlossen werden konnte, hatte man die Schüler vorsorglich zur Verschwiegenheit verpflichtet. Dennoch handelte es sich um einen Verstoß gegen § 97 Abs. 1 Satz 1 und Abs. 3 ThürBG, da das Schulamt als personalaktenführende Stelle verpflichtet ist, seine Personalakten vertraulich zu behandeln und sie vor unbefugter Einsichtnahme zu schützen. Demzufolge dürfen nur diejenigen Personen Zugang zu Personalaktendaten erhalten, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Dabei bleibt es bei der datenschutzrechtlichen Bewertung unbeachtlich, dass die beauftragten Personen auf das Datengeheimnis verpflichtet waren. Insbesondere bei den eingesetzten Schülern lief eine solche Verpflichtung ohnehin ins Leere, da bei Verstößen gegen die Schweigepflicht weder eine disziplinarische Maßnahme eingeleitet

werden kann noch ein Verstoß gegen arbeitsrechtliche Pflichten begründet wird. Bereits in seiner Stellungnahme hat mir das zuständige Schulamt mitgeteilt, dass der Sachverhalt unter Mitwirkung der beteiligten Personen im Staatlichen Schulamt unverzüglich ausgewertet worden war und die gegebenen Hinweise zukünftig beachtet werden.

6.4 Akteneinsichtsrecht des Bediensteten

Aus Anlass der Eingabe eines Lehrers, der sich bei mir darüber beschwerte, dass das TKM ihm die Einsicht in alle über ihn geführten Unterlagen nicht gewährt habe, führte ich eine Kontrolle im TKM durch, da dieses zunächst an der Auffassung festhielt, wonach der Bedienstete zwar ein Recht auf Einsicht in seine vollständige Personalakte hat (§ 100 Abs. 1 ThürBG bzw. § 13 Abs. 1 BAT-O), nicht jedoch in die Personalakte aufgenommene Schriftstücke, die „Sachvorgänge“ seien. Zum angekündigten Kontrolltermin erklärten die Vertreter des TKM, dass der Petent zwischenzeitlich in alle ihn betreffenden Unterlagen Einsicht nehmen konnte. Im Ergebnis der Kontrolle verwies ich das TKM zunächst auf § 100 Abs. 4 ThürBG, wonach Beamte ein Recht auf Einsicht auch in andere Akten haben, die personenbezogene Daten über sie enthalten und für deren Dienstverhältnis verarbeitet oder genutzt werden, soweit gesetzlich nichts anderes bestimmt ist. Zu beachten ist hierbei, dass in der Praxis beamtenrechtliche Vorschriften auch beim Umgang mit Personalakten von Angestellten entsprechende Anwendung finden. Insoweit besteht auch bei den geprüften „Sachvorgängen“ ein Einsichtsrecht für den Betroffenen. Sofern bestimmte Unterlagen für das Dienstverhältnis nicht relevant sind, hat die Daten verarbeitende Stelle gemäß § 13 Abs. 1 ThürDSG dem Betroffenen auf Antrag Auskunft über die zu seiner Person verarbeiteten Daten zu erteilen. Zur Vermeidung des Entstehens von Aktendoppel oder der zeitweisen Herausnahme von Unterlagen aus der Personalakte wird das TKM in den Fällen, in den sich das TKM vorbehält, eine eigene Sachentscheidung zu treffen, zukünftig die gesamte Akte beim Schulamt als personalaktenführende Stelle anfordern und nach Abschluss der getroffenen Sachentscheidung dorthin zurückgeben. Hiergegen bestehen aus meiner Sicht keine Bedenken. Das TKM schloss sich meiner Auffassung an, wonach die in Personalakten eingefügten Prozessunterlagen hieraus zu

entfernen und der im Prozessregister geführten Prozessakte zuzufügen sind. Abschließende Urteile sind nur dann in die Personalakte aufzunehmen, wenn diese für das Dienstverhältnis von Bedeutung sind. Darüber hinaus ist nach meiner Auffassung dem Bediensteten in entsprechender Anwendung des § 100 Abs. 4 ThürBG in der Regel Einsicht in seine Prozessakte zu gewähren, da diese personenbezogene Daten über ihn enthalten und für sein Dienstverhältnis verarbeitet oder genutzt werden. Eine Ausnahme vom Einsichtsrecht in Prozessakten für die Dauer des Verfahrens aus prozesstaktischen Überlegungen kann § 100 Abs. 4 ThürBG nicht entnommen werden. Weiterhin empfahl ich, von Bediensteten im Schriftverkehr beigefügte Unterlagen, die für die Aufgabenerfüllung nicht erforderlich sind, zur eigenen Entlastung an diese zurückzugeben. Abschließend bat ich das TKM, dessen „Dienstanweisung zur Schriftgutverwaltung“ in verschiedenen Punkten zu überarbeiten und insbesondere auf das den Bediensteten zustehende Auskunfts- und Einsichtsrecht hinzuweisen. Die Dienstanweisung zur Schriftgutverwaltung wurde entsprechend meinen Empfehlungen geändert.

6.5 Beihilfebearbeitung

Wie bereits in den bisherigen Berichtszeiträumen spielte auch in diesem Berichtszeitraum die Thematik des Datenschutzes bei der Beihilfebearbeitung eine Rolle (1. TB, 6.2.3; 2. TB, 6.1.6; 3. TB, 6.4). In einer größeren Kommune wurde das Verfahren der Beihilfebearbeitung einer datenschutzrechtlichen Kontrolle unterzogen. Dabei habe ich erneut feststellen müssen, dass die Abschottung der Beihilfestelle von der übrigen Personalverwaltung nicht in jedem Fall entsprechend den Vorgaben des § 98 ThürBG ausreichend gewährleistet ist. Die aus datenschutzrechtlicher Sicht ohnehin problematische Einordnung der Beihilfestelle in das Personalamt wurde in der Kommune dahingehend verschärft, dass durch fehlende schriftliche Regelungen zur Zuständigkeit und zur Unterschriftsbefugnis jederzeit die Gefahr bestand, dass Personen, die an Personalentscheidungen mitwirken, aufgrund ihrer Weisungsbefugnisse Zugriff auf Beihilfedaten erhalten konnten. Darüber hinaus entsprach die Verfahrensweise, dass der oberste Dienstvorgesetzte die Entscheidung im Widerspruchsverfahren traf, gleichzeitig aber an Personalentscheidungen beteiligt ist, nicht dem vom Gesetzgeber vorgesehenen Trennungsge-

bot. Um mögliche Konfliktsituationen auszuschließen, wurde deshalb empfohlen, die Beihilfestelle, soweit möglich, organisatorisch außerhalb des Personalamtes einzuordnen. Desweiteren sollte durch eine entsprechende Regelung festgelegt werden, dass auch die abschließende Bearbeitung von Widersprüchen in Beihilfeangelegenheiten ausschließlich von Beschäftigten erfolgt, die an keinen Personalentscheidungen mitwirken. Im Ergebnis meiner Forderungen und Hinweise wurde deshalb in der betreffenden Stelle die Fachaufsicht, die Unterschriftsbefugnis und die Schlüsselordnung dahingehend geändert, dass ein Zugang von Personen, die an Personalentscheidungen mitwirken, zu den Unterlagen der Beihilfebearbeitung nunmehr ausgeschlossen werden kann. Die Bearbeitung von Widersprüchen wurde dem Rechtsamt übertragen. Darüber hinaus wurden auch bisher fehlende schriftliche Regelungen zum Umgang mit Beihilfeunterlagen, zur Verschlusssicherheit der Räume und zur Postbearbeitung und zur Aufbewahrungsdauer von Beihilfeunterlagen getroffen.

Es gibt aber auch andere Verfahrensweisen bei der Beihilfeverarbeitung durch Kommunen. Wie ebenfalls im 3. TB (6.4) dargestellt, lässt ein großer Teil Kommunen ihre Beihilfebearbeitung durch private Versicherungsunternehmen durchführen. Eine entsprechende Rechtsgrundlage dafür existiert nicht. Nach einem Gespräch hierüber hat das TIM auf Anregung des Thüringischen Landkreistags signalisiert, eine Änderung des Beamtenrechts in die Wege leiten zu wollen, wonach eine Übertragung der Beihilfebearbeitung auf private Dritte ermöglicht werden soll. Ein konkreter Gesetzentwurf liegt aber bislang noch nicht vor. Um für den Zeitraum, bis eine solche Änderung in Kraft getreten ist, die Datenschutzrechte der Betroffenen sicherzustellen, hat der Thüringische Landkreistag in Zusammenarbeit mit dem Versicherungsunternehmen eine Zusatzvereinbarung empfohlen, mit der sich das Unternehmen verpflichtet, bei der Verarbeitung und der Nutzung personenbezogener Daten die Vorschriften des ThürDSG zu beachten. Der Entwurf wurde mir vorab zur Abstimmung zugesandt und sodann den Landkreisen und parallel auch den Kommunen zur Unterzeichnung empfohlen. Nach Auskunft des Versicherungsunternehmens haben ca. 390 Kommunen diese Zusatzvereinbarung unterzeichnet, sodass auf diesem Wege für eine Übergangszeit zumindest den Grundforderungen des TLfD entsprochen wurde.

6.6 Was hat der Personalrat bei der Beratung durch Außenstehende in Personalratsangelegenheiten zu beachten?

Aufgrund von Zweifeln an der Rechtsauffassung der Dienststellenleitung hatte der Personalrat einer Behörde beschlossen, einen unabhängigen Rat einzuholen. Hierzu sollte das Angebot einer einschlägigen Fachzeitschrift, die in ihrem Ratgeberteil dafür warb, genutzt werden. Entsprechend dem Beschluss des Personalrats wurde die Problemstellung mit der Bitte um eine rechtliche Bewertung an die Zeitschrift übermittelt. In der Anlage des Schreibens hatte man zur Darstellung des Sachverhalts Kopien behördeninterner Schreiben beigefügt, die zwangsläufig, da die Fragestellung Personalangelegenheiten betraf, eine Vielzahl von Mitarbeiterdaten enthielten. Diese hatte man nur insoweit „anonymisiert", dass die Namen der betreffenden Bediensteten geschwärzt waren. Begründet wurde dies damit, dass nach Auffassung des Personalrats für die detaillierte Sachverhaltsdarstellung ein berechtigtes Interesse vorlag, dem kein überwiegendes schutzwürdiges Interesse der Betroffenen gegenüber gestanden habe. Darüber hinaus war man davon ausgegangen, dass die Übermittlung der Daten nur zur Einholung eines Rechtsrates und nicht für die Veröffentlichung vorgesehen war und die für den Ratgeberteil der Zeitschrift verantwortliche Person durch ihre Tätigkeit ohnehin zur Verschwiegenheit verpflichtet sei.
Diese Auffassung des Personalrats teilten die Dienststelle und die Betroffenen nicht und baten deshalb den TLfD um eine datenschutzrechtliche Bewertung. In meiner Stellungnahme habe ich zunächst deutlich gemacht, dass die Annahme, durch Schwärzung von Namen wird bereits eine ausreichende Anonymisierung personenbezogener Daten erreicht, nicht zutrifft. Aufgrund der im konkreten Fall übermittelten Vielzahl personenbeziehbarer Merkmale, wie Amtsbereiche, Aufgabengebiet, konkrete Beschäftigungszeiten und Abschlüsse war es durchaus möglich, die Daten mit entsprechendem Zusatzwissen (z. B. durch Telefonverzeichnisse, durch telefonische Auskünfte oder Besuche u. a.) konkreten Bediensteten der Behörde zuzuordnen. Gemäß § 3 ThürDSG sind personenbezogene Daten nicht nur Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten sondern auch einer bestimmbaren natürlichen Person. Dar-

unter fallen auch nicht nur Daten, an deren Geheimhaltung der Betroffene ein Interesse zeigt, sondern jedwede Angabe zu einer natürlichen Person. Insoweit ist es auch bei der Prüfung der Zulässigkeit der Übermittlung unerheblich, welche personenbezogenen Daten gegenüber Dritten offenbart werden. Hierzu bedarf es stets einer gesetzlichen Ermächtigung oder der Einwilligung des Betroffenen, es sei denn, die Daten können aus öffentlich-zugänglichen Quellen entnommen werden. Bestimmbar ist die Person, wenn ihre Identität mit Hilfe von verfügbaren Daten (Zusatzwissen) oder auch durch besondere Umstände hergestellt werden kann. Selbst wenn einzelne Unterlagen an sich genügend anonymisiert sind, ist stets zu beachten, dass bei der Zusammenführung von Daten aus verschiedenen Quellen und den sich daraus ergebenden neuen Informationen ein Personenbezug möglich werden kann. Anonymisieren ist gemäß § 3 ThürDSG das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand und Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Gerade im öffentlichen Bereich wird häufig zur Transparenz der Verwaltung Zusatzwissen (Behördenverzeichnisse, Namensschilder, Organigramme, Haushaltspläne u. ä.) an Dritte vermittelt, welches wie im konkreten Fall zur Zuordnung der personenbezogenen Daten beitragen kann. Aufgrund des Inhalts der im konkreten Fall an die Zeitschrift übersandten Unterlagen waren zweifelsfrei personenbezogene Daten übermittelt worden, wozu es, da keine schriftliche Einwilligung der Betroffenen vorlag, einer gesetzlichen Ermächtigung bedurft hätte. Soweit spezialgesetzliche Vorschriften den Umgang mit personenbezogenen Daten regeln, gehen diese den allgemeinen datenschutzrechtlichen Bestimmungen im ThürDSG vor. Für den Umgang mit Personaldaten, die dem Personalrat von der Dienststelle zur Aufgabenerfüllung zur Verfügung gestellt werden, gelten deshalb die Vorschriften des Thüringer Personalvertretungsgesetzes. Nach § 10 ThürPersVG haben Personen, die Aufgaben oder Befugnisse nach diesem Gesetz wahrgenommen haben oder wahrnehmen, über die ihnen dabei bekannt gewordenen Angelegenheiten und Tatsachen Stillschweigen zu bewahren. Eine Übermittlung von Daten zum Zweck einer unverbindlichen Rechtsberatung an Dritte ist danach nicht vorgesehen. Da die der Zeitschrift mitgeteilten Sachverhalte weder Angelegenheiten und

Tatsachen betraf, die offenkundig waren, noch Daten sind, die keiner Geheimhaltung bedürfen, handelte es sich um eine unzulässige Datenübermittlung. Dies bedeutet jedoch nicht, dass es damit den Personalräten verboten wäre, sich rechtlichen Rat zu holen. Es dürfen dabei nur nicht die geltenden datenschutzrechtlichen Bestimmungen unterlaufen werden. Im konkreten Fall wäre es bei Beachtung der Schweigepflicht möglich gewesen, in allgemeinster und anonymisierter Form ohne die Übersendung der Kopien und der Einzelangaben der Mitarbeiter, da diese hierfür nicht ausdrücklich ihre Einwilligung erklärt hatten, der Redaktion den Sachverhalt zu schildern und um eine rechtliche Würdigung zu bitten (sofern damit nicht gegen das Rechtsberatungsgesetz verstoßen wird). Dieses gebietet im Übrigen auch der datenschutzrechtliche Grundsatz der Erforderlichkeit und der Datensparsamkeit, der allen öffentlichen Stellen jede Datenübermittlung über das erforderliche Maß hinaus ausdrücklich verbietet. Hinsichtlich der Annahme des Personalrats bezüglich der bestehenden Schweigeverpflichtung des bei der Redaktion beschäftigten „Ratgebers“, war klarzustellen, dass die Übermittlungsvorschriften unabhängig von bestehenden Schweigeverpflichtungen gelten. Auch wenn der Empfänger einer solchen unterliegt, bedarf es zur Übermittlung personenbezogener Daten einer gesetzlichen Ermächtigung oder der Einwilligung des Betroffenen. Es gilt letztlich die Schweigepflicht auch unter Schweigeverpflichteten.

6.7 Umfang zu erhebender Personaldaten

Im Berichtszeitraum gab es wiederum Anfragen, welche Daten insbesondere im Bewerbungsverfahren von Betroffenen erhoben werden dürfen. Vom Grundsatz her gilt, dass von einer öffentlichen Stelle, wobei hierzu auch Wettbewerbsunternehmen nach § 26 ThürDSG zählen, nur die Daten erhoben werden dürfen, die für die Auswahl der Bewerber und zur Begründung des Dienstverhältnisses erforderlich sind. Dass ein Bewerber um eine Stelle im öffentlichen Dienst seinen Namen, seine Adresse, seinen Geburtstag, seinen Familienstand und auch seinen beruflichen Werdegang angeben muss, ist keine Frage. Mitunter werden aber auch Daten abverlangt, deren Erforderlichkeit zu hinterfragen ist. Das fängt schon mit dem Familienstand an. In einem Fragebogen für Bewerber, der mir zur datenschutzrechtlichen Würdigung zugeleitet worden war, sollte neben den

von mir als erforderlich angesehenen Angaben „ledig“ oder „verheiratet seit“ auch die Wiederverheiratung, die Angabe, ob jemand geschieden oder verwitwet ist mit der jeweiligen Datumsangabe eingetragen werden. Gründe hierfür sind nicht erkennbar. Daten des Ehegatten sind als Daten Dritter besonders sparsam zu erheben. Neben dem Geburtsnamen, Vornamen und Geburtsdatum dürfte beispielsweise nicht auch noch der Geburtsort oder ähnliches erhoben werden. Die Angabe, ob er im öffentlichen Dienst tätig ist, wird erst dann relevant, wenn es zu einer Einstellung kommt und die Bezahlung von Zuschlägen in Rede steht. Auch nach Kindern wird regelmäßig gefragt. Die Angabe zu Kindern ist auch nur dann erforderlich, wenn dies Auswirkungen auf die Vergütung haben sollte. Relevant ist aber nicht, ob es sich um ein leibliches Kind, Enkelkind, Geschwister und Pflegekind handelt, sondern nur, ob für eine der beschriebenen Personen vom Bewerber Kindergeld erhalten wird. Soweit die Bewerber gefragt werden, ob sie gesund und in der Lage sind, jede dienstliche Tätigkeit auszuüben, kann dies nur als persönliche Einschätzung verlangt werden. Dabei stellt sich zunächst die Frage des beabsichtigten Einsatzes. Bewirbt sich jemand auf eine bestimmte Stelle, dürfte wohl vorausgesetzt werden, dass man sich auch dahingehend einschätzt, in der Lage zu sein, diese auszufüllen.
Soweit man im Bewerbungsverfahren besondere Kenntnisse wie „Kurzschrift“, „Schreibmaschine“, „Kraftfahrzeug-Führerscheinklassen“, „Fremdsprachen“ oder sonstige Fähigkeiten erfragt, sollte dies auf die zu besetzende Stelle zugeschnitten sein.
Die Frage nach einer „Gebundenheit zum gegenwärtigen Dienstort“ setzt voraus, dass dies für das Dienstverhältnis erheblich ist. Die Angabe, bei welcher öffentlichen Stelle ein Bewerber früher mit welcher Vergütungsgruppe eingestellt wurde und wann Höhergruppierungen erfolgten, geht meines Erachtens über das erforderliche Maß hinaus. Es kann lediglich auf die letzte Eingruppierung ankommen. Zumal Höhergruppierungen immer von verschiedenen Faktoren abhängen können (Stellenplan, Haushaltsmittel etc.) sollte der Nutzen dieser Angaben hinterfragt werden. Wird bei einer Datenerhebung auf die Freiwilligkeit verwiesen, etwa zur Höhe der letzten Bruttobezüge, was in einem konkreten Fall damit begründet wurde, dies sei für die Ermittlung des zukünftigen Gehalts notwendig, sind die Voraussetzungen nach § 4 Abs. 2 und 3 ThürDSG oder § 4 a BDSG für eine wirksam erteilte Einwilligung zu beachten. Eine sol-

che Frage muss aber entfallen, wenn eine Vergütung tariflich gebunden ist. Bei Personalbögen von Bewerbern, die eingestellt werden, stellt sich bezüglich der weiteren Verwendung auch die Frage, ob der Bogen in die Personalakte eingeheftet werden soll. Soweit bei der Bewerbung personenbezogene Daten erhoben werden, die für das beabsichtigte Beschäftigungsverhältnis nicht erforderlich sind, ist darauf zu achten, dass diese nicht zur Personalakte gehören. In der Personalakte dürfen nur die für das Dienstverhältnis in unmittelbarem Zusammenhang stehenden Daten enthalten sein, wie es in der Personalaktenführungsrichtlinie (ThürStAnz. 1998, S. 1812 ff), deren Anwendung allen öffentlichen Stellen des Landes empfohlen ist, differenziert dargelegt wird.
In einem andern Fall ging es um die Frage, in welchem Umfang Personaldaten bei den unterschiedlichen Teilakten führenden Stellen erforderlich und zulässig sind. So wurde durch die personalaktenführende Stelle im Rahmen einer Überprüfung der gespeicherten Personaldaten unter Einbeziehung der Betroffenen u.a. die Bankverbindungsdaten, die Zahl der Kinder sowie die Angaben, ob der Ehegatte im Öffentlichen Dienst beschäftigt ist, erhoben, was zur Frage führte, ob hierfür eine Erforderlichkeit besteht. Dies war zu bejahen, da z.B. die Zahlung der Jubiläumszuwendung oder die Abrechnung von Reisekosten nicht von der Zentralen Gehaltsstelle sondern in der Personalverwaltung bearbeitet wird, sodass die hierfür erforderlichen Angaben auch dort erforderlich sind.

6.8 Entfernung eines Feststellungsbescheids nach § 4 Schwerbehindertengesetz (SchwbG) aus der Personalakte

Ein Petent wandte sich an mich mit dem Anliegen, ihm gegenüber seiner Beschäftigungsdienststelle behilflich zu sein, die Kopie eines Feststellungsbescheides nach § 4 SchwbG aus seiner Personalakte zu entfernen. Dieses Anliegen begründete der Petent damit, dass er zwar wegen zweier äußerlich nicht erkennbarer Krankheiten einen Feststellungsbescheid des Versorgungsamtes nach § 4 SchwbG über einen Grad der Behinderung (GdB) von 40 % erhalten habe. Die Schutzrechte des Schwerbehindertenrechts greifen jedoch bei einer Behinderung unterhalb eines Grades der Behinderung von 50 % nur dann ein, wenn ein so genannter Gleichstellungsbescheid nach § 2

SchwbG beantragt und erteilt wurde. Einen solchen Antrag hat der Petent jedoch nie gestellt, da seine Tätigkeit durch seine Behinderung nicht beeinträchtigt ist. Im Rahmen seiner Ausbildung wurde er von der Ausbildungsdienststelle um die Kopie des Bescheides nach § 4 SchwbG gebeten, die zu seiner Ausbildungspersonalakte genommen wurde. Nach Abschluss der Ausbildung sind seine Personalunterlagen einschließlich der Kopie des Feststellungsbescheides nach § 4 SchwbG in die neue Personalakte bei seiner Beschäftigungsdienststelle eingegangen. Seine Beschäftigungsdienststelle hat sich zunächst geweigert, diesen Feststellungsbescheid aus der Personalakte zu entfernen und ihm zu übergeben und dies mit der Fürsorgepflicht begründet.

Der einschlägigen Kommentierung der Beamtengesetze zum Umfang der Fürsorgepflicht ist jedoch zu entnehmen, dass eine Schwerbehinderteneigenschaft nur bei mindestens 50 % GdB oder bei einer nach § 2 SchwbG festgestellten Gleichstellung (30 bis 50 % GdB) zu Ansprüchen des Beamten nach den Grundsätzen der Fürsorgepflicht führt. Im Umkehrschluss ist jedoch davon auszugehen, dass sich aus einer Behinderung, die keine Schwerbehinderung im Sinne des Schwerbehindertengesetzes darstellt, keine Fürsorgepflichten des Dienstherrn abzuleiten ist. Daher ist der Einwand des Petenten, dass durch die Kenntnis der auf dem Feststellungsbescheid notierten ärztlichen Diagnosen die Gefahr besteht, dass bei künftigen Personalentscheidungen ihm diese möglicherweise zum Nachteil gereichen könnten, nicht ganz unbegründet. Entscheidend war jedoch, dass sich an die im Bescheid nach § 4 SchwbG bescheinigte Behinderung keinerlei rechtliche Konsequenzen für das Dienstverhältnis anknüpfte. Diese Rechtsauffassung habe ich der Beschäftigungsbehörde mitgeteilt. Diese hat in ihrer Stellungnahme darauf verwiesen, dass die Kopie des Feststellungsbescheides nach § 4 SchwbG aus der Ausbildungspersonalakte nur deshalb in die Personalakte übernommen worden sei, weil man irrtümlicherweise davon ausgegangen sei, dass ein Gleichstellungsantrag gestellt worden sei und ein Gleichstellungsbescheid nach § 2 SchwbG noch nicht vorliege. Im Anschluss daran wurde dem Petenten die Kopie des Feststellungsbescheides nach § 4 SchwbG ausgehändigt. Die Beschäftigungsdienststelle habe ich darauf hingewiesen, dass künftig sorgfältiger darauf zu achten sei, nur solche Nachweise über Schwerbehinderteneigen-

schaften in die Personalakten aufzunehmen, aus denen sich Rechtsfolgen für das Dienstverhältnis ergeben können.

6.9 Aufbewahrungsfristen für Personalakten der Angestellten

Die Aufbewahrung von Personalakten der Beamten ist in § 103 ThürBG geregelt. Mit Inkrafttreten der Personalaktenführungsrichtlinie für Beamte am 25.09.1998 wurden darin die gesetzlichen Vorgaben durch spezielle Verwaltungsvorschriften in Ziff. 3.5 und 8 zum Umgang und zu den Aufbewahrungsfristen von Personalakten der Beamten in Thüringen untersetzt. Wie in der Praxis festzustellen ist, besteht jedoch in vielen öffentlichen Stellen Unsicherheit über die Aufbewahrungsfristen für Personalakten der Angestellten. Aus diesem Grund erfolgte ein Meinungsaustausch mit dem für das Personalwesen sowie die Archivierung von Unterlagen zuständigen TIM. Im Ergebnis dessen wurde Einvernehmen darüber erzielt, dass für die Personalakten der Angestellten die beamtenrechtlichen Vorschriften sinngemäß anzuwenden sind. Das bedeutet, dass grundsätzlich die Personalakten der Angestellten nach Ausscheiden der Betroffenen aus dem öffentlichen Dienst weitere 5 Jahre aufbewahrt werden sollten. Den Besonderheiten in den neuen Bundesländern Rechnung tragend ist im Anschluss daran zu prüfen, ob in den Unterlagen noch Nachweise über Beschäftigungszeiten vor dem 03.10.1990 enthalten sind. Soweit dies zutrifft, der ehemalige Beschäftigte zu diesem Zeitpunkt das gesetzliche Rentenalter noch nicht erreicht hat und nicht bekannt ist, dass die Angaben bereits bei den Rentenversicherungsträgern vorliegen, sollte nach Ablauf dieser allgemeinen Aufbewahrungsfrist grundsätzlich unter Beachtung der Bestimmungen des § 16 ThürDSG von einer Vernichtung abgesehen werden, da Grund zur Annahme besteht, dass ansonsten schutzwürdige Interessen des Betroffenen beeinträchtigt werden könnten. Dies resultiert aus der Tatsache, dass für einen großen Teil der Beschäftigten bisher noch keine Kontenklärung mit den Rentenversicherungsträgern erfolgte und somit die Unterlagen teilweise noch zur Nachweisführung von Beschäftigungszeiten vor 1990 benötigt werden. Da diese Personalunterlagen aber nach Ablauf der 5–Jahres-Frist für Verwaltungsaufgaben nicht mehr benötigt werden, sind sie bis längstens zum Rentenalter des Betroffenen gemäß § 15 ThürDSG zu sperren. Eine Über-

mittlung von Daten daraus oder jegliche sonstige Nutzung ist dann ohne Einwilligung der Betroffenen nur noch zu den im Gesetz genannten Zwecken zulässig. Ungeachtet dieser allgemeinen Regeln für die Personalakten haben die öffentlichen Stellen steuer- und sozialversicherungsrechtliche Bestimmungen für die bei ihnen verarbeiteten Personaldaten zu beachten. Danach sind insbesondere die Lohnkonten gemäß § 41 EStG bis zum Ablauf des sechsten Kalenderjahres nach der zuletzt eingetragenen Lohnzahlung aufzubewahren. Lohnabrechnungsunterlagen, die für die Besteuerung von Bedeutung sind, müssen gemäß § 147 AO 10 Jahre aufbewahrt werden. Darüber hinaus sind die Aufzeichnungspflichten und die Nachweisführung der Beitragsabrechnungen für die Krankenpflege- und Rentenversicherung gemäß § 28 f SGB IV zu beachten.
Selbstverständlich unterliegen die Personalakten vor ihrer Vernichtung wie alle bei öffentlichen Stellen entstandenen Unterlagen auch der gemäß § 11 ThürArchivG festgelegten Anbietungspflicht bei den zuständigen Archiven. Diese haben zu prüfen, ob die jeweilige konkrete Personalakte aufgrund ihres rechtlichen, politischen, wirtschaftlichen, sozialen und kulturellen Wertes als Quelle für die Erforschung und das Verständnis von Geschichte und Gegenwart dauerhaft aufbewahrt werden muss. Wird im Ergebnis dessen die Archivwürdigkeit der Akte nach § 12 ThürArchivG festgestellt, gelten von diesem Zeitpunkt an für ihre weitere Benutzung die Bestimmungen für personenbezogenes Archivgut gemäß § 17 ThürArchivG.

6.10 Einsichtnahme des Personalrats in die Personalakte?

Von einer Personalvertretung wurde an mich die Frage herangetragen, ob und in welchem Umfang dem Personalrat Einsicht in Personalakten bzw. Bewerberunterlagen zur Erfüllung seiner Aufgaben nach dem Personalvertretungsgesetz gewährt werden darf. Dabei ist zwischen der Einsichtnahme in Personalakten nach § 68 Abs. 2 Satz 4 und die Auskunftserteilung nach § 68 Abs. 2 Satz 2 ThürPersVG zu unterscheiden. Eine Einsicht in Personalakten ist nach § 68 Abs. 2 Satz 4 ThürPersVG nur mit Zustimmung des Beschäftigten und nur von den von ihm bestimmten Mitgliedern der Personalvertretung zulässig. Auch bei den Aufgaben, in denen die Beteiligung des Personalrats nach § 68 Abs. 1 ThürPersVG ausdrücklich vorgesehen ist, darf der Dienststellenleiter dem Personalrat Einsicht

nur gewähren, wenn der Betroffene ausdrücklich zustimmt. Etwas anderes gilt bei der Frage nach der Auskunftspflicht nach § 68 Abs. 2 Satz 2 ThürPersVG, wonach der Personalvertretung die Unterlagen vorzulegen sind, die die Dienststelle zur Vorbereitung der von ihr beabsichtigten Maßnahmen beigezogen hat. § 68 Abs. 2 Satz 3 ThürPersVG beschränkt diese Vorlagepflicht bei Einstellungen auf Bewerbungsunterlagen einschließlich denen der Mitbewerber. Danach hat die Personalverwaltung das Recht, zur Durchführung der Aufgaben rechtzeitig und umfassend unterrichtet zu werden, was nach allgemeiner Auffassung auch das Recht beinhaltet, im Rahmen der umfassenden Unterrichtung Auskünfte aus der Personalakte durch den Dienststellenleiter zu erhalten, wenn diese Information für die Beschlussfassung der Personalvertretung erforderlich, d. h. für die Aufgabenerfüllung der Personalvertretung unerlässlich ist. Dabei ist allerdings stets darauf zu achten, dass durch die Auskunftserteilung nicht der vom Gesetzgeber als vorrangig angesehene Schutz der Persönlichkeitssphäre umgangen wird. Diese Auffassung habe ich der Personalvertretung mitgeteilt.

6.11 Bewerbungen per E-Mail

Im Berichtszeitraum war festzustellen, dass auch öffentliche Dienststellen in Stellenausschreibungen darauf verweisen, dass Bewerbungen per E-Mail zugesandt werden können. Dies ist aus Datenschutzsicht problematisch. Denjenigen, die von der Möglichkeit der Bewerbung per E-Mail Gebrauch machen wollen, muss die Möglichkeit eingeräumt werden, sich durch technische Maßnahmen gegen unbefugte Kenntnisnahme und Verfälschung zu schützen. Es wird allgemein davon ausgegangen, dass je nach Sensibilität der übertragenen Daten der erforderliche Schutz nur durch kryptographische Verfahren gewährleistet werden kann, die eine Ende-zu-Ende-Verschlüsselung ermöglichen. Zu derartigen Daten zählen insbesondere auch die Daten, die im Lebenslauf und in Zeugnissen im Rahmen von Bewerbungsunterlagen übermittelt werden. Wenn von der Möglichkeit der E-Mail-Kommunikation bei Stellenausschreibungen Gebrauch gemacht werden soll, muss der Interessent zum einen auf die mit einer unverschlüsselten E-Mail verbundenen Gefahren hingewiesen und ihm gleichzeitig die Möglichkeit eröffnet werden, Bewerbungen in verschlüsselter Form zu übermitteln. Die Landesre-

gierung hat zur Nutzung der elektronischen Post in den Ministerien und der Staatskanzlei in der gemeinsamen Geschäftsordnung ausdrücklich darauf hingewiesen, dass bis zum Vorliegen einer gesonderten verbindlichen Verfahrensweise, mit der Vertraulichkeit, Unversehrtheit und Authentizität der übermittelten Daten gewährleistet werden, auf die elektronische Übermittlung personenbezogener Daten zu verzichten ist.

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

Bereits in meinen vorangegangenen Tätigkeitsberichten (1. TB, 6.3.1; 2. TB, 6.7; 3. TB, 6.7) hatte ich auf eine ausstehende Verwaltungsvorschrift zum Umgang mit den Bezügeakten, die bei der OFD – Zentrale Gehaltsstelle – geführt werden, hingewiesen. In ihrer Stellungnahme zum 3. TB verwies die Thüringer Landesregierung darauf, dass die für die Schaffung der ausstehenden Verwaltungsvorschrift erforderliche Änderung des § 9 Abs. 3 des Thüringer Besoldungsgesetzes im Rahmen des 2. Änderungsgesetzes zum Thüringer Besoldungsgesetz vorgesehen sei. Nachfolgend wurde mitgeteilt, dass derzeit ein Referentenentwurf dieses Änderungsgesetzes vorbereitet werde. Im Hinblick auf die landesrechtliche Umsetzung der Novellierung der Leistungsbesoldung der Professoren hat mich das TFM wissen lassen, dass derzeit keine konkreten Angaben zum weiteren Verlauf des Gesetzgebungsverfahren gemacht werden können.

6.13 Versand von Lohnabrechnungen

Ein Beschwerdeführer hatte mitgeteilt, dass sich in dem für ihn bestimmten Umschlag mit seiner Lohnabrechnung auch die Lohnabrechnungen zweier anderer Kollegen der gleichen Verwaltungseinheit befanden. Damit erhielt er Kenntnis von personenbezogenen Daten anderer Beschäftigter.
Ich habe die zuständige ZG der OFD Erfurt um Sachverhaltsaufklärung gebeten. Die OFD teilte mit, dass bei einem nach Rekonstruktion des Verfahrensablaufes durchgeführten Testlauf die Kuvertierung

der Lohnabrechnungen ordnungsgemäß verlaufen ist. Es konnte auch nach Prüfung der Ursachen und Erörterung des Sachverhaltes mit den Mitarbeitern nicht nachvollzogen werden, welcher Umstand für die fehlerhafte Kuvertierung ursächlich gewesen ist. In Anbetracht dessen, dass der Vorfall ausgewertet und die Mitarbeiter auf ihre Sorgfaltspflicht hingewiesen wurden, um eine etwaige Wiederholung zu vermeiden, konnte von weiteren Maßnahmen abgesehen werden.

6.14 Verfahren bei Gehaltspfändungen

Wie bereits in meinem 3. TB (6.6) dargestellt, hatte ich mich gegenüber dem TFM für eine differenzierte Regelung der Benachrichtigung personalverwaltender Stellen durch die ZG der OFD bei Vorliegen von Gehaltspfändungen eingesetzt.
Vom TFM wurde bislang die Auffassung vertreten, dass unterschiedslos jeder Pfändungs- und Überweisungsbeschluss von der Bezügestelle der Personalverwaltung mitzuteilen sei um leichtfertiges Schuldenmachen zu erkennen. Demgegenüber bestand aus meiner Sicht kein Erfordernis dafür, jede zu vollstreckende Forderung der personalverwaltenden Stelle mitzuteilen, da bei einer einmaligen Pfändung in geringer Höhe im Regelfall nicht von einem leichtfertigen Schuldenmachen auszugehen ist. Daher habe ich vorgeschlagen, die personalverwaltende Stelle erst dann zu informieren, wenn

- die zu vollstreckenden Forderungen einen bestimmten Betrag überschreiten oder wenn
- innerhalb eines Jahres mehr als drei oder in drei aufeinander folgenden Kalenderjahren mindestens ein Pfändungs- und Überweisungsbeschluss bzw. eine Abtretung eingegangen ist.

Das TFM hat meinen Vorschlag aufgegriffen, sodass die Zentrale Gehaltsstelle künftig die personalführenden Dienststellen gemäß der vorgeschlagenen Verfahrensweise informiert.

6.15 Datenerhebungen im Rahmen von Fortbildungsveranstaltungen

Das TMSFG als Herausgeber einer Broschüre des gemeinsamen Fortbildungsprogramms 2001 bat mich zu einem vorgesehenen Antragsformular zur Anmeldung für Fortbildungsveranstaltungen im Bereich des TKM die darin enthaltenen datenschutzrechtlichen Hin-

weise zu überprüfen. Meine Änderungsvorschläge wurden vor der Veröffentlichung entsprechend eingearbeitet. Das Formblatt enthält nunmehr die erforderlichen Hinweis- und Aufklärungspflichten. Ferner sind die Angabe der privaten Telefon- und Faxnummer als freiwillig gekennzeichnet.

6.16 Kontrolle in einer Personalverwaltung

Im Rahmen einer Beschwerde wurde mir vorgetragen, dass eine Gemeinde, mit der der Beschwerdeführer im arbeitsgerichtlichen Streit lag, ein Schreiben bei der Thüringer Verwaltungsschule angefordert hatte. In diesem Schreiben hatte der Beschwerdeführer, der dort an einem Lehrgang teilgenommen hatte, seine gesundheitlichen und privaten Gründe dafür dargelegt, dass er nicht an der Abschlussprüfung teilnehmen werde. Im Rahmen der von mir durchgeführten Kontrolle stellte sich heraus, dass die Anforderung des Schreibens, die eine Datenübermittlung im öffentlichen Bereich zur Folge hatte, datenschutzrechtlich nicht zulässig war. Nach § 21 Abs. 1 in Verbindung mit § 20 ThürDSG ist eine Datenübermittlung nur dann zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelten oder des Empfängers liegenden Aufgaben erforderlich ist. Gleichzeitig müssen die Voraussetzungen vorliegen, die eine Nutzung nach § 20 ThürDSG zulassen, wobei nach § 21 Abs. 2 ThürDSG bei Übermittlung auf Ersuchen des Empfängers dieser die Verantwortung trägt. Die Anforderung des Schreibens war deshalb nicht erforderlich, da der Gemeinde schon vorher bekannt war, dass der Beschwerdeführer an der Prüfung nicht teilgenommen hatte. Es zeigte sich auch, dass die Personalaktenführungsrichtlinie des Landes, die den Gemeinden zur Übernahme empfohlen ist, nicht bekannt war und sich Originalschriftstücke, die in die Personalakte hineingehört hätten, sich in den Prozessakten befanden. Die Gemeinde hat mir mitgeteilt, dass die Personalakte entsprechend ergänzt wird. Weiter wurde der Empfehlung des TLfD gefolgt, einen behördeninternen DSB zu bestellen.

7. Polizei

7.1 Änderung des Polizeiaufgabengesetzes (PAG)

Gegen Ende des Berichtszeitraumes wurden Überlegungen zur Änderung des Polizeiaufgabengesetzes bekannt. Diese sahen die Erweiterung der Befugnisse der Polizei zur Fertigung von Videoaufzeichnungen, die nunmehr auch anlassunabhängig an öffentlich zugänglichen Orten möglich sein sollen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Straftaten verabredet, vorbereitet oder verübt werden sollen. Zu begrüßen ist die vorgesehene Verkürzung der Speicherfrist für polizeiliche Videoaufnahmen auf einen Monat. Auch ist nunmehr geplant, die gesetzlichen Voraussetzungen dafür zu schaffen, dass schon präventiv in bestimmten Fällen eine Datenerhebung durch Telekommunikationsüberwachung erfolgen kann. Ich habe hierzu die Auffassung vertreten, dass ein derartiger Eingriff höchsten Anforderungen hinsichtlich der Erforderlichkeit, Unausweichlichkeit und Verhältnismäßigkeit sowie Geeignetheit genügen muss, um einen Eingriff in das Grundrecht des Bürgers auf das Recht der Privatsphäre zu rechtfertigen. Unter bestimmten Voraussetzungen erscheint ein Eingriff in das geschützte Fernmeldegeheimnis im Zuge der Abwehr einer dringenden Gefahr für Leben, Gesundheit und Freiheit einer Person aus meiner Sicht vertretbar. Zwischenzeitlich wurde ein Gesetzentwurf in den Landtag eingebracht.

7.2 INPOL-neu

Im vorangegangenen Tätigkeitsbericht (3. TB, 7.5) habe ich zum Vorhaben INPOL-neu, welches das bisherige Verfahren INPOL ablösen soll, berichtet. Im Rahmen der vorgesehenen Neukonzeption des polizeilichen Informationssystems INPOL sollen neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank gespeichert werden. Die DSB haben zu INPOL zwei Entschließungen gefasst. Sie haben zum einen deutlich gemacht, dass inpolrelevante Delikte nur bei Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung vorliegen (Anlage 3). In einer weiteren Entschließung (Anlage 8) haben sie zum Ausdruck gebracht, dass eine dauerhafte zentrale Datenhaltung beim BKA die informationelle Trennung von Landesdaten und Verbunddaten aufweichen würde. Eine Betriebsaufnahme von INPOL-neu erfolgte im Berichtszeitraum nicht.

7.3 Polizeiliche Videoüberwachung der Erfurter Synagoge

Im Rahmen eines Vorortttermins informierte ich mich über die Installation von Videokameras zur Sicherung der Erfurter Synagoge, nachdem zuvor dort ein Brandanschlag versucht worden war. Die Einrichtung dieser Videoüberwachungsmaßnahmen durch die Thüringer Polizei stellte die erste derartige Maßnahme dar, bei der zur Sicherung eines nicht öffentlichen Gebäudes Kameras installiert wurden, deren Bilder in eine Polizeidienststelle übertragen werden. Die Konzeption ist vom LKA erstellt worden, für die praktische Durchführung liegt die Verantwortung bei der PD Erfurt. Die Aufzeichnungen von den Kameras erfolgen durch ein automatisiertes System, das nach einem festgelegten Zeitraum darauf angelegt ist, Aufzeichnungen zu überschreiben. In der PD Erfurt gehen die übertragenen Bilder von der Synagoge auf einem Monitor ein. Die Technik ermöglicht es, von Kamera zu Kamera zu schalten und auch zeitgleiche Ansichten aus allen Kameras wiederzugeben. Meiner datenschutzrechtlichen Bewertung habe ich allgemeine datenschutzrechtliche Grundsätze, wie sie in der Entschließung zu den Risiken und Grenzen der Videoüberwachung anlässlich der Datenschutzkonferenz am 14./15. März 2000 (Anlage 6) zum Ausdruck kommen, zugrunde gelegt. Das PAG trifft für Bildaufnahmen, zu denen auch Videoaufnahmen zu zählen sind, nur in § 33 eine Regelung. Diese betrifft Datenerhebungen bei öffentlichen Veranstaltungen und Ansammlungen soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung bestehen. Auch wenn im vorliegenden Fall keine öffentliche Veranstaltung oder Ansammlung vorliegt, gehe ich bei der datenschutzrechtlichen Bewertung aber davon aus, dass das Kriterium der tatsächlichen Anhaltspunkte die Annahme rechtfertigt, von Gefahren für die öffentliche Sicherheit oder Ordnung auszugehen, die den Einsatz der Videoüberwachung hier rechtfertigt. Meiner Forderung nach Schildern, die auf die Videoüberwachung durch die PD Erfurt hinweisen sowie nach einer Dienstanweisung zum Umgang mit der Technik kam die PD nach.

7.4 Videoaufzeichnungen bei Polizeieinsätzen

Zu Videoaufzeichnungen durch die Polizei erreichten mich im Berichtszeitraum auch Anfragen zur datenschutzrechtlichen Bewertung der Maßnahmen. In einem Fall ging es darum, dass Besucher eines Volksfestes auf einem baumbewachsenen Gelände von der Polizei aufgezeichnet wurden, ohne dass für diese eine polizeilich relevante Situation erkennbar war. Was der Petent nicht wissen konnte, war, dass es eine Unwetterwarnung gab und auf dem Gelände, auf dem sich die Besucher befanden, Gefährdung durch herabstürzende Äste und Bäume nicht ausgeschlossen werden konnte, sodass auch im Hinblick auf Folgeveranstaltungen durch die Videoaufzeichnungen Erkenntnisse gewonnen werden sollten. Von der Videoaufzeichnung habe ich mich persönlich überzeugt. Die Aufzeichnung wurde, wie dies nach § 33 Abs. 1 Satz 3 PAG vorgesehen ist, binnen einer Frist von 2 Monaten nach der Veranstaltung gelöscht. In einem anderen Fall lagen die Voraussetzungen nach § 33 Abs. 1 PAG vor, wonach die Polizei personenbezogene Daten durch Videoaufzeichnungen erheben kann, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit und Ordnung bestehen. Nach den mir gegenüber gegebenen Schilderungen konnte davon ausgegangen werden, dass die Voraussetzung für die Zulässigkeit von Videoaufzeichnungen vorlagen. Diese wurden ebenfalls innerhalb der 2-Monatsfrist gelöscht.

7.5 Verarbeitung von Polizeidaten in einem anderen Bundesland

Im vorangegangenen 3. TB (7.13) hatte ich die vorliegende Vereinbarung zur Verarbeitung von personenbezogenen Daten im Polizeibereich außerhalb des Freistaats Thüringen kritisiert. Dies betraf insbesondere die fehlenden Kontrollrechte des TLfD, was beanstandet wurde. Im Berichtszeitraum habe ich die Datenverarbeitung im LKA kontrolliert und Empfehlungen zu ergänzenden technischen und organisatorischen Maßnahmen ausgesprochen, deren Umsetzung zugesagt wurde. Zusammen mit dem Bayerischen Landesbeauftragten für den Datenschutz wurde die Auftragsdatenverarbeitung im Bayerischen LKA angesehen, wobei alle erbetenen Auskünfte erteilt wurden. Bezüglich der geänderten Fassung der Vereinbarung zur

Auftragsdatenverarbeitung wurde ich beteiligt und habe in diesem Zusammenhang einige Ergänzungsvorschläge unterbreitet.

7.6 Datenerhebungen im Zusammenhang mit dem Besuch eines hohen Staatsgastes

Im Zusammenhang mit dem Besuch des iranischen Staatspräsidenten in Weimar im Jahre 2000 kontrollierte der TLfD die vorgenommenen Datenerhebungen bei den betreffenden zuständigen Stellen und die diesbezüglich erfolgten Datenabgleiche dahingehend, ob die datenschutzrechtlich geltenden Bestimmungen eingehalten worden sind. Nach § 44 PAG kann die Polizei von öffentlichen oder nichtöffentlichen Stellen zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person die Übermittlung personenbezogener Daten bestimmter Personengruppen aus Dateien zum Zweck des Abgleichs mit anderen Datenbeständen verlangen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Abwehr der Gefahr erforderlich ist. Bei dem vorgesehenen Staatsbesuch wurde von der höchsten Gefährdungsstufe ausgegangen. Weiter war die Verfahrensweise bei Staatsbesuchen zu beachten, die in einer bundeseinheitlichen Dienstvorschrift festgelegt ist. Es wurde zur Sicherung der Fahrtstrecke und der Aufenthaltsorte des Staatsgastes in Weimar einer Überprüfung von Personen, die an dieser Strecke gemeldet waren, vorgenommen. Bei dieser Auskunftserteilung durch das Meldeamt ist § 29 Abs. 1 ThürMeldeG einschlägig. Im Rahmen der datenschutzrechtlichen Kontrolle wurde festgestellt, dass im Anschluss an den Polizeieinsatz zeitnah die Löschung personenbezogener Daten erfolgte. Datenschutzrechtliche Maßnahmen waren insoweit nicht erforderlich. Ich habe jedoch gegenüber dem TIM angeregt, bei einer Novellierung des PAG die Voraussetzungen für das Vorliegen einer Rasterfahndung im Gesetzestext zu präzisieren, da es sich dabei um einen maschinellen Abgleich automatisiert geführter Dateien handeln muss.

7.7 Umgang mit personenbezogenen Daten bei der Thüringer Polizei

Im November 1999 berichtete die Presse über vermeintliche Datenschutzverstöße der Arbeitsgruppe „Interne Ermittlungen“. So sollen Betroffene über die gegen sie in Gang gesetzten Verfahren nicht informiert, über unbescholtene Bürger Daten erhoben und gespeichert, Akten angelegt und entgegen der geltenden Richtlinie gelagert worden seien. Maßnahmen zur Herstellung des gesetzmäßigen Zustands in der Arbeitsgruppe waren seitens des TIM bereits angekündigt worden. In diesem Zusammenhang erfolgte eine Anfrage im TIM zum Sachverhalt und im Weiteren eine Vorortkontrolle gemäß § 37 ThürDSG.
Zu den Aufgaben der AG „Interne Ermittlungen“ zählen Ermittlungen zu Vorwürfen gegen Polizeibedienstete und Aufarbeitung der gewonnenen Erkenntnisse, damit bei der Bestätigung eines Anfangsverdachtes eine Abgabe an die Staatsanwaltschaft und ggf. die Einleitung von Disziplinarmaßnahmen erfolgen kann. Unterlagen, die nach den KAN-Richtlinien aufzubewahren sind, waren zwischenzeitlich in einen Stahlschrank verbracht und Prüflisten zur Vernichtung festgesetzt worden.
So weit Disziplinarunterlagen von verschiedenen Bediensteten noch nach Bekanntwerden der Probleme vorgefunden wurden, wurden diese nach Abschluss der Untersuchung an die jeweiligen Dienststellen zurückgeführt. Die Benachrichtigung von Dienstvorgesetzten über eingeleitete Ermittlungsverfahren und den Abstimmungen mit der Staatsanwaltschaft über den Ausgang des Verfahrens erfolgten. Die erforderlichen Regelungen und Festlegungen zum Umgang mit personenbezogenen Daten wurden getroffen.

7.8 Rasterfahndung

Nach den Terroranschlägen am 11. September 2001 wurde weltweit von einer erhöhten Gefahrenlage ausgegangen. Auch in Thüringen wurde eine Rasterfahndung durchgeführt. Rechtsgrundlage hierfür ist § 44 Abs. 1 PAG, wonach die Polizei von öffentlichen oder nicht öffentlichen Stellen zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zweck des Abgleichs mit anderen Datenbeständen verlangen kann, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass

dies zur Abwehr der Gefahr erforderlich ist. Eine derartige Maßnahme bedarf der Zustimmung des TIM. Auch ist der TLfD von der Maßnahme unverzüglich zu unterrichten, was seitens des TIM ebenfalls geschehen ist. Der TLfD kontrolliert die Verarbeitung der personenbezogenen Daten und die Einhaltung der gesetzlichen Bestimmungen in diesem Zusammenhang.

7.9 Terrorismusbekämpfung

Schon kurz nach den terroristischen Anschlägen in New York und Washington wurden Pläne der Bundesregierung bekannt, durch ein Gesetz zur Bekämpfung des internationalen Terrorismus zahlreiche Rechtsvorschriften zu ändern, die auch Auswirkung auf den Datenschutz haben. In einer eigens einberufenen Konferenz haben die DSB des Bundes und der Länder in einer Entschließung (Anlage 22) darauf hingewiesen, dass die effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz schon durch die geltende Rechtslage sichergestellt ist und Vollzugsdefizite kein Datenschutzproblem darstellen. Sie haben vor übereilten Maßnahmen gewarnt, die die Freiheitsrechte der Bürgerinnen und Bürger einschränken, aber keinen wirksamen Beitrag zur Bekämpfung des Terrorismus leisten, und sich dafür ausgesprochen, neue Eingriffsbefugnisse zu befristen und tief greifende Eingriffsbefugnisse einer ergebnisoffenen Erfolgskontrolle zu unterziehen. Zum 01.01.2002 trat das Terrorismusbekämpfungsgesetz in Kraft, durch das u. a. das Bundesverfassungsschutzgesetz insofern geändert wird, als das BfV nunmehr bei Kreditinstituten, Finanzleistungsinstituten und Finanzunternehmen im Einzelfall Auskünfte zu Konten, Kontoinhabern und sonstigen Berechtigten einholen kann, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist und tatsächliche Anhaltspunkte für schwer wiegende Gefahren für die Schutzgüter nach § 3 Abs. 1 Nr. 2 - 4 BVerfSchG bestehen. Unter den gleichen Voraussetzungen kann auch über Telekommunikationsverbindungs- und Nutzungsdaten Auskunft eingeholt werden. Ähnliche Befugnisse werden dem Bundesnachrichtendienst aufgrund der Änderung des BND-Gesetzes eingeräumt. Im Sicherheitsüberprüfungsgesetz des Bundes wurde der Kreis derjenigen erweitert, für die eine Sicherheitsüberprüfung durchzuführen ist. Das BKA hat nunmehr die Befugnis erhalten, zur Erfüllung seiner Aufgabe als Zentralstelle, Daten zur Ergänzung vorhandener Sachverhalte oder sonst zu

Zwecken der Auswertung mittels Auskünften oder Anfragen bei öffentlichen oder nicht öffentlichen Stellen erheben zu können. Das SGB X hat in § 68 eine Änderung dahingehend erfahren, dass nunmehr auch die Übermittlung der in Abs. 1 Satz 1 genannten Sozialdaten zur Durchführung einer nach Bundes- oder Landesrecht zulässigen Rasterfahndung ermöglicht. Große Aufmerksamkeit in der öffentlichen Diskussion erhielt der Vorschlag, Pass- und Personalausweis um biometrische Merkmale zu ergänzen und die Einzelheiten lediglich durch eine Rechtsverordnung festlegen zu lassen, um den Schutz vor Verfälschungen, Missbrauch und die eindeutige Identifizierung von Ausweisinhabern zu gewährleisten. In Art. 7 und 8 des Terrorismusbekämpfungsgesetzes ist nunmehr vorgesehen, dass die Einzelheiten durch ein Bundesgesetz zu regeln sind. Die DSB des Bundes und der Länder haben anlässlich ihrer 62. Datenschutzkonferenz (Anlage 28) auf die mit der Nutzung biometrischer Merkmale in Personalausweisen und –pässen verbundenen Folgeprobleme hingewiesen. Die Notwendigkeit und Zweckmäßigkeit für die Erhebung und Aufnahme derartiger biometrischer Merkmale in Personal- und Passdokumenten gelten nach wie vor als umstritten. Auch wenn den Bedenken der DSB folgend, im Gesetz ausdrücklich auf die Einrichtung einer zentralen Referenzdatei verzichtet wird, darf nicht übersehen werden, dass ein automatischer Abgleich der in den lokalen Referenzdateien gespeicherten Informationen mit weiter erhobenen biometrischen Daten möglich wird, sodass eine strikte Zweckbindung notwendig ist.

7.10 Vernichtung von erkennungsdienstlichen Unterlagen

Gegen einen Betroffenen wurde im Rahmen eines strafrechtlichen Ermittlungsverfahrens eine erkennungsdienstliche Behandlung durchgeführt. Dabei werden üblicher Weise Lichtbilder gefertigt, Fingerabdrücke abgenommen und weitere personenbezogene Daten erhoben. Nachdem das Ermittlungsverfahren von der Staatsanwaltschaft eingestellt worden war, weil die Ermittlungen nicht genügend Anlass zur Erhebung der öffentlichen Klage boten (§ 170 Abs. 2 StPO) wandte er sich an mich mit der Bitte um datenschutzrechtliche Überprüfung, ob die von ihm beantragte Vernichtung der erkennungsdienstlichen Unterlagen bzw. seiner Unterlagen zur erkennungsdienstlichen Behandlung, die ihm auch bestätigt worden war,

tatsächlich durchgeführt worden war. Die ordnungsgemäß protokollierte Vernichtung der in Frage kommenden Unterlagen auf Anweisung der zuständigen Staatsanwaltschaft wurde mir von der zuständigen Polizeidienststelle bestätigt. Dem Betroffenen konnte ich daher mitteilen, dass nach meinen Feststellungen die zu ihm gespeicherten personenbezogenen Daten gelöscht wurden.

8. Verfassungsschutz

8.1 Änderung des Verfassungsschutzgesetzes

Zusammen mit Änderungen im Polizeiaufgabengesetz wurden auch Änderungen zum Verfassungsschutzgesetz diskutiert. Zu den Aufgaben des LfV soll künftig auch die Beobachtung von Bestrebungen und Tätigkeiten der Organisierten Kriminalität zählen. Da die Bekämpfung organisierter Kriminalität zum Zuständigkeitsbereich der Polizeibehörden zählt, bedarf es hier normenklarer gesetzlicher Regelungen, die Zuständigkeiten zwischen Polizei und Verfassungsschutz eindeutig voneinander abgrenzen. Es reicht hier nicht aus, die erforderliche Koordinierung über Richtlinien vorzunehmen, wie dies der kürzlich in den Landtag eingebrachte Gesetzentwurf vorsieht. Dies habe ich schon in einer Stellungnahme zum Referentenentwurf deutlich gemacht. Zum vorgesehenen Umfang des verdeckten Einsatzes besonderer technischer Mittel in Wohnungen habe ich datenschutzrechtliche Bedenken geäußert und empfohlen, neue Eingriffsbefugnisse zu befristen.

8.2 Kontrolle im Thüringer Landesamt für Verfassungsschutz

Auf Grund einer vorliegenden Beschwerde führte der TLfD eine Kontrolle im TLfV durch. Dabei sollte auch festgestellt werden, welche Maßnahmen der Personalrat der Behörde zum Umgang mit seinen Unterlagen getroffen hat, um zu gewährleisten, dass Unbefugte keinen Zugang zu oder Zugriff auf seine Personalratsunterlagen nehmen können.
Der Personalrat ist Teil der öffentlichen Stelle des TLfV. Sofern nicht besondere Rechtsvorschriften wie bspw. das ThürPersVG vorgehen, gelten auch für den Personalrat die Vorschriften des

ThürDSG für die Verarbeitung personenbezogener Daten. Soweit personenbezogene Daten vom Personalrat automatisiert verarbeitet werden, ist § 34 ThürDSG zu beachten, indem für die Verarbeitung personenbezogener Daten eine vorherige schriftliche Freigabe erforderlich ist. Gemäß § 44 Abs. 2 ThürPersVG hat die Dienststelle im erforderlichen Umfang Räume, den Geschäftsbedarf und Büropersonal zur Verfügung zu stellen. Der TLfD hat im Rahmen der Kontrolle angeregt, dass der Personalrat unter Berücksichtigung datenschutzrechtlicher Vorschriften Festlegungen trifft, ob und in welchem Umfang zukünftig personenbezogene Daten automatisiert verarbeitet werden sollen. In diesem Zusammenhang sind geeignete technische und organisatorische Maßnahmen gemäß § 9 ThürDSG zur Gewährleistung von Datenschutz und Datensicherheit zu veranlassen. Im Rahmen der Stellungnahme zum Kontrollbericht des TLfD hat das TLfV mitgeteilt, dass sich der Personalrat dafür entschieden hat, innerhalb des internen Netzes durch die Einrichtung eines besonderen Kennworts zu gewährleisten, dass ausschließlich Personalratsmitglieder Zugriff auf Ihr Verzeichnis nehmen können. Damit war dem datenschutzrechtlichen Anliegen Genüge getan.

8.3 Sicherheitsüberprüfungsgesetz

Schon in den bisherigen Tätigkeitsberichten (1. TB, 8.1; 2. TB, 8.2; 3. TB, 8.2) hatte ich darauf verwiesen, dass für die Durchführung von Sicherheitsüberprüfungen in Thüringen eine gesetzliche Grundlage zu schaffen ist. Die Landesregierung hat mitgeteilt, dass sie meine Auffassung zur Notwendigkeit einer entsprechenden Rechtsgrundlage teilt. Im Berichtszeitraum wurde noch kein Gesetzentwurf vorgelegt.

9. Finanzen - Steuern

9.1 Föderales Integriertes Standardisiertes Computerunterstütztes Steuererklärung (FISCUS)

Wie ich im 3.TB (9.2) berichtet hatte, sollte auf der Grundlage eines Verwaltungsabkommens der Bundesländer und des Bundes aus dem Jahre 1995 ein gemeinsames bundesweites Automatisierungsprojekt mit der Bezeichnung FISCUS (Föderales Integriertes Standardisier-

tes Computerunterstütztes Steuersystem) entwickelt werden. Es war vorgesehen, in den kommenden Jahren alle bestehenden automatisierten Verfahren der Steuerverwaltung schrittweise durch das Verfahren FISCUS abzulösen. Die Projektentwicklung erfolgte bislang in dezentralen Gruppen, die im BMF koordiniert wurden.
Nach Auskunft der OFD vom Dezember 2000 „... befindet sich das Projekt FISCUS seit Mitte 2000 in einer umfassenden Umbruchphase“. Entsprechend der Entscheidung der Finanzminister wird das Projekt nunmehr zentral durch die FISCUS GmbH fortgeführt. Gesellschafter dieser GmbH sind Bundesländer und der Bund. Zur Sicherung der Projektentwicklung solle ein externes Unternehmen mit IT-Erfahrung in die Gesellschaft eingebunden werden.
Nach Mitteilung der Arbeitsgruppe FISCUS im Arbeitskreis Steuern der DSB des Bundes und der Länder besteht die Absicht, innerhalb der FISCUS-GmbH, alle bisherigen Entwicklungen bis Ende 2001 einer Überprüfung zu unterziehen. Zugleich werde eine Arbeitsgruppe der Steuerverwaltung des Bundes und der Länder aufgebaut, deren Aufgabe darin besteht die fachlichen Anforderungen gegenüber der FISCUS-GmbH vorzugeben.

9.2 Elektronische Steuererklärung (ELSTER)

In meinem vorangegangenen Tätigkeitsbericht (3. TB, 9.3) berichtete ich über die Möglichkeit, dass Bürger und Steuerberater, die über die entsprechende technische Ausstattung verfügen, im Rahmen eines Feldversuches, an dem auch die Thüringer Finanzverwaltung beteiligt ist, die Steuererklärung auf elektronischem Wege per Internet abgeben können.
Die Arbeitskreise Technik und Steuerverwaltung der DSB des Bundes und der Länder vereinbarten damals, die weitere Entwicklung und Einführung des Verfahrens **El**ektronische **St**euer**er**klärung (ELSTER) datenschutzrechtlich zu begleiten und sich darüber auszutauschen. Seit dem 1. Januar 2000 ist das Verfahren ELSTER bundesweit im Einsatz. Dem ersten halbjährlichen Bericht der Landesregierung zum Stand der Verwaltungsmodernisierung im Freistaat Thüringen ist zu entnehmen, dass sich bereits in den ersten acht Wochen des Einsatzes der Erfolg dieses Projektes gezeigt hat. In Thüringen wurden in diesem Zeitraum 1.022 Steuererklärungen mit dieser Software über das Internet abgegeben, bundesweit waren es 16.000. Das Ver-

fahren ELSTER soll schrittweise so erweitert werden, dass hiermit künftig auch Lohnsteuerbescheinigungsdaten per Datenfernübertragung vom Arbeitgeber über eine Clearingstelle an das zuständige Finanzamt, sowie Kraftfahrzeugzulassungsdaten von den Zulassungsstellen an die Finanzverwaltung übermittelt werden können. Ende März 2001 konnte man der Presse entnehmen, dass wegen Sicherheitslücken bei ELSTER, dieses bundesweit kurzfristig zur Verbesserung der Software vom Netz genommen wurde. Das TFM teilte auf meine diesbezügliche Nachfrage mit, dass

- die Integrität und Authentizität des Nutzerprogramms einschließlich deren Updates wesentlich verbessert wurde,
- die eigentliche Download-Datei ab sofort signiert wird,
- mit einem Signaturprüfprogramm auf dem Nutzerrechner jetzt festgestellt werden kann, ob die Dateien von der deutschen Steuerverwaltung herausgegeben worden sind und
- um die Sicherheit von ELSTER-Formular zu erhöhen, ebenfalls die Webseiten von ELSTER-Formular nur noch über HTTPS nutzbar sind, d. h. diese jetzt mit Verschlüsselung arbeiten.

Im Rahmen eines Kontrollbesuchs habe ich mir einen allgemeinen Überblick über die Verfahrensabläufe bei ELSTER verschafft. Es ergab sich daraus folgender Sachstand: Für die Nutzung von ELSTER ist von Seiten der Benutzer ein Rechner mit Internetzugang und eine bereits vorhandene Steuernummer notwendig. Die Nutzung von ELSTER ist kostenfrei. Nach Eingabe der Steuererklärung werden die Daten vor dem Versenden automatisch von der Software komprimiert, verschlüsselt und signiert. Die ausgedruckte abgesandte Steuererklärung, auf der sich auch eine automatisch vergebene Tele-Nummer befindet, muss anschließend vom Nutzer unterschrieben an das zuständige Finanzamt gesendet werden. Die Verschlüsselung der Daten erfolgt nach dem so genannten Hybridverfahren (2. TB, 15.7). Das TFM teilte mit, dass dabei sämtliche Nutzdaten länderspezifisch verschlüsselt vom Rechner des Benutzers übertragen werden. Die Entschlüsselung der Daten erfolgt erst im jeweiligen Landesrechenzentrum der Steuerverwaltung, für Thüringen im ZIV, welches der Oberfinanzdirektion zugeordnet ist. Die Signierung der Steuerdaten erfolgt durch einen in der Software integrierten Schlüssel und dient der Prüfung im Rechenzentrum, ob die Steuerdaten mit der Originalsoftware übertragen wurden.

Nach den Grundsätzen für die elektronische Übermittlung von Steuererklärungsdaten (Bundessteuerblatt 1999 - Teil I, S. 1051 ff.) ist der Nutzer von ELSTER für die Daten bis zum Eingang bei der vom Empfänger bestimmten Adresse verantwortlich. Aus datenschutzrechtlicher Sicht kann die Verantwortlichkeit des Nutzers und damit des Bürgers für den gesamten Übertragungsweg bis zu der vom Empfänger bestimmten Adresse nicht gegeben sein. Verwaltungen, die Bürgern und Bürgerinnen eine internetbasierte Kommunikation ermöglichen, haben durch technische und organisatorische Vorkehrungen sicherzustellen, dass Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können. Damit liegt die Verantwortlichkeit bei der Steuerverwaltung.

Die Datenübertragung der vom Nutzer abgesandten Daten an die zuständige Steuerverwaltung erfolgt über die zentrale Clearingstelle von ELSTER in München. Für die Clearingstelle lesbar sind nur Daten, die keine personenbezogenen Daten des Nutzers enthalten.
Die künftige Nutzung der zentralen Clearingstelle durch die Länder soll noch in einer Verwaltungsvereinbarung festgelegt werden. Diese Vereinbarung, die mir bisher als Entwurf vorliegt, regelt die Zusammenarbeit der beteiligten Länder mit dem Ziel, die zentralen Aufgaben einer Clearingstelle zur elektronischen Datenübermittlung im Verfahren ELSTER durch den Freistaat Bayern abzuwickeln.
Die Ansicht des BMF, wonach die Clearingstelle ausschließlich Providerleistung erbringt und somit keine Verarbeitung der Daten erfolgt, kann ich nicht teilen. Die Clearingstelle nimmt die verschlüsselte elektronische Steuererklärung entgegen, speichert diese, übermittelt sie an die zuständige Steuerverwaltung und löscht sie nach einem gewissen Zeitraum. Gemäß § 3 ThürDSG umfasst Verarbeiten u. a. auch das Speichern, Übermitteln und Löschen personenbezogener Daten. Für die Abholung der Daten von der Clearingstelle wird ein ausschließlich für diesen Zweck eingerichteter PC im ZIV vorgehalten. Der Datenübertragung, die täglich in einem bestimmten Zeitfenster erfolgt, geht ein Authentifizierungs-Verfahren zwischen dem PC der OFD und der Clearingstelle voraus. Nach erfolgreichem Datenaustausch wird die Verbindung zur Clearingstelle getrennt und die Daten für die weitere Bearbeitung mit einem aufgabenspezifischen Bearbeitungsprogramm aufbereitet und auf den Großrechner, auf den die Finanzämter Zugriff haben, übertragen. Die Kontrolle ergab, dass

Löschfristen nicht der internen Arbeitsanweisung entsprachen. Dies wurde zwischenzeitlich behoben. Der Zugriff der Finanzämter auf die vorliegenden Daten erfolgt aufgrund der genannten TeleNummer, die der in Papierform vorliegenden Steuererklärung zu entnehmen ist. Sofern keine Rückfragen notwendig sind, erhalten die Bürger in der Regel innerhalb von vier Wochen nach Eingang der ausgedruckten Steuererklärung in Kurzform, ihren Steuerbescheid und die Steuererstattung auf ihr Konto. Liegt neun Monate nach Erhalt einer elektronischen Steuererklärung noch kein Posteingang vom Nutzer vor, werden die Daten auf dem Großrechner im ZIV gelöscht. Über den aktuellen Stand von ELSTER-Formular und über die umgesetzten Sicherheitsmaßnahmen kann sich der Bürger im Internet unter der Adresse http://www.Elster-Formular.de informieren.

9.3 Zugriff der Finanzverwaltung auf DV-gestützte Buchhaltungssysteme

Mit dem Steuersenkungsgesetz von Oktober 2000 (BGBl. I, S. 1433) ist den Finanzbehörden mit Wirkung ab 01.01.2002 durch die Ergänzung der Abgabenordnung (AO) um § 147 Abs. 6 das Recht eingeräumt worden, die DV- gestützte Buchführung der Steuerpflichtigen im Rahmen der Außenprüfung zu nutzen. Die Neuregelung erlaubt der Finanzverwaltung, hierzu zwischen drei Zugriffsmöglichkeiten zu wählen. So kann sie das DV–System zur Prüfung der aufbewahrungspflichtigen Unterlagen einsehen oder verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet oder ihr die gespeicherten Daten auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden. Bereits im Gesetzgebungsvorhaben wurde seitens der DSB des Bundes und der Länder sowie einer Reihe von Verbänden datenschutzrechtliche Bedenken geäußert. Insbesondere wurde kritisiert, dass bei einer Nutzung der Datenverarbeitungssysteme vor Ort keine Pflicht zur Protokollierung des Zugriffes der Betriebsprüfer vorgesehen ist, um die Ordnungsmäßigkeit der vorgenommenen Prüftätigkeit nachvollziehen zu können. Dies ist erforderlich, da die Neuregelung keine Begrenzung der Bereiche enthält, die dem Zugriff der Finanzbehörde unterliegen. Ich hatte gegenüber dem TFM darauf aufmerksam gemacht, dass bei vermischter Speicherung von Personal- und Buchführungsdaten, der Betriebsprüfer Kenntnis von Arbeitnehmerdaten erlangen kann, die für Zwecke der Be-

triebsprüfung nicht erforderlich sind und angeregt, die Nutzung des DV-Systems vor Ort in jenen Fällen, in denen systembedingt eine Beschränkung auf die erforderlichen Daten nicht oder nur unter unverhältnismäßigem Aufwand möglich ist, zumindest für eine Übergangszeit, von der Zustimmung der Steuerpflichtigen abhängig zu machen. Ungeachtet der datenschutzrechtlichen Bedenken hat die Neuregelung inzwischen Gesetzeskraft erlangt. Mit Schreiben vom 03.11.2000 hat das Bundesministerium der Finanzen (BMF) den Entwurf eines mit den obersten Finanzbehörden der Länder abgestimmten Schreibens des BMF „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ vom 06.10.2000 mit der Möglichkeit zur Stellungnahme veröffentlicht. Das Schreiben des BMF enthält Konkretisierungen zur Anwendung des § 147 Abs. 6 AO. Laut Schreiben des BMF ist vorgesehen, dass vor dem 01.01.2002 archivierte Buchführungsdaten nur dann nochmals in das DV-System einzuspeisen sind, wenn dies nicht mit unverhältnismäßigem Aufwand für den Steuerpflichtigen verbunden ist. Dies hat der BfD für nicht praktikabel angesehen, da dies dazu führen kann, dass nach einem Wechsel der EDV-Technik vom Steuerpflichtigen Altgeräte ggf. bis zur Löschfrist älterer Daten betriebsfähig gehalten werden müssten.

9.4 Steuerliche Behandlung von Internetzugängen

Das BMF hatte mit Erlass vom 24.05.2000 („Auslagenersatz, Werbungskosten und geldwerter Vorteil im Zusammenhang mit Telekommunikation des Arbeitnehmers“, BStBl I S. 290) die Finanzbehörden verpflichtet, auf der Vorlage detaillierter Einzelverbindungsnachweise zur Erlangung steuerlicher Vergünstigungen und zur Besteuerung der privaten Nutzung von Telekommunikationsanlagen und Internetanschlüssen des Arbeitgebers zu bestehen. Das im Erlass vorgesehene Verfahren ist wegen des erforderlichen Mehraufwandes auf deutliche Kritik aus Wirtschaft und Verwaltung gestoßen. Die DSB des Bundes und der Länder vertraten die Auffassung, dass die Nachweisführung bei Telekommunikationsdaten, einen unverhältnismäßigen Eingriff in das Telekommunikationsgeheimnis und das Grundrecht auf Datenschutz bedeuten würden, ohne dass die Abgabenordnung hierfür eine gesetzliche Grundlage enthält. Darüber hinaus würde die vollständige Protokollierung der beruflich veran-

lassten Zugriffe der Arbeitnehmer auf das Internet dem Grundsatz der Datensparsamkeit widersprechen. Hinzu kommt, dass anhand der herkömmlichen Telekommunikationsrechnungen nicht festgestellt werden kann, ob das Internet aus dienstlichen oder privaten Gründen genutzt wird. Eine Speicherung der hierfür geeigneten Adressen der aufgerufenen Seiten durch die Diensteanbieter nach Ende der Verbindung besitzt keine Rechtsgrundlage und wäre unverhältnismäßig. Nach Erörterung mit den obersten Finanzbehörden der Länder hat der BMF den Erlass vom 24.05.2000 mit Schreiben vom 16.10.2000 aufgehoben.

9.5 Kontrolle eines Thüringer Finanzamtes

Im Berichtszeitraum habe ich die Datenverarbeitung im Finanzamt geprüft. Die Finanzämter des Freistaates nutzen das Integrierte Automatische Besteuerungsverfahren (IABV). Zu einzelnen Komponenten des IABV hatte ich in der Vergangenheit mehrfach berichtet (2. TB, 9.4; 3.TB, 9.5; 9.7; 15.6.4). Bei den Meldungen zum Datenschutzregister bezüglich einzelner Teilverfahren des IABV stellte sich in einigen Fällen heraus, dass die Bezeichnung der Dateien im Finanzamt nicht mit den Angaben im Datenschutzregister übereinstimmten, wodurch sich Schwierigkeiten bei der Zuordnung von Datenschutzregistermeldungen ergaben. Der Forderung zur Überarbeitung der Datenschutzregistermeldungen wurde nachgekommen.
Hinsichtlich der Verarbeitung von Dateien zur Telefongebühren- und Zeiterfassung habe ich darauf verwiesen, dass die erforderlichen datenschutzrechtlichen Freigaben nicht vorlagen. Dieser Mangel ist im Zuge der Kontrolle durch Vorlage der Freigaben behoben worden.
Die Dienstvereinbarung mit dem örtlichen Personalrat bildet die gemäß § 4 Abs. 1 ThürDSG erforderliche Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Es wurde festgestellt, dass die vorliegende Dienstvereinbarung bezüglich der Zeiterfassungsdaten keine Regelung enthielt, die die praktizierte Speicherung dieser Daten für die Dauer von einem Jahr erlaubte. Durch die Einführung einer neuen Software für die Zeiterfassung sind mittlerweile die technische Voraussetzung für eine dreimonatliche Löschfrist geschaffen worden. Die Dienstvereinbarung ist entsprechend angepasst worden.

In einem allgemein zugänglichen Postraum des Finanzamtes wurden auf einem Regal mit den Postfächern der Sachgebiete mehrere Aktenordner mit Einkommenssteuerunterlagen von Anfang der 90er Jahre festgestellt. Es wurde mitgeteilt, dass die Unterlagen ausgesondert werden sollten und im Postraum zwischengelagert worden sind. Nachfolgend erfolgte eine Archivierung bzw. Vernichtung. Es wurde amtsintern verfügt, auszusondernde Unterlagen künftig in verschlossenen Archivräumen zwischen zu lagern.
Ein Schrank, in welchem die Lohnsteuerkarten für eine Auswertung beim Statistischen Landesamt zwischengelagert werden, war bei der Kontrolle wegen Abwesenheit der zuständigen Mitarbeiter nicht zugänglich. Ich habe gefordert, dass Maßnahmen zu treffen sind, um eine Verfügbarkeit dieser Daten auch im Falle der Abwesenheit zu gewährleisten. Um die Zugänglichkeit personenbezogener Daten sicherzustellen, wurde eine Vertretungsregelung geschaffen.
Auch wurde gefordert, eine unbefugte Kenntnisnahme personenbezogener Daten zu verhindern. Dem wurde durch eine Ergänzung des Vertrages zwischen Finanzamt und Reinigungsfirma entsprochen. Weiterhin hatte ich den Umfang von technisch - organisatorischer Maßnamen im Hauptgebäude des Finanzamtes kritisiert, wodurch weder die elektronisch gespeicherten noch die in Regalen gelagerten Steuerakten angemessen gegen Verlust und Beschädigung gesichert waren. Im Nachgang ist diesem Mangel abgeholfen worden.

9.6 Kontrolle der Bearbeitung von Lohnsteuerkarten im Zentrum für Informationsverarbeitung (ZIV)

Bereits im 2. (9.7) und 3. TB (9.11) habe ich über den Druck und Versand von Lohnsteuerkarten berichtet. Im Berichtszeitraum wurde im ZIV eine Kontrolle durchgeführt.
Dabei wurde festgestellt, dass der Druck und die Kuvertierung der Lohnsteuerkarten als Datenverarbeitung im Auftrag im Sinne von § 8 ThürDSG erfolgt. Das ZIV handelt hierbei, soweit es auf Weisung des TLRZ tätig wird, als Unterauftragnehmer. Da kein Vertrag zum Unterauftragsverhältnis zwischen TLRZ und ZIV vorlag, habe ich auf das Erfordernis einer schriftliche Auftragserteilung gemäß § 8 Abs. 2 Satz 2 ThürDSG hingewiesen.
Die im ZIV kuvertierten Lohnsteuerkarten werden im Auftrag des TLRZ von mehreren beauftragten Firmen versandt. In diesem Zu-

sammenhang wurde gefordert, Ermächtigungen zum Abschluss von Unterauftragsverhältnissen vertraglich festzulegen.
Die Überprüfung ergab, dass beim Versand der Lohnsteuerkarten das Verfahren „Infopost“ (3. TB, 9.12) angewandt wird. Gemäß spezieller Leistungsbeschreibung des Versandunternehmens erklären sich die Kunden bei Einlieferung von Infopostsendungen in verschlossenen Umschlägen „mit einer stichprobenweisen Öffnung zur Inhaltsprüfung einverstanden“. Laut Auskunft des Auftragnehmers werden nach Annahme der Sendungen vom Prüfer der Post ohne Anwesenheit weiterer Personen zwei Umschläge geöffnet. Dies dient der Prüfung, ob das Äußere der Sendungen die vereinbarte Beschaffenheit aufweist, lässt allerdings auch eine Kenntnisnahme personenbezogener Daten zu. Aus meiner Sicht bestehen in diesem speziellen Falle bei Übergabe der Sendungen in Anwesenheit eines Mitarbeiters des TLRZ keine Bedenken (Vieraugenprinzip). Zum Transport der Lohnsteuerkarten werden offene Behälter verwendet. Obwohl sich die Lohnsteuerkarten in verschlossenen Umschlägen befinden, habe ich empfohlen, verschließbare Transportbehälter zu verwenden. Im Nachgang hat sich das mit dem Versand beauftragte Unternehmen meiner o. a. Wertung bezüglich der Kontrollen der Infopostsendungen gegenüber dem TLRZ angeschlossen und hinsichtlich der Verwendung von verschließbaren Transportbehältern eine Lösung für das Jahr 2002 in Aussicht gestellt.

9.7 Leistungsvergleich zwischen Finanzämtern

Von Seiten des TFM wurde mir Informationsmaterial zum Projekt „Leistungsvergleich zwischen Finanzämtern“ zur Kenntnisnahme übersandt. Im Leistungsvergleich, an dem vier Thüringer Finanzämter in der Pilotphase teilnehmen, werden die Kriterien Auftragserfüllung, Mitarbeiterzufriedenheit, Kundenzufriedenheit und Wirtschaftlichkeit untersucht, um Verbesserungspotenziale aufzuzeigen. Zum Zwecke des Datenschutzes der Zeit-, Leistungs- und Personaldaten, die im Rahmen des Projektes „Leistungsvergleich zwischen Finanzämtern“ gewonnen werden, wurde zwischen der OFD und dem zuständigen Personalrat eine Dienstvereinbarung gemäß § 72 i. V. m. § 74 Abs. 3 Nr. 19 ThürPersVG unterzeichnet. Hierin ist u.a. geregelt, dass die abgegebenen Zeiterfassungsbögen der Mitarbeiter, die im betreffenden Finanzamt erfasst werden, spätestens sechs Wochen

nach der erfolgreichen Erfassung zu vernichten sind. Zeitgleich sind auch die im Erfassungssystem gespeicherten personenbezogenen Daten zu löschen. Bezüglich der übersandten Fragebögen zur Kundenzufriedenheit habe ich darauf hingewiesen, dass auf dem zugehörigen Merkblatt ein Hinweis fehlte, zur Wahrung der Anonymität auf die Absenderangabe auf dem Rückumschlag zu verzichten. Da die Fragebögen bereits verschickt waren, habe ich empfohlen, die rückgesandten Umschläge nach Eingang zu vernichten. Die Finanzverwaltung teilte mit, dass dies geschehen sei. Aus dem Informationsmaterial zum Mitarbeiterverhalten ging hervor, dass im Projekt Mitarbeiternummern verwendet werden. Diese dienen dazu, Mitarbeiter auf einen ggf. fehlerhaft ausgefüllten Fragebogen hinweisen zu können. Insoweit ist eine Zweckbindung der personenbezogenen Daten gegeben. Es wurde bestätigt, dass eine Zuordnung zwischen Namen der Mitarbeiter und verwendeten Mitarbeiternummer ausschließlich dem Projektgruppenleiter möglich ist und der Inhalt der Aktivitätenerfassungsbögen nur den unmittelbar am Projekt beteiligten Personen bekannt werden kann. Datenschutzrechtlichen Bedenken bezüglich des Projekts bestanden nicht.

9.8 Unbefugte Weitergabe von Prüffeststellungen durch ein Finanzamt

Im Wege der Beschwerde hatte sich jemand wegen der Verfahrensweise eines Finanzamtes gemäß § 11 ThürDSG an mich gewandt. Der Beschwerde lag folgender Sachverhalt zugrunde:
Anlässlich einer Betriebsprüfung hatte der Petent gegenüber der Außenprüfung den im Prüfzeitraum bevollmächtigten Steuerberater als Auskunftsperson benannt und zugleich dessen steuerliche Bevollmächtigung widerrufen. Vor Abschluss der Prüfung wurden allerdings die steuerlichen Prüffeststellungen dem nunmehr nicht mehr bevollmächtigten Steuerberater vom Finanzamt übermittelt.
Ich habe gegenüber dem Finanzamt die Auffassung vertreten, dass die Übermittlung der Prüffeststellungen unbefugt erfolgte und einen Verstoß gegen das Steuergeheimnis im Sinne von § 30 Abs. 2 AO darstellt. Hierdurch ist der Petent in seinem informationellen Selbstbestimmungsrecht verletzt worden. Mein Vorschlag, durch geeignete Maßnahmen sicherzustellen, dass künftig eine unzulässige Datenübermittlung unterbleibt, wurde seitens der Finanzverwaltung aufge-

griffen. Mit Verfügung hat die OFD Erfurt die Finanzämter angewiesen, dass eine Übersendung von Unterlagen des Steuerpflichtigen an dessen früheren Steuerberater (z.B. als Auskunftsperson im Rahmen einer Außenprüfung) nur erfolgen darf, soweit eine schriftliche Vollmacht des Steuerpflichtigen bzw. dessen Zustimmung vorliegt.

9.9 Führung eines Fahrtenbuches durch Ärzte

Wie im 2. (9.6) und 3. TB (9.14) berichtet, waren Ärzte seit Anfang 1998 bei der Führung eines steuerlichen Fahrtenbuches verpflichtet, neben Datum, Kilometerstand und Ort auch den Namen und die Anschrift des besuchten Patienten aufzuzeichnen. Nach übereinstimmender Auffassung der DSB des Bundes und der Länder ist die Verpflichtung zur Mitteilung von Name und Anschrift der Patienten datenschutzrechtlich bedenklich und verstößt gegen das Auskunftsverweigerungsrecht gemäß § 102 Abs. 1 Nr. 3 Buchstabe c AO. Danach steht Ärzten ein Auskunftsverweigerungsrecht über das zu, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist. Dies umfasst auch die Information über die Tatsache, dass der Arzt den Patienten aufgesucht hat. Diese Vorschrift dient der Wahrung der ärztlichen Schweigepflicht, deren Verstoß nach § 203 StGB strafbar ist. Dieser Rechtsstandpunkt wurde gegenüber den BMF und den obersten Finanzbehörden der Länder vertreten, welche zunächst beabsichtigten, die Neuregelung unverändert beizubehalten. Mitte 1999 konnte auf Initiative des BfD eine Kompromisslösung mit dem BMF erzielt werden, wonach Name und Adresse des besuchten Patienten in einem vom Fahrtenbuch getrennt zu führenden Verzeichnis festgehalten werden. Die Finanzämter sollen dieses Verzeichnis nur dann einsehen, wenn Zweifel an der Richtigkeit oder Vollständigkeit der Eintragungen im Fahrtenbuch bestehen und diese Zweifel nicht mit anderen Mitteln auszuräumen sind. Auf Grund des Erlasses des TFM vom 24.01.2000 hat die OFD Erfurt die Finanzämter angewiesen, künftig dementsprechend zu verfahren.

9.10 Kontrolle in einer Außenstelle des Staatlichen Amtes zur Regelung offener Vermögensfragen (StARoV)

Bei der im Berichtszeitraum durchgeführten Kontrolle in einer Außenstelle des StARoV wurde festgestellt, dass nicht alle automatisiert

geführten Dateien mit personenbezogenen Daten gemäß § 34 ThürDSG freigegeben waren und diesbezüglich auch keine Meldungen zum Datenschutzregister vorlagen. Im Nachgang zur Kontrolle sind die erforderlichen Freigaben erteilt, die Meldungen zum Datenschutzregister nachgeholt und Datenschutzregistermeldungen überarbeitet worden.
Die Telefongebührendaten von Mitarbeitern der Außenstelle des StARoV werden durch das Landratsamt als Betreiber der Telefonanlage verarbeitet. Dabei handelt es sich um Auftragsdatenverarbeitung im Sinne von § 8 ThürDSG. Die Verarbeitung von Telefongebühren erfordert aber auch gemäß § 74 Abs. 3 Nr. 18 ThürPersVG den Abschluss einer Dienstvereinbarung, da sie geeignet ist, das Verhalten oder die Leistung der Beschäftigten zu überwachen. Zum Zeitpunkt der Kontrolle lag keine Dienstvereinbarung zur Telefongebührenerfassung vor. Meiner Forderung, dies nachzuholen, wurde entsprochen.
Nach § 9 Abs. 1 ThürDSG haben öffentliche Stellen technische und organisatorische Maßnahmen zu treffen, um unbefugten Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verhindern. In diesem Zusammenhang habe ich gefordert, auf sämtlichen PC der Außenstelle ein Bootpasswort einzurichten und die Bootpassworte im Rahmen einer Organisationslösung gemäß § 9 Abs. 2 Nr. 10 ThürDSG (Organisationskontrolle) sicher zu hinterlegen. Eine weitere Forderung war, zur Verhinderung des Einspielens von unerwünschter Software, die Diskettenlaufwerke verschließbar zu gestalten. Zu diesem Zweck habe ich empfohlen, Diskettenschlösser einzubauen. Dieser Forderung wurde nachgekommen.
Die Schlüssel zu den Diensträumen werden den Bediensteten der Außenstelle von den Pförtnern des Landratsamtes ausgehändigt, wobei eine Regelung zur Herausgabe der Schlüssel nicht vorlag. Um der datenschutzrechtlichen Verpflichtung der Zugangskontrolle im Sinne von § 9 Abs. 2 Nr. 1 ThürDSG nachzukommen, habe ich den Abschluss einer Vereinbarung zwischen dem StARoV und dem Landratsamt zur Schlüsselverwaltung empfohlen. Bei dieser Gelegenheit wurde festgestellt, dass der Außenstelle mit Aufgabenübernahme von den ehemaligen kommunalen Ämtern zur Regelung offener Vermögensfragen zu Anfang des Jahres 1999 sowohl Altakten der ehemaligen Räte der Städte bzw. Kreise als auch Verfahrensakten

zu vermögensrechtlichen Anträgen zur dienstlichen Verwendung übergeben wurden. Im Ergebnis der Kontrolle wurde gegenüber dem TFM angeregt, in Zusammenarbeit mit dem TMWFK als oberster Archivbehörde, eine für alle Gebietskörperschaften einheitliche und nachvollziehbare Regelung zur Archivierung der Altunterlagen zu schaffen.

9.11 Bankkontennachweis beim Bundesaufsichtsamt für Kreditwesen

Nach den Terroranschlägen vom 11. September 2001 sind Pläne der Bundesregierung bekannt geworden, im Rahmen der Novellierung des Finanzmarktförderungsgesetzes, ein umfassendes Nachweisregister für etwa 300 bis 400 Millionen Giro-, Spar- und Depotkonten beim Bundesamt für das Kreditwesen (Kontenevidenzzentrale) einzurichten. Diese Absicht wurde damit begründet, dass hierdurch Konten terroristischer Organisationen und Einzeltäter leichter als bisher aufgedeckt werden könnten.
Im Kreise der DSB des Bundes und der Länder wurde dieses Gesetzesvorhaben kritisch diskutiert. Die Einrichtung einer Kontenevidenzzentrale für alle in Deutschland geführten Bankkonten wurde für unverhältnismäßig gehalten. Darüber hinaus besteht für eine solche Maßnahme keine Erforderlichkeit.
Im November 2001 hat das Bundeskabinett einen geänderten Gesetzentwurf zum Vierten Finanzmarktförderungsgesetz vorgelegt, der das Konzept einer Kontenevidenzzentrale aufgibt. Stattdessen werden die Banken verpflichtet, eine Liste der geführten Konten zum Zwecke eines automatisierten Abrufs durch die Bundesanstalt für das Kreditwesen bereitzuhalten. Der Datenabruf kann bei besonderer Eilbedürftigkeit beispielsweise im Falle des Verdachts von Verstößen gegen das Geldwäschegesetz oder bei betrügerischen Bankgeschäften erfolgen. Bisher sieht der vorliegende Entwurf nicht zwingend vor, dass jeder einzelne Datenabruf für die Banken nachvollziehbar zu protokollieren ist. Dies ist jedoch im Sinne der Transparenz eine unverzichtbare datenschutzrechtliche Forderung.

10. Justiz

10.1 Strafverfahrensänderungsgesetz (StVÄG) - Umsetzung

Im Berichtszeitraum wurde das Strafverfahrensänderungsgesetz 1999 (StVÄG 1999) vom 02. August 2000 verabschiedet (BGBl. I, S. 1253). Damit ist eine Lücke bei den bereichsspezifischen Regelungen geschlossen worden.
Im 3. TB (10.2) hatte ich den Gesetzentwurf der Bundesregierung vom 16.08.1999 (BT-Drucksache 14/1484) wegen Verschlechterungen aus datenschutzrechtlicher Sicht gegenüber dem Vorentwurf kritisiert. Im Berichtszeitraum wurde durch den Bundestag am 27.01.2000 (BT-Drucksache 14/2595) das StVÄG 1999 mit Änderungen beschlossen und dem Bundesrat zugeleitet. Dessen Ausschüsse empfahlen unter einer Reihe von Änderungen den Vermittlungsausschuss einzuberufen. Mit den geforderten Änderungen wäre eine weitere Senkung des Datenschutzniveaus vorprogrammiert gewesen. Darauf wiesen die DSB des Bundes und der Länder mit der Entschließung der 59. Konferenz (Anlage 4) hin. Die mit dem StVÄG 1999 in die StPO eingefügten Vorschriften betreffen die Öffentlichkeitsfahndung nach Beschuldigten und Zeugen, die Erteilung von Auskünften und Akteneinsicht, die sonstige Verwendung von Informationen für verfahrensübergreifende Zwecke, Dateiregelungen und das länderübergreifende staatsanwaltschaftliche Verfahrensregister. So ist beispielsweise bei einer Fahndungsanordnung durch die Staatsanwaltschaft die richterliche Kontrolle unter bestimmten Voraussetzungen erforderlich und Datenübermittlungen und -nutzungen sind differenziert festgeschrieben.
Die im 3. TB beispielhaft aufgeführten Änderungsforderungen wurden nicht alle erfüllt:

- dem nicht anwaltlich vertretenen Beschuldigten wird nur ein Recht auf Auskünfte und Abschriften eingeräumt, aber keine Akteneinsicht,
- die Aufnahmen einer Benachrichtigungspflicht für nicht beschuldigte Personen im Rahmen der längerfristigen Observation ist unterblieben,
- die im Entwurf des StVÄG 1996 enthaltene Verpflichtung zur Löschung von bereits bei der Polizei vorhandenen Daten wurde nicht beibehalten.

Mit dem Inkrafttreten des StVÄG 1999 ist die Neufassung der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) als auch der Richtlinien über die Inanspruchnahme von Publikationsorganen zur Fahndung nach Personen bei der Strafverfolgung (Anlage B zu den RiStBV) erforderlich geworden.
Das TJM hat um Stellungnahme zu den beabsichtigten Änderungen gebeten. Als begrüßenswert habe ich die Aufnahme des Gebots der Vermeidung von Überschussinformationen bei Datenübermittlungen aus Strafverfahrensakten gesehen. Positiv ist auch die Möglichkeit einer partiellen Akteneinsicht nur in jeweils erforderlichem Umfang, wovon allerdings Gerichte, Staatsanwaltschaften und andere Justizbehörden ausgenommen sein sollen. Berichte der mit der Durchführung des Täter-Opfer-Ausgleichs beauftragten Stellen ebenfalls gesondert zu heften, wurde vom TJM unterstützt.
In Anlage B zu der RiStBV über die Inanspruchnahme von Publikationsorganen zur Fahndung bei Personen nach der Strafverfolgung habe ich die Ansicht vertreten, dass eine Verweisung lediglich auf die gesetzlichen Vorschriften bei der Nutzung des Internets zum Zweck der Öffentlichkeitsfahndung auch nach Zeugen nicht ausreicht. Insbesondere ist eine Konkretisierung des Begriffs „überwiegende schutzwürdige Interessen des Zeugen“ im Entwurf nicht enthalten. Darüber hinaus sollten Prüffristen zur Löschung bei öffentlichen Ausschreibungen, bei denen es sich um schwer wiegende Eingriffe in die Grundrechte der Betroffenen handelt, gekürzt werden.

10.2 Parlamentarische Kontrolle der akustischen Wohnraumüberwachung

Nachdem, wie im 3. TB (10.4) dargelegt, die rechtlichen Grundlagen geschaffen wurden, liegen zwischenzeitlich drei Berichte der Bundesregierung über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten akustischen Wohnraumüberwachungen vor. Diese sind als BT-Drs. 14/2452 GG vom 27.12.1999 für das Berichtsjahr 1998, 14/3998 vom 17.08.2000 für 1999 und 14/6778 vom 06. 08. 2001 für das Jahr 2000 veröffentlicht worden. Aufgrund der jährlichen Berichte der Bundesregierung soll eine laufende parlamentarische Kontrolle der mit Grundrechtseingriffen verbundenen Maßnahmen des „großen Lauschangriffs“ ermöglicht werden. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessen-

heit und Eignung der Maßnahme zu überprüfen. Den ersten Bericht der Bundesregierung gemäß Art. 13 Abs. 6 Satz 1 GG vom 27.12.1999 (BT-Drs. 14/2452), der beispielsweise nur die Gesamtzahl der von der Anordnung Betroffenen wiedergibt, zwischen beschuldigten und nichtbeschuldigten Wohnungsinhabern aber nicht unterscheidet, haben die DSB des Bundes und der Länder zum Anlass einer Umlaufentschließung „Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung“ im Juni 2000 (Anlage 7) genommen und die Bundesregierung aufgefordert, die Berichte entsprechend zu ergänzen, um eine wirksame parlamentarische Kontrolle der besonders intensiven Eingriffe in die räumliche Schutzsphäre des Einzelnen zu gewährleisten. Das Gremium nach Art. 13 Abs. 6 GG im Bundestag hat die Anregungen der DSB begrüßt. Sie sollten zur Gewährleistung der parlamentarischen Kontrolle in die Beratungen einfließen. Die Bundesministerin der Justiz hatte auf die Entschließung gegenüber dem BfD mitgeteilt, dass die Berichtspflicht der Bundesregierung auf der Basis der von den Landesjustizverwaltungen erstellten Ländermitteilungen ausgeführt wird. Hierfür war vom Strafrechtsausschuss der Konferenz der Justizministerinnen und Justizminister im Vorfeld der erstmals für das Jahr 1998 durch die Staatsanwaltschaften zu erstattenden Berichte ein an den gesetzlichen Kriterien orientiertes Erhebungsraster erarbeitet worden. Das TJM hat mitgeteilt, dass die Auffassung vertreten wird, der von der Bundesregierung vorgelegte Bericht erfülle den Zweck der im Grundgesetz vorgesehenen Berichtspflicht. Die verwendeten Kriterien orientierten sich exakt am Wortlaut des § 100 e Abs. 1 StPO, den vom Gesetzgeber geäußerten Erwartungen an den Inhalt des Berichts werde entsprochen. Auch die beiden weiteren Berichte der Bundesregierung gemäß Art. 13 Abs. 6 Satz 1 GG für die Jahre 1999 und 2000 enthalten keine über die im ersten Bericht enthaltenen Angaben hinaus. Allerdings wird im letzten Bericht darauf hingewiesen, dass eine Arbeitsgruppe mit der Prüfung der erhobenen Forderungen betraut wurde. Da nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle in den Ländern zu gewährleisten ist, sind diese Forderungen gleichermaßen auch für die den Landesparlamenten vorzulegenden jährlichen Berichte über von der Polizei zur Gefahrenabwehr veranlassten Überwachungsmaßnahmen gültig. Die Entschließung habe ich daher auch an die Mitglieder der parlamentarischen Kontrollkommission

zur Kenntnis gegeben. Das TIM hat mitgeteilt, es sei beabsichtigt, einen abgestimmten Erhebungsbogen, der an die Rechtslage in Thüringen angepasst wurde, als Grundlage für den zu erstellenden Bericht zu verwenden. Der Thüringer Landtag hat in seiner 36. Plenarsitzung die Landesregierung aufgefordert, dem Landtag über die Maßnahmen zur akustischen Wohnraumüberwachung zum Zwecke der Strafverfolgung nach Art. 13 Abs. 3 GG, die seit dem Inkrafttreten dieser Grundgesetzänderung in Thüringen durchgeführt wurden, zu berichten. Künftige Berichte sollen jährlich dem Justizausschuss spätestens zum Ablauf des 3. Quartals des Folgejahres erstattet werden.

10.3 Telekommunikationsüberwachung

Zu der im 3. TB (10.5) angesprochenen Evaluierung der Eingriffsbefugnisse anhand objektiver Kriterien und damit der Vergabe eines Forschungsvorhabens zum Thema „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO“ liegt bislang kein Ergebnis vor. Zur Unterstützung des Forschungsvorhabens waren die Landesjustizverwaltungen gebeten worden, eine Auflistung aller Verfahren aus dem Jahre 1998, in dem Telekommunikationsüberwachungen angeordnet wurden, zu übersenden. Solche Listen wurden auch von den Thüringer Staatsanwaltschaften an das durchführende Institut übermittelt. Wie aus dem TJM zu erfahren war, sind bislang noch keine Verfahrensakten angefordert worden.
Mit dem Gesetz zur Änderung der Strafprozessordnung vom 20. Dezember 2001 (BGBl. I, S. 3879) hat der Bundestag die Einfügung von §§ 100g und 100h StPO zum 01.01.2002 beschlossen. Der Zugriff auf Telekommunikationsdaten ist damit neu geregelt worden, nachdem § 12 FAG am 31. 12. 2001 nach mehrmaligen Verlängerungen außer Kraft treten sollte. Durch diese gesetzlichen Grundlagen darf, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von erheblicher Bedeutung begangen, zu begehen versucht oder durch eine Straftat vorbereitet hat, angeordnet werden, dass diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, unverzüglich Auskunft über näher bezeichnete Telekommunikationsverbindungsdaten zu erteilen haben, soweit die Auskunft für die

Untersuchung erforderlich ist. Die Auskunft darf auch über zukünftige Telekommunikationsverbindungen angeordnet werden. Das Gesetz bestimmt weiterhin, dass diese eingefügten Paragraphen am 1. Januar 2005 wieder aufgehoben werden. Hintergrund ist, dass nach der Gesetzesbegründung (BT-Drs. 14/7008) umfassendere Änderungen im Bereich der Überwachung des Fernmeldeverkehrs ausstehen und die jetzt beschlossenen §§ 100g und 100h StPO einzugliedern sind.

10.4 Ermittlung strafbarer Inhalte im Internet

Im November 2001 wurde von Vertretern aus 26 Europaratsländern sowie den USA, Kanada, Japan und Südafrika eine internationale Konvention gegen Internet-Kriminalität (Cyber-Crime-Convention) unterzeichnet. Dieses erste internationale Vertragswerk definiert die Vergehen, die mit Hilfe des Internets verübt werden können, wie Eindringen in fremde Netzwerke und Dateien (Hacken), Urheberrechtsverstöße (z. B. Software-Piraterie), die Verbreitung von Kinderpornografie sowie Verbrechen, die unter Ausnutzung von Computernetzwerken begangen werden können (Betrug, Geldwäsche, Vorbereitung terroristischer Akte). Die Unterzeichner der Konvention verpflichteten sich, die Verfolgung und Ahndung dieser Straftatbestände in ihre nationale Gesetzgebung aufzunehmen. Hierzu sind auch grenzüberschreitende Verfahren und Mechanismen bei der Strafverfolgung nötig.

Zu den Beratungen der Konvention über Datennetzkriminalität (Cyber-Crime-Convention) haben die DSB des Bundes und der Länder auf ihrer 61. Konferenz eine Entschließung gefasst (Anlage 16). Bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität wurde die Bundesregierung aufgefordert, sich für die datenschutzrechtlichen Forderungen einzusetzen. Mit der eingefügten Garantieklausel ist sichergestellt worden, dass die rechtsstaatlichen Prinzipien wie Verhältnismäßigkeit, Interessenabwägung und justizielle Kontrolle nicht eingeschränkt werden und die traditionellen Strukturen des innerstaatlichen Rechts erhalten bleiben.

10.5 DNA-Analyse – Genetischer Fingerabdruck

Die DNA-Analyse wird auf der Grundlage des DNA-Identitätsfeststellungsgesetzes von 1998 (BGBl. I, S. 2646) zum Zweck der Strafverfolgung durchgeführt. Im vorangegangenen 3. TB (10.8) habe ich bereits Ausführungen dazu gemacht.
Die Konferenz der DSB des Bundes und der Länder hat am 12. März 2001 eine Entschließung (Anlage 19) gefasst: Eine Datenerhebung auf Vorrat, die alle Männer und damit die Hälfte der Bevölkerung als potentielle Straftäter behandelt, ist verfassungsrechtlich unzulässig.
Für Klarstellungen im Rahmen der Durchführung des § 2 DNA-Identitätsfeststellungsgesetz, nach dem verurteilte Straftäter der DNA-Analyse unterzogen werden können, hat das Bundesverfassungsgericht mit Beschluss vom 15.03.2001 (2 BvR 1841/00) gesorgt. Es hat festgestellt, dass die Gerichte bei der Anwendung und Auslegung des § 2 DNA-Identitätsfeststellungsgesetz gehalten sind, die Bedeutung und Tragweite des Rechts auf informationelle Selbstbestimmung hinreichend zu berücksichtigen. Vorausgesetzt ist als Anlass für die Maßnahme im Vorfeld eines konkreten Strafverfahrens eine Straftat von erheblicher Bedeutung, wobei das Vorliegen eines Regelbeispiels im Sinne des § 81g Abs. 1 StPO nicht in jedem Fall von einer einzelfallbezogenen Prüfung der Erheblichkeit der Straftat entbindet. Die erforderliche Prognoseentscheidung im Sinne von § 81g StPO setzt von Verfassungswegen voraus, dass eine zureichende Sachaufklärung, insbesondere durch Beiziehung der verfügbaren Straf- und Vollstreckungsakten, des Bewährungshelfers und zeitnahe Auskünfte aus dem Bundeszentralregister vorausgegangen ist und die für sie bedeutsamen Umstände nachvollziehbar und einzelfallbezogen abgewogen werden. Das bedeutet, dass im Rahmen der Anordnung einer DNA-Analyse zum Zweck der Identitätsfeststellung nicht nur auf das Vorliegen von Katalogstraftaten Bezug genommen werden darf, sondern dass in die Prognoseentscheidung, ob jemand wieder straffällig werden wird, die erheblichen Einzelheiten einzubeziehen sind. Zu der Richtlinie zur Verfahrensweise und Anwendung der „DNA-Analyse-Datei“ in der Thüringer Polizei wurde ich um Stellungnahme gebeten. Dabei habe ich unter anderem Hinweise zum Formblatt zur Belehrung/ Einwilligungserklärung der Betroffenen, denen Körperzellen zum Zweck der Identitätsfeststellung gemäß § 81g StPO/ § 2 DNA-IFG entnommen werden sollten, gegeben. Um eine wirksame Einwilligung der Betroffenen zu errei-

chen, müssen sie ausreichend über alle wesentlichen Voraussetzungen und die Tragweite der Entscheidung informiert sein. Meine Änderungsanregungen sowie der Vorschlag, wie in anderen Ländern auch, ein ausführliches Merkblatt für die Betroffenen beizufügen, wurden aufgegriffen. Im Rahmen meiner Kontrolltätigkeit habe ich die Einhaltung der gesetzlichen Bestimmungen kontrolliert. Meine Anregungen und Hinweise wurden weitgehend umgesetzt. Lediglich in einem Punkt erfolgte dies nicht. Das betrifft die Übersendung von Sammelrechnungen über in einem gewissen Zeitraum durchgeführte DNA-Analysen durch ein Universitätsinstitut an das LKA, denen eine Liste der gekürzten Daten der Betroffenen beizufügen war. Mein Vorschlag, nur jeweils den sachbearbeitenden Polizeidienststellen, die die Untersuchung in Auftrag gegeben haben, neben der Mitteilung des Ergebnisses der Probe auch die Rechnung zu übersenden, wurde nicht aufgegriffen.

10.6 Kontrollbefugnis des TLfD bei Gerichten

Die Diskussion zur Kontrollbefugnis des TLfD bei Gerichten war bereits im 3. TB (10.7) dargelegt. Durch eine bundesweite Umfrage eines Landesjustizministeriums wurde sie erneut angeregt. Dort hatte der LfD beabsichtigt, in die bei den Gerichten eingesetzten EDV-Programme Einsicht vor Ort zu nehmen, um die technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes zu überprüfen. Die Diskussion zu dieser Thematik führte bislang in Thüringen zu keiner einvernehmlichen Lösung. Nach wie vor bin ich der Auffassung, dass beim Einsatz eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten bei Gerichten die Voraussetzungen zur Einhaltung der datenschutzrechtlichen Vorschriften zu schaffen sind und unter dem Gesichtspunkt, dass die richterliche Unabhängigkeit nicht tangiert wird, durch den TLfD kontrollierbar sein müssen. In Anbetracht der Gefahren für die zu bearbeitenden personenbezogenen Daten, welche eventuell durch Viren, unzureichenden Passwortschutz, zu weit reichende Zugriffsrechte, Anbindung an das Internet, unverschlüsselte Datenübertragung etc. entstehen können, halte ich eine Kontrolle durch den TLfD, ob die erforderlichen technischen und organisatorischen Maßnahmen gemäß § 9 ThürDSG getroffen sind, zum effektiven Schutz des Grundrechts auf informationelle Selbstbestimmung der Betroffenen sowie auch zum

Schutz und zur Sicherheit der Gerichte, die für datenschutzrechtliche Verstöße als öffentliche Stelle einzustehen haben, für unverzichtbar.
Bevor ich von der neuerlichen aktuellen Diskussion erfuhr, hatte ich einen Informationsbesuch zum Einsatz des elektronischen Grundbuchs angekündigt, das bis dahin als Pilotprojekt bei dem betreffenden Gericht eingesetzt war. Vorbehalte hiergegen waren seitens des TJM zunächst nicht geäußert worden. Vor Ort allerdings war man seitens der Justizverwaltung nur dazu bereit, Fragen des TLfD zu beantworten. Eine Einsicht in das elektronisch geführte Grundbuch wurde jedoch wegen einer angeblich fehlenden Kontrollkompetenz nicht gewährt. Da das Grundbuch Echtdaten von Grundstückseigentümern enthalte, sei dies nicht möglich. Diese Auffassung widerspricht dem gesetzlichen Kontrollauftrag des TLfD. Hinsichtlich der datenschutzrechtlichen Aspekte bei der Einführung des elektronischen Grundbuchs wurde ich frühzeitig beteiligt. Der Informationsbesuch zur Feststellung der getroffenen technischen und organisatorischen Maßnahmen konnte letztendlich nicht wie vorgesehen durchgeführt werden. Im Nachgang wurden mir weitere Unterlagen zum Verfahren zur Kenntnis gegeben.
An der Auffassung, dass das elektronische Grundbuch im praktischen Betrieb für den TLfD nicht einsehbar ist, hat das TJM bislang festgehalten. Das Programm sei ausschließlich auf den Kernbereich der Rechtsanwendung hin angelegt, für Verwaltungsangelegenheiten werde es nicht eingesetzt und unterliege damit nicht dem 5. Abschnitt des ThürDSG. Anders als bei der herkömmlichen Aktenbearbeitung, bei der das Papiergrundbuch im Grundbuchamt selbst registriert, aufbewahrt und nach den Vorschriften eigener Aktenführungsregeln verwaltet wird, seien die elektronischen Grundbuchdaten im Grundbuchamt nicht vorrätig. Die Daten werden auf einem Rechner im ZIV gespeichert.
Aus meiner Sicht handelt sich aber gerade bei der Einführung eines automatisierten Verfahrens auch bei Gerichten bereits um eine Verwaltungstätigkeit, bei der die datenschutzrechtlichen Vorschriften, insbesondere § 9 ThürDSG zu den erforderlichen technischen und organisatorischen Maßnahmen einzuhalten sind. Dass die Einhaltung dieser Vorschriften erst im Betrieb des Verfahrens konkret überprüft werden kann, dürfte selbstverständlich sein. Weitere Ausführungen zum elektronischen Grundbuch werden unter Punkt 10.13 abgehandelt.

10.7 Kontrollbefugnis des TLfD im strafrechtlichen Ermittlungsverfahren

Ausgelöst durch eine Länderumfrage hatten sich die Justizverwaltungen zur Frage der datenschutzrechtlichen Kontrolle im Rahmen laufender staatsanwaltschaftlicher Ermittlungsverfahren positioniert.
Nach § 37 ThürDSG kontrolliert der Landesbeauftragte für den Datenschutz bei allen öffentlichen Stellen die Einhaltung der Vorschriften des ThürDSG und anderer Rechtsvorschriften über den Datenschutz. Hierbei wird nicht unterschieden, ob es sich bei den anderen Rechtsvorschriften über den Datenschutz um Bundes- oder Landesvorschriften handelt. Auch wenn besondere Rechtsvorschriften des Bundes (StPO) oder des Landes den Vorschriften des ThürDSG vorgehen, bedeutet dies nicht, dass das Kontrollrecht des TLfD in diesen Fällen eingeschränkt wäre.

Im Ergebnis der Diskussion mit dem TJM konnte Einigkeit dahingehend erzielt werden, dass die Kontrollbefugnis des TLfD bei den Staatsanwaltschaften des Freistaats Thüringen keinen Beschränkungen nach dem ThürDSG unterliegt. Die Prüfung der fachlichen Zweckmäßigkeit von Maßnahmen im Ermittlungsverfahren durch den TLfD ist nicht vorgesehen. Bei Vorliegen einer richterlichen Anordnung oder Zustimmung zur Durchführung einer Ermittlungsmaßnahme scheidet eine datenschutzrechtliche Bewertung durch den TLfD aus, da die der richterlichen Unabhängigkeit unterliegenden Entscheidung nicht der Kontrollzuständigkeit unterliegen. Unter diesen Voraussetzungen hat das Thüringer Justizministerium keine Bedenken dagegen, wenn datenschutzrechtliche Kontrollen auch im Rahmen laufender staatsanwaltschaftlicher Ermittlungsverfahren durchgeführt werden, soweit im Zuge dieser Kontrollmaßnahmen kein Eingriff in das Ermittlungsverfahren erfolgt. Gemäß den Regelungen der StPO und im Sinne einer funktionstüchtigen Strafrechtspflege gehe ich selbstverständlich davon aus, dass im Rahmen einer Kontrollmaßnahme kein Eingriff in das Ermittlungsverfahren erfolgt.

10.8 Ordnungswidrigkeit oder Strafsache

Ein Petent wandte sich an mich, weil er sich zu Unrecht mit einer Strafsache in Verbindung gebracht sah. Wegen eines Parkverstoßes war er vom Gericht zu einem Bußgeld verurteilt worden, nachdem er gegen das von der Ordnungsbehörde auferlegte Verwarngeld Einspruch und gegen den Bußgeldbescheid Widerspruch eingelegt hatte. Im Rahmen der Vollstreckung wurde er von der zuständigen Staatsanwaltschaft und der Justizzahlstelle aufgefordert, die Geldbuße sowie die Kosten des Verfahrens in seiner „Strafsache“ zu bezahlen. Schnell wurde von der zuständigen Staatsanwaltschaft eingeräumt, es habe sich um einen Irrtum gehandelt, die vermeintliche Strafsache sei aber erkennbar dem Ordnungswidrigkeitsverfahren zuordenbar. Dennoch erhielt der Petent weiterhin die Aufforderung, in seiner „Strafsache“ zu bezahlen. Ich habe dies zum Anlass genommen, bei der zuständigen Staatsanwaltschaft eine datenschutzrechtliche Kontrolle durchzuführen. Dabei wurde festgestellt, dass das an den Betroffenen gesandte übliche formularmäßige Schreiben zur Zahlungserinnerung mangels entsprechender Textbausteine nicht zwischen Strafsache und Bußgeldsache unterschieden hatte. Dieses Formular war selbst dann noch benutzt worden, nachdem der Staatsanwaltschaft der Sachverhalt bereits bekannt war. Auch der Justizzahlstelle war ursprünglich übermittelt worden, dass es sich in der Angelegenheit des Betroffenen um eine Strafsache handelte, was noch während der Kontrolle richtig gestellt wurde.
Im Ergebnis der Kontrolle teilte die zuständige Staatsanwaltschaft mit, dass durch die Einführung neuer formularmäßiger Anschreiben und die Änderung der Textbausteine im verwendeten Schreibprogramm SIJUS-Straf für die Zukunft organisatorisch sichergestellt ist, dass Betroffene im Bußgeldverfahren nicht mehr mit einer Strafsache in Verbindung gebracht werden.

10.9 Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Wie im 3. TB (10.11) habe ich unter Bezugnahme auf die Entschließung der 58. Konferenz der DSB des Bundes und der Länder darauf hingewiesen, dass die Aufbewahrung von Schriftgut der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften einer gesetzlichen Grundlage bedarf. Im Berichtszeitraum hat sich eine länderoffene, von der Konferenz der Justizministerinnen und –minister (JuMiKo) berufene

Arbeitsgruppe „Aufbewahrungsbestimmungen“ konstituiert. Diese hat sich auch mit der Frage beschäftigt, ob eine gesetzliche Regelung zur Aufbewahrung erforderlich ist. Die Mehrheit der Sitzungsteilnehmer kam zu dem Schluss, eine solche sei entbehrlich.
Das TJM hält dagegen eine bereichsspezifische Regelung für erforderlich. Die in Thüringen geltenden allgemeinen datenschutz- und archivrechtlichen Bestimmungen gelten zwar formal für den Bereich der Gerichtsbarkeiten, erfassen jedoch die zu regelnden Tatbestände bestenfalls generalklauselartig und können daher bereichsspezifische Regelungen nicht ersetzen. Perspektivisch müsse ein nach der jeweiligen Aktenart und den dort gespeicherten personenbezogenen Daten abgestuftes, ausreichend bestimmtes und für den Betroffenen auch ohne Mühe nachvollziehbares Regelungswerk aus Gesetz, Verordnung und gegebenenfalls untergesetzlichen Regelungen geschaffen werden.
Die 72. Konferenz der Justizministerinnen und –minister vom 11. bis 13. Juni 2001 hat sich für die Einsetzung einer neuen länderoffenen Arbeitsgruppe ausgesprochen, die nun den Entwurf für ein Aufbewahrungsgesetz erarbeiten soll.

Unabhängig davon wurde von der erstgenannten Arbeitsgruppe unter Federführung Nordrhein-Westfalens länderübergreifend die Überarbeitung der Aufbewahrungsbestimmungen in Angriff genommen. Den Ländern wurden dabei einzelne Bereiche zur Bearbeitung übertragen. Im Arbeitskreis Justiz der Konferenz der DSB des Bundes und der Länder hatte man sich darauf verständigt, Stellungnahmen sowie etwaige allgemeine Forderungen zu den Aufbewahrungsbestimmungen in einer gemeinsamen Stellungnahme zusammen zu führen. Das TJM wird mich zu dem überarbeiteten Entwurf beteiligen.

10.10 Umzug in der Justiz – Ungesicherte Aktenlagerung

Es hat sich wieder bestätigt, dass der Beachtung der datenschutzrechtlichen Vorschriften bei der Vorbereitung und Durchführung bei Behördenumzügen erhebliche Bedeutung zukommt. In der Presse wurde berichtet, dass im neu bezogenen Justizzentrum Gerichts- und staatsanwaltschaftliche Ermittlungsakten offen zugänglich in der Tiefgarage lagerten. Ich habe unverzüglich eine datenschutzrechtli-

che Kontrolle veranlasst. Dabei war festzustellen, dass mehrere hunderttausend Akten von abgeschlossenen Verfahren der Staatsanwaltschaft in der Tiefgarage in Umzugskartons zwischengelagert wurden, ohne dass die erforderlichen organisatorischen und technischen Maßnahmen getroffen waren, den Zugang durch Unbefugte auszuschließen. Hintergrund war, dass die Vielzahl der Akten nicht in die vorgesehenen Archivräume verbracht werden konnten und deshalb in einem Teil der Tiefgarage abgestellt wurden. Die Tiefgarage wurde zwischenzeitlich zur Nutzung der Parkplätze freigegeben, ohne dass man berücksichtigte, dass dort Akten mit sensiblen personenbezogenen Daten zwischengelagert waren. Ich habe dies noch am Tag des Bekanntwerdens gemäß § 39 ThürDSG beanstandet und die Staatsanwaltschaft aufgefordert, unverzüglich die erforderlichen Sicherungsmaßnahmen zu treffen, was auch erfolgte. Im Zusammenhang mit der ausgesprochenen Beanstandung wurde auch die Forderung einer Vollständigkeitskontrolle aufgemacht.
Hinzu kam noch, dass die Umzugskisten von der Transportfirma eingepackt wurden. Die ungenügenden Sicherheitsvorkehrungen in Vorbereitung und Durchführung des Umzugs habe ich zum Anlass einer zweiten Beanstandung genommen.
Während der Kontrolle durch den TLfD bei der Staatsanwaltschaft war festzustellen, dass durch die Generalstaatsanwaltschaft bereits Stichprobenkontrollen durchgeführt wurden. Eine Vollständigkeitskontrolle im Zuge des Umzugs ist nach Angaben des TJM und der Auffassung der zu diesem Zweck eingesetzten Arbeitsgruppe nicht machbar. Zwischenzeitlich habe ich mich mit der Staatsanwaltschaft und der Generalstaatsanwaltschaft über die Durchführung einer aussagefähigen Stichprobenkontrolle bezüglich des vorhandenen Aktenbestandes verständigt.

10.11 Mitteilung des Verfahrensausgangs an die Polizei

In Umsetzung des Art. 32 Justizmitteilungsgesetz bestimmt Nr. 11 der Mitteilungen in Strafsachen (MiStra) (3. TB, 10.2), dass die Staatsanwaltschaft der Polizeibehörde, die mit dem Verfahren befasst war, den Ausgang des Verfahrens mitteilt.
Im Rahmen meiner Kontrolltätigkeit habe ich festgestellt, dass dies in manchen Fällen nicht geschieht. Geht bei der Polizei keine Mitteilung ein, hat dies zur Folge, dass die Polizei gegebenenfalls die er-

forderlichen Maßnahmen wie Verkürzung der Speicherungsfristen oder Löschung der gespeicherten Daten nicht ergreifen kann. Ein Betroffener bleibt dann weiterhin im polizeilichen Informationssystem gespeichert. Damit wird das Recht des Betroffenen auf informationelle Selbstbestimmung beeinträchtigt. Eine fehlende Mitteilung über die Verfahrenseinstellung gegenüber der Polizei wurde bspw. mit einem Versehen der Geschäftsstelle der Staatsanwaltschaft begründet. Der Vorgang wurde in der Staatsanwaltschaft ausgewertet und um zuverlässiges Ausführen der staatsanwaltschaftlichen Verfügungen gebeten.

10.12 Weitergabe personenbezogener Daten an gemeinnützige Einrichtungen

Die in vorangegangenen Tätigkeitsberichten dargestellte Diskussion um die datenschutzrechtliche Problematik der Datenübermittlungen im Zusammenhang mit der Entrichtung von Geldern an gemeinnützige Einrichtungen durch Beschuldigte bzw. Angeklagte ist einer Lösung zugeführt worden. Mit der Einführung des Textverarbeitungssystems bei den Thüringer Staatsanwaltschaften wird künftig so verfahren, dass die gemeinnützige Einrichtung als möglicher Zahlungsempfänger nur noch eine anonymisierte Mitteilung erhält, die gleichzeitig mit der Anhörung des Beschuldigten, ob er der vorläufigen Einstellung zustimmt, versandt wird. Die Personalien des Beschuldigten werden nicht mehr übermittelt. Damit ist dem datenschutzrechtlichen Anliegen hinreichend Rechnung getragen.

10.13 Elektronisches Grundbuch

Wie bereits im 1. TB (10.13) angesprochen, sollte durch die Einführung des elektronischen Grundbuchs im Freistaat Thüringen die Protokollierung der Einsichtnahmen erfolgen. Im Juni des Jahres 2001 wurde das Projekt „Elektronisches Grundbuch“ für Thüringen gestartet. Zu den dem IMA-IT vorliegenden Unterlagen habe ich aus datenschutzrechtlicher Sicht Fragen gestellt und Hinweise gegeben. Die Justiz hat sich für das Softwareprogramm SOLUM-Star entschieden, das auch in anderen Bundesländern zum Einsatz kommt. Zukünftig entfällt damit die Führung der Grundbücher in Papierform.

Im Rahmen eines Informationsbesuches bei einem Grundbuchamt, bei dem das elektronische Grundbuch als Pilotprojekt eingesetzt war, wollte ich mich von den technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes überzeugen. Vor Ort allerdings war man seitens der Justizverwaltung nur dazu bereit, Fragen des TLfD zu beantworten. Eine Einsicht in das elektronisch geführte Grundbuch wurde jedoch wegen einer angeblich fehlenden Kontrollkompetenz nicht gewährt (vgl. 10.6). Daher konnte der Informationsbesuch zur Feststellung der getroffenen technischen und organisatorischen Maßnahmen letztendlich nicht wie vorgesehen durchgeführt werden. Im Nachgang wurden mir weitere Unterlagen zum Verfahren zur Kenntnis gegeben.
Eine nach § 65 Grundbuchverfügung (GBV) vorgeschriebene Dienstanweisung zur Regelung der Zugangssicherung und Datensicherungsverfahren lag zu dem Zeitpunkt nicht vor. Die Erfassungsphase der Grundbuchblätter war zum Zeitpunkt des Informationsbesuchs nahezu abgeschlossen. Die technischen und organisatorischen Sicherungsmaßnahmen beim Transport der Unterlagen zur Erfassungsstelle und zurück zum Grundbuchamt waren getroffen. Die eingegebenen Daten werden nicht im Grundbuchamt selbst vorrätig gehalten, sondern zentral auf einem Rechner im ZIV gespeichert. Bei der Speicherung der Daten im ZIV handelt es sich um eine Auftragsdatenverarbeitung im Sinne des § 8 ThürDSG. Eine konkrete Vereinbarung unter Bestimmung der erforderlichen Maßnahmen lag jedoch noch nicht vor. Das elektronische Grundbuch wird in naher Zukunft Online-Abrufe der im ZIV gespeicherten Daten ermöglichen. Dies wird zunächst über Einsichts-PC in den Grundbuchämtern geschehen.

10.14 Grundbucheinsicht/Auszüge aus dem Grundbuch

Ein Petent befürchtete, dass Personen mit Interesse am Kauf eines seiner Grundstücke seine gesamten Eigentumsverhältnisse inklusive Belastungen zur Kenntnis gelangen könnten. Grund hierfür sah er in dem Umstand, dass zu seinen Grundstücken in einem Grundbuchbezirk ein gemeinschaftliches Grundbuchblatt angelegt worden war. Darin waren alle seine Grundstücke aufgeführt. Der finanzierenden Bank eines der Grundstücke war ein Grundbuchauszug zu allen seinen Grundstücken übersandt worden.

Nach § 12 Grundbuchordnung (GBO) ist die Einsicht des Grundbuchs jedem gestattet, der ein berechtigtes Interesse darlegt. Das berechtigte Interesse wird sich in der Regel jedoch nur auf ein konkretes Objekt beziehen. Eine Gewährung der Einsicht in alle Eintragungen in einem gemeinschaftlichen Grundbuchblatt dürften daher nur in wenigen Ausnahmefällen erfolgen. Das zuständige Grundbuchamt hatte mir mitgeteilt, dass ein berechtigtes Interesse eines Gläubigers vorliege, wenn er z. B. nur ein Grundstück belastet hätte, da er mit der Grundschuldbestellungsurkunde einen Vollstrekkungstitel besitze, mit welchem er auch in andere Vermögenswerte und somit auch in andere Grundstücke vollstrecken könnte. Dabei ist es auch bei der Führung von gemeinschaftlichen Grundbuchblättern jederzeit möglich, einen Teilgrundbuchauszug für nur ein Grundstück zu erteilen. Ob nur ein Teilgrundbuchauszug erteilt wird, hängt vom entsprechenden Antrag ab. Aus der Darlegung zu der vorliegenden Eingabe konnte ich keine Anhaltspunkte dafür entnehmen, dass unberechtigterweise Grundbuchauszüge mit zu vielen Angaben erteilt wurden.
Die Befürchtung, dass auch potentielle Käufer eine Grundbucheinsicht und damit eine Auflistung sämtlicher Grundstücke erhalten könnten, erwies sich als unbegründet. In einem solchen Fall erfolgt eine beschränkte Einsicht auf das betroffene Grundstück, sofern eine Vollmacht des Eigentümers vorliegt oder bereits eine Auflassungsvermerkung eingetragen wurde.
Die Möglichkeit der beschränkten Einsicht in das Grundbuch wird sich durch die Einführung des elektronischen Grundbuchs erleichtern, da am Bildschirm auch nur die Teile aufgezeigt werden können, zu denen eine berechtigtes Interesse besteht. Eine Abdeckung der übrigen Teile, wie dies bei Grundbüchern in Papierform erforderlich sein kann, entfällt.

10.15 Elektronischer Rechtsverkehr bei den Gerichten

Die gesetzlichen Voraussetzungen für die maschinelle Führung des Handels-, Partnerschafts- und Genossenschaftsregisters sind vorhanden. Es wird daran gearbeitet, die technischen Voraussetzungen der elektronischen Registerführung weiter zu schaffen. Das Gesetz über Elektronische Register und Justizkosten für Telekommunikation – ERJuKoG vom 10. Dezember 2001 (BGBl. I, S: 3422) enthält Re-

gelungen zur Nutzung des Online-Abrufs aus den maschinell geführten Registern wie das Handels-, Vereins- und Genossenschaftsregister aber auch zu den Gebühren für den Abruf von Daten aus maschinell geführten Registern. Darin enthalten ist auch die Verpflichtung, die Nutzer des Handels- und Vereinsregisters darauf hinzuweisen, dass die übermittelten Daten nur zu Informationszwecken verwendet werden dürfen. Wird z. B. durch Stichproben festgestellt, dass die zulässige Einsicht überschritten oder Daten missbraucht wurden, kann ein Nutzer von der Teilnahme am automatisierten Abrufverfahren ausgeschlossen werden; dasselbe gilt bei drohender Überschreitung oder drohendem Missbrauch.
Davon unabhängig beschäftigt sich eine Arbeitsgruppe „Elektronischer Rechtsverkehr“ der Bund-Länder-Kommission für Datenarbeitung und Rationalisierung in der Justiz. Da auch die Realisierung des elektronischen Geschäftsverkehrs mit den Gerichten und Staatsanwaltschaften datenschutzrechtliche Fragen und Probleme aufwirft, wird die weitere Entwicklung durch die DSB des Bundes und der Länder begleitet werden.

10.16 Veröffentlichung von Insolvenzdaten im Internet

Bei vorliegender oder drohender Zahlungsunfähigkeit einer natürlichen Person oder auch Überschuldung einer juristischen Person kann auf Antrag eines Gläubigers ein Insolvenzverfahren eröffnet werden. Neben der Zustellung an die Betroffenen sind beispielsweise die Eröffnung des Insolvenzverfahrens, der Aufruf an die Gläubiger, ihre Forderungen anzumelden, Verfügungsbeschränkungen oder der Abschluss eines Insolvenzverfahrens auch öffentlich bekannt zu machen. In Thüringen kann man solches regelmäßig im Staatsanzeiger oder auch in der Tageszeitung nachlesen.
In manchen Bundesländern war man dazu übergegangen, Insolvenzdaten auch in das Internet einzustellen, sodass die Daten weltweit abgerufen werden können. Eine Rechtsgrundlage hierfür wurde erst mit dem am 1. Dezember 2001 In Kraft getretenen Gesetz zur Änderung der Insolvenzordnung und anderer Gesetze geschaffen. Unterstützt durch die gemeinsame Entschließung der DSB des Bundes und der Länder vom 24. April 2001 (Anlage 20) zu „Veröffentlichung von Insolvenzinformationen im Internet“ wurde der ursprüngliche

Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung und anderer Gesetze modifiziert.
§ 9 Insolvenzordnung, der die Veröffentlichung vorschreibt, wurde dahingehend ergänzt, dass die Veröffentlichung auch in einem für das Gericht bestimmten elektronischen Informations- und Kommunikationssystem erfolgen kann. Darüber hinaus wird ergänzend das BMJ ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrats die Einzelheiten der Veröffentlichung in einem elektronischen Informations- und Kommunikationssystem zu regeln. Dabei sind besondere Löschungsvorschriften vorzusehen sowie Vorschriften, die sicherstellen, dass die Veröffentlichungen unversehrt, vollständig und aktuell bleiben, jederzeit ihrem Ursprung nach zugeordnet werden können und nach dem Stand der Technik durch Dritte nicht kopiert werden können. Dies entspricht weitgehend den Forderungen der DSB des Bundes und der Länder.
Auch der im Berichtszeitraum bereits vorliegende Entwurf der genannten Verordnung wurde mir vom TJM zur Stellungnahme übersandt. Da die Forderung nach einem wirksamen Kopierschutz und der wirklichen Tilgung von einmal ins Internet eingestellten Daten der Schuldner zumindest gegenwärtig noch nicht realisierbar ist, habe ich angeregt, eine zusätzliche Regelung aufzunehmen, die den Zugriff auf oder das Herunterladen ganzer Datenbanken ausschließt. Dies würde zur Begrenzung der Eingriffe in das informationelle Selbstbestimmungsrecht beitragen. Dem kommt die als BR-Drs. 1082/01 vom 18.12.2001 vorliegende Verordnung des BMJ nach.

10.17 Die beschwerliche Bearbeitung einer Petition aus dem Notarbereich

Verwundert darüber, welche Informationen der Betroffene mit einem Grundbuchauszug von einem Notar erhielt, wandte sich dieser gemäß § 11 ThürDSG an den TLfD. Der Grundbuchauszug, der ein Grundstück in Bruchteilsgemeinschaft an Wohnwegen, Grünflächen und Abstellplätzen betraf, enthielt Angaben zu allen Miteigentümern und insbesondere auch Belastungen durch Grundschulden und Hypotheken. Unschwer war daraus ablesbar, dass es sich dabei um die Höhe der Belastungen der einzelnen anliegenden Hausgrundstücke handelte. Damit wusste jeder über die Belastung der Grundstücke der Nachbarn Bescheid.

Diese Petition habe ich zum Anlass genommen, den Notar um Mitteilung der Rechtsgrundlage bzw. um Darlegung der Erforderlichkeit zur Übermittlung der genannten personenbezogenen Daten anderer Eigentümer zu bitten. Auch auf die Erinnerung an meine Anfrage erhielt ich keine Auskunft. Ich habe dies gemäß § 39 i. V. m. § 38 ThürDSG beanstandet. Macht jemand von seinem Recht Gebrauch, unbeschadet des allgemeinen Petitionsrechts und anderer Rechte sich an den Landesbeauftragten für den Datenschutz mit dem Vorbringen zu wenden, dass er sich bei der Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen in seinen schutzwürdigen Belangen beeinträchtigt fühlt, hat er ein Recht darauf, dass seine Petition bearbeitet und zeitnah beantwortet wird. Nach § 38 ThürDSG ist der LfD und seine Beauftragten von allen öffentlichen Stellen in der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist im Rahmen der Kontrollbefugnis nach § 37 ThürDSG insbesondere Auskunft zu ihren Fragen zu gewähren. Dieser Verpflichtung kam der Notar auch nach Einschaltung der Aufsichtsbehörden nicht im erforderlichen Umfang nach, so dass die Bürgeranfrage bislang nicht beantwortet werden konnte. Vielmehr berief er sich auf die Verschwiegenheitspflicht der Notare nach § 18 BNotO. Eine Auskunft zu personenbezogenen Daten war allerdings meinerseits auch nicht verlangt. Die Verschwiegenheitsverpflichtung der Notare spielt somit auch nach Auffassung des TJM im vorliegenden Fall keine Rolle.

10.18 Neufassung der bundeseinheitlichen Anordnung über die Benachrichtigung in Nachlasssachen

Im Zusammenhang mit der Neufassung o. g. bundeseinheitlicher Anordnung fand auch unter den DSB eine Diskussion statt. Inhalt dieser Anordnung war u. a., dass die Stellen, bei denen sich Testamente und Erbverträge sowie Erklärungen, nach deren Inhalt die Erbfolge geändert wird, in amtlicher Verwahrung befinden, das Standesamt benachrichtigen, das die Geburt einer Erblasserin oder eines Erblassers im Inland beurkundet hat. In allen anderen Fällen ist die Benachrichtigung an die Hauptkartei für Testamente beim Amtsgericht Schöneberg in Berlin zu richten. Dies soll dazu dienen, dass bei Eintritt des Erbfalls das Vorhandensein einer solchen Verfügung von Todes wegen bekannt ist. Unstreitig fehlt für diese Benachrichti-

gung eine spezielle Rechtsgrundlage. Ich habe die Auffassung vertreten, dass der Zweck der Benachrichtigung zumindest in den meisten Fällen dem Willen und den Interessen der betroffenen Verfasser entspricht. Durch die Benachrichtigung wird sichergestellt, dass die Verfügung von Todes wegen nach dem Eintritt des Erbfalls zur Wirkung kommen kann. Sollten allerdings Zweifel bestehen, ob die Übermittlung der Daten an die Standesämter auch im Interesse der Betroffenen erfolgt, hielt ich es auch für einen gangbaren Weg, die Einwilligung der Betroffenen einzuholen oder die Betroffenen von der beabsichtigten Übermittlung zu informieren und eine Widerspruchsmöglichkeit einzuräumen. Meine Stellungnahme wurde vom TJM an das federführende Justizministerium weitergeleitet. Diesem erschien die vorgeschlagene Einwilligungslösung wenig praxisgerecht. Es wurde vielmehr davon ausgegangen, dass mit der Neufassung der Anordnung keine Erweiterung der bisherigen Datenübermittlungen bewirkt werde, sondern lediglich das seit Jahrzehnten praktizierte Verfahren aktualisiert wird. Aus meiner Sicht wird aber dadurch das Verfahren für den Betroffenen nicht transparenter. Die Verwaltungsvorschrift des TJM zur Benachrichtigung in Nachlasssachen als gemeinsame Verwaltungsvorschrift des TJM und des TIM vom 5. April 2001 ist im JMBl. 2001, S. 37 und im ThürStAnz. 2001, S. 2063 veröffentlicht worden.

10.19 Was passiert mit unfrei versandten Behörden- und Gerichtsakten?

Datenschutz bedeutet auch, personenbezogene Daten gegen Verlust zu sichern. Der BfD hat die LfD aus gegebenem Anlass darüber informiert, dass auf dem Postweg versandte Sendungen mit Behörden- und Gerichtsakten unwiederbringlich verloren gehen können, wenn sie vom Absender unfrei versandt und vom Adressat deshalb nicht angenommen werden. Wenn nämlich während der anschließenden Lagerfrist bei der Frachtpostermittlungsstelle kein Nachforschungsauftrag vorliegt, können solche Sendungen an eine Verwertungsfirma veräußert und dort entsorgt werden.
Obwohl in Thüringen kein solcher Fall bekannt geworden war, habe ich diese Information zum Anlass genommen, die Ministerien, in deren Geschäftsbereich möglicherweise Behörden- und Gerichtsakten versandt werden, um Mitteilung der getroffenen Maßnahmen für

solche Fälle zu bitten. Dabei hat sich ergeben, dass grundsätzlich unfrankierte Post nicht entgegengenommen wird. Da aber insbesondere zwischen den Behörden der Behördenkurierdienst in Anspruch genommen wird, sind die Fälle einer Zurückweisung wegen Nachportokosten selten. Sollten dennoch unfrankierte Sendungen eingehen, wurde mir berichtet, dass differenziert gehandelt wird. Zum einen werden, falls möglich, die Absender von der Verweigerung der Annahme benachrichtigt, in anderen Bereichen wird von Fall zu Fall entschieden, ob gegebenenfalls doch das Porto nachgezahlt wird, insbesondere wenn es sich erkennbar um Akten handelt. Die bestehenden Regelungen halte ich insgesamt für ausreichend. Aufgrund der Nachfrage sind die einzelnen Bereiche für die Problematik sensibilisiert worden.

10.20 Datenschutz im Strafvollzug

10.20.1 Strafvollzugsgesetz

Mit dem Vierten Gesetz zur Änderung des Strafvollzugsgesetzes (4. StVollzGÄndG), das am 1. Dezember 1998 in Kraft getreten ist (BGBl. I, S. 2461), wurden in das Strafvollzugsgesetz, wie im 3. TB (10.18) erwähnt, bereichsspezifische datenschutzrechtliche Regelungen eingefügt. Beispielsweise bedarf die Überwachung von Unterhaltungen der Strafgefangenen mit Besuchern einer Einzelfallentscheidung, von Telefongesprächsüberwachungen ist sowohl der Gefangene als auch der Gesprächspartner zu unterrichten und Informationen, die bei der Besuchs- und Postüberwachung gewonnen werden, unterfallen einer besonderen Zweckbestimmung. Bei durch erkennungsdienstliche Maßnahmen erlangten Daten besteht auf Antrag des Gefangenen eine Vernichtungspflicht. Es gilt der Grundsatz der Datenerhebung beim Betroffenen, eine Datenerhebung bei Dritten darf nur dann erfolgen, wenn die Voraussetzungen des § 13 Abs. 2 BDSG vorliegen, Daten über Dritte dürfen nur erhoben werden, wenn dies unerlässlich ist. Die Mitteilung über den Aufenthaltsort des Gefangenen an öffentliche Stellen und an private Empfänger ist jeweils unter besonderen Voraussetzungen zulässig. Gesundheitsdaten sowie Daten über das religiöse und weltanschauliche Bekenntnis dürfen innerhalb der Anstalt nicht allgemein kenntlich gemacht werden. Unter bestimmten Voraussetzungen darf der An-

staltsarzt dem Arztgeheimnis unterliegende Daten weitergeben. Darauf sind Gefangene vor der ärztlichen Untersuchung hinzuweisen. In Dateien gespeicherte personenbezogene Daten unterfallen einer zweijährigen Löschfrist, für Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter gilt eine generelle zwanzigjährige maximale Aufbewahrungsfrist; Gefangenenbücher dürfen dreißig Jahre aufbewahrt werden. Darüber hinaus haben die Betroffenen einen Auskunftsanspruch, bei einem besonderen rechtlichen Interesse auch einen Akteneinsichtsanspruch.

10.20.2 Kontrolle in einer Justizvollzugsanstalt

Die Umsetzung der datenschutzrechtlichen Vorschriften des geänderten Strafvollzugsgesetzes habe ich bei einer im Berichtszeitraum durchgeführten Kontrolle in einer Justizvollzugsanstalt einbezogen.
So habe ich unter anderem die Führung und Aufbewahrung von Gefangenenpersonalakten überprüft. Den Gefangenen wurde bei der Aufnahme ein Vordruck mit der Überschrift „Belehrung“ vorgelegt. Darin war die Erklärung enthalten, dass sich der Betroffene grundsätzlich damit einverstanden erklärt, dass von Seiten der Anstalt bei etwaigen Anfragen privater Personen oder Stellen Auskunft erteilt wird. Dieses grundsätzliche Einverständnis habe ich als zu unbestimmt angesehen. Das geänderte Formblatt lässt nunmehr Eintragungen oder Differenzierungen zu.
Darüber hinaus habe ich festgestellt, dass psychologische Gutachten von Gefangenen mit im Rahmen der Erstellung vom Gefangenen angegebenen Daten Dritter, beispielsweise Angaben zu Opfern oder Bezugspersonen, zur Gefangenenpersonalakte genommen werden. Hierzu hat die JVA dargelegt, die Aufnahme von psychologischen Gutachten in die Gefangenenpersonalakte sei als Grundlage für vollzugliche Entscheidungen unverzichtbar. In den Fällen, in denen Daten Dritter enthalten sind, wird allerdings zukünftig darauf geachtet, inwieweit diese für das Gutachten von entscheidender Bedeutung sind.
Die Herausgabe von Gefangenenpersonalakten zur Einsicht durch Bedienstete der JVA wird handschriftlich auf einem Fehlblatt protokolliert. Eine solche Protokollierung wurde allerdings nicht vorgenommen, wenn in den Räumen der Vollzugsgeschäftsstelle Einblick genommen wurde. Aus Sicht des TLfD besteht jedoch kein Grund für

diese Ausnahmeregelung. Im Zuge der Kontrolle wurde die Verfahrensweise dahingehend geändert, dass zukünftig alle Einsichtnahmen protokolliert werden.
Änderungsbedarf war aus Sicht des TLfD auch bezüglich der von den betroffenen Gefangenen formularmäßig abzugebenden Erklärung zur Befreiung des behandelnden Arztes von der Schweigepflicht gegeben. Eine solche Erklärung ist von den Betroffenen dann abzugeben, wenn sie außerhalb der Justizvollzugsanstalt ärztlich behandelt werden müssen. Die abverlangte Erklärung war zu allgemein gehalten. Eine unbestimmte Befreiung von nicht näher bezeichneten Ärzten zu einem nicht bezeichneten Zweck kann nicht verlangt werden. Auch hier ist die JVA meiner Empfehlung nachgekommen und hat das Formblatt entsprechend geändert.

10.20.3 Privatisierung des Strafvollzugs

Der Strafvollzug gehört zum Kernbereich staatlicher Aufgabenwahrnehmung und ist als solcher im Hinblick auf Artikel 33 Abs. 4 und 5 GG nicht privatisierungsfähig. Dennoch kann der Staat gewisse Aufgaben an Private übertragen. Die Verantwortung verbleibt beim Staat. Auf meine Anfrage hat mir das TJM mitgeteilt, dass in Thüringen im Wesentlichen die Aufgaben der Ausbildung der Gefangenen, die Durchführung des Einkaufs für die Gefangenen, die ärztliche Betreuung der Gefangenen und die Sicherstellung der Arbeit für Gefangene in den Justizvollzugsanstalten im Wege des Auftrags privaten Dritten übertragen wurden.

11. Gesundheits- und Sozialdatenschutz

11.1 Gesundheitsreform 2000 - Datentransparenzgesetz

Wie bereits im 3. TB (11.1) dargestellt, wurden die auf Betreiben der DSB des Bundes und der Länder durch den Gesundheitsausschuss des Deutschen Bundestages (BT-Drs. 14/1977) zum Gesundheitsreformgesetz 2000 vorgenommenen Änderungen hin zu einem Patientendatenschutz durch Pseudonymisierung nicht geltendes Recht. Ende 2000 hat das BMG eine Projektgruppe eingesetzt, die nunmehr Vorschläge für ein Gesetz über Datentransparenz und Datenschutz in der gesetzlichen Krankenversicherung (Datentransparenzgesetz)

erarbeiten sollte. Hierzu wurden den DSB des Bundes und der Länder auch Vorentwürfe für ein solches Gesetz zur Stellungnahme vorgelegt. Diese orientierten sich zwar an den vom Bundestag in der Beschlussempfehlung des Gesundheitsausschusses zum Gesundheitsreformgesetz (BT-Drs. 14/1977) formulierten Bestimmungen. Allerdings waren keine klaren Regelungen für die Reidentifikation pseudonymisierter Datensätze vorgesehen und zudem eine zu großzügige Möglichkeit von Reidentifizierungen geplant. Eine weitere wesentliche Abweichung von der Beschlussempfehlung des Gesundheitsausschusses war die Tatsache, dass nicht mehr Abrechnungsdaten aller Leistungserbringer vor ihrer Weiterleitung an die Krankenkasse pseudonymisiert werden sollten, sondern bei einem Teil der Leistungserbringer weiterhin eine personenbezogene Speicherung bei den Krankenkassen vorgesehen war. Schließlich war auch in den Überlegungen keine klare Trennung der Vertrauensstelle von den übrigen Daten verarbeitenden Stellen des Systems vorgesehen. Auf diese Punkte hat der BfD in Übereinstimmung mit den LfD‘s das BMG hingewiesen. Weder eine Stellungnahme des BMG zu den Anregungen der DSB des Bundes und der Länder noch eine erkennbare Gesetzgebungsaktivität war jedoch seither zu verzeichnen.

11.2 Drittes Gesetz zur Änderung des Heilberufegesetzes

Im Berichtszeitraum stand auch die Änderung des Heilberufegesetzes auf der Tagesordnung. Das TMSFG hat mich im Gesetzgebungsverfahren beteiligt. In diesem Rahmen habe ich auf datenschutzrelevante Aspekte hingewiesen und zum Teil auch Formulierungsvorschläge unterbreitet. Bei der vorgesehenen Präzisierung der Rechtsgrundlage zur Errichtung von Versorgungswerken bspw. wurde auf meine Anregung hin in der Satzungsermächtigung in § 5b Abs. 1 Satz 4 eine Nummer 13 ergänzt, wonach auch Art und Umfang der zur Erfüllung der Aufgaben des Versorgungswerks erforderlichen personenbezogenen Daten in der Satzung zu regeln sind. In § 5 a Abs. 2 war zunächst vorgesehen, dass die Kammern berechtigt sein sollten, soweit hinreichende Anhaltspunkte für eine Verletzung von Berufspflichten vorliegen, die zur Aufklärung erforderlichen personenbezogenen Daten des betroffenen Kammerangehörigen zu erheben und zu verarbeiten. Als Grund hierfür wurde angegeben, dass eine Ahndung von geringfügigen Verletzungen der Berufspflichten möglich sein sollte. Ich

habe diese Regelung für entbehrlich gehalten, da bereits im geltenden Heilberufegesetz in den §§ 47 ff das Verfahren im Zusammenhang mit der Verletzung von Berufspflichten explizit geregelt ist. Das TMSFG hat sich meiner Meinung angeschlossen und als ein dem berufsgerichtlichen Verfahren vorgelagertes Sanktionsmittel die Rüge in § 46 a eingefügt. In einem geänderten § 5 Abs. 3 sollte die originäre Zuständigkeit der Kammern für die Durchführung von Qualitätssicherungsmaßnahmen geregelt werden. Gemäß der vorliegenden Gesetzesbegründung sollen die Befugnisse der Kammern dahin präzisiert werden, dass diese neben der Erhebung auch zur Verarbeitung und Nutzung von personenbezogenen Daten befugt sind. Nachdem ich die ursprünglichen Formulierungen als viel zu unbestimmt bewertet habe, wurde im Folgenden festgelegt, dass Patientendaten ausschließlich in anonymisierter Form erhoben werden dürfen. Auch die Erhebung und Verarbeitung von Daten der Kammerangehörigen bedarf aus meiner Sicht einer normenklaren gesetzlichen Grundlage. Bei Vorliegen der Erforderlichkeit zur Erhebung und Verarbeitung personenbezogener Daten der Kammerangehörigen aus der Berufsausübung sind gleichfalls die Rahmenbedingungen im Heilberufegesetz selbst vorzugeben. Mit der Ergänzung im § 5 Abs. 3, dass die Satzungsregelungen der Kammern zur Datenerhebung, Verarbeitung und Nutzung sowie zur Teilnahme der Kammerangehörigen an eigenen Qualitätssicherungsmaßnahmen nach Maßgabe des 6. Abschnittes des Heilberufegesetzes – der die Berufsausübung regelt – erfolgen soll sowie der Anfügung einer Nummer 17 in § 23, dass in der Berufsordnung weitere Vorschriften über Berufspflichten bezogen auf die Teilnahme der Kammerangehörigen an Maßnahmen der Qualitätssicherung zu treffen sind, wurde dem datenschutzrechtlichen Anliegen Genüge getan.

Nicht gefolgt wurde meinem Vorschlag, im Heilberufegesetz eine Regelung aufzunehmen, den Kammern in bestimmten Notsituationen die Aufgabe zu übertragen, Patientenakten zur Sicherung der gesetzlichen und berufsrechtlichen Aufbewahrungsfristen zeitweise in Obhut zu nehmen. Unter den DSB des Bundes und der Länder wurde dieses Thema bereits mehrfach angesprochen. Bei den Ausnahmesituationen geht es bspw. um solche Fälle, wenn ein niedergelassener Arzt plötzlich verstirbt oder erkrankt ist und kein Praxisnachfolger vorhanden ist. Im Rahmen meiner Kontrolltätigkeit wurde ich des öfteren nach entsprechenden Zuständigkeitsregelungen in Thüringen

gefragt. Obwohl eine ausdrückliche Regelung im Heilberufegesetz nicht aufgenommen worden ist, halte ich es für wichtig, eine Verfahrensweise für die geschilderten Fälle festzulegen.

11.3 Änderung des Thüringer Krankenhausgesetzes

Im Rahmen der im Berichtszeitraum vorgesehenen Änderung des Thüringer Krankenhausgesetzes wurde der TLfD von Seiten des TMSFG beteiligt.
Hingewiesen habe ich in diesem Zusammenhang auf einen Konkretisierungsbedarf der Bestimmungen zur Auftragsdatenverarbeitung im Hinblick auf eine Fernwartung von EDV-Anlagen, bei der die Kenntnisnahme von personenbezogenen Daten, die dem besonderen Schutz des § 203 StGB unterliegen, durch den Auftragnehmer nicht ausgeschlossen werden kann. In Anbetracht der in Kraft getretenen EU-Datenschutzrichtlinie ist zu beachten, dass die Bestimmungen zur Datenverarbeitung im Auftrag in den Landeskrankenhausgesetzen der Länder unter Art. 8 Abs. 4 der EG-DSRL fallen.
Dem besonderen Schutz sensibler Daten ist aufgrund der sich rasch entwickelnden automatisierten Datenverarbeitung, neuer Techniken und Technologien im besonderen Maße Rechnung zu tragen. In diesem Zusammenhang wird in der Beschlussempfehlung und dem Bericht des Innenausschusses zum 15. TB des BfD in der BT-Drs. 13/11168 vom 23.06.1998 dem Bundestag zur Beschlussfassung empfohlen:
„Der Deutsche Bundestag wiederholt die Auffassung in Nummer 8 seines Beschlusses vom 11. Dezember 1997 und bittet die Bundesregierung, eine Gesetzesinitiative zu ergreifen, um beim Einsatz moderner Informationstechnik im Gesundheitswesen den gebotenen Schutz dieser Daten auch außerhalb von Arztpraxen und Krankenhäusern sicherzustellen. Der Deutsche Bundestag hält den Handlungsbedarf für gesetzliche Regelungen zur Nutzung von Gesundheitsdaten für gegeben und erwartet umgehend eine Initiative der Bundesregierung, nicht nur um eventuelle Fehlentwicklungen zu vermeiden, sondern auch um Entwicklungssicherheit und Akzeptanz zu fördern."
Der Entwurf eines Ersten Gesetzes zur Änderung des ThürKHG wurde dem TLfD mit der Bitte um Stellungnahme aus datenschutzrechtlicher Sicht zugeleitet. Im Rahmen der abgegebenen Stellung-

nahme wurden auch Formulierungsvorschläge bezüglich der Regelungen zur Auftragsdatenverarbeitung unterbreitet.

11.4 Änderung adoptionsrechtlicher Vorschriften

Die Bundesrepublik Deutschland hat am 7. November 1997 das Haager Übereinkommen vom 29. Mai 1993 über den Schutz von Kindern und die Zusammenarbeit auf dem Gebiet der internationalen Adoption unterzeichnet. Zur Umsetzung in innerstaatliches Recht wurde im Berichtszeitraum neben dem Vertragsgesetz von der Bundesregierung der Entwurf eines Begleitgesetzes vorgelegt. Ziel des Haager Übereinkommens ist in erster Linie die Wahrung der Rechte des Kindes bei grenzüberschreitenden Adoptionen. Zu diesem Zweck sieht das Übereinkommen auch die Übermittlung personenbezogener Daten sowohl der Adoptiveltern als auch des Adoptivkindes zwischen den jeweiligen Behörden des Heimatstaates vor. Im Gesetzgebungsverfahren sind auch einige Anregungen der DSB des Bundes und der Länder in das Gesetz aufgenommen worden. So ist in § 4 des Adoptionsübereinkommens-Ausführungsgesetzes eine Pflicht der Auslandsvermittlungsstelle aufgenommen worden, die deutschen Adoptionsbewerber darauf hinzuweisen, wenn nach den Vorschriften des Herkunftslandes des Kindes im Rahmen des Adoptionsverfahrens - anders als nach § 1758 BGB in Deutschland - das Adoptionsgeheimnis gegenüber den leiblichen Eltern nicht gewahrt werden kann. Darüber hinaus wurden auf Vorschlag der DSB des Bundes und der Länder in § 2a Abs. 6 des Adoptionsvermittlungsgesetzes Protokollierungspflichten aufgenommen, um eine nachträgliche Datenschutzkontrolle zu gewährleisten. Ebenso wurde in § 9 b Adoptionsvermittlungsgesetz die Aufbewahrungsdauer der Vermittlungsakte auf 60 Jahre nach der Geburt des Kindes festgelegt. In § 9 d Adoptionsvermittlungsgesetz wurde vom BMJ bereits eine bereichsspezifische Datenschutzvorschrift vorgesehen, die die Zweckbindung der im Zusammenhang mit der Adoptionsvermittlung verarbeiteten Daten einer strengen Zweckbindung in Anlehnung an die Vorschriften des Sozialdatenschutzes unterstellt. Das Gesetz zur Regelung von Rechtsfragen auf dem Gebiet der internationalen Adoption und zur Weiterentwicklung des Adoptionsvermittlungsrechts (vom 05.11.2001, BGBl. I, S. 2950) tritt am 1. Januar 2002 in Kraft.

11.5 Pflege-Qualitätssicherungsgesetz und Änderung des Heimgesetzes

In der Vergangenheit war es immer wieder zu Vernachlässigungen und Missständen in Pflegeheimen gekommen, sodass sich der Bundesgesetzgeber dazu entschlossen hat, im Rahmen der Änderung des Heimgesetzes (vom 5. November 2001, BGBl. I, S. 2960) und des SGB XI (Pflege-Qualitätssicherungsgesetz vom 09. September 2001, BGBl. I, S. 2320) u.a. auch die Regelungen zur Kontrolle der Heime durch die Heimaufsichtsbehörde, die Pflegekassen sowie den Medizinischen Dienst der Krankenversicherung zu überarbeiten. Im Rahmen des Gesetzgebungsverfahrens haben die DSB des Bundes und der Länder auch Gelegenheit bekommen, sich zu den vorgesehenen Regelungen aus datenschutzrechtlicher Sicht zu äußern. Dabei konnten einige Hinweise gegeben werden, die entweder in die Gesetzesformulierung oder aber in die Begründung aufgenommen wurden, um den datenschutzrechtlichen Belangen Rechnung zu tragen. Es wurden in § 13 HeimG einerseits die Aufzeichnungspflichten des Heimträgers wesentlich erweitert, um eine effektive Kontrolle der Heimunterbringung zu ermöglichen. Eine weitere zentrale Vorschrift ist der neue § 20 HeimG, der die zur Überwachung der Pflegeheime zuständigen Stellen zur Zusammenarbeit in Arbeitsgemeinschaften verpflichtet. Aus datenschutzrechtlicher Sicht ist zu begrüßen, dass damit eine normenklare Vorschrift geschaffen wurde, die die zum Teil bestehenden Zweifel, ob die Heimaufsichtsbehörden den Pflegekassen und dem Medizinische Dienst der Krankenversicherung die für eine effektive Kontrolle erforderlichen personenbezogenen Daten übermitteln dürfen, beseitigt. Darüber hinaus ist in § 20 Abs. 3 HeimG festgelegt, dass die für die Zusammenarbeit der Stellen erforderlichen Angaben einschließlich der bei der Überwachung gewonnenen Erkenntnisse untereinander ausgetauscht werden und dies bei personenbezogenen Daten grundsätzlich in anonymisierter Form erfolgt. In § 20 Abs. 3 HeimG wird davon eine Ausnahme gemacht, soweit es für die Zwecke nach dem SGB XI erforderlich ist. Die den Vorschriften des Heimgesetzes korrespondierenden Neuregelungen des Pflege-Qualitätssicherungsgesetzes sehen in § 117 SGB XI die Pflicht der Pflegekassen und des MDK zur engen Zusammenarbeit mit den Heimaufsichtsbehörden einschließlich der hierzu erforderlichen Datenübermittlungen vor. Weil die zuständigen örtlichen Träger

der Sozialhilfe häufig auch Kostenträger von Pflegeleistungen sind, wurde diesen neben den Heimaufsichtsbehörden in § 97 b SGB XI die Befugnis eingeräumt, von den Pflegekassen nach den §§ 80, 112 bis 115, 117 und 118 erhobenen personenbezogenen Daten zu verarbeiten und zu nutzen, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.

11.6 Sicherung der Selbstbestimmung bei genetischen Untersuchungen

Mit der im Jahr 2000 weitgehend erreichten Entschlüsselung des menschlichen Genoms sind neue und sehr schwierige Fragestellungen zum Schutz des Persönlichkeitsrechts sowohl des Betroffenen als auch seiner genetisch Verwandten aufgetreten. Bereits Ende der Achtziger Jahre, als sich diese Entwicklung der Wissenschaft angedeutet hat, haben die DSB des Bundes und der Länder auf ihrer Konferenz am 26. Oktober 1989 auf die besonderen Risiken für das informationelle Selbstbestimmungsrecht der Betroffenen bei der Durchführung von Genomanalysen hingewiesen und Grundsätze formuliert, an denen sich eine gesetzliche Regelung zur Genomanalyse orientieren sollte. Die 60. Konferenz der DSB des Bundes und der Länder am 12./13. Oktober 2000 hat diese Grundsätze in einer Entschließung (Anlage 11) nochmals bekräftigt. Ausgangspunkt für die besondere Gefährdungslage für das Persönlichkeitsrecht bei der Entschlüsselung des menschlichen Genoms stellt der Umstand dar, dass durch gentechnische Untersuchungen nur winziger Mengen organischen Materials (Speichel, Haarspitzen etc.) hochsensible Informationen über einen Menschen, dessen Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf gewonnen werden können. Bereits heute sind für viele, oft vererbliche Krankheiten Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Damit entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Würden diese Angaben systematisch ausgewertet und erfasst, entstünde ein bisher nie gekanntes Persönlichkeitsprofil hinsichtlich der Veranlagung zu bestimmten Erkrankungen. Weil diese genetischen Informationen aber auch relativ leicht, z. B. durch einen Speichelrest an einem Glas, gewonnen werden können, bedarf es zur

Sicherung des informationellen Selbstbestimmungsrechts klarer Regelungen, ob und wann genetische Untersuchungen durchgeführt und wem die Untersuchungsergebnisse zugänglich gemacht werden dürfen. Da durch Genomanalysen häufig auch Veranlagungen zu Krankheiten festgestellt werden können, für die es bislang noch keine Heilungsmöglichkeiten gibt und sich dadurch für den Betroffenen psychische Belastungen ergeben können, umfasst das informationelle Selbstbestimmungsrecht auch ein Recht auf Nichtwissen. Das bedeutet, dass der Betroffene ein Recht hat Ergebnisse von genetischen Untersuchungen nicht zur Kenntnis nehmen zu müssen. Die zentrale Forderung der DSB für die Sicherung des informationellen Selbstbestimmungsrechts im Bereich von genetischen Untersuchungen besteht darin, dass solche Untersuchungen grundsätzlich nur mit Einwilligungen des Betroffenen vorgenommen werden dürfen, nachdem dieser umfassend über die Folgen einer solchen Untersuchung beraten und aufgeklärt worden ist. Ausnahmen hiervon sind in einem Gesetz normenklar festzuschreiben. Dies ist bereits für den sog. genetischen Fingerabdruck zur Identifizierung bei der Strafverfolgung durch das DNA-Identitätsfeststellungsgesetz vom 7. September 1999 (BGBl. I, S. 2646) erfolgt. Der Betroffene muss zudem die Möglichkeit haben, die Einwilligung jederzeit zu widerrufen mit der Konsequenz, dass die bereits gespeicherten Daten zu löschen oder an den Betroffenen herauszugeben sind. Da vielfach Erkenntnisse über erbliche Veranlagungen auch die genetisch Verwandten betreffen, müssen diese im notwendigen Umfang in das Unterrichtungs- und Einwilligungsverfahren einbezogen werden. Die Einwilligung stellt jedoch beim Arbeits- oder Versicherungsverhältnis keine ausreichende Gewährleistung des informationellen Selbstbestimmungsrechts dar, weil der Arbeitsplatzbewerber oder der Versicherungsantragsteller durch die faktische Zwangssituation keine wirklich freie Entscheidung treffen kann. Deshalb sind die Anordnungen von Genomanalysen oder die Verwendung ihrer Ergebnisse in diesem Bereich grundsätzlich zu verbieten und Ausnahmen hiervon durch ein Gesetz zu regeln. In einer Entschließung auf Antrag von Rheinland-Pfalz vom 10. November 2000 (BR-Drs. 530/00) hat sich der Bundesrat gegen die Verwertung von Genomanalysen in der Privatversicherung ausgesprochen und die Bundesregierung aufgefordert, einen Gesetzentwurf mit spezifischen Regelungen vorzulegen, nach denen es Versicherern verboten ist, eine Genomanalyse zur Voraussetzung des

Abschlusses eines Versicherungsvertrages zu machen und der Versicherer nicht berechtigt ist, nach genetischen Dispositionen zu fragen, die dem Antragsteller oder den von der Schweigepflicht entbundenen Ärzten aufgrund anderweitig durchgeführter Analysen bekannt sind. Ausnahmen sollten nur unter engen begrenzten Voraussetzungen insbesondere zur Vermeidung missbräuchlicher Ausnutzung des Versicherungssystems zugelassen werden. Gleichzeitig hat die 60. Konferenz der DSB des Bundes und der Länder eine Arbeitsgruppe eingerichtet, die die in der Entschließung formulierten Anforderungen konkretisieren sollte. So wurde eine unter den DSB des Bundes und der Länder abgestimmte Stellungnahme an die Enquete-Kommission „Recht und Ethik der modernen Medizin“ des Deutschen Bundestages abgegeben, in der nochmals detailliert auf die in der Entschließung angeführten Forderungen und den sich daraus ergebenden Regelungsbedarf für den Gesetzgeber hingewiesen wurde. Das Ergebnis der Arbeitsgruppe wurde schließlich in der 62. Konferenz der DSB des Bundes und der Länder in Form einer Entschließung (Anlage 24) zusammengefasst, in der die bereits dargestellten Anforderungen an eine gesetzliche Regelung weiter konkretisiert und zum Teil ergänzt wurden.

11.7 Telematik im Gesundheitswesen – „Medikamentenchipkarte“

Auch im vergangenen Berichtszeitraum sind Überlegungen zum Einsatz von telematischen Anwendungen im Gesundheitswesen weiterentwickelt worden. So hat ein im Jahr 1999 bei der Gesellschaft für Versicherungswissenschaft und -gestaltung e. V. (GVG) mit den Bundesministerien für Gesundheit (BMG) und für Bildung und Forschung (BMBF) gegründetes „Aktionsforum Telematik im Gesundheitswesen“ (ATG) vier Teams zu den Themenbereichen „Elektronisches Rezept“, „Elektronischer Arztbrief“, „Sicherheitsinfrastruktur“ und „Europäische und internationale Dimensionen von Telematik im Gesundheitswesen“ eingesetzt. Von diesen Teams sind Handlungsempfehlungen für die Selbstverwaltungen und ggf. für die Gesetzgebung in Form von Managementpapieren erstellt und zur Kommentierung im Internet veröffentlicht worden (http://atg.gvg-koeln.de). Der AK Gesundheit und Soziales der Datenschutzkonferenz des Bundes und der Länder hat sich dabei insbesondere mit dem Managementpa-

pier zum Elektronischen Arztbrief befasst und hierzu eine gemeinsame Stellungnahme gegenüber der ATG abgegeben. Darin wurde insbesondere darauf hingewiesen, dass auch bei einer Übermittlung von Patienteninformationen auf elektronischem Weg grundsätzlich diejenigen rechtlichen Anforderungen gelten, die bei herkömmlicher Kommunikation zwischen den Ärzten oder den Ärzten und Dritten anzuwenden sind. Das bedeutet insbesondere, dass der Arzt grundsätzlich der Schweigepflicht nach § 203 StGB unterliegt und Patientendaten nur aufgrund einer gesetzlichen Norm oder einer in der Regel schriftlichen Einwilligung des Betroffenen an Dritte offenbaren darf. Zudem sollte vor der Offenbarung personenbezogener Daten auch geprüft werden, inwieweit für die vorgesehenen Zwecke auch eine Verarbeitung anonymisierter oder pseudonymisierter Daten (z. B. bei Qualitätssicherungsverfahren) für die Erreichung des beabsichtigten Zwecks ausreicht. Bei einer elektronischen Übermittlung müssen die bestehenden Patientenrechte z. B. auf Auskunft, Berichtigung, Sperrung und Löschung gewährleistet bleiben. Schließlich sind bei der Übermittlung im Rahmen von öffentlichen Netzen wirksame technische und organisatorische Sicherungsmaßnahmen zu ergreifen, die die Authentizität und Integrität der Daten gewährleistet. Hierzu kommt in erster Linie der Einsatz der elektronischen Signatur in Betracht. Zudem muss auf dem Übertragungsweg die Vertraulichkeit der Daten gewährleistet sein, was durch geeignete kryptographische Verschlüsselungsverfahren möglich ist.

Das Managementpapier zum elektronischen Rezept enthält weniger konkrete Aussagen. Dies liegt vor allem daran, dass man sich offenbar noch nicht auf eine von zwei möglichen Varianten einigen konnte, auf welchem das elektronische Rezept transportiert werden soll. Die erste Variante sieht vor, dass das elektronische Rezept vom verordnenden Arzt auf eine elektronische Chipkarte übertragen wird und diese vom Patienten in der Apotheke seiner Wahl eingelöst wird, wobei der Apotheker die auf der Chipkarte vermerkten Daten in seinen Rechner übernimmt, auf der Chipkarte löscht und die Daten zur weiteren Abrechnung mit den Krankenkassen weiterverarbeitet. Die zweite Variante sieht demgegenüber vor, dass der verordnende Arzt das elektronische Rezept an einen zentralen Server sendet und der Patient durch Vorlage einer Chipkarte den Apotheker seiner Wahl ermächtigt, dieses Rezept vom zentralen Server abzurufen, um dann zu Abrechnungszwecken weiterzuverarbeiten. Beide Varianten

setzen jedoch den Einsatz erheblicher finanzieller Mittel zur Einführung eines solchen elektronischen Rezepts voraus. Auch dies dürfte ein Grund sein, weshalb die Überlegungen bislang noch nicht weiter fortgeschritten sind.
Als eine weitere telematische Anwendung hat die in den letzten Jahren ausführlich erörterte Gesundheitschipkarte im Zusammenhang mit der Lipobay-Affäre in den letzten Monaten eine Wiederbelebung erfahren. Aus dem Bundesgesundheitsministerium wurden Pläne bekannt, wonach ein „Arzneimittelpass“ in Form einer elektronisch nutzbaren Medikamentenchipkarte eingeführt werden soll, auf der alle ärztlichen Verordnungen verzeichnet werden. Nach Auffassung des BMG soll damit eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Die DSB des Bundes und der Länder haben auf ihrer 62. Konferenz vom 24.-26.10.2001 in einer Entschließung (Anlage 23) erhebliche Bedenken gegen eine Medikamentenchipkarte als Pflichtkarte erhoben, weil die Patientinnen und Patienten damit rechtlich oder faktisch gezwungen wären, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde auch eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Gleichzeitig haben die DSB des Bundes und der Länder darauf hingewiesen, dass bei der Einführung einer solchen Medikamentenchipkarte die in den Entschließungen der 47. und 50. Konferenz aufgestellten Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten beachtet werden müssen (1. TB, 11.10). Von den DSB wurde eine Verknüpfung des „Arzneimittelpasses“ mit der Krankenversichertenkarte gemäß § 291 SGB V als problematisch eingestuft, weil damit die Patienten bei einem Arzt- oder Apothekenbesuch gezwungen wären, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Eine solche Verknüpfung wäre nur dann denkbar, wenn durch die technische Ausgestaltung der Karte sichergestellt wäre, dass der Versicherte nur jeweils diejenigen Gesundheitsdaten offenbaren kann, die er möchte. Konkrete Pläne des BMG wurden allerdings bislang nicht vorgelegt.

11.8 Kontrolle in einem Krankenhaus

Bei einer Kontrolle in einem Krankenhaus wurden schwerpunktmäßig die technischen und organisatorischen Maßnahmen zum Schutz der Patientendaten insbesondere beim Einsatz eines automatisierten Patientenverwaltungssystems sowie die Einbeziehung Externer in den Krankenhausbetrieb überprüft. Nach § 27 Abs. 10 ThürKHG hat das Krankenhaus diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Beachtung der in den § 27 Abs. 1 bis 9 ThürKHG enthaltenen Bestimmungen zu gewährleisten. So war festzustellen, dass im Krankenhaus umfängliche organisatorische Regelungen in einer Dienstanweisung zum Umgang mit Patientenunterlagen sowie Regelungen zum Einsatz der elektronischen Datenverarbeitung in einer EDV-Ordnung vorhanden waren. Von der Geschäftsführung des Krankenhauses wurde nach meinem Eindruck dem Datenschutz der ihm zukommende Stellenwert beigemessen, was sich u. a. daran zeigte, dass die im Rahmen der Prüfung angeregten Ergänzungen bzw. Klarstellungen der organisatorischen Regelungen umgehend umgesetzt wurden. In den Erfassungsmasken des Patientenverwaltungssystems war festzustellen, dass mitunter vorgefertigte Datenfelder enthalten waren, deren regelmäßige Eingabe nicht erforderlich ist. So waren die Felder „VIP“, „Organspender“ und „Kultur“ enthalten, ohne dass diese nach Auskunft des Krankenhauses von den Mitarbeitern genutzt werden. Zu diesen Feldern habe ich eine Überarbeitung angeregt. Dies wurde in die Wege geleitet, wobei übergangsweise das Ausfüllen der Datenfelder in einer organisatorischen Anweisung an die Mitarbeiter untersagt wurde. Ein weiteres Feld war mit „Schwarze Liste“ gekennzeichnet. In dieses Feld wurden nach Auskunft des Krankenhauses Angaben von Patienten aufgenommen, bei denen es in der Vergangenheit Unregelmäßigkeiten bei der Begleichung von Krankenhausrechnungen gegeben hat. Das Krankenhaus hat dabei argumentiert, dass bereits bei der Wiederaufnahme von Patienten, die ihre Rechnung nach zweimaliger Mahnung nicht bezahlt haben, ein Forderungsausfall vermieden werden soll. Durch die Bezeichnung „Schwarze Liste“ wird jedoch eine für den Betroffenen diskriminierende Wirkung erzeugt. Ich habe deshalb das Krankenhaus aufgefordert, die Ausfüllung dieses Datenfelds auszuschließen, wobei es grundsätzlich erlaubt ist, in einem Patientenverwaltungssystem zu vermerken, ob der betreffende Patient Krankenhausrechnungen noch nicht bezahlt hat. Zudem war auch regelmäßig die Eintragung des

Arbeitgebers vorgesehen, obwohl eine Erforderlichkeit der Erhebung und Speicherung nur bei einem Berufsunfall gegeben ist. Auch insoweit wurde das Krankenhaus aufgefordert, in einer organisatorischen Regelung festzulegen, dass dieses Datum nur ausgefüllt werden darf, falls eine Aufnahme wegen eines vermuteten oder erwiesenen Arbeitsunfalls erfolgt, was auch geschehen ist. Der Zugriff durch Mitarbeiter der Krankenhausverwaltung auf die Daten im Patientenverwaltungssystem erfolgt durch die Festlegung von differenzierten Rollen, denen dann die jeweiligen Mitarbeiter zugeordnet werden, um im Rahmen ihrer Aufgabenerfüllung möglichst nur auf die hierfür erforderlichen Daten zugreifen zu können. Dabei wurden den jeweiligen Rollen bestimmte Rollentyp-Aktionen zugewiesen, die nicht eindeutig erkennen ließen, auf welche personenbezogenen Datenarten durch den Rolleninhaber zugegriffen werden kann. Durch die nur sehr allgemein gehaltene schriftliche Dokumentation des Zugriffsberechtigungskonzepts ist es mitunter schwierig, den konkreten Umfang des Zugriffs der jeweiligen Mitarbeiter auf personenbezogene Daten zu ermitteln. Im Rahmen der Anforderungen an eine Zugriffskontrolle nach § 27 Abs. 10 und Abs. 2 ThürKHG i. V. m. § 9 Abs. 2 Satz 1 Nr. 9 ThürDSG ist es erforderlich, dass die Grundzüge der Zugriffsberechtigung ohne größeren Aufwand für die beteiligten Mitarbeiter des Krankenhauses ersichtlich sind. Deshalb habe ich das Krankenhaus aufgefordert, das Zugriffsberechtigungskonzept nachvollziehbar zu regeln. Das Krankenhaus hat daraufhin mitgeteilt, dass im Rahmen der Zuteilung der Zugriffsrechte nach den geltenden organisatorischen Regelungen ein Antrag zu stellen ist, bei dem über die Maskenübersicht jederzeit nachvollzogen werden könne, welche konkreten Zugriffsrechte jeder Nutzer besitzt. Das habe ich akzeptiert aber empfohlen, zukünftig auch die Zugriffsrechte auf die konkreten Datenarten schriftlich zu dokumentieren.

Was die Einbeziehung Externer in den Krankenhausbetrieb angeht, so war hier zunächst festzustellen, dass mit einem Privatunternehmen ein Vertrag zur Fernwartung der Datenverarbeitungsanlage des Krankenhauses abgeschlossen wurde. Obwohl vertragliche und organisatorische Vorkehrungen zum Schutz der Patientendaten getroffen worden waren, konnte das Krankenhaus nicht ausschließen, dass im Rahmen einer notwendigen Fernwartung aufgrund von Störungen im Betriebsablauf ein Zugriff auf Patientendaten erfolgen kann. Bei einem Zugriff auf Datenverarbeitungsanlagen von Krankenhäusern

ist aber auch Artikel 8 Abs. 3 der EG-Datenschutzricht-linie zu beachten. Danach dürfen sensible Daten über die Gesundheit nur dann zum Zweck der Behandlung sonstigen Personen zugänglich gemacht werden, wenn diese einer dem Berufsgeheimnis entsprechenden Geheimhaltungspflicht unterliegen. Die allgemeinen Auftragsdatenverarbeitungsvorschriften stellen dies nicht sicher. In Thüringen ist in § 27 Abs. 5 Satz 2 ThürKHG geregelt, dass eine Auftragsdatenverarbeitung zulässig ist, wenn das Krankenhaus sicherstellt, dass beim Auftragnehmer besondere technisch-organisatorische Schutzmaßnahmen eingehalten werden und solange keine Anhaltspunkte dafür bestehen, dass durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden. Wie bereits im 2. TB (11.10) dargelegt, gehe ich jedoch davon aus, dass durch das Verbringen (hier in elektronischer Form) der Daten aus dem Krankenhaus zu einem externen Auftragnehmer regelmäßig entgegenstehende Interessen des Patienten beeinträchtigt werden. So habe ich das Krankenhaus aufgefordert, einen Zugriff auf patientenbezogene Daten durch externe Auftragnehmer nur in den Fällen zu erlauben, in denen dies zur Erhaltung der Arbeitsfähigkeit des Krankenhausbetriebs unumgänglich ist. Das hat mir das Krankenhaus zugesichert.

Im Krankenhausbetrieb ist auch ein privater Caterer einbezogen, der die Essensversorgung des Krankenhauses sicherstellt und sich auf dem Gelände des Krankenhauses befindet. Die Essensbestellung und –abwicklung kommt dabei mit relativ wenigen Angaben aus. Die Patienten haben für jede Mahlzeit eine maschinenlesbare Karte durch Ankreuzen der jeweils gewünschten Menübestandteile und Angabe von Name, Station und Zimmer auszufüllen. Diese werden eingesammelt und nur die Angaben der Menübestandteile in das Datenverarbeitungssystem eingelesen und zur Essensabwicklung gespeichert. Dies dient dazu, festzustellen, wie viele Portionen jeweils gebraucht werden. Die Karten werden dann dem Küchenpersonal übergeben, das nach den dort aufgeführten Angaben die Menüs in die Transportbehältnisse portioniert und die Karte dem Behältnis zur Essensausgabe durch das Pflegepersonal beifügt. Es bestünde somit nur die Möglichkeit, dass bei diesem Vorgang vom Küchenpersonal kurzzeitig zur Kenntnis genommen werden könnte, welcher Patient sich in welcher Station des Krankenhauses aufhält und welche Kostart dieser bekommt. Da das Küchenpersonal keine weiterführende Zusatzin-

formationen zur Identität der Patienten hat, ging ich von einer weit gehenden Pseudonymisierung aus, wobei ich angeregt habe, zur Zuordnung der Mahlzeiten zu den Patienten neben der Station und der Zimmernummer nur den Nachnamen des Patienten zu verwenden. Das wurde vom Krankenhaus dahingehend aufgegriffen, dass neben dem Nachnamen nur noch der erste Buchstabe des Vornamens verwendet wird.

11.9 Umsetzung des § 73 Abs. 1 SGB V im Krankenhausbereich

Der im Rahmen der Gesundheitsreform 2000 aufgenommene § 73 Abs. 1 b SGB V hat bei der Umsetzung zu Anfragen geführt. Im AK Gesundheit und Soziales der Datenschutzkonferenz ist daraufhin das Verhältnis der Landeskrankenhausgesetze (in Thüringen: § 27 Abs. 6 Nr. 2 ThürKHG) zu § 73 Abs. 1 b SGB V diskutiert worden. Dabei ging es um die Frage, ob es auch bei der Übersendung des Krankenhausentlassungsberichts an den nachbehandelnden Arzt stets einer schriftlichen Einwilligungserklärung des Patienten nach § 73 Abs. 1 b SGB bedarf. Im Ergebnis bestand Einigkeit, dass § 73 Abs. 1 b SGB V aufgrund seiner Entstehungsgeschichte nur die Fälle umfasst, bei denen nach dem Hausarztmodell Zentrale Dokumentationen bei einem (Haus-) Arzt eingerichtet werden, wobei der Patient nicht mit einer derartigen Datenübermittlung rechnen muss. Die Landeskrankenhausgesetze und die Berufsordnungen der Ärzte erfassen dagegen Behandlungszusammenhänge, bei denen Datenübermittlungen möglich sind. Soweit daher in § 27 Abs. 6 Nr. 2 ThürKHG geregelt ist, dass eine Übermittlung von Patientendaten ohne Einwilligung des Betroffenen zur Durchführung des Behandlungsvertrages einschließlich der Nachbehandlung zulässig ist, wenn nicht die Patienten nach Hinweis auf die beabsichtigte Übermittlung etwas anderes bestimmt haben, sind damit solche Übermittlungen erfasst, die im Behandlungszusammenhang stehen und mit denen der Versicherte regelmäßig rechnen muss. Der BfD hat diese Auffassung auch mit dem Bundesgesundheitsministerium erörtert, das die Auffassung der DSB teilt. Damit bedarf es für die Übersendung des Krankenhausentlassungsberichts an den nachbehandelnden Arzt nach dem ThürKHG keiner ausdrücklichen Einwilligung des Patienten. Dieser kann einer solchen nach Hinweis auf die Übermittlung jedoch

widersprechen. Der Anwendungsbereich des § 73 Abs. 1 b SGB V umfasst dagegen die Errichtung von neuen zentralen Patientensammlungen, bspw. beim Hausarzt, ohne dass es hierzu eines konkreten Behandlungszusammenhangs bedarf.

11.10 Abrechnung interkurrenter medizinischer Behandlungen im Maßregelvollzug

Aufgrund einer Anfrage wurde ich auf datenschutzrechtliche Probleme im Rahmen des Verfahrens zur Abrechnung interkurrenter medizinischer Behandlungen im Maßregelvollzug aufmerksam. Dazu wurde eine Verwaltungsvorschrift des TMSFG zu Kostenregelungen für Unterbringungen in Maßregelvollzugseinrichtungen des Freistaats Thüringen vom 01.07.1998 erlassen. Darin ist u. a. das Verfahren zur Erstattung der Kosten für die interkurrente medizinische Behandlung von Patienten, die in Maßregelvollzugseinrichtungen untergebracht sind, geregelt. Interkurrente Behandlungen sind solche Behandlungen von niedergelassenen Ärzten oder Krankenhäusern, die nicht in der Maßregelvollzugseinrichtung selbst erbracht werden können, wie z. B. Operationen, Zahnbehandlungen usw. Wegen der bundesweit einmaligen Situation in Thüringen, dass der Geschäftsbereich des TMSFG zwar die fachlichen Angelegenheiten des Maßregelvollzugs nach §§ 63, 64 StGB umfasst, jedoch die Haushaltsmittel vom TJM bewirtschaftet werden, sieht die nicht veröffentlichte Verwaltungsvorschrift vor, dass die Angaben über die Abrechnung der Kosten für die interkurrente Behandlung (zumindest in einem Teil der Fälle) von den Maßregelvollzugseinrichtungen sowohl dem TMSFG nachgeordneten Landesverwaltungsamt zur Vorprüfung als auch anschließend den jeweiligen Kostenstellen der einweisenden Gerichte und Staatsanwaltschaften zur Abrechnung vorgelegt werden müssen. Dabei werden sensible Daten über den Gesundheitszustand der Betroffenen übermittelt. Dies führt dazu, dass diese sensiblen Daten auf der Grundlage des praktizierten Verfahrens an mehreren Stellen doppelt vorgehalten werden, ohne dass hierfür ein zwingender Grund ersichtlich ist. Darüber hinaus erfolgt eine Übermittlung dieser Gesundheitsdaten an Behörden und Gerichte, ohne dass es eine gesetzliche Grundlage zur Offenbarung dieser, der ärztlichen Schweigepflicht unterliegenden Daten, gibt. Von dieser Praxis habe ich mich auch bei einem Kontrollbesuch beim TLVwA überzeugt. Dort zeigte

sich auch, dass die Verfahrensweise in Thüringen von derjenigen der anderen Bundesländer abweicht. In einem Fall, bei dem die Kostenübernahme für eine Operation eines von einer Staatsanwaltschaft außerhalb Thüringens eingewiesenen Patienten geprüft wurde, hat das TLVwA die Abrechnungsunterlagen an die einweisende Staatsanwaltschaft übersandt. Als ich beim Kontrollbesuch darauf hingewiesen habe, dass die Verwaltungsvorschrift doch nur für Thüringen gelte und nach meiner Kenntnis in keinem anderen Bundesland die Kostenabrechnung durch die einweisenden Staatsanwaltschaften und Gerichte erfolge, hat sich nach einem durchgeführten Anruf durch das TLVwA bei der besagten Staatsanwaltschaft ergeben, dass diese unzuständig war und die Unterlagen seinerzeit an das dort zuständige Zentrum für Psychiatrie weitergeleitet hat. Würde auch in Thüringen die Abrechnung ausschließlich über die Landesfachkrankenhäuser bzw. über das die Fachaufsicht führende Landesverwaltungsamt durchgeführt, so wäre es wohl auch nicht zu dieser Übermittlung von sensiblen Daten an eine unzuständige Stelle gekommen. Im Nachgang zur Kontrolle hat das Landesverwaltungsamt mitgeteilt, dass bei unklarer Zuständigkeitslage künftig vor einer Übermittlung von Abrechnungsdaten insbesondere an Stellen außerhalb von Thüringen zunächst die Zuständigkeit des Empfängers geklärt werden soll.

Das aufgrund dieser Verwaltungsvorschrift praktizierte Verfahren habe ich gegenüber dem TMSFG nach § 39 ThürDSG beanstandet und gefordert, den Umgang mit Patientendaten im Maßregelvollzug rechtskonform zu regeln, wobei sowohl die Zuständigkeiten der Stellen eindeutig zu bestimmen sind, die zulässigerweise mit den Patientendaten der Untergebrachten umgehen dürfen als auch der Umfang der Patientendaten festgelegt wird, die für Abrechnungszwecke erhoben, verarbeitet und genutzt werden dürfen, wobei dieser Umfang sich streng am Grundsatz der Erforderlichkeit zu orientieren hat. Nach längeren Gesprächen hat das TJM im Einvernehmen mit dem TFM den Vorschlag unterbreitet, zur Abhilfe der Beanstandung die Bewirtschaftung der Haushaltsmittel vom TJM auf das TMSFG zu übertragen. Damit würde die doppelte Vorhaltung von sensiblen Gesundheitsdaten bei zwei Stellen entfallen. Mit diesem Vorschlag wären aus meiner Sicht die datenschutzrechtlichen Probleme gelöst, wenn gleichzeitig normenklar festgelegt würde, welche Datenarten zu Abrechnungszwecken von der Maßregelvollzugseinrichtung dem

TLVwA zu Abrechnungszwecken übermittelt werden sollen. Eine neue Lage ist dadurch eingetreten, dass die psychiatrischen Landeskrankenhäuser zum 01.01.2002 privatisiert und den Trägern nach § 31 Abs. 1 ThürPsychKG in Beleihungsverträgen die Aufgabe des Maßregelvollzugs übertragen wurden. Das TMSFG hat mir mitgeteilt, dass nunmehr ein neues Verfahren der Leistungserbringung zwischen Justiz und den Trägern gefunden werden muss, was die nicht erforderliche Einschaltung weiterer Stellen überflüssig macht. Aus meiner Sicht ist die Beanstandung bisher nicht ausgeräumt.

11.11 MDK Gutachtentransfer zur AOK Thüringen

Die AOK Thüringen hat mit dem MDK Thüringen ein Verfahren zur Mitteilung von Gutachtenergebnissen nach § 277 Abs. 1 SGB V eingeführt, bei dem die Gutachtenergebnisse vor ihrem Ausdruck in eine sog. PDF-Datei umgewandelt und per E-Mail kryptographisch verschlüsselt der AOK Thüringen zur weiteren Bearbeitung übermittelt werden. Der MDK selbst löscht die Gutachtendatei nach Ausdruck des Gutachtens. Eine Übersendung des Gutachtens in Papierform erfolgt nicht mehr. Bei Kontrollen vor Ort habe ich festgestellt, dass die bei der AOK Thüringen eingegangenen Dateien vom MDK Thüringen an Sammelablagen der AOK Thüringen (sog. Ordner) gesandt werden, auf die jeweils alle Mitarbeiter eines Krankenhausfallbearbeiterteams (mit bis zu 35 Personen) sowie Führungskräfte und Innenrevisoren Zugriff haben. Diese Verfahrensweise habe ich gegenüber der AOK Thüringen und dem MDK Thüringen als einen Verstoß gegen das Speicherverbot des § 276 Abs. 2 Satz 6 SGB V bewertet und formell gemäß § 39 ThürDSG beanstandet. Der MDK darf nach dieser Vorschrift in Dateien nur Angaben zur Person und Hinweise auf bei ihm vorhandene Akten aufnehmen. Alle anderen Angaben zu medizinischen Sachverhalten darf der MDK nicht in Dateien speichern. Das wurde im Gesetzgebungsverfahren damit begründet, dass die Entstehung zentraler auswertbarer automatisierter Datensammlungen mit medizinischen Inhalten beim MDK verhindert werden sollten. Dadurch, dass die Gutachtenergebnismitteilungen vor deren Löschung beim MDK in eine PDF-Datei umgewandelt und an die AOK Thüringen versandt werden, wird aber gerade diese vom Gesetzgeber nicht gewollte zentrale Sammlung medizinischer Daten bei der AOK Thüringen eingerichtet. Es erscheint nicht vorstellbar,

dass der Gesetzgeber die Errichtung einer solchen Datensammlung beim MDK, dessen Mitarbeiter fast ausschließlich als Ärzte oder ärztliche Gehilfen der über § 203 StGB geschützten Schweigepflicht unterliegen, unterbinden wollte, diese aber bei der AOK Thüringen, bei der der Kreis der Zugriffsberechtigten noch erheblich größer ist, zulassen wollte. Diese gesetzgeberische Absicht kann nur im Sinne eines Erst-recht-Schlusses so verstanden werden, dass wenn schon beim MDK keine derartigen Datensammlungen errichtet werden dürfen, dies auch erst recht nicht bei den Krankenkassen zulässig ist. Meine Rechtsauffassung habe ich auch dem TMSFG mitgeteilt und dieses um eine Stellungnahme gebeten. Nach längerer Diskussion hat sich das TMSFG meiner Rechtsauffassung angeschlossen. Im Rahmen der Diskussion war von der AOK Thüringen immer wieder vorgetragen worden, dass mit diesem Verfahren eine schnelle und kostengünstige Übermittlung der Gutachtenergebnismitteilungen vom MDK an die AOK Thüringen erfolgen soll. Um dies zu ermöglichen, ohne jedoch gegen bestehende datenschutzrechtliche Vorschriften zu verstoßen, habe ich gefordert, dass bei den vom MDK übermittelten Gutachtenergebnismitteilungen die Integrität und Authentizität der Mitteilung sichergestellt ist und bei der AOK Thüringen keine automatisiert auswertbare Datensammlung über medizinische Daten entsteht, was dadurch zu erreichen ist, dass die Gutachten nach elektronischem Eingang ausgedruckt und die elektronischen Dateien dann gelöscht werden. Das TMSFG als zuständige Aufsichtsbehörde hat daraufhin dem MDK empfohlen, die Gutachtenergebnismitteilungen mit einer elektronischen Signatur zu versehen, um die erforderliche Authentizität und Integrität der Mitteilungen zu erreichen. Vom MDK wurde signalisiert, dass dies auf der Grundlage des überarbeiteten Signaturgesetzes und der Signaturverordnung umgesetzt werden soll. Der AOK Thüringen hat das TMSFG empfohlen, die übermittelten elektronischen Dateien nach deren Ausdruck zu löschen. Die AOK Thüringen hat daraufhin mitgeteilt, dies umzusetzen. Der Vorgang ist noch nicht abgeschlossen.

11.12 Datenanforderung der Krankenkassen zur Abrechnungsprüfung

Die Befugnis der Krankenkassen zur Erhebung medizinischer Daten bei Krankenhäusern zur Abrechnungsprüfung hat ihre Grundlage in

den für die gesetzliche Krankenversicherung abschließend im SGB V geregelten Übermittlungsbefugnissen der Leistungserbringer. § 301 SGB V ist dabei nicht nur eine Regelung für die Fälle der maschinenlesbaren Übermittlung von Leistungsdaten, sondern grundsätzlich eine abschließende Regelung zulässiger Datenübermittlungen zu Abrechnungszwecken zwischen Krankenhaus und Krankenkasse. Nach dieser Vorschrift sind die Krankenhäuser jedoch nicht zur Übermittlung von Krankenhausentlassungsberichten, Arztbriefen, Befundberichten, ärztlichen Gutachten, Röntgenaufnahmen etc. verpflichtet. In § 301 Abs. 1 Satz 1 Nr. 3 SGB V wird lediglich vorgegeben, dass auf Verlangen der Krankenkassen die medizinische Begründung für die Überschreitung der Dauer der Krankenhausbehandlung zu übermitteln ist. Diese Vorschrift eröffnet jedoch nicht die Befugnis zur Erhebung von Krankenhausentlassungsberichten etc., sondern vielmehr zur Übermittlung von Antworten auf bestimmte Fragen im erforderlichen Umfang. Die Einholung einer Einwilligungserklärung des Versicherten zur Übermittlung von darüber hinausgehenden medizinischen Unterlagen an die Krankenkasse stellt daher eine Umgehung der gesetzlichen Regelung zur Prüfung der medizinischen Sachverhalte durch den MDK dar. Daher sind Forderungen der Krankenkassen an Krankenhäuser und Ärzte, bei Vorliegen einer Einwilligungserklärung des Versicherten die oben genannten Unterlagen direkt an die Krankenkassen zu übermitteln, unzulässig.

Durch Anfragen wurde ich auf eine in diesem Zusammenhang stehende Praxis in Thüringen hingewiesen, wonach detaillierte medizinische Daten ohne eine Einwilligung oder eine Rechtsgrundlage zur Vorlage direkt bei den Krankenkassen angefordert worden seien. Ich habe daraufhin Kontrollbesuche bei zwei Krankenkassen durchgeführt und dabei folgende Feststellungen gemacht: Bei einer Krankenkasse habe ich zunächst ungenügende Datensicherungsmaßnahmen zum Schutz des Sozialgeheimnisses festgestellt, die von mir beanstandet wurden. Dabei waren im Bereich der Krankenhausfallbearbeitung Unterlagen für die Krankenhausfallbearbeitung in den jeweiligen Büros in Kartons oder Hängeschränken in nicht unbeträchtlichem Maß in Kartons offen auf Regalen aufbewahrt. Außerdem waren z. B. Fehlausdrucke, die ebenfalls Krankenhausabrechnungsdaten enthalten, offen in einer Ablage gelagert, um später als Notizpapier verwendet zu werden. Zudem waren in den Fluren Fotoko-

piergeräte aufgestellt, bei denen sich jeweils ein Papierkorb befand, in welchen Fehlkopien geworfen werden konnten. Hinzu kam, dass die Reinigung der Räume außerhalb der Dienstzeiten durch ein privates Reinigungsunternehmen erfolgte, wobei die Entsorgung des Altpapiers einschließlich der Unterlagen mit personenbezogenen Daten durch die Reinigungskräfte in der Form erfolgte, dass diese nach Dienstschluss die in den Papierkörben der Büros befindlichen Papierabfälle in einen Behälter gaben und anschließend durch ein Entsorgungsunternehmen vernichtet werden. Dadurch, dass es den Reinigungskräften nach Dienstschluss objektiv möglich war, ungehindert auf die in den Regalen offen gelagerten Krankenhausabrechnungsunterlagen zuzugreifen und diese zur Kenntnis zu nehmen ebenso wie die in die Papierkörbe eingeworfenen Papierabfälle mit sensiblen personenbezogenen Daten, sind keine ausreichenden technisch-organisatorischen Maßnahmen nach § 78a SGB X getroffen worden, die verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle). Daran änderte auch die Tatsache nichts, dass es dem Personal des Auftraggebers vertraglich untersagt war, dies zu tun. Da es sich bei der Krankenhausfallbearbeitung um äußerst sensible personenbezogene Daten handelt, habe ich diesen Verstoß nach § 39 ThürDSG beanstandet und gefordert, entweder durch das Unter-Verschluss-Halten sämtlicher Unterlagen oder durch die Vornahme der Reinigung unter Aufsicht des Krankenkassenpersonals durchzuführen, Abhilfe zu schaffen. Die Krankenkasse hat daraufhin die erforderlichen Maßnahmen getroffen und verschließbare Schränke zur Lagerung der Unterlagen angeschafft sowie das Personal in einer Dienstanweisung verpflichtet, Fehldrucke nicht als Notizpapier zu verwenden sowie Fehlkopien im Arbeitszimmer zu entsorgen.

Bezüglich der Anforderung von Unterlagen bei den Krankenhäusern zu den Krankenhausabrechnungsfällen ist die Krankenkasse dazu übergegangen, in bestimmten Krankenhäusern auf der Grundlage eines mit dem MDK Thüringen erarbeiteten Zielverweildauerkataloges für bestimmte Krankenhausbehandlungen befristete Kostenübernahmeerklärungen abzugeben, die mitunter auch unterhalb der von den Krankenhäusern nach § 301 Abs. 1 Nr. 3 SGB V mitgeteilten voraussichtlichen Behandlungsdauer liegen. Gleichzeitig wurden die Krankenhäuser aufgefordert, bei Überschreitung der Frist auf einem standardisierten Bogen Angaben über die durchgeführten diagnosti-

schen und therapeutischen Maßnahmen sowie eine medizinische Begründung für die Überschreitung der Behandlungsdauer anzugeben. Die von den Krankenhäusern vorgelegten Unterlagen werden dem MDK im Rahmen einer sog. Vorberatung übergeben, der dann entscheidet, ob die Begründung ausreichend ist oder ob weitere Unterlagen an den MDK übersandt werden sollen. Bei diesen - teilweise auch mehrfach zu einem Fall erfolgenden - Vorberatungen wird kein Gutachtenauftrag an den MDK erteilt und dieser teilt demzufolge auch dem Krankenhaus das Ergebnis seiner Begutachtung nach § 277 Abs. 1 SGB V nicht mit. Die Krankenkasse war der Auffassung, dass es sich hierbei um eine Beratung des MDK auf der Grundlage des § 275 Abs. 4 SGB V handele. Bei der anderen Krankenkasse habe ich eine vergleichbare Praxis dahingehend festgestellt, dass Kostenübernahmeerklärungen nur im Rahmen von durchschnittlichen Verweildauern abgegeben wurden, die in einem vom Medizinischen Dienst der Spitzenverbände (MDS) herausgegebenen Verweildauerkatalog entsprachen und damit in Einzelfällen auch medizinische Begründungen für diejenigen Fälle abgefordert wurden, in denen vom Krankenhaus ursprünglich eine längere voraussichtliche Behandlungsdauer angegeben worden war. Diese Verfahrensweise stellt eine Umgehung von § 301 Abs. 1 Nr. 3 sowie von § 275 Abs. 1 bis 3 SGB V dar. Der Katalog des § 301 SGB V stellt grundsätzlich eine abschließende Regelung zulässiger Datenübermittlungen zu Abrechnungszwecken zwischen Krankenhaus und Krankenkasse dar. In § 301 Abs. 1 Satz 3 SGB V ist ausdrücklich festgelegt, dass das Krankenhaus verpflichtet ist, der Krankenkasse die voraussichtliche Dauer der Krankenhausbehandlung mitzuteilen. Erst wenn die zunächst vom Krankenhaus angegebene voraussichtliche Dauer der Krankenhausbehandlung überschritten wird, kann die Krankenkasse vom Krankenhaus eine „medizinische Begründung“ bezüglich des Überschreitens verlangen. Die Krankenkasse kann daher nicht unabhängig von der Prognose des Krankenhauses anhand von ihr zugrunde gelegter Zeiträume Patientendaten anfordern. Zudem haben die Krankenkassen kein medizinisches Vorprüfungsrecht; dies obliegt ausschließlich dem MDK. Die gesetzlich vorgegebenen Prüfmechanismen bieten meines Erachtens umfängliche und hinreichende Möglichkeiten zur Überprüfung der Einhaltung der Wirtschaftlichkeit. Weitere Prozeduren, die nicht vom Gesetzgeber vorgegeben sind und zusätzliche Datenerhebungen und Datenflüsse bedingen, sind von

§ 301 Abs. 1 Nr. 3 SGB V nicht gedeckt und daher nicht zulässig. Sofern die von einem Krankenhaus angegebene voraussichtliche Dauer der Krankenhausbehandlung Zweifel bei der Krankenkasse weckt, kann sie den MDK nach den §§ 275 ff. SGB V einschalten und beauftragen. Dabei stellt die Verfahrensweise, bei der dem MDK medizinische Daten des Patienten übermittelt werden, ohne dass hierzu eine Beauftragung nach § 275 Abs. 1 SGB V erfolgt, eine Übermittlung ohne Rechtsgrundlage dar. Die Auffassung der Krankenkasse, wonach eine Datenübermittlung durch § 275 Abs. 4 SGB V gedeckt sei, ist unzutreffend, da dieser sich ausdrücklich auf andere als in Abs. 1 bis 3 genannten Aufgaben bezieht. Bei § 275 Abs. 4 SGB V handelt es sich vielmehr um eine Aufgabenzuweisung an den MDK, der eine Beratung zu allgemeinen medizinischen Fragen der gesundheitlichen Versorgung etc. zum Gegenstand hat. Auch wenn der Katalog nicht abschließend gefasst ist, so stellen jedenfalls die Absätze 1 bis 3 eine abschließende Regelung zur medizinischen Begutachtung von Einzelfällen dar. Um eine solche Einzelfallbegutachtung handelt es sich aber bei den so genannten „Vorberatungen". Im Übrigen setzt § 276 Abs. 2 Satz 2 SGB V voraus, dass bei einer Einschaltung des MDK nach § 275 Abs. 4 die Krankenkassen Sozialdaten vor der Übermittlung zu anonymisieren haben, was bei der festgestellten Verfahrensweise eben gerade nicht der Fall war, weshalb § 275 Abs. 4 nicht einschlägig ist. Mit der Verfahrensweise der so genannten medizinischen Einzelfallberatung zwischen Krankenkasse und MDK außerhalb der eigentlichen Begutachtung nach §§ 275 ff. SGB V werden meines Erachtens die hierbei geltenden Bestimmungen umgangen. Von meiner Rechtsauffassung habe ich die Krankenkassen sowie das TMSFG unterrichtet. Von TMSFG wurde mir mitgeteilt, dass diese Thematik auch unter den Aufsichtsbehörden des Bundes und der Länder erörtert wird.

11.13 Wirtschaftlichkeitsprüfung nach § 106 SGB V

In § 106 SGB V ist vorgesehen, dass die Krankenkassen und Kassenärztlichen Vereinigungen gemeinsam die Wirtschaftlichkeit der vertragsärztlichen Versorgung überprüfen. Hierzu wird ein besonderer Prüfungsausschuss eingerichtet. Datenschutzrechtliche Fragestellungen ergeben sich dabei, wenn es um die für die Wirtschaftlichkeitsprüfung erforderlichen Datengrundlagen geht. Dazu sind in den

§§ 296 und 297 SGB V detaillierte Regelungen enthalten. Bei Auffälligkeitsprüfungen finden bspw. arztbezogene Prüfungen derjenigen Ärzte statt, die Auffälligkeiten bei der Verordnung von Medikamenten aufweisen. In § 296 SGB V ist vorgesehen, dass die Kassenärztlichen Vereinigungen den Krankenkassen die Zahl der von einem Arzt veranlassten Behandlungsfälle sowie die Krankenkassen den Kassenärztlichen Vereinigungen die je Arzt verordneten Medikamente übermittelt. In Thüringen haben Ende 1999 die Landesverbände der Krankenkassen eine Vereinbarung auf Landesebene geschlossen, mit der sie ein privates Rechenzentrum mit der zur kassenartenübergreifenden Zusammenführung von Rezeptdaten zur Vorbereitung von Wirtschaftlichkeitsprüfungen beauftragt haben. Dabei gingen sie von einer gemeinsamen Auftragsdatenverarbeitung nach § 80 SGB X aus. Nachdem ich mir den hierzu abgeschlossenen Vertrag angefordert und überprüft habe, konnte ich diese Bewertung nicht teilen. Die unterschiedlichen Krankenkassen erteilten darin keine einzelne Datenverarbeitungsaufträge bezogen auf ihren eigenen Bereich, sondern es war Hauptzweck des Vertrages, dass ein neuer kassenartenübergreifender Datensatz über das Verordnungsverhalten jedes einzelnen Arztes gebildet wird, sodass die Vorschriften der Auftragsdatenverarbeitung, wonach der Auftraggeber für die Verarbeitung seiner Daten verantwortlich bleibt (§ 80 SGB X), schon begrifflich nicht anwendbar waren, weil ein Verantwortlicher für diesen neuen Datensatz nicht festgelegt war. Vielmehr handelte es sich nicht um eine Datenverarbeitung im Auftrag, sondern um eine Funktionsübertragung, d. h. die Erfüllung einer eigenständigen Aufgabe. Diese Aufgabe der Datenzusammenführung und –aufbereitung für die Wirtschaftlichkeitsprüfungen ist jedoch nach den Vorschriften des SGB V (§ 296 Abs. 3 i. V. m. Abschnitt 5 § 7 Abs. 3 der Datenträgeraustauschvereinbarung) nicht der jeweiligen Krankenkasse sondern der Kassenärztlichen Vereinigung zugewiesen. Nach § 296 Abs. 3 SGB V sind die einzelnen Krankenkassen berechtigt und auch verpflichtet, der Kassenärztlichen Vereinigung für die Wirtschaftlichkeitsprüfung die dort genannten Verordnungsdaten für jedes Quartal arztbezogen zu übermitteln, nicht jedoch mehrere Krankenkassen gemeinschaftlich. Allerdings sieht § 303 Abs. 2 SGB V vor, dass die Krankenkassen zum Zweck der Vorbereitung der Wirtschaftlichkeitsprüfung eine Arbeitsgemeinschaft nach § 219 SGB V bilden können, die diese Aufgabe komplett übernimmt. Zwischen den Lan-

desverbänden der Krankenkassen und der Kassenärztlichen Vereinigung war jedoch eine Prüfvereinbarung abgeschlossen worden, wonach die Krankenkassen – nicht etwa eine Arbeitsgemeinschaft – kassenartenübergreifend zusammengeführte Datensätze erstellen und diese der Kassenärztlichen Vereinigung zur Vorbereitung der Wirtschaftlichkeitsprüfungen übermitteln sollte. Diese mit den datenschutzrechtlichen Vorgaben in Widerspruch stehende Prüfvereinbarung sowie die Beauftragung eines privaten Rechenzentrums mit der Aufgabe der Datenzusammenführung habe ich dem TMSFG als Rechtsaufsichtsbehörde mitgeteilt und gebeten, auf die seiner Aufsicht unterstehenden Krankenkassen bzw. der KV einzuwirken, um insoweit rechtmäßige Zustände herzustellen. Im Anschluss daran haben sich die Landesverbände der Krankenkassen geeinigt, eine Arbeitsgemeinschaft als datenzusammenführende Stelle im Sinne von § 303 Abs. 2 SGB V zu bilden. Allerdings hat der Entwurf einer Datenschutzvereinbarung, die Anlage zum Arbeitsgemeinschaftsvertrag war, noch Formulierungen enthalten, die auf eine Auftragsdatenverarbeitung zugeschnitten waren und der alleinigen Verantwortung der nunmehr neu gebildeten Arbeitsgemeinschaft als Daten verarbeitende Stelle nicht gerecht wurde. Daher habe ich die meiner Kontrolle unterliegende Krankenkasse darum gebeten, die Datenschutzvereinbarung so zu formulieren, dass sie den Anforderungen der alleinigen Verantwortlichkeit der Arbeitsgemeinschaft nach § 35 Abs. 1 SGB I gerecht wird. Eine Anpassung der Prüfvereinbarung dahingehend, dass die kassenartenübergreifenden Datensätze nicht von den Krankenkassen sondern von der Arbeitsgemeinschaft erstellt und der Kassenärztlichen Vereinigung unter Einschaltung des privaten Rechenzentrums übermittelt werden, ist bislang nicht erfolgt, obwohl mir von Kassenseite die unaufgeforderte Vorlage der geänderten Prüfvereinbarung zugesagt wurde.

11.14 Krankenhausplanung in Thüringen

Im Erfahrungsaustausch unter den DSB des Bundes und der Länder erhielt ich Kenntnis, dass zwischen einigen Krankenkassen der neuen Bundesländer und einem Gesundheitsforschungsinstitut ein Vertrag über die Strukturierung und Analyse des vollstationären Leistungsbedarfs als Grundlage für einen Krankenhausrahmenplan in den betreffenden Bundesländern abgeschlossen wurde. Meine Nachfrage

bei der Krankenkasse in Thüringen hat ergeben, dass diese auf der Grundlage des o. g. Vertrags einen Ergänzungsvertrag mit dem Institut abgeschlossen hatte und im Rahmen dieser Analyse des regionalen Bedarfs an Krankenhäusern von der Krankenkasse Abrechnungsdaten nach § 301 SGB V aufbereitet und dem externen Gutachter übermittelt worden sind. Dabei musste ich feststellen, dass die übermittelten Angaben nicht ausreichend anonymisiert waren. Gegenüber der Krankenkasse habe ich dies als beanstandungswürdigen Tatbestand erklärt und meine Auffassung auch dem TMSFG mitgeteilt. Die Krankenkasse hat im Ergebnis das Institut veranlasst, die übermittelten Daten bis zur Klärung der Rechtsgrundlage für die Verarbeitung, für eine weitere Nutzung zu sperren. Für eine zweckändernde Nutzung oder Übermittlung der von den Krankenhäusern den Krankenkassen nach § 301 SGB V zu Abrechnungszwecken übermittelten Daten lag keine Rechtsgrundlage vor. Wegen der Sensibilität dieser Daten muss es bei dem Grundsatz bleiben, dass diese Daten nur für Abrechnungszwecke nicht aber für Zwecke der Krankenhausplanung verwendet werden, zumal diese Aufgabe eindeutig in die Zuständigkeit des TMSFG und nicht der Krankenkasse fällt.

11.15 Zu großzügige Datenübermittlung von Landesärztekammer an Kassenärztliche Vereinigung

Im Rahmen einer Petition wurde ich darauf hingewiesen, dass von der Landesärztekammer Thüringen der Kassenärztlichen Vereinigung Thüringen eine Liste über die Einkünfte der niedergelassenen Ärzte übermittelt worden ist, bei der für die jeweilige Arztgruppe (z. B. Allgemeinmediziner) die Anzahl der niedergelassenen Ärzte dieses Fachgebiets sowie die in dieser Ärztegruppe insgesamt erzielten Einkünfte enthalten war. Darunter befanden sich aber auch Ärztegruppen, zu der nur ein oder zwei Ärzte aufgelistet waren. Meine Überprüfung bei der Landesärztekammer sowie bei der Kassenärztlichen Vereinigung hat ergeben, dass die Landesärztekammer die Kassenärztliche Vereinigung bei der Ermittlung der durchschnittlichen Einkommen der unterschiedlichen Arztgruppen unterstützen wollte. Die Landesärztekammer kann aufgrund des in der Beitragssatzung festgelegten Prozentsatzes aus den gezahlten Beiträgen, die auf der Basis von vorzulegenden Kopien von Einkommenssteuerer-

klärungen oder Bestätigungen der Steuerberater bei der Landesärztekammer festgesetzt werden, für jeden Arzt zumindest die Größenordnung seines jährlichen Einkommens zurückrechnen. Bei der Übermittlung dieser Einkommensdaten waren jedoch nicht alle auf der Liste verzeichneten Ärzte als ausreichend anonymisiert anzusehen. Da für eine personenbezogene Übermittlung dieser Daten keine Rechtsgrundlage vorhanden war, habe ich diese Verletzung datenschutzrechtlicher Vorschriften gegenüber der Landesärztekammer beanstandet. Diese hat mir in der Folge mitgeteilt, dass sie zukünftig keine personenbezogenen Daten, die im Rahmen der Beitragsfestsetzung erhoben worden sind, an dritte Stellen weitergeben werde.

11.16 Kassenarztverzeichnis im Internet

Im Berichtszeitraum gab es erneut Anfragen von Bürgern, ob eine Auskunftserteilung über die niedergelassenen Ärzte durch die KV Thüringen möglich sei. Die Bereitstellung von Namen, Anschriften, Fachgebietsbezeichnungen und Öffnungszeiten von niedergelassenen Ärzten durch die Kassenärztliche Vereinigung an Krankenkassen oder Rettungsleitstellen wurde bereits im 2. TB (11.15) dargestellt. Schließlich hat sich die KV Thüringen selbst an mich mit der Fragestellung gewandt, unter welchen Voraussetzungen ein komplettes Vertragsarztverzeichnis im Internet veröffentlicht werden kann, bei dem die Betroffenen nach Namen und Wohnort sowie Fachgebietsbezeichnung die für sie in Frage kommenden Ärzte recherchieren können. Die KV Thüringen war der Auffassung, dass eine solche Übermittlung von Sozialdaten an eine unbestimmte Öffentlichkeit auf der Grundlage von § 59 Bundesmantelvertrag-Ärzte (BMV-Ä) zulässig sei, wonach die Kassenärztliche Vereinigung zur Erstellung eines Arztregisters verpflichtet ist, die dieses den Kassen zu übergeben haben. Die Kassen haben wiederum die Verpflichtung, dieses Verzeichnis nach § 59 Abs. 2 BMV-Ä den Versicherten zur Einsichtnahme zur Verfügung zu stellen. Unabhängig davon, dass es sich beim BMV-Ä um keine gesetzliche Ermächtigungsgrundlage zur Einschränkung des informationellen Selbstbestimmungsrechts handelt, sondern um eine vertragliche Regelung zwischen den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung, regelt der Mantelvertrag nur die Bereitstellung der Daten für die Einsichtnahme durch Versicherte, nicht aber für die Öffent-

lichkeit als eine Aufgabenstellung der Kassen. Aus diesem Grund habe ich gegenüber der KV Thüringen gefordert, dass die Einstellung eines Arztverzeichnisses im Internet, welches für einen völlig unbestimmten Empfängerkreis bestimmt und für jeden beliebigen Zweck genutzt werden kann, nur mit Einwilligung der Betroffenen erfolgen darf. Hierbei war allerdings auch zu beachten, dass selbst mit einer Einwilligung eine Datenübermittlung nur dann für eine öffentliche Stelle zulässig ist, wenn sie eine entsprechende Aufgabenstellung hat. Eine solche Aufgabenstellung ist bezüglich der nicht gesetzlich Krankenversicherten auch nicht ohne weiteres zu begründen. Die KV Thüringen hat in diesem Zusammenhang vorgetragen, dass es jährlich eine große Anzahl von Einzelanfragen an die KV Thüringen nach den Anschriften und Sprechzeiten der Vertragsärzte gibt und somit eine wesentliche Entlastung der KV durch ein solches Internetangebot erreicht werden kann. Die KV Thüringen hat dann im Rahmen des ohnehin zu erfolgenden vierteljährlichen Schriftwechsels im Rahmen der Abrechnung die Vertragsärzte um deren Einwilligung in die Aufnahme in das Vertragsarztverzeichnis gebeten, sodass nunmehr eine Recherchierbarkeit derjenigen Ärzte möglich ist, die ihre Einwilligung hierzu gegeben haben.

11.17 ICD-10 Diagnoseschlüssel im Einsatz

Nachdem zum 1. Januar 2000 durch Bekanntmachung des Bundesministeriums für Gesundheit vom 24. Juni 1999 im Bundesanzeiger (Nr. 124 vom 8. Juli 1999, Seite 10985) eine Fassung des ICD-10-Codes (so genannter ICD-10-SGB) in Kraft gesetzt wurde, war Anfang 2000 der Fachpresse zu entnehmen, dass es zum Teil Umsetzungsschwierigkeiten beim flächendeckenden Einsatz des ICD-10-SGB V gab. Diese Meldungen habe ich zum Anlass genommen, sowohl bei der Kassenärztlichen Vereinigung Thüringen als auch bei einer größeren Krankenkasse Erkundigungen zum flächendeckenden Einsatz des ICD-10-Codes in Abrechnungsunterlagen einzuholen. Von beiden Stellen wurde bestätigt, dass es sowohl bei den Vertragsärzten als auch bei den Krankenhäusern noch technische Probleme bei der Umsetzung dieser Anforderungen gab. Diese Schwierigkeiten waren erst Ende 2000 ausgeräumt, sodass ab diesem Zeitpunkt von einem flächendeckenden Einsatz des Diagnoseschlüssels auszugehen war.

Durch die nach § 17 b Krankenhausfinanzierungsgesetz vorgesehene Einführung eines pauschalisierenden Entgeltsystems für die Abrechnung der Krankenhausleistungen hat sich das Bundesgesundheitsministerium dazu entschlossen, den ICD-10 hierfür als Grundlage heranzuziehen und entsprechend der australischen Fassung eines diagnosenorientierten Fallpauschalensystems (DRG - Diagnosis Related Groups) anzupassen. Der Bundesbeauftragte für den Datenschutz hat hierzu auch die Landesbeauftragten für den Datenschutz um eine Stellungnahme gebeten. Die Erweiterung der medizinischen Klassifikation gegenüber der derzeit maßgeblichen Veröffentlichung ist durch § 301 Abs. 2 SGB V i. V. m. § 17b Krankenhausfinanzierungsgesetz grundsätzlich abgedeckt. Allerdings haben die DSB des Bundes und der Länder gegenüber dem BMG zum Ausdruck gebracht, dass eine Erweiterung des ICD-10-Codes nur insoweit zulässig ist, als die einzelnen Schlüssel zur Erfüllung der Aufgaben nach dieser Vorschrift erforderlich sind und nicht unverhältnismäßig - insbesondere durch zu tief gehende Spezifizierung - in die Privatsphäre des jeweils Betroffenen eingreifen. In der daraufhin ergänzten Fassung des ICD-10-Codes wurde dies berücksichtigt.

11.18 Datenübermittlung durch LVA an Drittbeteiligte im Widerspruchsverfahren

Ein Petent wandte sich an mich mit dem Anliegen, dass von der LVA Thüringen personenbezogene Daten ohne Rechtsgrundlage an einen privaten Träger von Betreuungsleistungen übermittelt worden sind. Eine Nachfrage bei der LVA Thüringen ergab folgenden Sachverhalt. Der Petent hatte als langjähriger Freund einer allein erziehenden Mutter die zeitweise Betreuung ihrer beiden Kinder während der Durchführung einer Rehabilitationsmaßnahme in einer Kureinrichtung übernommen. Die von ihm nicht sicherzustellenden Betreuungszeiten der Kinder wurden von einem privaten Träger abgesichert. Im Rahmen der Abrechnung dieser Betreuungsleistungen durch die LVA Thüringen nach § 29 SGB VI (Haushaltshilfe) ergaben sich zeitliche Überschneidungen der Betreuungsleistungen. Daraufhin hat die LVA Thüringen die von der Versicherten beantragte Abrechnung der vom Petenten erbrachten Betreuungszeiten gekürzt und ist den Angaben des privaten Trägers gefolgt. Dagegen erhob die Versicherte Wider-

spruch. Zur Klärung der zeitlichen Überschneidungen hat daraufhin die LVA den privaten Träger angeschrieben und eine Kopie des Widerspruchsschreibens der Petentin übermittelt, in der auch der Name und die Anschrift des Petenten enthalten war.

Aus datenschutzrechtlicher Sicht war darin eine Übermittlung von Sozialdaten an den privaten Träger zu sehen, was nach § 69 Abs. 1 Nr. 1 2. Alt. SGB X für die Erfüllung der gesetzlichen Aufgabe der übermittelnden Stelle zulässig ist. Zu den Aufgaben der LVA gehört es neben der Kostenerstattung von Leistungen nach § 29 SGB VI auch, im Rahmen eines Widerspruchsverfahrens eventuelle Rückforderungstatbestände bei möglicherweise zu ungerecht gezahlten Sozialleistungen zu überprüfen und hierzu die erforderlichen Datenübermittlungen vorzunehmen. Allerdings sind hierbei die Anforderungen an die Erforderlichkeit einer derartigen Datenübermittlung zu beachten. Von der LVA konnte nicht begründet werden, warum es zunächst nicht ausgereicht hätte, den privaten Träger ohne Namensnennung mit den von einer dritten Person erbrachten Betreuungszeiten zu konfrontieren und um eine nachvollziehbare Belegung der erbrachten Leistungen zu bitten. Dabei ist zu berücksichtigen, dass Empfänger der Kostenerstattungen die Versicherte war, der es oblegen hätte, mit dem Petenten diese Unstimmigkeiten zu klären. Eine namentliche Nennung des Petenten und der von ihm erbrachten Betreuungszeiten wäre erst dann erforderlich gewesen, wenn sich aus den weiteren Ermittlungen keine Aufklärung des Sachverhalts ergeben hätte. Ich ging daher davon aus, dass es zwar grundsätzlich eine Übermittlungsbefugnis der abgerechneten Betreuungszeiten an den privaten Träger im Rahmen eines Widerspruchsverfahrens nach § 69 Abs. 1 Satz 1 SGB X gibt, diese jedoch im Rahmen der Erforderlichkeit zunächst ohne Namensnennung hätte erfolgen können. Diese Rechtsauffassung habe ich der LVA Thüringen mitgeteilt und diese aufgefordert, künftig dafür Sorge zu tragen, dass in ähnlich gelagerten Fällen auf eine Namensnennung so lange verzichtet wird, als es zur Sachverhaltsermittlung nicht zwingend erforderlich ist. Daraufhin hat mir die LVA Thüringen mitgeteilt, dass künftig derartige Auskünfte und Anfragen zentral durch ein Referat der LVA Thüringen vorgenommen werden soll, um die Einhaltung datenschutzrechtlicher Vorschriften sicherzustellen.

11.19 Anonyme Beratungstätigkeit durch eine Erziehungs- und Familienberatungsstelle

Zwischen einem freien Träger der Jugendhilfe und einem Jugendamt war der Abschluss einer Vereinbarung über die Erbringung von Leistungen der Erziehungs-, Familien- und Eheberatung nach § 16, 17 und 28 SGB VIII vorgesehen. Der freie Träger hat mir den Entwurf dieser Vereinbarung vorgelegt. Darin war hinsichtlich der Leistung der Erziehungsberatung nach § 28 SGB VIII vorgesehen, dass die Erziehungsberatungsleistungen nach § 28 SGB VIII grundsätzlich durch einen Verwaltungsakt des Jugendamt beschieden werden, unabhängig davon, ob sich der Hilfe Suchende an das Jugendamt oder an die Beratungsstelle des freien Trägers wendet. Der freie Träger befürchtete nunmehr, dass damit in diesem Bereich eine anonyme Beratung von Hilfe Suchenden nicht mehr möglich ist, weil sich die Ratsuchenden zwingend einer weiteren Stelle mit ihrem Anliegen offenbaren müssen und damit die Niederschwelligkeit des Beratungsangebotes nicht mehr gegeben sei.

Das von mir in dieser Frage um Stellungnahme gebetene Jugendamt nahm daraufhin eine Regelung in die Vereinbarung auf, wonach der Ratsuchende sich nicht mehr selbst an das Jugendamt wenden, sondern auf freiwilliger Basis einer Übermittlung der zur Bewilligung seines Antrags durch das Jugendamt erforderlichen Daten an dieses zustimmen sollte. Aber auch diese Regelung löste die Frage nicht, ob das Jugendamt für die Bewilligung von Leistungen der Erziehungsberatung nach § 28 SGB VIII auch in denjenigen Fällen, in denen die Beratungsleistungen von einem freien Träger erbracht werden, einen Verwaltungsakt erlassen muss, was mit einer Offenbarung von Daten des Antragsteller verbunden wäre. Nach § 62 Abs. 1 SGB VIII ist eine Datenerhebung durch das Jugendamt nur dann zulässig, wenn ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. Das TMSFG als oberste Landesjugendbehörde vertrat die Auffassung, dass die in der Vereinbarung vorgesehene Regelung den Grundprinzipien der Erziehungsberatung widerspricht, weil dadurch ein unmittelbarer Zugang zu den Beratungsleistungen nicht mehr gegeben sei. Damit fehlte es für die zusätzliche Einbeziehung des Jugendamtes und der damit verbundenen Datenübermittlung bereits an der Erforderlichkeit. Deswegen lagen die Voraussetzungen des

§ 62 Abs. 1 SGB VIII nicht vor, sodass auch eine Einwilligung der Ratsuchenden die Datenerhebung durch das Jugendamt nicht rechtfertigen konnte. Zudem zeigte bereits eine weitere Regelung der Vereinbarung, wonach bei verweigerter Einwilligung die Erziehungsberatung nach § 28 SGB VIII auch ohne Einbeziehung des Jugendamtes durch den freien Träger erfolgen soll, dass eine Erforderlichkeit der Datenerhebung durch das Jugendamt nicht gegeben ist. Das vom Jugendamt vorgetragene Argument, die Verweigerung einer Einwilligung dürfte nur in wenigen Ausnahmefällen erfolgen, war nicht nachvollziehbar. Gerade durch das Einwilligungserfordernis wird die innere Schwelle der Leistungsberechtigten, sich mit den persönlichen bzw. familiären Problemen an Dritte zu wenden, unnötig erhöht und damit der weitere Zugang zur Beratungsstelle erschwert.
Das Jugendamt hat sich daraufhin dieser Argumentation angeschlossen und die zunächst in anderer Weise getroffene Vereinbarung dahingehend geändert, dass eine Datenübermittlung mit Einwilligung der Betroffenen zur regelmäßigen Antragstellung beim Jugendamt entfällt und sich die Ratsuchenden nunmehr direkt an die Beratungsstelle des freien Trägers wenden können. Gleichzeitig konnte ich dem Jugendamt einige Hinweise zur Ausgestaltung der Antragsformulare geben, um keine unnötigen Daten der Ratsuchenden, die sich an das Jugendamt selbst wenden, zu vermeiden. Diese Hinweise wurden aufgegriffen. So wurden z. B. bei den Angaben zum Einkommen Hinweise eingefügt, dass diese Angaben nur bei Leistungen zu machen sind, bei denen eine Kostenbeteiligung der Eltern gesetzlich vorgesehen ist. Auch die bereits von den freien Trägern an das Jugendamt übersandten personenbezogenen Daten im Rahmen des zunächst eingeführten Verfahrens wurden vom Jugendamt gelöscht.

11.20 Datenerhebung im Rahmen von Förderanträgen

In einer Petition wurde vorgetragen, dass das TMSFG im Zusammenhang mit der Bewilligung einer Fördermaßnahme versucht haben soll, eine komplette Mitgliederliste des betreffenden Verbandes über das zuständige Amtsgericht zu erhalten.
Dies nahm der TLfD zum Anlass, im Rahmen eines Kontrollbesuches im TMSFG, den Sachverhalt unter datenschutzrechtlich relevanten Aspekten zu prüfen. Dabei wurde festgestellt, dass das Amts-

gericht wegen anstehender Förderentscheidungen lediglich um Mitteilung über die Anzahl der Mitglieder des betreffenden Vereins gebeten wurde. Eine personenbezogene Datenerhebung bzw. eine Übersendung einer Namensliste der Vereinsmitglieder war nachweislich nicht beantragt worden. Dies war für die Entscheidung über die Bewilligung der Fördermaßnahme auch nicht erforderlich.
Dem Petenten wurde mitgeteilt, dass eine Verletzung datenschutzrechtlicher Vorschriften durch das TMSFG im zugrundeliegenden Sachverhalt nicht festzustellen war.

11.21 Verhältnis zwischen begutachtenden Stellen und Sozialämtern

Fragestellungen in welchem Umfang Ergebnisse von medizinischen oder sozialpädagogischen Gutachten an beauftragende Träger der Sozialhilfe übermittelt werden dürfen, tauchen insbesondere bei der Bearbeitung von Anträgen auf Leistungen der Eingliederungshilfe nach § 40 BSHG auf. Dabei werden vom Sozialhilfeträger zur Entscheidung über den Antrag auf Eingliederungshilfe Gutachter mit der Untersuchung des Antragstellers beauftragt. Obwohl derartige Untersuchungen mit Einwilligung des Betroffenen - allerdings beeinflusst durch die diesem obliegenden Mitwirkungspflichten nach §§ 60 ff SGB I - erfolgen, stellt sich wegen der Sensibilität der in solchen Gutachten enthaltenen personenbezogenen Daten die Frage, in welchem Umfang die Gutachtenergebnisse dem Sozialhilfeträger vom Gutachter übermittelt werden dürfen. Gegenüber dem TMSFG habe ich hierzu die Auffassung vertreten, dass mangels spezialgesetzlicher Vorschriften zum zulässigen Umfang solcher Mitteilungen vom Gutachter an den Sozialhilfeträger dies nach dem Erforderlichkeitsgrundsatz zu erfolgen hat. Ein Vergleich mit den Vorschriften im Bereich der Kranken- und Pflegeversicherung zeigt, dass der Gutachter dort nicht pauschal alle von ihm zur Erstellung des Gutachtens erhobenen sensiblen personenbezogenen Daten an den Kranken- bzw. Pflegeversicherungsträger übermitteln darf, sondern bspw. nach § 277 Abs. 1 Satz 1 SGB V bzw. § 18 Abs. 5 Satz 1 SGB XI auf das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund beschränkt bleibt. Diese Grundsätze sind nach meiner Auffassung auch entsprechend auf die Begutachtung im Bereich der Sozialhilfe anzuwenden. Das TMSFG scheint eine solche Einschrän-

kung nicht als zwingend anzusehen und geht davon aus, dass das Ergebnis der Begutachtung im Bereich der Eingliederungshilfe (§ 40 BSHG) so individualisiert sein muss, dass der Sozialhilfeträger über den körperlichen, geistigen und/oder seelischen Zustand des Betroffenen umfänglich in Kenntnis gesetzt wird. Diese Auffassung teile ich nicht, da dies bedeuten würde, dass der Sozialhilfeträger eine Vielzahl von sensitiven Daten der Betroffenen erhielte, die für die Entscheidung nicht erforderlich sind. Dass im Ausnahmefall zusätzliche Angaben vom Gutachter angefordert werden können, der diese auch zu dokumentieren hat, rechtfertigt jedoch meiner Ansicht nach nicht, dass der Sozialhilfeträger regelmäßig alle Angaben über medizinische und psychosoziale Umstände des Betroffenen zur Verfügung hat, die auch der Gutachter zur Beantwortung der mit dem Gutachtenauftrag aufgeworfenen Fragen benötigt. Diese Auffassung habe ich dem TMSFG mitgeteilt. Aufgrund eines durchgeführten Kontrollbesuchs bei einem Sozialhilfeträger bin ich zu dieser Thematik sowohl mit der kontrollierten Stelle als auch mit der Aufsichtsbehörde noch im Gespräch.

12. Statistik

12.1 Registergestützter Zensus 2001

Erwartungsgemäß wurde im Jahr 2001 das Testgesetz für einen registergestützten Zensus beschlossen (Zensusvorbereitungsgesetz vom 27. Juli 2001, BGBl. I, S. 1882 ff.). Mit Hilfe des Tests soll geprüft werden, inwieweit und in welcher Form künftig für sog. Volkszählungen ein Paradigmenwechsel von Primärstatistiken bzw. Totalerhebungen zu registergestützten Systemen vollzogen werden kann. Das Testverfahren soll dabei insbesondere zu Erkenntnissen über geeignete methodische Grundlagen für die künftigen Zählungen führen. Gleichzeitig ist mit dem Test eine Prüfung der Qualität von Registerdaten bei den Meldebehörden und der Bundesanstalt für Arbeit verbunden, indem diese miteinander sowie mit den Angaben der Betroffenen selbst aufgrund persönlicher Befragungen abgeglichen werden. Desweiteren erfolgt auch eine Gebäude- und Wohnungsstichprobe in ausgewählten Gemeinden mit dem Ziel, zu prüfen, ob die Erhebung von Wohnungsdaten bei den Eigentümern zu anderen Ergebnissen führen, als die bisher üblichen Befragungen bei

den Wohnungsnutzern. Von besonderer Bedeutung für die Zählung ist die Entwicklung und der Test von Verfahren zur Haushaltsgenerierung bei registergestützten Zensen, da Informationen über die Zahl, Größe und Struktur von Haushalten in Verbindung mit Wohnungsdaten wichtige Informationsquellen zur Analyse der sozialen und wirtschaftlichen Lage der Gesellschaft darstellen. Die für den Test erforderlichen personenbezogenen Daten werden ausschließlich von den statistischen Landesämtern und dem statistischen Bundesamt erhoben und verarbeitet. Sie unterliegen der statistischen Geheimhaltung und dürfen auch nicht an die am Test beteiligten und mit Sicherheit daran interessierten Kommunen zum Abgleich mit ihren Registern weitergeleitet werden. Da sich bei der Zusammenführung der Daten aus den verschiedenen Quellen auch Widersprüche ergeben werden, deren Ursachen zu untersuchen sind, bedurfte es klarer verbindlicher gesetzlicher Regelungen, die eine Durchbrechung der statistischen Geheimhaltung, insbesondere jeglichen Rücklauf in den Verwaltungsvollzug ausschließen. Aufgrund dessen wurde auch auf die Beteiligung der Gemeinden als Erhebungsstellen verzichtet und ausschließlich Erhebungsbeauftragte der statistischen Landesämter eingesetzt. Die Ende 2001/Anfang 2002 gewonnenen Daten sollen nunmehr bis zum Jahr 2003 ausgewertet werden. Der TLfD wird die Einhaltung des Datenschutzes und der Datensicherheit in diesem Zusammenhang kontrollieren.

12.2 Datenübermittlung der Standesämter an das Thüringer Landesamt für Statistik

Das Bevölkerungsstatistikgesetz gilt in seiner gegenwärtigen Fassung seit März 1980 und ist seit dieser Zeit nur unwesentlich modifiziert worden, obwohl es nicht den Anforderungen, die das Volkszählungsurteil des Bundesverfassungsgerichts an die Verarbeitung und Nutzung personenbezogener Daten gestellt hat, im ausreichenden Maße entspricht. Dies wurde bereits mehrfach von den DSB des Bundes und der Länder angemahnt.
Als ein datenschutzrechtliches Problem erwies sich im Zusammenhang mit dieser statistischen Erhebung auch, dass die verwendeten Zählkarten bei Geburten und Sterbefällen, die von den Standesämtern an das Statistische Landesamt zu übersenden sind, Eintragungen für die Namen der betreffenden Personen zulassen, obwohl diese

Daten für die statistische Bearbeitung nicht benötigt werden. Lediglich in einer Fußnote werden die Ausfüller auf dem Vordruck darüber informiert. Auf meine Bitte hat deshalb das Statistische Landesamt die Standesämter in Thüringen nochmals ausdrücklich darauf hingewiesen, dass in den Feldern für den Namen des Kindes bzw. des Verstorbenen auf den Zählkarten keine Angaben zu machen sind. Gegenwärtig füllen bereits nur noch 12 der insgesamt 173 Standesämter in Thüringen die Vordrucke manuell aus. Die übrigen Standesämter nutzen zur Übermittlung bereits automatisiert erstellte Datenträger, die sich auf die erforderlichen Daten beschränken. Nach Information des TLS werden auch die 12 Standesämter die Übermittlung in den nächsten Monaten auf entsprechende Verfahren umstellen, sodass in Zukunft auch jede versehentliche Übermittlung der Namen von Geborenen oder Verstorbenen auf den Zählkarten an das TLS ausgeschlossen werden kann.

13. Bildung, Wissenschaft, Forschung

13.1 Thüringer Hortkostenbeteiligungsverordnung (ThürHortkBVO)

In der Vergangenheit tauchten hinsichtlich der Heranziehung der Erziehungsberechtigten zu den Personal- und Betriebskosten für die Hortbetreuung immer wieder Unsicherheiten über den erforderlichen Umfang der zur Beitragsveranlagung abgeforderten Unterlagen auf.
Ich habe daher zu dem mir zugeleiteten Entwurf einer ThürHortkBVO darauf hingewiesen, dass hierin alle zur Aufgabenerfüllung benötigten Unterlagen konkret benannt und insbesondere auch die kommunalen Träger verpflichtet werden sollen, in ihren Satzungen genau festzulegen, welche personenbezogenen Daten zur Beitragsfestsetzung erhoben, verarbeitet und genutzt werden und welche Nachweise in welcher Form hierfür vorzulegen sind.
In der ThürHortkBVO vom 12.02.2001 (GVBl. Nr. 2, S. 16-17) sind meine Vorschläge und Hinweise berücksichtigt worden, sodass Eltern und Träger darüber informiert sind, welche Daten erforderlich und welche Nachweise zu erbringen sind.

13.2 Schulärztliche Untersuchungen

In allen vorangegangenen Tätigkeitsberichten hatte ich aufgrund von damit im Zusammenhang stehenden vorliegenden Eingaben die nach dem Schulgesetz vorgesehene Verordnung zur Schulgesundheitspflege angemahnt. Wie nunmehr vom zuständigen Ministerium angekündigt, scheint diesbezüglich eine Realisierung absehbar. Nach Informationen des TMSFG liegt dort zwischenzeitlich ein entsprechender Verordnungsentwurf vor und befindet sich gegenwärtig bereits in der Ressortabstimmung. Im Zuge dessen dürften dann auch die immer wieder auftretenden Fragen zur Rechtmäßigkeit von Untersuchungen bzw. den damit verbundenen Datenerhebungen im schulärztlichen Bereich der Vergangenheit angehören. Zu begrüßen ist in diesem Zusammenhang, dass im Jahr 2000 ein landesweit einheitlicher Vordruck zur „Einladung zur Schuleingangsuntersuchung“ vom Landesverwaltungsamt erarbeitet und den Gesundheitsämtern zur Verfügung gestellt wurde. Die von mir im Vorfeld dazu gegebenen Hinweise wurden entsprechend berücksichtigt. Gleichzeitig habe ich angeregt, den Schulärzten im Interesse einer einheitlichen Verfahrensweise in Thüringen in gleicher Weise auch Musteranschreiben für die nachfolgenden Untersuchungen sowie einen verbindlichen Anamnesebogen zur Verfügung zu stellen.

13.3 Kontrollen in Schulen

In Schulen werden zur Aufgabenerfüllung zahlreiche Schüler-, Eltern- und Lehrerdaten erhoben und verarbeitet. Hierzu steht den Schulen seit einiger Zeit unterschiedliche Schulsoftware zur Verfügung, die durch das TKM gemäß § 34 Abs. 2 ThürDSG zentral freigegeben und zum Datenschutzregister gemeldet wurde. Bei den Kontrollen war festzustellen, dass in den Schulen die Nutzungsmöglichkeiten des Verfahrens sehr unterschiedlich ausgeprägt ist und dabei insbesondere vor Ort die Festlegung konkreter Verantwortlichkeiten mitunter fehlt. Auch bestand teilweise aufgrund unzureichender Kenntnisse auf dem Gebiet der EDV eine unmittelbare Gefährdung der Datensicherheit. So wurde bspw. ein Verfahren bedenkenlos innerhalb des schulinternen Computernetzes betrieben, welches darüber hinaus Zugang zum Internet hat, ohne dass ausreichende Abschottungsmaßnahmen eingerichtet oder vorgesehen waren. Passwörter fehlten, Regelungen zur Vergabe von Zugriffsrechten oder Protokollierungen waren ebenso wenig vorhanden wie Festlegungen

zur Datensicherung oder Löschung. Zwischenzeitlich wurden technische und organisatorische Maßnahmen getroffen, um die Ausführung der Vorschriften des ThürDSG zu gewährleisten. Weiterhin wurden, wie allgemein üblich, auch in den Thüringer Schulen die Telekommunikationseinrichtungen (Telefon, Fax) nicht nur für dienstliche Zwecke, sondern im Einzelfall gegen Gebühr auch vom Schulpersonal und Schülern privat genutzt. Bei den Kontrollen stellte ich fest, dass Einzelverbindungsdaten auf schuleigenen Telefonanlagen mitunter ohne den Abschluss einer entsprechenden Dienstvereinbarung mit dem Personalrat gemäß § 74 Abs. 3 ThürPersVG erhoben und gespeichert werden. Ebenso verwies ich auf § 6 Abs. 7 TDSV, wonach die Übermittlung von Einzelverbindungsnachweisen durch Telekommunikationsdienstunternehmen an Betriebe und Behörden nur zulässig ist, „wenn der Kunde schriftlich erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden oder eine solche Beteiligung nicht erforderlich ist.“ Insbesondere hatte ich einer Schule widersprochen, die davon ausging, dass eine Personalratsbeteiligung nicht erforderlich wäre, wenn private Gespräche an Dienstapparaten grundsätzlich untersagt sind.

Schließlich bestanden bei den kontrollierten Schulen auch Unklarheiten hinsichtlich der Aufbewahrungsfristen von personenbezogenen Unterlagen sowie darüber, welche konkreten Unterlagen bei einem Schulwechsel an der bisherigen Schule verbleiben und welche an die aufnehmende Schule zu übermitteln sind. So werden teilweise über 80 Jahre alte Unterlagen aufbewahrt, ohne dass archivrechtliche Bestimmungen beachtet werden. Die Schulen haben sich auf meine Aufforderung hin an die für sie zuständigen Staatsarchive zur Klärung des weiteren Umgangs mit diesen Unterlagen gewandt.

An personenbezogenen Lehrerdaten wurden in einer Schule außer der zur Aufgabenerfüllung der Schule erforderlichen Stammdaten der Lehrer auch weitere Unterlagen geführt, ohne dass hierfür eine Erforderlichkeit bestünde und die, wenn auch lose abgeheftet als Personalakten im Sinne von § 97 Abs. 1 Satz 2 Thüringer Beamtengesetz, der auch auf Angestellte Anwendung findet, zu qualifizieren waren. Danach gehören zur Personalakte alle Unterlagen, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Handelt es sich hierbei um

Kopien, die sich auch in der Grund- oder in Teilakten befinden, sind diese Unterlagen als von der Schule geführte Nebenakten zu qualifizieren. Nebenakten dürfen nur dann geführt werden, wenn die enthaltenen Unterlagen zur rechtmäßigen Aufgabenerledigung erforderlich sind (§ 97 Abs. 2 Satz 3 ThürBG). In der Personalaktenführungsrichtlinie des TIM (ThürStAnz. Nr. 42/1998, S. 1812-1816) wird unter 2.2.1 dazu näher ausgeführt, dass Personalnebenakten nur dann geführt werden dürfen, wenn mehrere personalverwaltende Stellen für den Beamten zuständig sind oder weil die personalverwaltende Behörde nicht mit der Beschäftigungsbehörde identisch ist. Das Thüringer Kultusministerium hat hierzu festgelegt, dass die Führung von Nebenakten in den Schulen nicht erforderlich und personalaktenführende Stelle grundsätzlich die jeweils zuständigen Staatlichen Schulämter sind.
Unterlagen, die Personalaktendaten enthalten und bislang keinen Eingang in die Personalakte gefunden hatten, waren dem Schulamt zu übergeben. Soweit eine Erforderlichkeit aufgrund des Zeitablaufs für die weitere Aufgabenerfüllung der Schule nicht mehr gegeben war und diese Unterlagen auch nicht Bestandteil der Personalakte sind (z. B. Anwesenheitslisten, Dienstreiseanträge, Fragebögen für die Gehaltsstelle zur Ergänzung von Daten) waren diese auszusondern und zu vernichten.
Ebenso wurde die Schule von mir aufgefordert, alle beim Schulwechsel eines Schülers übergebenen Unterlagen, die nicht in die laufende Schülerakte gehören, hieraus zu entfernen, z. B. an den Schularzt bei Unterlagen zur Schulgesundheitspflege (jugendärztliche Beurteilungen gemäß §§ 55, 57 Abs. 3 ThürSchulG), Rückgabe an die Sorgeberechtigten bei nicht benötigten Urkunden oder Vernichtung nach § 16 Abs. 1 ThürDSG. Zwischenzeitlich hat die Schule meine datenschutzrechtlichen Forderungen umgesetzt.

13.4 Ungeeignete Anwesenheitskontrolle im Internat

In der Eingabe eines Schülers, der in einem zu einer Schule gehörenden Internat untergebracht war, beschwerte sich dieser über vielfältige Beeinträchtigungen durch das Internatspersonal in seinem informationellen Selbstbestimmungsrecht. Bei einer daraufhin erfolgten Vor-Ort-Begehung war feststellbar, dass die Internatsausweise aller Mieter, die Vor- und Zuname, Zimmernummer sowie ein Passfoto

enthalten, für alle Bewohner und Besucher des Internats sichtbar an der Wand des Eingangsflurs an einer Tafel ausgehängt waren. Bei Abwesenheit eines Bewohners war der Ausweis von der Wand zu entfernen oder umzudrehen. Hierin lag aus datenschutzrechtlicher Sicht eine zwangsweise Erhebung personenbezogener Daten, die darüber hinaus, wenn auch begrenzt öffentlich gemacht wurden. Die Internatsleitung versprach sich von dieser Verfahrensweise im Brandfall eine schnelle Übersicht über die genaue Anzahl der sich im Haus aufhaltenden Personen. Außerdem sei so eine Überwachung über die Einhaltung der Ausgehzeiten gewährleistet, ohne jedes Zimmer einzeln kontrollieren zu müssen. Da aber nach meiner Ansicht nie ausgeschlossen werden kann, dass eine An- oder Abwesenheit nur vorgetäuscht oder der Gebrauch der Anwesenheitstafel schlicht vergessen wird, ist im Ernstfall auf die Regelung kein Verlass. Ebenso fehlen Rechtsvorschriften, die das zwangsweise Durchführen des Verfahrens erlauben würden. Ich hatte daher das Internat aufgefordert, die Maßnahme ausschließlich mit Einwilligung der Internatsbewohner weiterzuführen, wobei die Passfotos auf den Ausweisen zu entfernen waren. Darüber hinaus gab es keine erkennbaren Gründe für eine zwangsweise Erhebung der An- und Abwesenheitszeiten für die volljährigen Internatsbewohner, sodass ich auf eine Einstellung der Führung von An- und Abwesenheitsbücher für diesen Personenkreis drang. Aufgrund der Fürsorge- und Aufsichtspflicht gegenüber den nicht volljährigen Bewohnern bestanden jedoch gegen die Führung von Übersichten zur An- und Abwesenheit keine Bedenken. Das Internat hatte mir abschließend mitgeteilt, dass alle datenschutzrechtlichen Forderungen umgesetzt wurden.

13.5 Schulhomepage im Internet

Auch in diesem Berichtszeitraum erreichten mich Anfragen von Schulen hinsichtlich der Zulässigkeit des Einstellens einer schulinternen Homepage in das Internet. Aus datenschutzrechtlicher Sicht ist es unproblematisch, wenn die Internetseite keine personenbezogenen Daten, sondern lediglich Fotos des Schulgebäudes, die Anschrift der Schule, die Schulhistorie, statistische Angaben usw. enthält. Ist jedoch eine Veröffentlichung von Lehrer-, Eltern und Schülerdaten geplant, so ist als bereichsspezifische Rechtsgrundlage das Thüringer Schulgesetz (ThürSchulG) heranzuziehen. Für diesen Fall gilt gemäß

§ 57 Abs. 4 Nr. 3 ThürSchulG, dass die Übermittlung personenbezogener Daten an Dritte nur zulässig ist, soweit eine rechtswirksame Einwilligung des Betroffenen vorliegt. In einer vom TKM erbetenen Stellungnahme zum Entwurf eines Gesetzes zur Änderung des ThürSchulG habe ich daher u. a. vorgeschlagen, eine eigene Regelung zur Veröffentlichung von personenbezogenen Daten im Internet einzufügen, wonach solche Veröffentlichungen im Internet aufgrund der weltweiten Zugriffsmöglichkeit nur mit der Einwilligung des Betroffenen zulässig sein sollten.

13.6 Forschungsprojekte an Thüringer Schulen (PISA, IGLU und Civic Education)

Zwischenzeitlich liegen in Thüringen bereits die ersten Ergebnisse der PISA-Schulleistungsstudie der OECD vor. Sie war jedoch im Berichtszeitraum nicht das einzige internationale Forschungsvorhaben zu Fragen des Wissensstandes und zum Leistungsvermögen schulpflichtiger Kinder, an denen sich Thüringer Schulen beteiligten. Neben der PISA-Studie sind in diesem Zusammenhang die Forschungsprojekte IGLU und Civic Education zu nennen. Im Vorfeld dieser Vorhaben hatten sich die DSB des Bundes und der Länder intensiv mit den bei der Durchführung der Untersuchungen auftretenden datenschutzrechtlichen Problemen beschäftigt (3. TB, 13.7). Unbefriedigend war hierbei jedoch - trotz der guten Zusammenarbeit mit den auf Landesebene Verantwortlichen - die mitunter sehr kurzfristige und späte Bereitstellung von Informationen und Unterlagen durch die Organisatoren, wodurch insbesondere auch der Meinungsaustausch und die Meinungsbildung unter den DSB unnötigerweise erschwert wurde.
Während bei der PISA-Studie, die in den Jahren 2000, 2003 und 2006 in 32 Industriestaaten mit 15-jährigen Schülern durchgeführt wird, im Jahr 2000 das Ziel darin bestand, den OECD-Mitgliedstaaten Vergleichsdaten über die Leistungsfähigkeit ihrer Bildungssysteme in den Bereichen Leseverständnis, Mathematik und Naturwissenschaften unter Berücksichtigung der sozialen Lern- und Lebensbedingungen der Schüler zur Verfügung zu stellen, wurde bei dem Forschungsprojekt IGLU im internationalen Vergleich die Lesekompetenz von Schülern der 4. Jahrgangsstufe untersucht. In einer weiteren internationalen Studie, an der sich 27 Staaten beteiligten,

wurden Schüler der 8. Jahrgangsstufe zur politischen Bildung befragt. Inhalt dieses Forschungsvorhabens waren Fragenkomplexe zum Thema Demokratie, Menschenrechte, Europa sowie Chancengleichheit und Familie unter dem Aspekt des Zugangs zu entsprechenden Informationen sowie dem Freizeitverhalten.
Neben den Fragen und Tests zum Kenntnisstand und der Leistungsfähigkeit der Schüler wurden bei den Untersuchungen auch Angaben über das soziale und schulische Umfeld der Schüler bei den Kindern, Eltern und Lehrern erhoben. Da die Forschungsvorhaben ausnahmslos auf die freiwillige Mitwirkung aller in die Stichprobe einbezogenen Schüler und Eltern ausgerichtet waren bzw. sind, galt es bei der datenschutzrechtlichen Prüfung besonderes Augenmerk auf die umfassende Aufklärung der Betroffenen über das Verfahren und den Umgang mit den erhobenen Daten sowie auf die Maßnahmen zur Gewährleistung der Geheimhaltung von Einzelangaben der Schüler, Eltern und Lehrer gegenüber allen nicht mit dem Forschungsauftrag betrauten Personen und Stellen (einschl. dem Schulpersonal und den Aufsichtsbehörden) zu richten. Aufgrund von Anregungen und Hinweisen der DSB des Bundes und der Länder erfolgten deshalb insbesondere Überarbeitungen der Anschreiben an die Schulen, Eltern und Schüler dahingehend, dass man die Beteiligten umfassender als zunächst vorgesehen über die beabsichtigten Verfahren und ihre auf freiwilliger Grundlage basierende Mitwirkung informierte. Desweiteren wurden in den Arbeitsanweisungen weitere Hinweise zur Gewährleistung des Datenschutzes und der Datensicherheit, insbesondere auch zum besseren Schutz der Einzelangaben gegen eine Kenntnisnahme durch die Schulen aufgenommen.
Aufgrund der vorgenannten Veränderungen wurden keine datenschutzrechtlichen Bedenken gegen eine Durchführung der vorgenannten Forschungsvorhaben an den Thüringer Schulen erhoben.

13.7 Veröffentlichung von personenbezogenem Archivgut

Der TLfD befasste sich im Berichtszeitraum mit mehreren Beschwerden, weil im Rahmen einer Ausstellung über die Arbeit Thüringer Archive die Ablichtung eines internen Polizeiprotokolls aus dem Jahre 1959 veröffentlicht wurde, ohne dass man zuvor die darin genannten Personen anonymisiert, d. h. unkenntlich gemacht hatte. Inhalt des Protokolls waren die Ergebnisse polizeilicher Ermittlungen

in Zusammenarbeit mit dem ehemaligen Staatssicherheitsdienst im Vorfeld eines zum damaligen Zeitpunkt stadtbekannten Schauprozesses, in dem Jugendliche wegen staatsfeindlichen Verhaltens beschuldigt worden waren. Begründet wurde die Nichtanonymisierung vom betreffenden Archiv damit, dass der Vorfall damals hinreichend und personenbezogen durch die Presse bekannt gemacht worden war. Darüber hinaus lag auch die Vermutung nahe, dass auch von den Betroffenen ein Interesse an einer öffentlicher Rehabilitation und Dokumentation des Unrechts bestehen würde. Dass dies nicht zwingend so sein muss, zeigten aber die Beschwerden, weil durchaus nicht alle in dem vertraulichen Dokument enthaltenen Informationen über die Beschuldigten bisher der Öffentlichkeit zugänglich gewesen waren. Darüber hinaus bestand bei den Beschwerdeführern Missbehagen darüber, dass sie erneut in die öffentliche Diskussion gebracht werden könnten. Dies kam insbesondere auch darin zum Ausdruck, dass ein Betroffener nicht die Anonymisierung in jedem Fall, aber bei einer Ausstellung in seinem Heimatort wünschte. Als besonders problematisch wurde von den Betroffenen die zusätzliche Veröffentlichung des Dokuments in einer zur Ausstellung herausgegebenen Begleitbroschüre angesehen. Dadurch ist die Kenntnisnahme nicht nur auf die unmittelbaren Ausstellungsbesucher beschränkt sondern ist damit jedermann dauerhaft möglich.
Im Ergebnis der datenschutzrechtlichen Prüfung des Sachverhaltes wurde festgestellt, dass die Vorgaben des Thüringer ArchivG bei der Festlegung und Präsentation der Ausstellungsexponate nicht ausreichend beachtet worden waren. Nach § 17 ThürArchivG wird Archivgut im Regelfall 30 Jahre nach Schließung für die Benutzung freigegeben, soweit es nicht bereits bei seiner Entstehung zur Veröffentlichung bestimmt war. Unbeschadet dieser allgemeinen Schutzfrist hat der Gesetzgeber bestimmt, dass personenbezogenes Archivgut erst 10 Jahre nach dem Tod der betreffenden Person benutzt werden darf. Ist das Todesjahr nicht oder nur mit hohem Aufwand feststellbar, endet die Schutzfrist 90 Jahre nach der Geburt der betreffenden Person. Ausnahmen hiervon sind möglich, insbesondere wenn dies im Einzelfall im öffentlichen Interesse liegt bzw. es sich um Personen der Zeitgeschichte handelt. Im vorliegenden Fall betraf das unzweifelhaft keine Personen der Zeitgeschichte und der Zweck der Ausstellung, wie auch die Veröffentlichung des Dokumentes, war keineswegs bei einer Anonymisierung gefährdet gewesen. Insoweit

bestand kein Erfordernis bzw. kein öffentliches Interesse an einer personenbezogenen Veröffentlichung des Protokolls. Dies wurde gemäß § 39 Abs. 1 ThürDSG beanstandet. Aufgrund der Tatsache, dass bereits eine größere Anzahl der Begleitbroschüren zur Ausstellung verkauft waren, konnte eine weitere Schadensbegrenzung nur noch durch eine Entfernung der Ausstellungstafel und eine Einstellung des Verkaufs der Broschüre oder durch eine Schwärzung der personenidentifizierenden Daten erreicht werden, was auch unverzüglich vom Aussteller veranlasst wurde.

13.8 Nutzung einer Personalakte aus einem Kommunalarchiv

Anlässlich eines Gründungsjubiläums einer Stadt hatte die Kommunalverwaltung eine Neuauflage der bereits vielen Jahren zuvor veröffentlichten „Stadtchronik“ veröffentlicht. Da die aus den 30-iger Jahren stammende ursprüngliche Veröffentlichung in ihrem Vorwort mit nationalsozialistischen Gedankengut durchzogen war, hatte man sich dazu entschlossen, stattdessen die Biographie des Autors, einem bekannten Heimatforscher, als „Vorwort“ aufzunehmen. Grundlage bildeten hierfür die im Kommunalarchiv noch vorhandenen Unterlagen in vorhandenen Personalakten.
Ungeachtet der von den Erben in Frage gestellten Urheberrechte baten diese den TLfD um Prüfung, ob und inwieweit Daten aus archivierten Personalakten veröffentlicht werden dürfen. Im Ergebnis der Prüfung des Sachverhaltes wurde Folgendes festgestellt. Gemäß § 16 ThürArchivG steht Jedem das Recht auf Benutzung von Archivgut in öffentlichen Archiven zu, der ein berechtigtes Interesse an einer Benutzung zu amtlichen, wissenschaftlichen, publizistischen oder Bildungszwecken sowie zur Wahrnehmung berechtigter persönlicher Belange glaubhaft macht und keine Schutzfristen oder sonstige Einschränkung einer Nutzung entgegenstehen. Schutzfristen gelten bei Archivgut, das sich auf natürliche Personen bezieht, bis 10 Jahre nach deren Tod oder soweit das Todesjahr nicht oder nur mit hohem Aufwand feststellbar ist, 90 Jahre nach Geburt der betroffenen Person. Darüber hinaus kann im Einzelfall eine Schutzfrist um 20 Jahre verlängert oder die Benutzung wegen schutzwürdiger Belange Dritter eingeschränkt werden. Im konkreten Fall sollte anlässlich eines Jubiläums der Gemeinde die vorhandene Ortschronik neu aufgelegt

werden, mit der Maßgabe, das das bisherige Vorwort durch die Biographie des Verfassers der Ortschronik ersetzt werden sollte. Insoweit bestand ein berechtigtes wissenschaftliches und publizistisches Interesse an der Benutzung des Archivgutes. Für die in der Veröffentlichung genannten Personen (dem Verfasser einschließlich seiner unmittelbaren Familienangehörigen) waren die regulären Sperrfristen bereits teilweise seit Jahrzehnten abgelaufen. Selbst unter Berücksichtigung der Tatsache, dass nach dem Archivgesetz eine Schutzfristverlängerung um 20 Jahre (soweit es im öffentlichen Interesse liegt), möglich ist, wäre auch die erweiterte Sperrfrist für die Daten des Betroffenen nicht mehr gegeben gewesen, sodass diesbezüglich einer Benutzung der Archivunterlagen nichts entgegenstand. Da Verwandte und Nachfahren weder ortsansässig waren, noch in irgend einer Form in der Biographie erwähnt wurden, sowie aufgrund der Tatsache, dass die veröffentlichten Ereignisse weit über ein halbes Jahrhundert zurücklagen, konnte man davon ausgehen, dass auch eine mögliche Beeinträchtigung oder Benachteiligung Dritter durch die Veröffentlichung weder im gesellschaftlichen noch im privaten Bereich zu erwarten war. Aufgrund dessen bestanden auch aus meiner Sicht keine datenschutzrechtlichen Bedenken gegen die Nutzung von den in Rede stehenden Personaldaten des verstorbenen Heimatforschers und Autors für die Veröffentlichung in der Ortschronik der Kommune.

14. Wirtschaft, Verkehr, Wohnungswesen, Umwelt

14.1 Veröffentlichung von Gewerbemeldedaten im Internet?

Eine Veröffentlichung von Gewerberegisterdaten im Internet ist nur mit Einwilligung der Betroffenen zulässig, da eine Rechtsgrundlage für solche Veröffentlichungen aus der Gewerbeordnung nicht zu entnehmen ist. Gemäß § 14 Abs. 8 GewO darf von einer Gewerbebehörde aus der Gewerbeanzeige Name, betriebliche Anschrift und angezeigte Tätigkeit des Gewerbetreibenden dann übermittelt werden, wenn der Auskunftsbegehrende ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft macht. Bei einer Veröffentlichung im Internet wäre hingegen nicht mehr zu kontrollieren, wer zu welchem

Zweck auf diese Daten zugreift und wie diese weiterverarbeitet werden. Indem aus dem Internet jeder Daten abrufen kann, ohne dass er hierfür seine Gründe darlegen muss, hat bspw. die Gemeinde oder der Landkreis keine Möglichkeit mehr, festzustellen, ob die Voraussetzungen für eine Datenübermittlung nach § 14 Abs. 8 GewO gegeben ist. Das informationelle Selbstbestimmungsrecht der Betroffenen wäre so in einem weitaus größeren Ausmaß berührt als bei begründeten Auskunftsersuchen gegenüber der Gewerbebehörde.

14.2 Aufbewahrungsfristen für Gewerbeanzeigen

Bereits seit geraumer Zeit bestanden Unklarheiten in den Gewerbeämtern hinsichtlich der Löschungsfristen für Daten aus Gewerbeanzeigen. Gemäß § 14 Abs. 11 GewO gelten aber für das Verändern, Sperren oder Löschen der gemäß § 14 Abs. 1 bis 4 GewO erhobenen Daten die Datenschutzgesetze der Länder. Nach § 16 ThürDSG sind personenbezogene Daten in Dateien immer dann zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Unter den DSB des Bundes und der Länder wurde daher diskutiert, dass einerseits eine Notwendigkeit von Rückgriffen durch die Gewerbeämter auf die Gewerbeanmeldung aus Gründen der Gewerbeüberwachung auch nach einer erfolgten Abmeldung besteht, etwa um Anfragen von anderen öffentlichen Stellen (Finanzamt, Sozialversicherung, Polizei, Staatsanwaltschaft usw.) zu beauskunften, andererseits gemäß § 14 Abs. 1 Sätze 3 u. 4 GewO die Gewerbeanzeige dem Zweck dient, der zuständigen Behörde die Überwachung der Gewerbeausübung zu ermöglichen und die erhobenen Daten nur für diesen Zweck verarbeitet und genutzt werden dürfen. Daher hatte ich das TLVwA auf die Problematik hingewiesen und vorgeschlagen, entsprechende Aufbewahrungsfristen etwa in einer Verwaltungsvorschrift festzulegen. Ein solcher Entwurf wurde mir dann aus dem TMWAI zur Abstimmung vorgelegt. Unter Berücksichtigung meiner datenschutzrechtlichen Verbesserungsvorschläge ist die Verwaltungsvorschrift am 10.08.2001 in Kraft getreten (ThürStAnz Nr. 37/2001 S. 1947-1948). Unter Berücksichtigung von steuer- und sozialrechtlichen Gesichtspunkten ist hierin eine Aufbewahrungsfrist von Gewerbeanzeigen von höchstens 10 Jahren festgelegt worden.

14.3 Erklärung des Antragstellers zur Gewährung von Zuschüssen

In mehreren Eingaben wurde ich auf eine Erklärung aufmerksam gemacht, die als Anlage 10 Bestandteil der Richtlinie über die Gewährung von Zuwendungen aus Mitteln des Freistaats Thüringen zur Förderung von Strukturanpassungsmaßnahmen (SAM) ist. Hierin müssen die Antragsteller von SAM gegenüber dem TMWAI eine Erklärung abgeben, wonach „nicht nach der „Technologie von L. Ron Hubbard“ (Scientology-Organisation) gearbeitet wird und keine Personen eingesetzt werden, die nach dieser Lehre geschult sind oder Kurse und Seminare nach dieser Lehre besuchen.“
Nach Ansicht der Antragsteller bestanden für diese weder die Zulässigkeit noch die Möglichkeit, das einzusetzende Personal hierzu zu befragen oder zu überprüfen.
Aus datenschutzrechtlicher Sicht bestanden gegen die Abgabe einer solchen Erklärung insoweit Bedenken, als der Antragsteller hierdurch veranlasst wurde, personenbezogene Daten bei den von ihm einzusetzenden Arbeitnehmern zu erheben und zu speichern. Ich wandte mich daher mit der Bitte um Angabe der entsprechenden Rechtsgrundlage, die eine solche Erklärung erlaubt bzw. vorschreibt an das hierfür zuständige TMWAI. Eine Rechtsvorschrift, die die Abforderung einer solchen Erklärung erlaubt, konnte jedoch nicht genannt werden. Das TMWAI teilte daraufhin mit, dass diese Erklärung zukünftig nicht mehr abverlangt wird. Ebenfalls konnte ich eine Löschung bzw. Sperrung aller bisher von Betroffenen unterschriebenen Erklärungen erreichen.
Eine wortgleiche Erklärung entdeckte ich dann ebenfalls in den Zuwendungsbestimmungen von drei weiteren Richtlinien für die Gewährung von Zuschüssen des Freistaats Thüringen im Bereich der beruflichen Ausbildung (ThürStAnz. Nr. 40/2000, S. 1932, 1934, 1939). Auch hier bat ich das TMWAI um eine Streichung dieser Zuwendungsbestimmung. Von Seiten des TMWAI wurde mir zugesagt, im Zuge einer Richtlinienänderung die entsprechenden Passagen zu streichen.

14.4 Online-Zugriff auf Kfz-Zulassungsdaten durch Sozialamt unverhältnismäßig

Ein Sozialamt hat mir mitgeteilt, dass es beabsichtige, ein automatisiertes Abrufverfahren einzurichten, bei dem einer Reihe von Mitarbeitern des Sozialamtes bei Verdacht auf Leistungsmissbrauch ein jederzeitiger Zugriff auf die Daten der Kfz-Zulassungsstelle eingeräumt werden sollte. Dabei sollte sich die Zugriffsberechtigung neben Name, Geburtsdatum und amtliches Kennzeichen auch auf den Fahrzeugtyp, die Farbe, den Zulassungstag sowie Angaben zur Fahrzeugversicherung erstrecken. Ich habe daraufhin dem Sozialamt mitgeteilt, dass ich die Einräumung derartiger Zugriffsrechte für unzulässig halte. Dadurch, dass den Mitarbeitern des Sozialamtes der jederzeitige Zugriff auf die Kfz-Zulassungsdaten sämtlicher bei der Kfz-Zulassungsstelle registrierte Kfz-Halter eingeräumt wird, obwohl selbst nach den Angaben des Sozialamtes nur ein Zugriff auf die Sozialhilfeantragsteller und auch hier nur für den Fall eines Verdachtes auf Sozialhilfemissbrauch erforderlich sein soll, ist eine solche Verfahrensweise als unverhältnismäßig und damit unzulässig anzusehen. Außerdem hat für den Bereich der Vermeidung rechtswidriger Inanspruchnahme von Sozialhilfe der Bundesgesetzgeber in § 117 Abs. 3 BSHG eine abschließende Vorschrift zum Datentransfer zwischen dem Sozialamt und der Kfz-Zulassungsstelle getroffen. Von der Kfz-Zulassungsstelle darf nach § 117 Abs. 3 Satz 4 Buchstabe f in Verbindung mit Satz 5 ausschließlich die Eigenschaft als Kraftfahrzeughalter an das Sozialamt übermittelt werden. Dies kann auch im Rahmen eines automatisierten Abgleichverfahrens erfolgen. Eine Übermittlung weiterer Daten, z. B. amtliches Kennzeichen, Fahrzeugtyp, Tag der Zulassung oder Angaben zur Fahrzeugversicherung sind daher nicht zulässig. Stellt das Sozialamt bei einer solchen Überprüfung die Eigenschaft eines Leistungsbeziehers als Kraftfahrzeughalter fest, müssen die näheren Einzelheiten im Rahmen der Mitwirkungspflichten mit dem Hilfeempfänger geklärt werden. Ich habe daher dem Sozialamt zusammenfassend mitgeteilt, dass dem Sozialamt auf konkrete Anfrage zu den mitgeteilten Personen von der Kfz-Zulassungsstelle lediglich die Mitteilung gemacht werden darf, ob diese Kfz-Halter eines oder mehrerer Fahrzeuge sind. Bei einem Kontrollbesuch war festzustellen, dass ein solches Verfahren noch nicht eingeführt worden war. Vom Sozialamt wurde dargelegt, dass aus Gründen der Verwaltungsökonomie über einen Antrag auf Sozialhilfe nach Möglichkeit bereits bei Vorsprechen des Antragstellers im Sozialamt abschließend entschieden werden soll. Wenn

sich aber im Rahmen der Antragstellung Zweifel ergeben, ob der Antragsteller Halter eines Kfz ist und zunächst eine schriftliche Anfrage bei der Kfz-Zulassungsstelle gestellt werden müsse, so sei eine solche abschließende Bearbeitung nicht möglich. Dem standen allerdings nach Angaben des Sozialamtes wöchentlich nur etwa 40 solche Verdachtsfälle gegenüber. Als ein im Vergleich zu dem beabsichtigten automatisierten Abrufverfahren weniger in das informationelle Selbstbestimmungsrecht der Kfz-Halter eingreifende Verfahren wurde mit dem Sozialamt auch die Möglichkeit eines automatisierten Abgleichs nach § 117 Abs. 3 BSHG erörtert. Nachdem das Sozialamt geprüft hatte, ob mit vertretbarem Aufwand ein solcher regelmäßiger automatisierter Abgleich mit den Kfz-Daten im Rahmen der verfügbaren EDV-Programme durchgeführt werden könnte und diese Prüfung negativ ausfiel, hat es meine Rechtsauffassung zur Unzulässigkeit eines Online-Zugriffs auf die Kfz-Daten akzeptiert und erfragt im Einzelfall die entsprechenden Daten bei der Kfz-Zulassungsstelle im schriftlichen Verfahren.

14.5 Anforderung eines medizinisch-psychologischen Gutachtens durch die Fahrerlaubnisbehörde

In Eingaben von Bürgern wandten sich diese an mich mit Fragen hinsichtlich des Umgangs von Gutachten der amtlich anerkannten Begutachtungsstellen für Fahreignung bei den Fahrerlaubnisbehörden. In einem Fall beschwerte sich der Petent, dass eine Begutachtungsstelle die Fahrerlaubnisakte mit einem zusätzlichen Vermerk „Untersuchung hat stattgefunden“ zurückgesandt hatte und die Fahrerlaubnisbehörde daraufhin die Beibringung eines weiteren Gutachtens ablehnte. Nach Rückfrage bei der entsprechenden Fahrerlaubnisbehörde beruht der Vermerk über eine stattgefundene Untersuchung auf einer Festlegung des TMWAI. Einerseits könnten auf diese Weise Antragsteller, denen ein günstiges Gutachten erstellt wurde und die irrig davon ausgehen, dass dieses nicht nur an den Probanden, sondern auch an die Fahrerlaubnisbehörde übersandt werden würde, um Vorlage des Gutachtens ersucht werden. Andererseits dürfe dem Antragsteller nicht die Missbrauchsmöglichkeit eröffnet werden, so lange die Untersuchungsstellen zu wechseln, bis ein für ihn günstiges Gutachten vorliegt, welches er dann der Fahrerlaubnisbehörde vorlegt. Ebenfalls soll auf diese Weise verhindert

werden, dass der Proband bei mehreren Gutachterstellen auf ein positives Gutachten hin „trainiert". Im Ergebnis meiner datenschutzrechtlichen Prüfung teilte ich dem Petenten mit, dass der Vermerk über eine stattgefundene Untersuchung zulässig ist, da die Fahrerlaubnisbehörde kein personenbezogenes Datum erfährt, was ihr nicht aus dem gesetzlich vorgesehenen Verfahren (§ 2 Abs. 8 Straßenverkehrsgesetz i. V. m. § 11 Abs. 6 Satz 2 Fahrerlaubnisverordnung) ohnehin ableitbar ist. Eine Fahrerlaubnisbehörde darf aber grundsätzlich nicht bestimmen, bei welcher amtlich zugelassenen Stelle das Gutachten zu erstellen ist.
In einem weiteren Fall hatte der Petent das geforderte Gutachten nicht vollständig, sondern nur seiner Meinung nach für den Sachverhalt wesentliche Teile daraus bei der Fahrerlaubnisbehörde vorgelegt. Ich musste dem Beschwerdeführer hierbei mitteilen, dass die Behörde die Beibringung des gesamten Gutachtens zur Entscheidungsfindung fordern darf. Der Betroffene ist aber nicht verpflichtet, das von ihm geforderte Gutachten vorzulegen. Nach § 11 Abs. 8 FeV darf die Stelle dann aber bei ihrer Entscheidung auf die Nichteignung des Betroffenen schließen.

14.6 Fahrerermittlung bei Verkehrsordnungswidrigkeiten

Eine regelmäßig wiederkehrende Frage oder Beschwerde an den TLfD (3. TB, 7.16) befasst sich mit der Zulässigkeit der Nutzung von Daten aus dem Melde- oder Passregister zur Ermittlung von Fahrern bei Verkehrsordnungswidrigkeiten. In einem konkreten Fall war bei einer Übertretung der Höchstgeschwindigkeit von dem betreffenden Fahrer sowie dem Kennzeichen des benutzten Fahrzeuges ein Tatfoto angefertigt worden. Auf der Grundlage des Kennzeichens wurde der Halter ermittelt und ihm, wie vom Gesetzgeber vorgesehen, ein Anhörungsbogen mit dem Tatvorwurf zugesandt, weil aus der Haltereigenschaft allein nicht geschlossen werden konnte, dass diese Person auch das Fahrzeug zur Tatzeit gefahren hat. Da trotz schriftlicher Erinnerung und Aufforderung zur Zeugenaussage der Halter des Kraftfahrzeuges zum Vorwurf der Fahrereigenschaft beharrlich schwieg, ist man beim zuständigen Ordnungsamt davon ausgegangen, dass dieser von seinem Zeugnisverweigerungsrecht Gebrauch machen möchte. Dieses steht jedermann zu, wenn es Angaben zu seiner Person oder unmittelbare Verwandte betrifft und die Betroffenen

davon ausgehen, sich bzw. die Angehörigen ggf. mit der Aussage zu belasten. Wie in den vergangenen Tätigkeitsberichten bereits mehrfach ausgeführt, besteht in diesem Fall nach § 2 PAuswG oder § 22 PAuswG auch die Möglichkeit eines Lichtbildabgleichs des Tatfotos mit dem im Pass- oder Personalausweisregister der zuständigen Meldebehörde gespeicherten Passbild des Betreffenden. Dabei ist es nach meiner Auffassung aufgrund der Voraussetzungen für die Inanspruchnahme des Zeugnisverweigerungsrechtes im Rahmen dieses Abgleiches in der Meldebehörde durchaus auch verhältnismäßig und gerechtfertigt, bei einer Nichtübereinstimmung des Tatfotos mit dem Halterfoto zu prüfen, ob nicht ein im Haushalt des Halters lebendes Familienmitglied bzw. eine unter gleichem Namen und gleicher Anschrift wohnende Person (insbesondere erwachsene Kinder) als potentieller Fahrer in Betracht gezogen werden kann. Aus diesem Grund wird häufig bei einem negativen Lichtbildabgleich in der Meldebehörde nochmals unter Beschreibung des Fahrers nachgefragt, ob eine entsprechende Person zur Familie des Fahrzeughalters gehört bzw. dort gemeldet ist. Bei einem positivem Bescheid erfolgt dann eine Anforderung des Lichtbildes, um die mögliche Identität mit dem Fahrer feststellen zu können. Diese Verfahrensweise erachte ich als datenschutzrechtlich zulässig, was ich auch dem Beschwerdeführer mitgeteilt habe.

Datenschutzrechtlich problematisch ist demgegenüber, wenn von den Meldebehörden unaufgefordert personenbezogene Daten übermittelt werden. So hatte in einem anderen Fall ein Meldeamt der Polizei im Rahmen einer Fahrerermittlung statt der geforderten Kopie eines Lichtbildes gleich den vollständigen Abdruck des Personalausweisantrages mit allen Daten als Beweismittel übergeben. Dies widerspricht selbstverständlich dem Grundsatz der Erforderlichkeit, da die weiteren auf dem Personalausweisantrag enthaltenen Daten weder zur Fahrerermittlung noch zur Verfolgung der Ordnungswidrigkeit benötigt wurden. Aufgrund meiner Kritik wurde deshalb in der betreffenden Meldebehörde ausdrücklich festgelegt, künftig bei entsprechenden Anforderungen nur die Kopie des Lichtbildes zu übersenden oder ggf. durch Schwärzungen u. ä. den Umfang der Datenübermittlung auf das angeforderte Maß zu beschränken. Da in dem betreffenden Fall darüber hinaus die Kopie des Personalausweisantrages im Rahmen eines Amtshilfeverfahrens von der Thüringer Poli-

zei auch an eine Polizeibehörde außerhalb Thüringens übermittelt worden war, wurde der Vorgang dort gleichfalls ausgewertet, mit der Maßgabe auch als amtshilfeleistende Behörde uneingeschränkt den Grundsatz der Erforderlichkeit bei der Übermittlung von Daten zu beachten.

14.7 Videoüberwachung in Bussen

Neben der Videoüberwachung im öffentlichen Bereich werden in Thüringen, wie im übrigen Bundesgebiet auch, Videoüberwachungsanlagen in öffentlichen Verkehrsmitteln installiert. Als Gründe für die Ausstattung von Bussen mit Videokameras und Aufzeichnungsmöglichkeit führen die Verkehrsbetriebe an, mit dieser Maßnahme durch Vandalismus entstandenen Sachbeschädigungen vorzubeugen und ggf. aufzuklären. In meiner Stellungnahme gegenüber einer regionalen Busgesellschaft wies ich darauf hin, dass meinerseits aus datenschutzrechtlicher Sicht keine grundsätzlichen Bedenken gegen den Gebrauch von Videoüberwachungsanlagen in Bussen bestehen, wenn die Erforderlichkeit einer solchen Maßnahme zuvor hinreichend geprüft wurde und die Verhältnismäßigkeit gegeben ist. Außerdem sind die Fahrgäste deutlich auf die Videoüberwachung hinzuweisen und die Regelungen zum Umgang mit der Videoüberwachungsanlage sollten schriftlich dokumentiert sein. Dabei ist insbesondere festzulegen, wer Zugang zu den Aufzeichnungen hat und wann diese zu löschen sind. Zwischenzeitlich sind in § 6 b BDSG, der auch für öffentliche Wettbewerbsunternehmen wie Verkehrsgesellschaften gilt, klare Regelungen zum Einsatz der Videoüberwachung getroffen worden (siehe auch 4.8).

14.8 „Zuweisung von Wohnraum“ wie in alten Zeiten

Durch eine Eingabe wurde ich auf die aus datenschutzrechtlicher Sicht problematische Verfahrensweise einer Kommune bei der Vermietung ihrer kommunalen Wohnungen aufmerksam. Bei einem daraufhin anberaumten Kontrollbesuch war Erstaunliches feststellen. Vom Stadtrat war eine sog. Wohnungsvergabekommission gebildet worden, in der neben zwei Stadtratsmitgliedern auch vier sachkundige Bürger vertreten waren. Hauptaufgabe dieser Wohnungsvergabekommission, die auf Verwaltungsseite vom Wohnungsamt betreut

wurde, war die Erörterung von „Anträgen auf einen Wohnberechtigungsschein“ der Bewerber für eine der etwa 300 städtischen Wohnungen. Anders als zu DDR-Zeiten bestand jedoch in dieser Stadt kein Wohnungsmangel mehr, die eine „Wohnraumlenkung“ erforderlich gemacht hätte. Vielmehr hatte die Stadt Mühe, alle Wohnungen zu vermieten, da diese zum Teil noch mit Ofenheizungen ausgestattet waren oder sonst nicht den Komfortanforderungen heutiger Mieter entsprachen. Daher fragten diese Wohnungen in erster Linie Mieter aus sozial schwachen Schichten nach. Dabei wurden vom Wohnungsamt neben den Angaben über Namen, Geburtsdatum, Familienstand, Verwandtschaftsverhältnis zu Mitbewohnern und Staatsangehörigkeit detaillierte Angaben zur bisherigen Wohnung sowie nach den Gründen gefragt, weshalb über die „regelmäßige Wohnungsgröße“ hinaus ein zusätzlicher Raumbedarf anerkannt werden sollte. Wie festzustellen war, hatten dabei die „Antragsteller“ vielfach Angaben zu ihrer sozialen und gesundheitlichen Situation gemacht. Diese Anträge wurden gesammelt und in den monatlichen Sitzungen der Wohnungsvergabekommission erörtert, wobei vom Wohnungsamt zu jeder Sitzung ein ausführliches Protokoll der erörterten Einzelfälle gefertigt und in Kopie dem Vorsitzenden, dem Bürgermeister, dem Bauamtsleiter sowie dem Wohnungsverwaltungsunternehmen, das für die Stadt die Abwicklung der Mietverträge übernommen hat, zugestellt wurde. Da ein Überangebot an Wohnungen bestand, wurden in der Vergangenheit alle Anträge, soweit der nachgefragte Wohnraum zur Verfügung stand, positiv beschieden und dem „Antragsteller“ ein „Wohnberechtigungsschein“ gegen eine Gebühr von 10,- DM ausgestellt. Obwohl es sich nicht um einen Wohnberechtigungsschein nach dem Wohnungsbindungsgesetz handelte - hierfür ist die Stadt überhaupt nicht zuständig - wurde der Antragsteller in einer Rechtsmittelbelehrung darauf hingewiesen, dass er innerhalb von zehn Tagen nach Zugang eine Beschwerde bei der zuständigen Stelle erheben konnte, ohne dass diese bezeichnet war. Dieser Berechtigungsschein hatte aber keinerlei Außenwirkung, sondern führte lediglich dazu, dass vom Wohnungsamt eine Mitteilung an das die städtischen Wohnungen verwaltende private Unternehmen gesandt wurde, wonach mit den betreffenden Inhabern des Wohnberechtigungsscheins ein Mietvertrag im Namen der Stadt abgeschlossen werden konnte.

Diese Verfahrensweise habe ich gegenüber der Stadt wie folgt bewertet: Durch die Verwendung des als „Antrag auf einen Wohnberechtigungsschein“ bezeichneten Formulars entstand bei den Wohnungssuchenden der irreführende Eindruck, als ob die Kommune für die Erteilung von Wohnberechtigungsscheinen nach dem Wohnungsbindungsgesetz zuständig sei. Das ist jedoch gerade nicht der Fall. Daher erfolgte die in diesem Zusammenhang durchgeführte Erhebung und Verarbeitung von zum Teil sensiblen Daten ohne jegliche Erforderlichkeit. Dies bewertete ich als einen nicht unerheblichen Verstoß gegen § 19 Abs. 1 ThürDSG, der voraussetzt, dass das Erheben personenbezogener Daten nur zulässig ist, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich und rechtlich zulässig ist. Zur Entscheidung, ob ein Mietvertrag mit einer Privatperson durch die Kommune abgeschlossen wird, war sowohl der Umfang der erhobenen Daten als auch der Kreis der hiermit befassten Personen weder erforderlich noch angemessen. Dadurch, dass die im Antrag gemachten personenbezogenen Daten in einer zum Großteil mit externen bestehenden Kommission erörtert und weiteren Personen in Form von Protokollen zur Verfügung gestellt wurden, ist zudem gegen § 20 Abs. 1 ThürDSG verstoßen worden, wonach jede Verarbeitung von personenbezogenen Daten zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgabe erforderlich sein muss. Eine gesetzliche Aufgabe für eine „Wohnungsvergabekommission“ zur Entscheidung über die Erteilung eines Wohnberechtigungsscheines gibt es aber seit der „Wende“ nicht mehr. Zusammengefasst bedeutet dies, dass sich ohne jegliche Erforderlichkeit in einem überbürokratisierten Verfahren eine Vielzahl von Personen in der Wohnungsvergabekommission mit zum Teil sensiblen personenbezogenen Daten befassten, ohne dass es hierfür eine Rechtsgrundlage gab. Diese datenschutzrechtlichen Verletzungen habe ich beanstandet und die Stadt aufgefordert, das Verfahren in dieser Form einzustellen sowie die bis dato von Anfang unzulässig erhobenen Daten zu löschen.

14.9 Übermittlung personenbezogener Einwendungen an privaten Vorhabenträger im Bauleitplanverfahren

Ein Bürger beschwerte sich in einer Eingabe darüber, dass ein von ihm an die Stadtverwaltung gerichtetes Schreiben an die Presse

übermittelt worden sei. Wie sich bei meiner Prüfung des Sachverhalts herausstellte, hatte der Bürger im Rahmen der Bürgerbeteiligung in einem Bauleitplanverfahren von seinem Recht gemäß § 3 Abs. 2 Baugesetzbuch Gebrauch gemacht und seine Anregungen schriftlich gegenüber der zuständigen Stadtverwaltung vorgebracht. Von einer Übermittlung an Dritte und gar einer Veröffentlichung ging der Petent keinesfalls aus. Diese hatte mit der Vorbereitung und Durchführung des Verfahrens einen privaten Vorhabenträger beauftragt und dabei auch das Schreiben des Beschwerdeführers dorthin übermittelt. Nach Ansicht der Stadtverwaltung lag der weitere Umgang mit diesem Schriftstück nunmehr ausschließlich im Verantwortungsbereich des Vorhabenträgers. Diese Auffassung konnte ich jedoch nicht teilen, weil der eingeschaltete Dritte lediglich Verwaltungshelfer ohne hoheitliche Befugnisse ist. Die Gemeinde muss stets Herr des Verfahrens sein und bleibt damit auch für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich. Die Übertragung der Bauleitplanung durch die Gemeinde an andere Personen oder Stellen schließt es aus, nicht erforderliche personenbezogene Informationen an den Vorhabenträger zu übermitteln. Grundsätzlich sind bei der Beauftragung von Dritten vertraglich die Beachtung datenschutzrechtlicher Vorschriften aufzunehmen und bei einem Verstoß hiergegen entsprechende Sanktionen festzulegen. Im Ergebnis teilte ich der Stadtverwaltung mit, dass die in § 22 Abs. 1 ThürDSG genannten Zulässigkeitsvoraussetzungen für eine Übermittlung an eine nicht öffentliche Stelle nicht gegeben waren und dies bei zukünftigen Bauleitplanungsverfahren zu berücksichtigen ist. Das TLVwA als zuständige Aufsichtsbehörde hat die Gemeinden und Landratsämter auf die Beachtung der datenschutzrechtlichen Vorschriften hingewiesen.

14.10 Datenerhebung bei Vermietern durch Abfallbehörden

Von Anschlusspflichtigen eines Landkreises wurde der TLfD informiert, dass das Abfallwirtschaftsunternehmen des Kreises sie verpflichtet hätte, Veränderungen bei den Mietern unter Angabe deren jeweiliger früheren Anschrift bei Zuzug bzw. künftiger Adresse beim Wegzug anzuzeigen. Da Zweifel an der Rechtmäßigkeit dieser Forderung bestanden, hatte man den TLfD um eine datenschutzrechtli-

che Beurteilung gebeten. Hierzu galt es zunächst zu prüfen, ob und für welchen Zweck die Kenntnis dieser Daten im Rahmen der Aufgabenerfüllung vom Abfallwirtschaftsunternehmen benötigt werden. Rechtsgrundlage für die Erhebung personenbezogener Daten bei der Abfallentsorgung einschließlich der Berechnung und Veranlagung von Abfallgebühren ist die jeweils geltende Abfallgebührensatzung. Im konkreten Fall konnte unmittelbar aus dem Wortlaut der Satzung keine Erforderlichkeit für die Erhebung aller früheren oder künftigen Anschriften von Benutzungspflichtigen abgeleitet werden. Eine Notwendigkeit für die Kenntnis aller aktueller Anschriften von früheren Benutzungspflichtigen, bei denen noch Gebührenschulden ausstehen, konnte in keiner Weise als Rechtfertigung für die „zwangsweise" Erhebung dieser Daten von allen bisherigen Benutzungspflichtigen durch die ehemaligen Vermieter mit dem Ziel der Übermittlung an das Abfallwirtschaftsunternehmen bzw. deren dortige Speicherung (unzulässige Datenvorratshaltung) akzeptiert werden, zumal von dort diese Information bei Erfordernis jederzeit von den Meldebehörden eingeholt werden kann. Im Ergebnis der Rücksprache mit dem Abfallwirtschaftsunternehmen wurde deshalb das Verfahren durch die Abfallwirtschaftsgesellschaft des Landkreises dahingehend geändert, dass von den Vermietern künftig keine Angabe mehr über die frühere Anschrift bei Zuzug bzw. künftige Adresse beim Auszug von Mietern verlangt wird und die Erhebung künftiger Anschriften von ehemaligen Benutzungspflichtigen bei ausstehenden Gebührenschulden von den Betroffenen selbst oder bei Erfordernis über das Meldeamt erfolgen wird.

14.11 Kontrolle eines Trink- und Abwasserzweckverbandes

Nach wie vor erhalte ich Anfragen und Eingaben von Bürgern hinsichtlich der Zulässigkeit der Erhebung und Verarbeitung personenbezogener Daten durch Zweckverbände. Dies war für mich Anlass, die Datenverarbeitung in einem Trink- und Abwasserzweckverband zu kontrollieren.
Zunächst konnte ich mich davon überzeugen, dass der vom Zweckverband genutzte Erhebungsbogen, welcher mir bereits vor geraumer Zeit zur datenschutzrechtlichen Überprüfung vorgelegen hatte, entsprechend meinen damaligen Forderungen umgearbeitet wurde. Al-

lerdings beklagte die Stelle die nur lückenhaft oder teilweise überhaupt nicht ausgefüllten Fragebögen. Da eine Bescheidung von Beiträgen und Gebühren auf dieser Grundlage nicht möglich wäre, werden von der Stelle Grundstücksdaten aus dem automatisierten Liegenschaftsbuch übernommen. Gegen diese „Doppelerhebung“ personenbezogener Daten bestehen in diesem Fall auch keine datenschutzrechtlichen Bedenken, weil sich die erhebende Stelle auf § 19 Abs. 2 Nr. 3 ThürDSG berufen kann, wonach personenbezogene Daten ohne Mitwirkung des Betroffenen erhoben werden dürfen, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde.
Weiterhin war auch anlässlich dieser Kontrolle festzustellen, dass zwar eine Datenschutzregistermeldung, wenn auch fehlerhaft ausgefüllt, vorlag, aber keine schriftliche Verfahrensfreigabe gemäß § 34 Abs. 2 ThürDSG. Ein Anlagen- und Verfahrensverzeichnis nach § 10 ThürDSG wurde ebenfalls nicht geführt.
Ebenfalls war festzustellen, dass verschiedene Aufgaben als Auftragsdatenverarbeitung an private Fremdfirmen übertragen worden waren. Beispielsweise wird die Programmbetreuung durch eine Fremdfirma vorgenommen, welche für Fernwartungsarbeiten Zugriffsrechte auf bestimmte Programmteile besitzt.
Da auf die Auftragnehmer die Vorschriften des ThürDSG nicht anwendbar sind, habe ich vom Zweckverband gefordert, gemäß § 8 Abs. 6 ThürDSG vertraglich sicherzustellen, dass die Auftragnehmer die Bestimmungen dieses Gesetzes befolgen und sich der Kontrolle durch den TLfD entsprechend der §§ 37 bis 40 unterwerfen.
Darüber hinaus hatte ich im Falle der Fernwartung verlangt, sowohl die Zugriffsrechte schriftlich festzulegen als auch den Auftragnehmer zu verpflichten, nur auf die zur Aufgabenerfüllung unbedingt erforderlichen Daten zuzugreifen und dies zu protokollieren.
Alle datenschutzrechtlichen Forderungen und Empfehlungen wurden vom Zweckverband umgesetzt.

14.12 Umfang der zulässigen Datenerhebungen durch Zweckverbände bei Stundungen

Bekanntlich bildet die Erhebung von Kommunalabgaben oft Anlass für Fragen und Diskussionen bei Bürgern. Die Gemeinde kann allen Beitragspflichtigen aufgrund des neu eingefügten § 7 b ThürKAG die

Möglichkeit einräumen, den Beitrag in bis zu fünf Jahresraten verzinslich zu begleichen, ohne dass ein Vorliegen einer erheblichen Härte im Sinne des § 222 AO erforderlich ist. Der Beitrag kann darüber hinaus zur Vermeidung einer erheblichen Härte in bis zu 20 Jahresraten verzinslich gestundet werden. Unsicherheiten bei der Anwendung dieser Regelung ergeben sich für die Beitragspflichten teilweise aus der rechtlichen Möglichkeit der Gemeinde in der jeweils zugrunde liegenden Satzung, etwa in der Wasser- und Abwassersatzung, bestimmte Ausnahmetatbestände zu schaffen. Bei Bagatellbeiträgen im niedrigen dreistelligen Bereich wurde z. B. in einem Fall die Stundung in mehreren Jahresraten nur bei Vorlage des Nachweises einer erheblichen Härte gewährt. Die Prüfung, ob eine erhebliche Härte vorliegt, ist wie bei allen unbestimmten Rechtsbegriffen, eng an eine Ermessensentscheidung geknüpft. In Eingaben von Betroffenen wurde mitunter der Umfang der vom Zweckverband hierzu erhobenen personenbezogenen Daten zur Begründung einer erheblichen Härte bezweifelt oder überhaupt die Verpflichtung bestritten, eine erhebliche Härte nachweisen zu müssen. Datenschutzrechtliche Verstöße gegen die von den Zweckverbänden gewählten Verfahrensweisen bei der Stundungsgewährung konnte ich in keinem Fall feststellen. Ich habe aber darauf hingewiesen, die dem Stundungsantrag beiliegenden Informationen für den Beitragspflichtigen ausführlich und verständlicher zu gestalten.

15. Technischer und organisatorischer Datenschutz

15.1 Das mobile Informationszeitalter

Die Informations- und Kommunikationsindustrie ist ohne Zweifel zu einer Schlüsselbranche geworden. Während die 90-iger Jahre vorwiegend von der Entwicklung neuer Medien, Netze, Produkte und Anwendungen geprägt waren, ist die derzeitige Etappe durch ein verstärktes dynamisches Zusammenwachsen von Telekommunikation, Informationstechnologie, Multimedia und Sicherheitsdienstleistungen gekennzeichnet. Die verwendeten Prozessoren, Speicher und Netzelemente sind mittlerweile so klein, leistungsfähig und kostengünstig, dass sie in sehr vielen Objekten integriert sind und so u. a. ein Zugriff auf Daten und Service unabhängig von Ort und Zeit möglich ist. Der Nutzer kann über Festnetz, Kabel, Funk und Satellit

kommunizieren. Der Standort für den Zugang zu Informationsquellen spielt somit nur noch eine untergeordnete Rolle.
Noch nie hat sich ein Medium so schnell entwickelt wie das Internet. Der Zugang zum Internet erfolgt dabei nicht mehr ausschließlich über stationäre Rechner oder PC. Immer mehr Nutzer gehen über mobile Rechner oder über Handy ins Netz. Nach Presseinformationen kommunizieren bereits heute etwa 48 Millionen Bundesbürger über das Handy. Der Trend hin zu mobilen Internetzugängen wird sich in naher Zukunft mit der Einführung der nächsten Mobilfunk Generation UMTS (Universal Mobile Telecommunications System), die eine erheblich höhere Datenübertragungsrate ermöglicht, möglicherweise noch verstärken. Die neuen Mobiltelefone bieten neben Sprache auch die Möglichkeit Textnachrichten und Bilder zu verschicken, im Internet zu surfen und kommerzielle Geschäfte (Mobile Commerce) zu tätigen. Zunehmend werden auch standortbezogene bzw. ortsspezifische Servicedienste wie Routenplanung, Reisedienste, Wetterdienste, Nachrichten angeboten und genutzt.
Aufgrund der Digitalisierung lassen sich verschiedene Nachrichtenformen wie Sprache, E-Mail und Fax in einem System integrieren und gegenseitig konvertieren. Mit diesem als Unified Messaging bezeichneten Dienst kann der Adressat die Nachricht in der von ihm gewünschten Form abrufen. Auch die Übertragung von Sprache über das Internet (Voice-Over-IP) wird zunehmend genutzt. Derzeit weist die Internet-Telefonie allerdings noch Schwächen hinsichtlich der Sprachqualität und des Gesprächsflusses auf.
Aus der Fachpresse sowie aus dem AK-Technik ist bekannt, dass in Firmen und Universitäten, zunächst noch in Ergänzung zu den verkabelten lokalen Netzen, auf Funkübertragung basierende drahtlose Netze (Wireless LAN) eingesetzt werden, um die lokale Mobilität zu erhöhen. Solche Systeme etablieren sich aber auch an stark frequentierten Plätzen, wie Flughäfen, Bahnhöfen oder Hotels.
Im Zuge der Einführung von E-Government bei Bund, Ländern und Gemeinden ist auch in der öffentlichen Verwaltung eine beschleunigte Entwicklung auf dem Gebiet der IuK zu verzeichnen. Im Mittelpunkt steht hierbei die elektronische Unterstützung von Informations- und Kommunikationsvorgängen sowie von Transaktionen. E-Government setzt an drei Schnittstellen an: Bei der Kommunikation zwischen Verwaltung und Bürger, bei Geschäftsbeziehungen zwischen Verwaltung und Wirtschaft sowie bei der Abwicklung von

Prozessen zwischen den Behörden. Allein von der damit verbundenen Vermeidung von Medienbrüchen verspricht man sich ein erhebliches Einsparpotenzial.
Den nahezu unbegrenzten Anwendungsmöglichkeiten der IuK steht eine Vielzahl von Bedrohungen gegenüber, welche die Integrität, Vertraulichkeit und die Verfügbarkeit von Informationen und Systemen sowie die Verbindlichkeit einer Kommunikation gefährden. Da auch in sensiblen und lebenswichtigen Bereichen zunehmend komplexe IuK-Systeme eingesetzt werden, ist unsere moderne Informations- und Wissensgesellschaft auf ein höchstmögliches Maß an Sicherheit, insbesondere zum Schutz der übermittelten und gespeicherten Daten, angewiesen. Das Thema IT-Sicherheit gewinnt stetig an Bedeutung. Die Risiken sind nicht unerheblich, wie allein schon die spektakulären Virenangriffe der letzten Zeit (15.5) und deren rasche Ausbreitung über Netze sowie auch die mit Erfolg durchgeführten Attacken auf öffentlich bekannte Server mit dem Ziel einer Diensteverweigerung (Denial of Service) deutlich zeigten. So verursachte allein der Computervirus „Nimda“, der als so genannter Wurm blitzschnell mehr als 2 Millionen Rechner auf der ganzen Welt infizierte, nach Presseinformationen einen geschätzten wirtschaftlichen Folgeschaden von 1,9 Milliarden Dollar. Auch durch das Verletzen der Sicherheitsrichtlinien einer Behörde oder eines Unternehmens kann die Sicherheit des eigenen Netzes gefährdet werden. Dies kann schon durch das gewollte oder unbewusste Herunterladen von ausführbaren Dateien aus dem WEB geschehen, welche in der Lage sind auf dem eigenen Rechner oder im Netz gespeicherte Daten auszuspähen, zu manipulieren oder zu löschen.
Aber auch Persönlichkeitsrechte der Nutzer können bei Nutzung der neuen Medien verletzt werden. So ist die Möglichkeit der Bildung von Nutzerprofilen anhand der übertragenen inhaltlichen Daten sowie der anfallenden Verbindungsdaten gegeben. Wer im Internet surft oder Mobilfunkdienste nutzt, zieht eine breite Datenspur hinter sich her. Anonymität ist immer noch ein Fremdwort. Spätestens wenn der Nutzer sich persönlich bei einer Transaktion mit Name und Adresse identifiziert, sind angelegte Profile ihm direkt zuordenbar. Hinzu kommt, dass die Nutzer oft nicht oder nur unzureichend seitens der Anbieter hierüber informiert werden, was vielfach zu einer Verunsicherung der Nutzer führt. Deshalb ist es wichtig und notwendig, dass seitens der Entwickler und Anbieter bei der organisatori-

schen und technischen Konzeptionen von Applikationen sowohl gesetzliche Anforderungen als auch sicherheitstechnische Erfordernisse beachtet und die Nutzer hierüber informiert werden. Dies ist ein wesentliches Kriterium für die Akzeptanz seitens der Nutzer und damit für den Erfolg der neuen Technologien.
Bemühungen die Sicherheit zu verbessern sind unverkennbar. Der zunehmende Einsatz neuer Sicherheitsprotokolle, verbesserter Authentisierungs- und Verschlüsselungsverfahren sowie moderner Zugangskontroll- und Erkennungsmechanismen zur Gefahrenprävention sind hier u. a. zu nennen. Auch für die mobile Kommunikation müssen die gleichen grundlegenden Sicherheitsanforderungen wie für die herkömmliche Kommunikation gelten. Mit dem neuen Signaturgesetz und dem Aufbau von Public Key Strukturen (PKI) sind wesentliche Voraussetzungen für eine rechtsverbindliche Kommunikation gegeben (15.7). An der Entwicklung von Verfahren, welche auch eine anonyme Nutzung des Internet ermöglicht, wird intensiv gearbeitet. Für die Fälle, in denen der Nutzer den Anbietern seine persönlichen Daten aber bewusst offenbart, weil er bspw. online ein Produkt bestellt und zur Lieferung seine Anschrift benötigt wird, sollte er wissen, wie der Anbieter mit diesen Daten umgeht. Für eine bessere Transparenz seitens der von den Web-Anbietern angewandten Praktiken zum Umgang mit den nutzerspezifischen Daten, hat im Jahr 2000 das internationale World Wide Web Consortium (W3C) einen neuen Web-Standard vorgestellt. Das als P3P offerierte Konzept beinhaltet ein (maschinenlesbares) Vokabular zur Beschreibung der Datenschutzpraktiken des Web-Anbieters und ein Protokoll zum automatischen Austausch dieser Informationen mit dem Browser des Nutzers. Statt mühsam klein Gedrucktes zu lesen, werden vom Browser anhand vorgegebener Präferenzen des Nutzers die standardisierten Vorgaben der Anbieter automatisiert verglichen, sodass der Nutzer zwischen für ihn akzeptablen und inakzeptablen Web-Seiten unterscheiden kann. Die Einhaltung der veröffentlichten Datenschutzpraktiken seitens des Anbieters wie auch die Zweckbindung der Nutzerdaten kann allerdings P3P nicht garantieren. Inwieweit und wann sich dieser technische Basisstandard zum Schutz der Privatsphäre durchsetzt, wird die nahe Zukunft zeigen.

15.2 Einsatz von Informationstechnik in der Landesverwaltung

Gemäß den „Richtlinien für den Einsatz von Informationstechnik in der Landesverwaltung Thüringen“ erstellt das TIM jährlich einen fortzuschreibenden IT-Gesamtplan. Dieser wird dem IMA-IT zur Beratung und Bestätigung vorgelegt. Der Gesamtplan weist u. a. in einer zusammenfassenden Darstellung die IT-Maßnahmen der Ressorts sowie die Bestandsentwicklung an Hard- und Software aus. Der im März 2001 veröffentlichte und vom IMA-IT bestätigte aktuelle IT-Gesamtplan umfasst den Zeitraum von 2000 bis 2002. Anhand der vorliegenden Dokumentation lassen sich nicht nur grundlegende Aussagen zur Entwicklung der IT in der Landesverwaltung selbst, sondern auch im Hinblick auf sicherheitstechnische Aspekte ableiten. So waren Ende des Jahres 2000 insgesamt 20.243 APC im Einsatz. Davon sind 17.261 APC, also die überwiegende Mehrheit, in 634 lokalen Netzen (LAN) eingebunden. In den LAN kommen 830 Server zum Einsatz. Allein 441 der LAN verfügen über einen Zugang zum CN. Neben derzeit fünf Großrechnern werden auch 200 Mehrplatzrechner mit 1.407 Terminalarbeitsplätzen eingesetzt. Während der Bestand an Mehrplatzrechnern bis Ende 2002 nahezu konstant bleibt, wird allerdings die Anzahl der hier angeschlossenen Terminals auf 889 stark abnehmen. Dagegen wird laut Planung der Ressorts bis Ende 2002 eine weitere beachtliche Steigerung an APC, Servern sowie LAN zu verzeichnen sein. Der Ausstattungsgrad der Büroarbeitsplätze mit IT wird bis Ende 2002 auf 85% steigen. 1994 lag dieser bei 44%. Nahezu 80% dieser IT-Arbeitsplätze werden im Jahr 2002 in lokale Netze eingebunden sein. Die Hälfte der an vernetzten APC arbeitenden Mitarbeiter werden Ende 2002 die elektronische Post, die im Intranet der Landesverwaltung angebotenen Dienste sowie das Internet nutzen. Der hohe Ausstattungsgrad der Arbeitsplätze mit IT sowie deren Vernetzung erfordert auch sicherheitstechnischen Aspekten nach wie vor große Beachtung beizumessen. Insbesondere sind die vorhandenen Sicherheitsmaßnahmen daraufhin zu prüfen ob sie dem Stand der Technik noch genügen, um sie gegebenenfalls den neuen Erfordernissen anzupassen. Dies gilt nicht nur in Bezug auf die Verfügbarkeit und Zuverlässigkeit der eingesetzten IT, sondern auch im Hinblick auf die Absicherung der Integrität und der Vertraulichkeit der zu verarbeitenden Daten. Hinzu kommt insbesondere bei einer Übertragung von Daten über Netze der

Nachweis für deren Authentizität, d. h. der Zuordenbarkeit ihres Ursprungs.
Seit jeher bieten Großrechner und Mehrplatz-Rechnersysteme ein günstiges Umfeld für eine ordnungsgemäße und gesicherte Datenverarbeitung, nicht zuletzt aufgrund ihrer zumeist abgeschlossenen Struktur, determinierten Verarbeitungsabläufe und zentralen Rechteverwaltung. Um den vielfältigen Anforderungen der IT-Benutzer vor Ort jedoch besser Rechnung zu tragen, kommt in der Landesverwaltung in erheblichen Umfang lokal vernetzte dezentrale Technik, z. B. Client-Server-Systeme, zum Einsatz. Gefahren für diese IT-Systeme und die hier zu verarbeitenden Daten ergeben sich insbesondere wenn diese Systeme auch an öffentliche Netze, wie das Internet angeschlossen sind. Um die internen Netze zu schützen, werden dazu spezielle Hard- und Software Produkte, so genannte Firewalls, eingesetzt. Hierbei handelt es sich um eine etablierte Technologie einer Zugangskontrolle um primär das eigene Netz gegenüber unbefugten Zugriffen aus dem externen Netz zu schützen. Mit diesem grundlegenden Schutz beim Anschluss von Netzen an das Internet wird aber nur einer von vielen möglichen Bedrohungen begegnet. Um auch Sicherheitsverletzungen in internen Netzen aufzuspüren, bietet sich zusätzlich der Einsatz eines Intrusion Detection Systems an, spezielle Programme, die auch intern hervorgerufene Sicherheitsverletzungen erkennen. Mit einer Firewall kann auch nicht die Vertraulichkeit, die Integrität und die Authentizität der zu übertragenen Daten abgesichert werden. Ebenfalls können ohne zusätzliche Kontrollprogramme die Datenströme nicht auf schadensstiftende Elemente wie Viren und Trojaner geprüft werden, die sowohl mittels E-Mail übertragen, als auch vom Benutzer zumeist unbewusst aus dem Internet mit herunter geladen werden können. Dass es sich hierbei durchaus um reale Bedrohungen handelt, zeigte sich insbesondere anhand der jüngsten weltweiten Virenattacken, wo sich im Anhang von E-Mails getarnte schadensstiftende Programme aufgrund der Vernetzung der IT-Systeme global und explosionsartig ausbreiten konnten. Auch das CN der Landesverwaltung und hier angeschlossene Stellen blieben davon nicht verschont (15.5). Derzeit verfügen ein Drittel der vernetzten IT-Arbeitsplätze der Landesverwaltung über die Möglichkeit, elektronische Post weltweit zu versenden und zu empfangen. Gefahren ergeben sich dadurch nicht nur für die Verfügbarkeit der IT-

Technik, sondern auch für die Integrität und die Vertraulichkeit der gespeicherten Daten.
Eine wesentliche Bedeutung für die Sicherheit der IT und der Daten besitzt die eingesetzte System- und Anwendungssoftware. Grundsätzlich ist hier festzustellen, dass die Software immer komplexer wird und in immer kürzeren Zyklen, neue Programmversionen auf den Markt kommen. Hierunter leidet auch die Transparenz für den Benutzer. Eine Entwicklung die auch aus sicherheitstechnischer Sicht nicht unbedenklich ist. Auf ca. 95 % der eingesetzten APC in der Landesverwaltung kommen Windows-Betriebssysteme zum Einsatz. Die unter Windows-NT-Server arbeitenden zentralen Rechner haben von 27 % im Jahre 1997 auf 46 % im Jahre 2000 zugenommen. Das von der Grundausstattung her nicht mit üppigen Sicherheitsfunktionen ausgestattete Mehrplatzrechner-Betriebs-system UNIX hat somit seine bisherige Dominanz verloren. Auf den APC wird vorwiegend Büro-Standard-Software zur Textverarbeitung oder Tabellenkalkulation eingesetzt.
Der IMA-IT empfiehlt den Ressorts für ressortneutrale sachgebietsorientierte Anwendungen einheitliche Produkte einzusetzen. Hierzu ist anzumerken, schon bei der Auswahl von Betriebssystemen und Anwendungssoftware ist mehr denn je sicherheitstechnischen Aspekten eine große Bedeutung beizumessen. So ist u. a. bei der Auswahl auf eine sichere Identifizierung und Authentifizierung der Benutzer, eine detaillierte und nachvollziehbare Zugriffsrechtevergabe, eine effektive Rechteverwaltung, eine umfangreiche Protokollierung relevanter Sicherheits- und Verarbeitungsereignisse und eine optionale Verschlüsselung sensibler Daten zu achten. Soweit wie möglich ist zertifizierten Produkten sowie solchen der Vorzug zu geben, deren Quelltext offen gelegt ist (Open Source Software, 15.15). Mit der derzeitigen Einführung der elektronischen Signatur und Verschlüsselung innerhalb der Landesverwaltung (15.8) und dem Einbinden entsprechender Tools in die gängige Kommunikationssoftware wird insbesondere notwendigen Sicherheitsaspekten bei der Übertragung von Daten über öffentliche Netze entsprochen.
Basis einer sicheren Datenverarbeitung ist jedoch nach wie vor, dass in ausreichender Anzahl hierfür qualifiziertes Personal zur Verfügung steht. Hier gilt es, zielgerichtet geeignete Maßnahmen einzuleiten und Kapazitäten einzuplanen, um den derzeitigen und zukünftigen Anforderungen an die IuK gerecht werden zu können.

15.3 Sicherheitskonzept des Corporate Network (CN)

Zum Aufbau und dem kontinuierlichen Ausbau des Daten-, Sprach- und Kommunikationsnetzes (CN) der Landesverwaltung wurden bereits Ausführungen in vorausgegangenen Tätigkeitsberichten gemacht (1. TB, 15.5.1; 2. TB, 15.2; 3. TB, 15.3). Mit Stand September 2001 sind nach Auskunft des TIM, als verantwortliches Ressort, für das CN 333 Landesbehörden, 15 Landratsämter und 65 kommunale Stellen am CN angeschlossen. Neben der Übertragung von Daten im Rahmen von IT-Anwendungen beispielsweise zwischen öffentlichen Stellen des Landes und dem ZIV, werden von den am CN angeschlossenen Benutzern insbesondere die Dienste E-Mail und WWW zunehmend genutzt. Mittels E-Mail können die angeschlossenen Teilnehmer untereinander, mit öffentlichen Stellen anderer Bundesländer und des Bundes, als auch weltweit Nachrichten und Dokumente austauschen. Der elektronische Postdienst ist sowohl auf Basis des X.400-Standards als auch des standardmäßigen Internet-E-Mail-Dienstes (SMTP) möglich. Auch der zentrale Web-Server der Landesverwaltung, auf dem die Internetpräsentationen der Landesbehörden und weiterer öffentlicher Stellen Thüringens vorgehalten werden, ist im CN eingebunden. Für die CN-Benutzer steht weiterhin seitens der Landesverwaltung ein Intranet-Informationsangebot zur Verfügung. Der Zugang aus dem CN in das Internet ist aus Sicherheitsgründen nur über ein zentrales Firewallsystem möglich, welches das CN gegenüber dem öffentlichen Netz absichert. Mit dem Betrieb des CN ist das TLRZ als Landesbetrieb beauftragt und betreut somit u. a. auch systemtechnisch dessen komplexe IT-Infrastruktur.
Eine wesentliche Forderung beim Aufbau dieses Netzes war die Erarbeitung eines Sicherheitskonzeptes für dessen Betrieb, was seitens des TIM erfolgte. Ausgehend von einer Schutzbedarfsfeststellung wurden mittels einer Bedrohungs- sowie einer darauf aufbauenden Risikoanalyse die notwendigen Maßnahmen für die gegen Bedrohungen zu schützenden Objekte (z. B. Infrastruktur, Hardware, Anwendungsdaten, Kommunikation, Personen etc.) konkret abgeleitet und festgelegt. Insbesondere für die vom Netzbetreiber angebotenen Dienste und Protokolle werden verschiedene, mit den Nutzern nach deren Bedürfnissen abgestimmte Sicherheitsmaßnahmen realisiert. Sodass die öffentlichen Stellen, welche das CN nutzen, anhand

ihrer IT-Anwendungen entscheiden können, ob gemäß deren datenschutzrechtlicher und sicherheitstechnischer Erfordernissen diese Maßnahmen ausreichen oder gegebenenfalls für einzelne Anwendungen noch zusätzliche spezielle Maßnahmen erforderlich sind. Da das CN ein universelles Kommunikationsnetz ist, wurden anstatt konkreter IT-Anwendungen die im CN realisierten Kommunikationsbeziehungen untersucht und für diese Schutzziele anhand der objektunabhängigen Grundbedrohungen, nämlich einem Verlust der Verfügbarkeit, der Vertraulichkeit und der Integrität, festgelegt. In meiner Stellungnahme wies ich das TIM u. a. auf das Nachfolgende hin:
Gerade deshalb, weil es sich beim CN in erster Linie um ein Kommunikationsnetz handelt, ist es auch erforderlich, über diese drei Sicherheitsfunktionen hinaus die Verbindlichkeit, mit der die kommunikativen Transaktionen vollzogen werden, einzubeziehen. Es geht hierbei darum abzuklären, inwieweit eine Zuordenbarkeit der über das CN ausgelösten Aktionen und übertragenen Daten möglich bzw. gewährleistet ist. Insbesondere im Hinblick auf eine rechtsverbindliche Kommunikation innerhalb des CN ist es neben der Integrität (Unversehrtheit) der übertragenen Daten erforderlich, dass diese einem Urheber zuverlässig zugeordnet werden können und die Nicht-Abstreitbarkeit des Ursprungs sichergestellt ist. Dies gilt insbesondere für Nachrichten und Dokumente. Desweiteren ging das Konzept für die Ausprägung der Bewertungskategorie „Sensitivitätsgrad der Information“ ausschließlich von den Geheimhaltungsgraden laut Verschlusssachenanweisung des Landes aus. Eine ausschließliche Einstufung der Sensitivität der Informationen nur hiernach wird jedoch den datenschutzrechtlichen Erfordernissen nicht gerecht, da letztere eine Einstufung der Sensitivität personenbezogener Daten nach dem Grad der Beeinträchtigung des informationellen Selbstbestimmungsrecht Betroffener erfordern. Ich schlug deshalb dem TIM vor, dass vom TLfD empfohlene Schutzstufenkonzept neben den Geheimhaltungsgraden als Kriterium für die Sensitivität der Informationen einzubeziehen.
Bei der Überarbeitung des CN-Sicherheitskonzeptes wurden meine Hinweise berücksichtigt. Zu meiner Forderung, auch zu untersuchen, inwieweit das CN eine verbindliche Kommunikation ermöglicht, ist seitens des TIM vorgesehen diesen wichtigen Komplex anschließend gesondert zu bearbeiten, was auch im Zusammenhang mit der Ein-

führung der elektronischen Signatur in der Landesverwaltung derzeit erfolgt.

15.4 Leitungsverschlüsselung im CN

Die Vertraulichkeit innerhalb des CN übermittelter Daten kann durch eine Verschlüsselung der Datenströme (Leitungsverschlüsselung) abgesichert werden. Das TIM als Betreiber des CN richtet auf Antrag der Benutzer eine solche gesicherte Verbindung zwischen den zwei Übermittlungsstellen ein. Aus Kostengründen ist allerdings Voraussetzung für eine solche Verbindung, dass zwischen den Benutzern als sensibel eingestufte Daten übermittelt werden. Derzeit nutzen mehrere Einrichtungen der Landesverwaltung solche Verbindungen für ihren Datenaustausch. Beispielsweise erfolgt hierüber der Datenaustausch zwischen den Finanzämtern und der OFD. In Anbetracht der Bedeutung dieses automatisierten Verfahrens für die Sicherheit der hiermit übermittelten Daten führte ich eine datenschutzrechtliche Kontrolle zur Leitungsverschlüsselung durch. Diese hatte zum Ziel, die sicherheitstechnischen Aspekte für das eingesetzte Verschlüsselungsverfahren, insbesondere das System- und Schlüsselmanagement, die Protokollierung von Daten, die Wartung, die technischen und organisatorischen Sicherheitsmaßnahmen und die Abgrenzung der Verantwortlichkeiten zwischen Betreiber und Nutzer der Leitungsverschlüsselung zu prüfen.
Für eine verschlüsselte Datenübertragung innerhalb des CN kommen so genannte Krypto-Boxen zum Einsatz. Durch den Einsatz von zumindest je einer Verschlüsselungsbox auf der Sender- und der Empfängerseite wird zwischen diesen eine verschlüsselte Übertragung der Datenströme ermöglicht, basierend auf einem symmetrischen Verschlüsselungsverfahren (2. TB, 15.7.3). D. h. sowohl die absendende als auch die empfangende Box arbeiten mit dem gleichen Schlüssel. Eingesetzt wird der DES-Algorithmus mit einer Schlüssellänge von 128 Bit. Die Integration von Krypto-Boxen in die Netzstruktur des CN bzw. zwischen Endgerät und Netzanschluss kommt somit der Einführung einer Sicherheitsschicht gleich, womit zumindest die Vertraulichkeit der übermittelten Daten und somit auch eine bewusste Manipulation dieser abgesichert wird. Die Boxen sind für die jeweiligen Nutzer völlig transparent, d. h. sie sind schnittstellenneutral und führen ihre Funktionen automatisch, ohne Zutun und

Kontaktierung der Nutzer aus. Insofern kann der Nutzer auch nicht in seinem Ermessen die Verschlüsselung ein- bzw. ausschalten. Der Datenstrom wird zwangsweise immer verschlüsselt, soweit die Verschlüsselungsbox dem gemäß eingestellt ist.
Die Krypto-Boxen selbst bestehen aus einer intelligenten Kommunikationseinrichtung und aus einem Sicherheitsmodul. In dem Sicherheitsmodul werden alle sicherheitsrelevanten Aktionen geschützt ausgeführt und gespeichert. Dieser Sicherheitsmodul ist physikalisch gekapselt und mit einer Sensorik ausgerüstet, die Angriffe erkennt und ggf. alle sicherheitsrelevanten Informationen wie geheime Schlüssel, Art der erlaubten Kommunikationsverbindungen, Logbücher aktiv löscht. Insofern sind keine Unbefugten in der Lage die Endgeräte zu manipulieren. Durch den Einsatz der Krypto-Boxen wird weiterhin erreicht, dass nur Verbindungen aufgebaut werden, die erlaubt sind und sicherheitsrelevante Ereignisse protokolliert und ausgewertet werden können.
Zum Zeitpunkt der Kontrolle war das eingesetzte Sicherheitssystem von der Herstellerfirma zur Zertifizierung beim BSI eingereicht. Kern des eingesetzten Systems ist ein zentrales Managementsystem, mit welchem die Krypto-Boxen über das Netz oder direkt administriert werden können. Das Managementsystem, welches auf einem separaten Rechner, der unter dem Betriebssystem UNIX arbeitet, installiert ist, dient insbesondere zur Administration der Sicherheitsfunktionen. Im Auftrag des TIM wird diese Tätigkeit ausschließlich durch befugte Administratoren des TLRZ ausgeübt. Deren Aufgaben umfassen u. a.:

- das Installieren der Boxen mit sicherheitsrelevanten Informationen und Konfigurationsdaten,
- das Generieren von Access-Listen, die vorgeben, wer mit wem kommunizieren darf,
- das Generieren und Verwalten der Schlüsselsysteme, wobei jede Box über den gleichen Pool von 64 Verbindungsschlüsseln verfügt, aus welchen den jeweils kommunizierenden Boxen nach dem Zufallsprinzip ein konkreter Schlüssel zugewiesen wird,
- das Auswerten von protokollierten Sicherheitsereignissen sowie die Durchführung von notwendigen Systemanalysen.

Die vor Ort bei den jeweiligen Nutzern vorgehaltenen Krypto-Boxen werden vom Administrator zumeist ferngesteuert. Die hierzu erforderliche Kommunikation wird aus Sicherheitsgründen ebenfalls ver-

schlüsselt durchgeführt. Desweiteren sind alle sicherheitsrelevanten Daten sowohl auf der Management-Station als auch in den Krypto-Boxen verschlüsselt abgelegt. Bevor eine Box eingesetzt wird, wird sie unmittelbar an der Systemmanagement-Station personalisiert, wobei sie u. a. eine eindeutige Identifizierungsadresse erhält sowie die geheimen Schlüssel geladen werden.
Im Ergebnis der Kontrolle ergaben sich datenschutzrechtliche Forderungen, die insbesondere das technisch organisatorische Umfeld zum Einsatz dieses Sicherheitssystemes betrafen. U. a. wurde gefordert, Regelungen zur Zutritts-, Zugangs- und Zugriffskontrolle der Komponenten sowie zum Schlüsselwechsel zu erlassen. Die Integrität des Systems und damit die Absicherung der Vertraulichkeit der verschlüsselten Datenströme hängt im erheblichen Maße von den Zugangskennungen, der sicheren Schlüsselverwaltung und des häufigeren Wechsels der für die Datenkryptierung eingesetzten Schlüssel. Hierzu fehlten diesbezügliche Regelungen für die Administration des Systems. Es wurde empfohlen, eine Information zur Leitungsverschlüsselung zu erstellen und den Nutzern zur Verfügung zu stellen. Diese Information soll gezielt die Funktionsweise und die sicherheitstechnischen Zusammenhänge des Systems darlegen sowie auch eine Orientierungs- und Entscheidungshilfe für einen angedachten Einsatz des Systems zur Verschlüsselung schutzwürdiger Daten sein. Weiter wurden auch eindeutige Regelungen an die Administratoren gefordert, die Nutzer im Vorfeld über eine Abschaltung der Verschlüsselung bzw. über die ordnungsgemäße Funktionsfähigkeit der Wiederherstellung der Leitungsverschlüsselung zu informieren. Grundsätzlich müssen die Nutzer vor der Abschaltung des Verschlüsselungsmechanismus informiert werden. Eine solche Abschaltung ist beispielsweise erforderlich bei notwendigen Wartungsarbeiten, Fehleranalysen oder in der Einrichtungsphase. Eine weitere Forderung bezog sich darauf, die Datensicherungskopien in einem einbruchs- und brandschutzhemmenden Behältnis gesichert und lokal getrennt von der Managementstation aufzubewahren sowie Festlegungen zur Auswertung der Protokolldateien zu erlassen und Löschfristen für diese festzusetzen.
Die Hinweise und Empfehlungen des TLfD wurden umgesetzt.

15.5 Virenschutz

Der Begriff Virus wird häufig als Pseudonym für schadensstiftende Software (Viren, Trojanische Pferde und Würmer) verwendet. In meinem 2. TB (15.11) stellte ich bereits die Gefahren für die Integrität und die Vertraulichkeit von personenbezogenen Daten die durch Viren ausgehen dar und machte deren Funktionsweise deutlich. Als Trojanische Pferde bezeichnet man Schadsoftware, die unter falschem Namen in das System gelangen, oft eine nützliche Tätigkeit suggerieren, aber in Wirklichkeit Schäden anrichten können. Sie sind insofern keine Viren, da sie sich weder vermehren noch andere Programme infizieren. Würmer sind eigenständige Programme, die sich selbständig in einem Netzwerk ausbreiten indem sie sich reproduzieren und sich vorhandener Netzwerkfunktionen bedienen. Dabei ist es eine beliebte Strategie bei den mitgesandten Anlagen doppelte Dateinamen-Suffixe wie AnnaKournikova.jpg.exe oder Loveletter.txt.vbs einzusetzen. Da bspw. der Windows Explorer bei der Standardeinstellung die Erweiterungen registrierter Dateitypen nicht anzeigt (wie .exe oder .vbs), wird so dem Nutzer eine harmlose Bild- oder Textdatei vorgetäuscht. Bei einem Doppelklick ruft das System nicht die Bild- oder die Textdatei auf, sondern ganz korrekt das Visual Basic Script und führt es dementsprechend aus. So war es auch beim Wurm mit dem Namen „AnnaKournikova“. Im Fall des Wurms „Nimda“, der sich ebenfalls u. a. mittels Anhang von E-Mails verbreitete, ist die Datei im Anhang eine nicht immer sichtbare admin.dll oder readme.exe. Dieser weit aus gefährlichere Wurm gibt u. a. auf befallenen Computern Laufwerke zum externen Zugriff frei und richtet sich einen Gast-Account mit den Rechten eines Administrators ein.
Im Berichtszeitraum war feststellbar, dass sich neben den Viren auch Trojanische Pferde und insbesondere Würmer stark verbreiten. Einer Statistik des BSI ist zu entnehmen, dass im Jahr 2000 von den gemeldeten Viren 41 % Würmer waren und bereits im Jahr 2001 das Auftreten von Würmern auf 71 % gestiegen ist. Durch geeignete Anti-Virenprogramme können in der Regel die o. g. Varianten an schadensstiftender Software erkannt werden.

Auch das CN der Thüringer Landesverwaltung wurde erstmalig durch einen von außen übertragenen Wurm infiziert. Es handelte sich um den bereits erwähnten Wurm „AnnaKournikova“, der sich weltweit im Februar 2001 per E-Mail verbreitete und als Anlage ein Bild der Tennisspielerin Anna Kournikova versprach. Durch Anklicken

dieses Anhangs wird der Wurm aktiv und versendet wiederum E-Mails mit dem Wurm an alle auf dem PC im Adressbuch gespeicherten E-Mail Adressen. So wurden bspw. von einem PC einer öffentlichen Stelle der Landesverwaltung durch das Anklicken dieses Anhangs viele E-Mails (aus dem globalen und persönlichen Adressbuch) aktiviert und an die entsprechenden Dienststellen des Landes Thüringen versandt. Infolge des erhöhten Mail-Aufkommens und durch das erneute Öffnen der E-Mail einschließlich Anhang in einigen der Dienststellen entstand daraufhin ein erheblicher Datenstau innerhalb des CN, sodass dadurch die Leitungen überlastet waren. Das TLRZ, welches die E-Mail Landeskopfstelle des CN betreibt, leitete entsprechende Maßnahmen ein, um eine Weiterverbreitung des Viruses zu verhindern. In Auswertung des Vorfalls und im Hinblick auf geeignete Datensicherungsmaßnahmen bat ich die betroffenen Stellen um eine entsprechende Stellungnahme. Den Stellungnahmen war zu entnehmen, dass die Ursache der Verbreitung innerhalb des CN zum einen in dem Fehlen von Anti-Viren-Programmen lagen, zum anderen installierte Anti-Viren-Programme nicht die aktuellen Versionen aufwiesen oder nicht korrekt eingestellt waren. Seitens der betroffenen Behörden wurde mir zugesichert, dass soweit noch nicht vorhanden geeignete Produkte gemäß den Empfehlungen des IMA-IT beschafft werden sollen, vorhandene Programme neu konfiguriert wurden und die Mitarbeiter für diese Problematik erneut sensibilisiert werden. Auch der IMA-IT nahm den Vorfall im CN zum Anlass, sich erneut mit der Sicherheit im CN zu befassen. Zentraler Diskussionspunkt war, durch das TLRZ prüfen zulassen, inwieweit schon zusätzlich auf zentraler CN-Ebene (Landeskopfstelle und Internet-Gateway) ein Anti-Virenschutz-Programm zum Einsatz kommen kann. Aus datenschutzrechtlicher Sicht begrüße ich daher ausdrücklich das Vorhaben vom TIM, den zentralen Anti-Virenschutz als Baustein in die vom Kabinett angeforderte Vorlage zum E-Government einbinden zu wollen. Ungeachtet eines eventuellen Einsatzes eines zentralen Virenscanners am Internet-Gateway, bleiben die öffentlichen Stellen weiter in der Pflicht, in einer zweiten Stufe auf allen Exchange-Standortservern und in der dritten Stufe auf Servern und Workstation im eigenen LAN Maßnahmen zum Einsatz von Anti-Virenprogrammen zu ergreifen.

15.6 Länderübergreifende Vernetzung TESTA

Über das Projekt TESTA, welches die öffentliche Verwaltung der Bundesländer und des Bundes sowie der EU-Länder miteinander vernetzt, habe ich schon ausführlich im 3.TB (15.5) berichtet. Inzwischen wurde die seitens der DSB des Bundes und der Länder geforderte und auch seitens des KoopA-ADV angedachte Leitungsverschlüsselung umgesetzt. Damit werden zwischen den jeweiligen Anschlussknoten der Länder an TESTA die zu übertragenen Daten durch ein hardwarebasiertes kryptographisches Verfahren automatisch, d. h. ohne Einflussnahme der Nutzer verschlüsselt übertragen. Dadurch wird die Vertraulichkeit der Informationen innerhalb von TESTA abgesichert und gezielte Manipulationen an deren Daten verhindert. Dies ist ein wesentlicher Schritt zu mehr Sicherheit. Die Nutzer müssen jedoch noch im eigenen Ermessen dafür Sorge tragen, wenn die Vertraulichkeit der übertragenen Daten durchgehend vom Absender bis zum Empfänger (Ende zu Ende Verschlüsselung) gewährleistet sein soll. Das trifft auch zu für die Prüfung der Unversehrtheit der empfangenen Daten und deren Authentizität. Somit regte ich gegenüber dem TIM an, für die Endnutzer den Einsatz kryptographischer Verfahren vorzusehen, wobei im Interesse einer breiten Nutzung ein einheitliches Produkt zum Einsatz kommen sollte.

Um die Einführung kryptographischer Verfahren zu unterstützen, beschloss der KoopA-ADV einen „Handlungsleitfaden für die Einführung der elektronischen Signatur und der Verschlüsselung in der Verwaltung“. Durch einen breiten Konsens, der vom Bund, Ländern und Kommunen getragen wird, soll erreicht werden, dass möglichst einheitliche, interoperable und sichere Lösungen etabliert werden, die durch ihre Breitenwirkung auch eine Kosten senkende Wirkung entfalten. Die Vorgaben beziehen u. a. eine sichere E-Mailübertragung als auch eine gesicherte Dokumentenübertragung ein. Sie gelten gleichermaßen für gesicherte Kommunikationsbeziehungen der öffentlichen Verwaltungen untereinander sowie zur Wirtschaft und zum Bürger (E-Government). Damit steht jetzt die umfassende Einführung der elektronischen Signatur und Verschlüsselung für eine sichere elektronische Kommunikation an. Die technologische Basis bildet hierzu TESTA. Auch das vom Bund getragene Projekt SPHINX, das insbesondere im Rahmen des elektronischen Informationsverbundes Berlin/Bonn konzipiert wurde, soll im Hinblick auf

die hierzu gewonnenen Erfahrungen einen wesentlichen Beitrag leisten. Entsprechende Tests wurden schon durchgeführt. Der Freistaat Thüringen beteiligte sich hier aktiv. Die Testphase ist in Thüringen abgeschlossen. Derzeit wird der Wirkbetrieb vorbereitet (15.8). Von der Arbeitsgruppe „Kommunikation und Sicherheit“ des Koop-ADV wurde inzwischen eine Dokumentation „Sichere Kommunikation zwischen Verwaltungsnetzen“ erarbeitet, das ich vom TIM erhielt. In diesem umfangreichen Papier sind für TESTA Sicherheitsanforderungen und deren Realisierung dargelegt sowie diesbezügliche Sicherungsmaßnahmen aufgezeigt. Diese Konzeption dient als sicherheitstechnische Grundlage für den weiteren Ausbau von TESTA. Für die länder- und verwaltungsübergreifende Kommunikation mittels TESTA wurde auf Beschluss des Koop-ADV desweiteren ein zentraler Verzeichnisdienst eingerichtet. In diesem Verzeichnis werden für die elektronische Kommunikation u. a. Namen und E-Mail-Adressen der TESTA-Nutzer vorgehalten. Seitens des TIM war deshalb zunächst das globale elektronische Adressbuch des CN, in dem alle Mitarbeiter der Landesverwaltung aufgeführt sind, die über eine dienstliche personenbezogene E-Mail Adresse verfügen, in das TESTA-Verzeichnis eingebunden worden, diese erfolgte allerdings ohne Einbeziehung der zuständigen Stellen, die gemäß § 2 und § 34 ThürDSG für die Verarbeitung und Nutzung der personenbezogenen Daten ihrer Mitarbeiter verantwortlich sind. Eine Bereitstellung personenbezogener Daten der Mitarbeiter zum Abruf durch andere öffentliche Stellen mittels eines automatisierten Verfahrens stellt aber eine Datenübermittlung dar, die gemäß § 21 in Verbindung mit § 20 ThürDSG nur zulässig ist, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelten Stelle oder des Dritten liegenden Aufgabe erforderlich ist und die Zweckbindung dieser Daten beachtet wird. Somit dürfen in das o. g. Verzeichnis seitens der Stellen nur die Daten von den Mitarbeiter eingestellt werden, die zur Wahrnehmung ihrer Aufgaben länderübergreifend von anderen öffentlichen Stellen elektronisch erreichbar sein müssen. Nicht jeder Mitarbeiter der im globalen Adressbuch des CN aufgeführt ist, benötigt aber zur Wahrnehmung seiner dienstlichen Aufgaben auch die Dienste von TESTA. Insofern ist zunächst in der Verantwortung der zuständigen öffentlichen Stellen eine Vorabprüfung auf die Erforderlichkeit der Einstellung diesbezüglicher Daten von Mitarbeitern in das TESTA Verzeichnis erforderlich. Das TIM teilte mir auf diesen Hinweis

zwischenzeitlich mit, dass die Daten des globalen Adressbuches des CN wieder aus dem TESTA-Verzeichnis heraus genommen sind. Desweiteren sollen alle beteiligten Verwaltungseinrichtungen im CN angeschrieben werden, um festzustellen, ob und in welchem Umfang Informationen aus dem globalen Adressbuch in das TESTA-Verzeichnis einzustellen sind.

15.7 Rechtsverbindlichkeit der elektronischen Signatur

Seit dem 22. Mai 2001 ist das „Gesetz über Rahmenbedingungen für elektronische Signaturen“ (SigG) in Kraft. Es löste das bisher in Art. 3 des Informations- und Kommunikationsdienste-Gesetz (IuKDG) verankerte Signaturgesetz vom 22. Juli 1997 (2. TB, 15.8) ab. Die Novellierung des bisherigen SigG, mit dem der Bundesgesetzgeber weltweit die erste Rechtssetzung zur digitalen Signatur erließ, war gemäß der Europäischen Signaturrichtlinie (Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 13. Dezember 1999) notwendig geworden. Mit der EU-Richtlinie hatten sich die 15 EU-Mitglieder in Brüssel einstimmig auf gemeinsame Grundregeln für elektronische Signaturen geeinigt. Sie legt Rahmenbedingungen für elektronische Signaturen mit dem Ziel fest, innerhalb des Europäischen Binnenmarktes marktgerechte Lösungen für verbindliche elektronische Dienste zu fördern. U. a. sollen die Regeln das Benutzen elektronischer Signaturen und deren gesetzliche Anerkennung, insbesondere für den grenzüberschreitenden Elektronic- und Mobil-Commerce, aber auch für den elektronischen Schriftverkehr mit Behörden (E-Government), vereinfachen. Die Mitgliedsstaaten der EU waren gefordert die Richtlinie bis zum 19. Juli 2001 in nationales Recht umzusetzen. Inhaltlich geht die EU-Richtlinie über das bislang geltende deutsche Signaturgesetz hinaus, weil sie vor allem eine Gleichstellung elektronischer Signaturen mit handschriftlichen Unterschriften fordert.
Das SigG hält an der bisherigen Konzeption fest, lediglich die Fragen der Sicherheitsinfrastruktur und die Anforderung an die Sicherheit der Erzeugung von elektronischen Signaturen zu regeln. Eine Genehmigungspflicht für Zertifizierungsdiensteanbieter wird nicht mehr zwingend gefordert. Für diese wird allerdings eine Haftungsregelung eingeführt. Das novellierte Signaturgesetz gibt weiterhin vor, dass sich die Anbieter freiwillig von der zuständigen Behörde akkreditie-

ren lassen können. Dadurch erhalten sie ein offizielles Gütesiegel, mit dem sie auch werben dürfen. Das SigG sieht vier verschiedene Typen von Signaturen vor: Die einfache elektronische Signatur (§ 2 Nr. 1 SigG), die fortgeschrittene elektronische Signatur (§ 2 Nr. 2 SigG), die qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG) und darüber hinaus zusätzlich noch die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung (§ 2 Nr. 3 i. V. m. § 15 SigG). Im Sinne des Gesetzes sind elektronische Signaturen Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentisierung dienen. Fortgeschrittene elektronische Signaturen sind elektronische Signaturen, die darüber hinaus ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind, dessen Identifizierung ermöglichen, mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann und mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Die einfachen oder fortgeschrittenen elektronischen Signaturen sind der handschriftlichen Unterschrift nicht gleichgestellt, unterliegen aber der freien Beweiswürdigung der Richter. Sie sind für einfache Geschäfte des täglichen Lebens im Internet oder innerhalb von Unternehmen oder Verwaltungen einsetzbar. Erst die qualifizierte elektronische Signatur ist rechtlich der handschriftlichen Unterschrift gleichgestellt. Sie ist eine fortgeschrittene elektronische Signatur, die mit einer sicheren Signaturerstellungseinheit gemäß § 17, § 23 und § 24 SigG erzeugt sein muss und auf einem qualifizierten Zertifikat gemäß § 5 und § 7 SigG basiert, das von einem Zertifizierungsdiensteanbieter ausgestellt sein muss. Um ein solches zu bekommen, muss der Benutzer sich bei einem Anbieter ausweisen. Er erhält ein persönliches Zertifikat sowie seinen persönlichen geheimen Schlüssel. Das Zertifikat enthält u. a. seinen öffentlichen Schlüssel, der mit dem geheimen Schlüssel des Zertifizierungsanbieters signiert ist. Soweit Zertifizierungsdiensteanbieter nicht über eine Akkreditierung verfügen, beruht die Güte qualifizierter elektronischer Signaturen allerdings weitgehend auf deren eigenen Erklärungen. Qualifizierte elektronische Signaturen mit freiwilliger Anbieter-Akkreditierung gemäß § 15 SigG dürfen nur von Zertifizierungsdiensteanbietern vergeben werden, deren Leistungs- bzw. Produktqualität von der Regulierungsbehörde für Post- und Telekommunikation (RegTP) geprüft und bestätigt ist. Diese

Zertifizierungsanbieter repräsentieren damit eine nachweisbare Sicherheit und somit höchste Beweisqualität für die durchgeführten elektronischen Transaktionen. Mit diesem Signaturtyp können elektronische Transaktionen ausgeführt werden, an die besondere Anforderungen gestellt werden.

Die Forderung der EU-Richtlinie einer Gleichstellung elektronischer Signaturen mit handschriftlicher Unterschrift wurde vom deutschen Gesetzgeber durch das am 1. August 2001 in Kraft getretene „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr“ vom 13. Juli 2001 berücksichtigt. Mit diesem Gesetz wurde die juristische Grundlage geschaffen, bislang nur mit eigenhändiger Unterschrift zu versehene Dokumente auch elektronisch zu signieren. Mit dem neuen § 126a BGB wird die Möglichkeit des Ersetzens der Schriftform durch die elektronische Form vorgesehen, sofern das entsprechende Dokument mit einer im SigG definierten und als „qualifiziert“ bezeichneten elektronischen Signatur versehen ist. Insgesamt wird damit geregelt, dass solchen elektronischen Signaturen in einem möglichen Gerichtsverfahren erhöhte Beweiskraft zukommt. Mit rechtlich anerkannten elektronischen Signaturen sind die Voraussetzungen für einen sicheren elektronischen Rechts- und Geschäftsverkehr geschaffen worden. Damit können künftig Verträge elektronisch unterzeichnet und verbindlich über das Internet abgeschlossen, aber auch amtliche Dokumente wie Steuererklärungen oder Bauanträge elektronisch abgegeben werden.
Da die Einrichtung eines Zertifizierungsdienstes für qualifizierte elektronische Signaturen sehr hohe Investitionen erfordert und mit nicht unerheblichen laufenden Betriebskosten verbunden ist, kann zunächst davon ausgegangen werden, dass nicht wenige Firmen und Behörden auf den Aufbau einer solchen Infrastruktur gemäß der Umsetzung des SigG verzichten.
Am 22.11.2001 trat die neue Verordnung zur elektronischen Signatur (SigV) vom 16.11.2001 in Kraft, welche die erforderlichen Bestimmungen zur Ausgestaltung des SigG enthält. Der sichere Einsatz elektronischer Signaturen setzt entsprechende Systeme zur Nutzung und nicht zuletzt auch ein diesbezügliches Sicherheitsbewusstsein des Nutzers voraus.

Aus der Sicht des Datenschutzes ist die Novellierung des SigG zu begrüßen. Das hohe Sicherheitsniveau des schon 1997 verabschiedeten SigG wird mit der Zulassung akkreditierter Zertifizierungsdiensteanbieter beibehalten. Auch die Möglichkeit zur Ausstellung von pseudonymen Zertifikaten wurde übernommen. Dies trägt zur Wahrung der Persönlichkeitsrechte der Nutzer bei. Da es im Rahmen eines gerichtlichen Verfahrens möglich ist, die wahre Identität des pseudonymen Inhabers aufzudecken, kann davon ausgegangen werden, dass zunehmend auch von kommerziellen Anbietern Signaturen akzeptiert werden, die anstatt des Namens des Signaturinhabers ein Pseudonym enthalten. Ebenso könnte für bestimmte elektronische Transaktionen die Verwendung eines Pseudonyms der elektronischen Signatur zu einem zusätzlichen Aufschwung verhelfen. Auch die Entwicklung auf dem Weg zu E-Government hin, erfordert die hierzu erforderlichen elektronischen Willenserklärungen mit elektronischen Signaturen abzusichern. Nur so kann eine moderne Verwaltung sicher und rechtsverbindlich mit dem Bürger und der privaten Wirtschaft elektronisch kommunizieren. Jetzt kommt es darauf an, Signaturverfahren auch in das Verwaltungsrecht einzubinden. Zuvor muss jedoch eine entsprechende diesbezügliche Modernisierung des Verwaltungsrechts erfolgen. Hierzu ist eine Anpassung durch das 3. Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften in Vorbereitung, im Rahmen dessen auch die Regelungen des VwVfG angepasst werden (5.1.5).

15.8 Einsatz von elektronischer Signatur und Verschlüsselung

Sowohl im privaten als auch im dienstlichen Bereich werden zunehmend elektronische Dienste genutzt, wobei immer häufiger Informationen oder Dokumente in elektronischer Form vorgehalten und ausgetauscht werden. Auch öffentliche Stellen streben eine interaktive Kommunikation mit den Bürgerinnen und Bürgern oder der Wirtschaft an, um elektronische Auskünfte oder Verwaltungsvorgänge serviceorientiert unter Nutzung des Internets durchzuführen. So spielt auch im Konzept der Landesregierung zur Verwaltungsmodernisierung des Freistaates diese als E-Government bekannte Zielsetzung eine wesentliche Rolle (5.1.6). E-Government erfordert insbesondere eine sichere Datenübertragung zwischen den Beteiligten. Ohne zu-

sätzliche Sicherheitsmaßnahmen ist jedoch die Vertraulichkeit und der Nachweis über die Unversehrtheit (Integrität) der zu übertragenen Daten nicht gewährleistet sowie eine sichere Feststellung der Identität der Kommunikationspartner bzw. des Urhebers einer übermittelten Nachricht oder eines Dokuments (Authentisierung) nicht möglich. Solange aber der Urheber nicht zweifelsfrei bestimmt werden kann, ist auch die Verbindlichkeit (Nichtabstreitbarkeit) der übersandten Informationen in Frage gestellt.
Die erwähnten Risiken, welche mit der elektronischen Übertragung von Daten generell verbunden sind, schließen aus datenschutzrechtlicher Sicht grundsätzlich eine Übertragung personenbezogener Daten durch öffentliche Stellen ohne ausreichende technische und organisatorische Sicherheitsmaßnahmen aus. Eine elektronische Übermittlung personenbezogener Daten, die sowohl auf leitungsgebundenen oder drahtlosen Übertragungswegen erfolgen kann, stellt gemäß § 3 Abs. 3 ThürDSG eine Verarbeitung personenbezogener Daten dar. Hierfür sind nach § 9 Abs. 2 Nr. 1, Nr. 2 und Nr. 4 ThürDSG Maßnahmen zu treffen, die je nach Art der zu schützenden Daten gewährleisten, dass nur Befugte personenbezogenen Daten zur Kenntnis nehmen können (Vertraulichkeit), diese Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität) und jederzeit ihrem Ursprung zugeordnet werden können (Authentizität). Eine geeignete Maßnahme hierzu stellt der Einsatz moderner kryptographischer Verfahren dar. Solche Verfahren ermöglichen die Sicherstellung der Vertraulichkeit der Daten durch ihre Verschlüsselung (2. TB, 15.7.2-15.7.4; 3. TB, 15.9) sowie mit einer elektronischen Signatur (2. TB, 15.7.5) den Nachweis der Integrität der Daten und der Überprüfung ihres Urhebers. Schon in ihren gemeinsamen Entschließungen vom März 1995, Mai 1996 und Oktober 1999 forderten die DSB des Bundes und der Länder den Einsatz solcher Verfahren, um eine sichere Übertragung insbesondere personenbezogener Daten zu gewährleisten (1. TB, S. 163; 2. TB, S. 298; 3. TB, S. 310). Diesen Forderungen wird seitens der Landesverwaltung und weiterer öffentlicher Stellen durch die Einführung der elektronischen Signatur und der Datenverschlüsselung sowie dem Aufbau einer entsprechenden Infrastruktur zum Schlüsselmanagement (PKI) entsprochen. So wurde im Frühjahr 2001 in der Landesverwaltung mit einigen ausgewählten Ressorts auf der Basis einer vom KoopA-ADV beschlossenen Lösung ein Testbetrieb zur elektronischen Signatur

und Verschlüsselung aufgenommen. Ziel dieses Tests war der Nachweis der Funktionsfähigkeit der Schlüsselzertifizierung und eines sicheren E-Mail-Betriebs mittels kryptographischer Verfahren. Der Testbetrieb wurde inzwischen erfolgreich abgeschlossen. Derzeit steht in der Landesverwaltung an, elektronische Signatur und Verschlüsselung für E-Mail und schutzwürdigen Dateien im breiten Umfang unter Nutzung der TESTA-Deutschland Plattform (2. TB, 15.5, 15.6) einzuführen. Als Zertifizierungsdiensteanbieter (CA - Certification Authority) (15.7) wird das Trust-Center der Deutschen Telekom (Telesec) genutzt. Dieses wird in das TESTA-Netz eingebunden (TESTA-CA), um auf elektronischem Weg die Schlüsselzertifizierung zu realisieren. Neben der Ausstellung von Zertifikaten stellt die TESTA-CA auch einen zentralen Verzeichnisdienst zur Verfügung, in dem die ausgestellten Zertifikate der Nutzer eingestellt werden können. Der Testbetrieb zeigte, dass die Installation und Handhabung der hierfür ausgewählten und auf den Nutzer-Clients einheitlich zum Einsatz kommenden Verschlüsselungs- und Signatursoftware ohne größere Probleme möglich ist. Eine wesentliche Aufgabe besteht nun im Aufbau einer Struktur von Registrierungsstellen (RA-Registration Authority) für die Landesverwaltung, die aus einer so genannten Master-RA und einer größeren Anzahl von Sub-RA´s bestehen wird. Eine RA ist für die Identifizierung und Registrierung der Nutzer sowie für die Freigabe der erstellten Zertifikate zuständig. Die Master-RA ist als oberste Registrierungsstelle im Wesentlichen für die Identifizierung und Registrierung von Registrierungsbeauftragten der Sub-RAs zuständig. Während letztere für die Identifizierung und Registrierung der Nutzer verantwortlich sind.

Die Einführung der elektronischen Signatur in der Landesverwaltung erfolgt nach einem Stufenkonzept, wobei in der Startphase die fortgeschrittene elektronische Signatur aber auch schon die qualifizierte elektronische Signatur (15.7) zum Einsatz kommen. Letztere nutzt Chipkarten mit einem hohen Sicherheitsstandard als Schlüsselträger.

Die Einstellung von Zertifikaten in den zentralen Verzeichnisdienst von TESTA erfolgt bei schriftlicher Zustimmung der Zertifikatinhaber. Darüber hinaus sollen aber auch mit Einwilligung der Nutzer die Zertifikate im Internet bereitgestellt werden. Welche Erforderlichkeit derzeit besteht, diese Zertifikate auch über das Internet weltweit zur Verfügung zu stellen, ist allerdings für die Nutzer nicht nachvollziehbar dargelegt. Da gemäß § 4 Abs. 3 ThürDSG der Betroffene,

dessen Einwilligung eingeholt wird, auf den Zweck der Verarbeitung oder Nutzung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen ist, bedarf es insofern aus datenschutzrechtlicher Sicht für eine Bereitstellung von Zertifikaten in einem Internetverzeichnisdienst noch diesbezüglicher Informationen für die Nutzer.
Für den Aufbau und den Betrieb der RA liegt ein Betriebshandbuch vor. In diesem sind die Komponenten der aufzubauenden PKI, deren Aufgaben sowie der Ablauf der Zertifikatsausstellung für die Nutzer und der RA`s dokumentiert. Auch gibt es eine Dokumentation zur Installation und Konfiguration der zum Einsatz kommenden kryptographischen Software, u. a. sind hier auch Sicherheitsrichtlinien für den Betrieb einer RA aufgezeigt, die aus meiner Sicht allerdings einiger Ergänzungen bedürfen. In meiner Stellungnahme zur Einführung der elektronischen Signatur unterbreitete ich dem TIM als verantwortlichem Ressort u. a. auch entsprechende Hinweise und Empfehlungen um die Sicherheit des Systems zu erhöhen. So regte ich bspw. an, die RA-PC aus Sicherheitsgründen nur für die Erfüllung von Aufgaben der Master- bzw. Sub-RA einzusetzen sowie hier schon in der Startphase den Einsatz von Chipkarten als Schlüsselträgermedium verbindlich vorzuschreiben. Auch schlug ich konkrete Maßnahmen vor, um die am TESTA-Netz angeschlossenen RA-PC`s vor unbefugten Zugriffen zu schützen.

15.9 Datenverarbeitung im ZIV

Das ZIV, welches zum 01.01.1999 aus fünf überwiegend dezentral vorhandenen Fachrechenzentren ressortübergreifend gegründet und der Oberfinanzdirektion Erfurt zugeordnet wurde, ist ein zentraler Dienstleister der Landesverwaltung für Großrechner- und zentrale Serververfahren öffentlicher Stellen im Freistaat Thüringen. Über die Datenverarbeitung im ZIV berichtete ich schon im 3. TB (15.4), da bei einem solchen Konzentrationsprozess auch datenschutzrechtliche und sicherheitstechnische Aspekte eine wichtige Rolle spielen. Zwischenzeitlich liegen für das ZIV das IT-Betriebs- und Servicekonzept sowie das IT-Sicherheitskonzept vor. Beide sind in vielen Teilen inhaltlich eng verzahnt. Das Betriebs- und Servicekonzept enthält vorwiegend Festlegungen zur Ablauforganisation und zum Dienstleistungsspektrum des ZIV sowie eine aktuelle Übersicht zu allen ein-

gesetzten Verfahren. Anhand von zwanzig Kriterien, bspw. zur Benutzerverwaltung, Datensicherung, Netzüberwachung, Störfall- und Notfallmanagement, IT-Sicherheits-Management und Wartung, sind für die beteiligten Einrichtungen (OFD, TLRZ, LKA, ZBS) hierzu konkrete Festlegungen aufgeführt. Das IT-Sicherheitskonzept enthält die Schutzbedarfsanalyse, eine Bedrohungs- und Risikoanalyse und das Sicherheitshandbuch mit dem Maßnahmenkatalog. Die den Verfahren zugehörigen Objekte wurden auf Schwachstellen, d. h. auf unterschiedliche Bedrohungen untersucht. Die aus den Bedrohungen resultierenden Risiken wurden benannt und in tragbare und untragbare Risiken klassifiziert. Für die untragbaren Risiken wurden Maßnahmen zur Beherrschung dieser Risiken entwickelt und in einem Sicherheitshandbuch aufgeführt. Die Schutzbedarfsanalyse ergab, dass nahezu alle Verfahren, die im ZIV betrieben werden, einen hohen bzw. sehr hohen Schutzbedarf aufweisen. Als eine diesbezügliche Zielstellung wird vom ZIV die gemäß § 9 Abs. 2 ThürDSG geforderte Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der zu bearbeitenden personenbezogenen Daten genannt. Insbesondere werde den Komponenten System- und Verfahrenssicherheit, Netzsicherheit, Zugriffssicherheit, Zutrittssicherheit, Ausfallsicherheit im Bereich der Technik und der Sicherheit im Bereich Infrastruktur eine große Bedeutung beigemessen. Auf meine Anfrage zum Stand der Umsetzung des Sicherheitskonzeptes zum Jahresende 2001 teilte mir das ZIV hierzu getroffene technische und organisatorische Maßnahmen mit. So ist der Zugang zum Hausnetz der OFD Erfurt durch eine Firewall abgesichert. Für die Übertragung sensibler Daten, beispielsweise zwischen der OFD und den Finanzämtern, werden Kryptoboxen (15.4) für eine verschlüsselte Datenübertragung eingesetzt. Die Vergabe bzw. Änderung von Zugriffsrechten für die einzelnen Nutzer beruht auf einem geregelten Antrags- und Genehmigungsverfahren. Die Zugriffsrechte sind dokumentiert und werden regelmäßig (mindestens 1x jährlich) überprüft. Für die ZIV-Bediensteten, Fremdfirmen und Besucher sind differenziert nach Sicherheitszonen Zutrittsberechtigungen festgelegt. Durch den redundanten Einsatz von aktiven Netzkomponenten konnte die Ausfallsicherheit im Bereich Technik erhöht werden. Insbesondere der Einsatz einer plattformübergreifenden Nutzung von Magnetplattentechnik mit Datenspiegelung soll für einen unterbrechungsfreien Betrieb sorgen. Umgesetzt wurden auch präventive Maßnahmen, die zur

Sicherheit im Bereich der Infrastruktur und somit für die Gewährleistung einer ordnungsgemäßen Datenverarbeitung wesentlich beitragen. So erfolgten Maßnahmen zur Rekonstruktion der Klimatechnik und zur Installation einer neuen Brandmeldeanlage. Durch den Einsatz eines mobilen Netzersatzaggregates wird einem längerfristigen Stromausfall begegnet.
Für die einzelnen Verfahren wurden auch die maximal zu tolerierenden Ausfallzeiten analysiert. Die tolerierbare Ausfallzeit wurde i. d. R. mit 1 Tag, teilweise sogar mit maximal nur 4 Stunden beziffert. Im Ergebnis dessen ergeben sich hohe Anforderungen an die Verfügbarkeit der eingesetzten IT-Komponenten. Beeinträchtigungen der räumlichen oder technischen Infrastruktur sowie technische Defekte an zentralen Komponenten können schwer wiegende Betriebsstörungen bis hin zum kompletten Ausfall einer der beiden ZIV-Rechnerstandorte in Erfurt oder Suhl verursachen. Da nicht alle solche Störungen auslösenden Ereignisse sicher ausgeschlossen werden können, bedarf es somit schlüssiger organisatorischer und technischer Konzepte für das Vorgehen in Störfall- oder Notfall-Situationen. Gemäß § 9 ThürDSG Abs. 2 Nr. 3 haben die zu treffenden technischen und organisatorischen Maßnahmen zu gewährleisten, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Wie mir das ZIV mitteilte, stellt die Projektarbeit zur Erstellung eines Katastrophenfall-Managements einen bedeutenden Schwerpunkt der gegenwärtigen Arbeit dar, wobei ein mit externer Unterstützung erarbeitetes Katastrophenschutz-Konzept jetzt vorliegt. Schon zu Beginn des Vorhabens informierte das ZIV hierzu die Anwender und den TLfD im Rahmen einer diesbezüglichen thematischen Veranstaltung, in der es auch aus datenschutzrechtlicher Sicht schon zu einer Diskussion und ersten Abklärung anstehender grundlegender Fragen zum geplanten Projekt kam. Nach den Ausführungen des ZIV liegt der Katastrophen (K)-Fall vor, wenn ein ZIV-Standort oder wesentliche Teile davon soweit beschädigt sind, dass ein Wiederanlauf der Anwendungen in diesem Rechenzentrum in einem vom Anwender tolerierten Zeitraum nicht möglich ist. In diesem Fall ist eine zeitnahe Verlagerung der Datenverarbeitungsprozesse unter Beachtung der infrastrukturellen und logistischen Erfordernisse auf einen Ausweichstandort notwendig. Für zwei ausgewählte Verfahren wurde schon anhand der im K-Fall-Handbuch niedergelegten Vorsorgemaßnahmen erfolgreich der

K-Fall praktisch getestet. Jetzt schließt sich die Phase der Konzeptumsetzung in enger Zusammenarbeit mit den Anwendern und weitere praktische K-Fall-Tests an. In Kürze werden die bisherigen Ergebnisse dem Anwenderbeirat des ZIV präsentiert, an dessen Sitzungen auch ein Vertreter des TLfD teilnimmt.
Wie im 3. TB (15.4) bereits dargelegt, wurden mit der Bildung des ZIV 1999 alle bis zu diesem Zeitpunkt vom TLRZ im Auftrag von Landes- und Kommunalbehörden ausgeführten rechentechnischen Leistungen vom ZIV übernommen. Allein die Auftragnehmerschaft für die Verfahren selbst sowie die verfahrensspezifische Betreuung verblieben weiterhin beim TLRZ. Dies war mir Anlass die konkrete Verfahrensweise bei der Verarbeitung von Daten aus dem Bereich Ausländerwesen (LADiVA) und im Meldewesen unter dem Aspekt der Zuständigkeiten bei der Gewährleistung des Datenschutzes und der Datensicherheit zu prüfen. Dabei wurde festgestellt, dass, obwohl es sich in allen Fällen um Auftragsdatenverarbeitungen des TLRZ im Sinne des § 8 ThürDSG mit einem Unterauftragsverhältnis mit dem ZIV handelt, in keinem Fall die vom Gesetzgeber geforderten schriftlichen Vereinbarungen zur Auftragsdatenverarbeitung vorlagen. Die Arbeiten im ZIV erfolgten lediglich auf der Grundlage von Absprachen und einzelnen Arbeitsanweisungen des TLRZ. Darüber hinaus waren die Auftraggeber (z. B. Gemeinden) nur allgemein über das Unterauftragsverhältnis zur maschinellen Verarbeitung der Daten im ZIV unterrichtet. Eine besondere Problematik ergibt sich dabei im Meldebereich, weil dort die Meldebehörden zur Bereitstellung von Meldedaten nach der Ersten Thüringer Meldedatenübermittlungsverordnung verpflichtet sind, deren Verarbeitung per Verordnung vom TLRZ wahrzunehmen ist. Im Ergebnis der Kontrollen wurden deshalb die beteiligten Stellen aufgefordert die notwendigen konkreten Vereinbarungen zu treffen, aus denen eindeutig und kontrollierbar die Rechte und Pflichten bzw. Aufgaben des TLRZ und des ZIV für alle Beteiligten, einschl. der kommunalen und staatlichen Auftraggeber, erkennbar werden. Zwischenzeitlich liegt auch der Entwurf eines Rahmenvertrages vor, der den datenschutzrechtlichen Forderungen entspricht und jeweils mit Ergänzungsregelungen für die einzelnen Verfahren untersetzt werden soll.

15.10 Technische und organisatorische Kontrolltätigkeit

Bei den im Berichtszeitraum vom TLfD auf der Grundlage des § 37 ThürDSG in den öffentlichen Stellen durchgeführten Kontrollen wurden auch die in den betreffenden Stellen zur Gewährleistung des Datenschutzes und der Datensicherheit getroffenen technischen und organisatorischen Maßnahmen einer Prüfung unterzogen. Soweit es dabei zweckmäßig oder erforderlich erschien, habe ich bei dieser Gelegenheit den Verantwortlichen Hinweise und Anregungen für geeignete Maßnahmen zur Verbesserung des Datenschutzes und der Datensicherheit gegeben. Diese betrafen im Berichtszeitraum insbesondere:

- Regelungen in Haus- und Schlüsselordnungen zur Gewährleistung der Verschlusssicherheit von Räumen und Behältnissen (z. B. bei Reparaturen und Reinigungsleistungen durch Fremdfirmen),
- Hinweise bei der Festlegung konkreter und verbindlicher Regelungen zur Aufbewahrung, Archivierung und Löschung bzw. Vernichtung von Unterlagen mit personenbezogenen Daten,
- Verfahrensfragen bei der datenschutzrechtlichen Freigabe gemäß § 34 ThürDSG,
- Notwendigkeiten einer restriktiven und differenzierten Vergabe von Zugriffsrechten auf personenbezogene Daten in automatisierten Verfahren für Administratoren und Nutzer,
- Fragen zur Vorhaltung aktueller Dokumentationen für die genutzten Programme und die eingerichteten Zugriffsrechte bei der Nutzung automatisierter Verfahren,
- Empfehlungen für die Gestaltung und Hinterlegung von Passwörtern (inhaltlich, Periodizität des Wechsels),
- Möglichkeiten zur Einstellung oder Nutzung von hard- und softwareseitigen Sicherheitsmechanismen (wie Diskettenschlösser, Boot- oder Setup-Passwörter, automatisierte Passwortverwaltung, Abstufung von Benutzerrechten u. a.),
- Anwendung von Protokollierungsverfahren und Regelungen zur stichprobenartigen Auswertung,
- Anregungen für die Erarbeitung von IT-Sicherheitskonzepten,
- Hinweise zur Festlegung verbindlicher Vorgaben für die Datensicherung (insbesondere zu Verantwortlichkeiten, Periodizität, brand- und einbruchssicherer Lagerung),

- Empfehlungen für die Vorgaben zur Nutzung des Internets bzw. für den Versand und Empfang von E-Mail mit personenbezogenem Inhalt,
- datenschutzrechtliche Fragen beim Einsatz von TK-Anlagen.

15.11 Neue Anforderungen an den technischen Datenschutz

Im vorangegangenen Tätigkeitsbericht (3. TB, 15.15) habe ich Ausführungen zur erforderlichen Anpassung der technischen und organisatorischen Regelungen in den Datenschutzgesetzen aufgrund der raschen Entwicklung auf dem Gebiet der Informations- und Kommunikationstechnologie gemacht.
Die Informationstechnologie entwickelt sich sehr dynamisch, die Komplexität der Technik nimmt erheblich zu und die technologischen Innovationszyklen werden immer kürzer. Telekommunikation, vernetzte IT-Systeme sowie grenzenlose, weltumspannende Kommunikation sind prägende Merkmale dieser Entwicklung. Im Vordergrund der automatisierten Datenverarbeitung steht hardwareseitig und logistisch nicht mehr eine monolytische Großrechnerwelt, deren Rechner in hermetisch abgeschirmten Rechenzentren betrieben werden. Große Rechenzentren wurden vielfach durch viele kleine Zentralen an lokalen Standorten abgelöst. Damit verbunden war auch eine weit gehende Dezentralisierung zuvor zentral vorgehaltener Daten. Diese Gegebenheiten muss auch der technische Datenschutz berücksichtigen, um den heutigen als auch den zukünftigen Bedingungen der Informationsverarbeitung Rechnung zu tragen.
Im Rahmen der Novellierung des ThürDSG wurde § 9 ThürDSG geändert. Es ist positiv zu bewerten, dass die Zielstellungen der technischen und organisatorischen Maßnahmen ausdrücklich im Gesetz verankert wurden, welche unabhängig vom aktuellen Speicherort, der Art und dem Stadium ihrer Verarbeitung und den technischen Verarbeitungskomponenten die Vertraulichkeit, Integrität und Authentizität der Daten zu sichern haben.
So heißt es nunmehr im § 9 Abs. 2:
„Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines Sicherheitskonzepts zu ermitteln und haben je nach der Art der zu schützenden Daten zu gewährleisten, dass

- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
- personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
- personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklungen der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen."

Den ersatzlosen Wegfall der bisherigen 10 Gebote zur Datensicherheit, die konkrete Sicherheitsmaßnahmen beinhalten, halte ich nicht für geglückt. Im Rahmen meiner abgegebenen Stellungnahmen im Gesetzgebungsverfahren habe ich darauf hingewiesen.

Im novellierten BDSG sind in der Anlage zu § 9 nach wie vor konkrete Gebote enthalten. Im Sinne der Rechtseinheitlichkeit und Rechtssicherheit im praktischen Vollzug hatte ich angeregt, neben der Neuaufnahme der Sicherheitsziele diesen konkreten Maßnahmekatalog auch im ThürDSG zu verankern. Dieser Anregung wurde nicht gefolgt. Es wird sich nunmehr bei der praktischen Anwendung zeigen müssen, wie sich die Regelung bewährt bzw. ob im Rahmen der Stufe der Novellierung der Datenschutzgesetze eine einheitliche Gesetzesvorgabe bei einer solchen grundlegenden Bestimmung sinnvoller ist.

15.12 Zugangs- und Zugriffsschutz mittels Passwörter

Einen wesentlichen Beitrag für eine sichere Nutzung der IT stellt die Identifikation und Authentifikation der Nutzer dar. Hierzu sind unterschiedliche Verfahren möglich. Nach wie vor identifizieren und authentifizieren sich noch die Mehrzahl der Nutzer gegenüber dem

IT-System mit der Eingabe einer Kombination aus Benutzerkennung und Passwort. Für diese Zugangskontrolle sind sowohl Kennung als auch Passwort, letzteres zumeist verschlüsselt, im System hinterlegt. Durch einen Abgleich (Login-Prozedur) der eingegebenen mit den hinterlegten Kennwörtern wird der Nutzer vom System entweder als Berechtigter akzeptiert oder als Unbefugter abgewiesen. Nach erfolgreicher Authentifikation erhält der Nutzer entsprechend seiner Rechte Zugriff auf Anwendungen, Daten oder Ressourcen des Systems. Nicht selten werden Passwörter als ein mehr oder weniger notwendiges Übel angesehen. Ein laxer Umgang mit Passwörtern kann zu Sicherheitslücken führen, indem bspw. der Zugang auf Rechner und ein Zugriff auf Daten und Programme unter Umständen sogar auf das gesamte IT-System durch Nichtberechtigte möglich ist. Ein offenbartes Passwort kann aber auch dem eigentlichen Besitzer zum Nachteil gereichen. Da Kennungen, mit denen sich die Nutzer identifizieren i. d. R. nicht geheim sind, zumeist werden hierfür Kürzel aus dem Namen der Benutzer verwandt, hängt die Zugangs- und Zugriffskontrolle letztendlich nur von der Kenntnis des Passwortes ab, mit der ein Nutzer seine Identität nachweist. Die Geheimhaltung seines persönlichen Passwortes ist somit für den Nutzer schon im eigenen Interesse eine unabdingbare Voraussetzung um einen Zugang und Zugriff unter seiner Kennung durch Andere, zu dem auch andere Mitarbeiter der Behörde gehören, zu verhindern. Denn ein unter seiner Kennung erfolgter Zugriff wird zunächst ihm zugeordnet. Damit ist die gemäß § 9 Abs. 2 Nr. 5 ThürDSG geforderte Revisionsfähigkeit, dass festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat, nicht gewährleistet. Was jeder Nutzer auch wissen sollte, der Administrator benötigt für seine Arbeit nicht das Nutzerpasswort. Eine diesbezügliche Anforderung sollte kritische Nachfragen seitens der Nutzer auslösen.
Neben der Pflicht der Nutzer zum sorgfältigen Umgang mit ihren Passwörtern, sind die Verantwortlichen angehalten, konkrete Richtlinien zum Passworteinsatz vorzugeben und deren Einhaltung auch angemessen zu kontrollieren. Die Systemadministration ist gefordert, den Passwortschutz soweit wie möglich technisch kontrolliert abzusichern. Entsprechende Einstellungen (Mindestlänge, Wechselzyklus, Passworthistorie, Anzahl unkorrekter Eingaben, Sperrfrist etc.) sind für die Login-Prozedur vorzunehmen.

Nicht selten müssen die Nutzer mehrere Passwörter einsetzen, um ihre Anwendungen nutzen zu können. Dies kann, insbesondere bei kurzen Passwortzyklen, zu einer Überforderung der Nutzer führen. Damit können Defizite im sicheren Umgang mit der Vielzahl an Passwörtern aber auch auftretende Ausfallzeiten durch vergessene Passworte verbunden sein. Um dies zu vermeiden, werden zunehmend so genannte SSO-Systeme eingesetzt. Solche SSO-Systeme bieten den Vorteil, dass sich ein Benutzer nur einmal mit einem Passwort authentifizieren muss, unabhängig davon wo seine Anwendungen physikalisch abgearbeitet werden. Kern eines SSO ist die zentrale Benutzerverwaltung, welche die Regeln und die Rollen der Benutzer für die jeweiligen Anwendungssysteme umfasst. Zusammen mit einer einmaligen Authentifizierung wird somit die Zugriffsverwaltung vereinfacht.
Neben biometrischen Identifizierungssystemen (3. TB, 15.14) und dem Einsatz elektronischer Zertifikate (2. TB, 15.8) zur Nutzerauthentisierung kann auch mit der Verwendung von Einmalpasswörtern eine höhere Sicherheit erreicht werden. Vielfach bekannt ist der zusätzliche Einsatz einmalig verwendbarer Transaktionsnummern zur Autorisierung des Nutzers bei den herkömmlichen Homebanking-Verfahren. Modernere Verfahren zum Einsatz von Einmalpasswörtern verwenden häufig so genannte Hardware-Token, die an die Nutzer ausgehändigt werden und auf dessen Display laufend Einmalpasswörter angezeigt werden, die synchronisiert auch auf einem zentralen Authentifizierungsserver erzeugt werden. Durch Eingabe von Kennung und Passwort sowie des aktuellen Einmalpasswortes kann sich der Nutzer authentifizieren.
Auch die Verwendung von Smart Cards (Chipkarten mit integriertem Mikroprozessor und Speicherbaustein), auf denen die Passwörter des Nutzers gespeichert sind, stellt eine sichere und nutzerfreundliche Lösung dar. Hier benötigt der Nutzer nur noch sein persönliches Passwort zur Aktivierung der Karte.
Regeln zur Bildung und Verwaltung von Passwörtern sind schon des Öfteren publiziert worden (1. TB, 15.14.2), sodass davon auszugehen ist, dass es hierzu keiner umfassenden Ausführungen mehr bedarf. Aufgrund der großen sicherheitstechnischen Relevanz der Zugangs- und Zugriffskontrolle erscheinen allerdings einige Ergänzungen und Hinweise im Hinblick auf ihre praktische Umsetzung und Handhabung jedoch noch angeraten.

Für jeden Nutzer sollte ein persönliches Benutzerkonto unter einer einmaligen Nutzerkennung angelegt werden. Eine Gruppenkennung ist zu vermeiden und nur bei begründeten Ausnahmen einzurichten. Das vom Administrator hierbei zunächst vergebene Passwort ist unverzüglich und persönlich vom Nutzer durch ein Neues zu ersetzen, welches nur noch der Nutzer kennt. Für die Nachvollziehbarkeit von Aktionen ist es wichtig, dass auch jeder Administrator über eine separate Kennung und Passwort verfügt. Das Nutzen der standardmäßigen Systemkennung ist auf die erforderlichen Fälle zu beschränken und das Passwort hierfür sicher zu hinterlegen. Nicht zu vergessen ist, etwaige vom Hersteller oder Lieferanten voreingestellte Standardpasswörter vor der Aufnahme des Wirkbetriebes zu ändern.
Zugangs- und Zugriffsrechte sind vom Administrator nur auf Anforderung des Verantwortlichen der jeweiligen fachlichen Stelle gemäß der dem Nutzer übertragenen Aufgaben, einzurichten, zu ändern oder zu löschen. Die Rechte sind auf die Erfüllung seiner Aufgaben zu beschränken. Der organisatorische Ablauf ist so zu gestalten, dass auch ein Löschen der Konten ausgeschiedener Nutzer erfolgt. Die Zugriffsrechte selbst sind im Rahmen der Angemessenheit so differenziert wie möglich zu vergeben (Lesen, Schreiben, Löschen etc.). Die diesbezüglichen Anforderungen sind nachvollziehbar vorzuhalten. Sie sind eine wichtige Dokumentation zur Rechteverwaltung und stellen insbesondere für den Administrator den Beleg für eine ordnungsgemäße Vorgabe des Vollzugs dar. Das Einrichten von Gruppen, in der Nutzer unter ihren persönlichen Kennungen mit gleichen Zugriffsrechten zusammengefasst werden, verbessert die Effektivität und Transparenz der Rechteverwaltung. Die Rechtevergabe sollte sowohl systembezogen mit Hilfe des Betriebssystems als auch anwendungsbezogen im Verfahren erfolgen. Eventuell kann hierzu auch der Einsatz von Zusatzsoftware erforderlich sein.
Ein Hinterlegen von Nutzerpasswörtern an einem vorgegeben Ort, z. B. beim fachlich zuständigen Leiter, mit dem Ziel bei einer unvorhersehbaren oder geplanten Abwesenheit des Nutzers unter dessen Kennung und Passwort jederzeit erforderliche Verarbeitungsvorgänge vornehmen zu können ist sicherheitstechnisch sehr bedenklich und sollte auf begründbare Ausnahmen beschränkt bleiben. Eine solche Verfahrensweise widerspricht dem Sinn eines persönlichen Passwortes. Alternativen hierfür sind unter Beachtung der Sensibilität der Anwendungen, der Größe der Einrichtung und anderer konkreter

Bedingungen vor Ort zu wählen. Wichtig ist jedoch, dass die Aktionen des Vertreters diesem auch nachvollziehbar zuordenbar sind. So kann er bspw. unter seiner eigenen Kennung die hierfür erforderlichen Zugriffsrechte erhalten, wobei ihm diese Rechte vom Administrator auf Anforderung der fachlichen Stelle freigeschaltet werden. Falls dies nicht zeitnah möglich ist, kann auch für benannte Vertreter eine zweite Kennung mit den notwendigen Zugriffsrechten vorsorglich eingerichtet werden und das Passwort für den Bedarfsfall sicher hinterlegt werden. Für Anwendungen ohne Schutzbedarf könnten auch die Zugangs- und Zugriffsrechte des zu Vertretenden dem Vertreter fortwährend mit zugeordnet werden.
Die Länge von Passwörtern und ihre inhaltliche Ausprägung sind wichtige Kriterien um ein Aufdecken der verschlüsselt abgelegten Passwörter wesentlich zu erschweren. Der zeitliche Aufwand hierfür steigt überproportional mit zunehmender Passwortlänge und der Anzahl der zur Passwortbildung verwendeten Sonderzeichen und Ziffern. Aus heutiger Sicht sollte für sensible Anwendungen die Länge des Passwortes mindestens acht Zeichen lang sein. Eine scheinbar zusammenhanglose Zeichenkombination von Buchstaben, Zahlen und Sonderzeichen für die Namensbildung ist ideal, um möglichen Attacken bspw. mittels eines Abgleichs mit Wörterbüchern zu begegnen. Dies kann benutzerfreundlich erreicht werden u. a. durch das bekannte Ableiten eines Wortes aus merkfähigen Sprichwörtern oder Sätzen und einer diesbezüglichen Ergänzung mit Ziffern/Sonderzeichen. Für Administratoren oder Nutzer, die mehrere Passwörter verwenden, bieten sich selbst angefertigte Matrizen an, deren Felder mit beliebigen Zeichen gefüllt werden. Durch Auswahl einer Zeile bzw. Spalte oder Teilfelder dieser ergibt sich das Passwort durch die Reihenfolge der in der jeweiligen Zeile oder Spalte aufgeführten Zeichen. Anstatt der Passwörter merkt sich der Nutzer hier nur die Kennzeichnung der ausgewählten Zeile(n) bzw. Spalte(n) oder Abschnitte der Teilfelder. Ohne Kenntnis dieser kann ein Unbefugter allein durch eine nur visuelle Kenntnisnahme der Matrix, im Gegensatz zu explizit aufgezeichneten Passwörtern, nicht unmittelbar die eingesetzten Passwörter erkennen. Er müsste dann schon über eine Kopie der Matrix verfügen, um anhand aller hier aufgeführten wahllosen Zeichenfolgen die Passwörter zu ermitteln.
Wie die Praxis zeigt, weist das vorgegebene zeitliche Limit, nach dessen Ablauf ein Passwortwechsel als zwingend erforderlich ange-

sehen wird, erhebliche Differenzen auf. Es umfasst i. d. R. einen Zeitraum von ein bis zu sechs Monaten. Erfahrungsgemäß kommen die Nutzer mit einer vierteljährlichen Passwortänderung gut zurecht. Darüber hinaus ist vermehrt mit einer Offenbarung des Passwortes zurechnen. Ein monatlicher Passwortwechsel überfordert dagegen in der Regel die Nutzer und sollte nur bei besonders schutzwürdigen Anwendungen gefordert werden.
Infolge der Vernetzung der IT-Systeme und der hiermit verbundenen Gefahr einer möglichen Ausspähung übertragener Daten ist zu beachten, dass Passwörter nicht nur verschlüsselt gespeichert werden, sondern auch verschlüsselt über das Netz übermittelt werden.

15.13 Datenschutz bei der Nutzung von Internet und Intranet

In der im Juni 2000 veröffentlichten Broschüre „Datenschutz und Datensicherheit im Internet“ habe ich aus datenschutzrechtlicher Sicht mögliche Risiken bei der Nutzung des Internets aufgezeigt sowie grundsätzliche Hinweise und Empfehlungen gegeben, wie diesen Risiken begegnet werden kann. Jeder, der im Internet surft, hinterlässt seine Datenspuren. Risiken bestehen für die über das Internet übertragenen Daten hinsichtlich der Absicherung ihrer Vertraulichkeit, Integrität (Unversehrtheit), Verfügbarkeit und Authentizität (Nachweis ihres Ursprungs). Aber auch die Sicherheit der angeschlossenen EDV-Technik und der darauf gespeicherten Daten ist beim Surfen im Internet ohne zusätzliche Schutzmaßnahmen gefährdet. So beinhaltet die vorliegende Broschüre auch Hinweise zu den Sicherheitseinstellungen der Browser, Hinweise zum Löschen des Cache und der URL-Verlaufsliste sowie Hinweise zum Umgang mit Cookies.
Diese Broschüre ist unter www.datenschutz.thueringen.de online verfügbar, kann aber auch von der Dienststelle des TLfD angefordert werden.
Ebenfalls kann die im Dezember 2000 vom Arbeitskreis Technik des Bundes und der Länder veröffentlichte Broschüre „Datenschutz bei der Nutzung von Internet und Intranet“, welche auch unter www.lfd.m-v.de/ak_tech/orhilfen/oh.html online verfügbar ist, angefordert werden. Diese beinhaltet folgende drei Orientierungshilfen:

- Datenschutzfragen bei der Nutzung von Internet und Intranet
  Diese Orientierungshilfe, erarbeitet vom AK Technik und AK Medien des Bundes und der Länder, 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. Der Anschluss an das Internet ist angesichts der Gefährdungslage aus Datenschutzsicht nur vertretbar, wenn zuvor eine Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und die Gefahren durch technische und organisatorische Maßnahmen hinreichend beherrscht werden können.
  In diesem Zusammenhang ist auch aus datenschutzrechtlicher Sicht die Zulässigkeit von Protokollierungen mittels einer Firewall betrachtet worden. Aus Gründen der Datensicherheit wurde von Seiten des Arbeitskreises Technik der DSB des Bundes und der Länder eine Protokollierung an Firewalls grundsätzlich als zulässig erachtet. Ob jedoch eine Protokollierung überhaupt erforderlich ist bzw. in welchem Umfang zu protokollieren ist, hängt wesentlich davon ab, ob eine solche Aktion dem Grundsatz der Angemessenheit und Erforderlichkeit Rechnung trägt. Inwieweit diesem Grundsatz entsprochen wird, muss primär am konkreten Einsatzfall abgeklärt werden.
- Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten
  Die verstärkte Nutzung neuer Kommunikationsformen, wie z. B. E-Mail, erfordert eine neue Art der Verbreitung der Kommunikationsadressen. Hierzu werden zunehmend elektronische Verzeichnisse eingesetzt. Zum Einsatz kommen sowohl ISO-konforme (X.500) Systeme als auch Industriestandards (z. B. Network Directory System, NDS). Die Daten verarbeitende Stelle legt dabei fest, welche Daten mit welchem Ziel in einem Verzeichnis zu speichern sind. Da in einem Verzeichnisdienst auch personenbezogene Daten gespeichert werden können, sind aus datenschutzrechtlicher Sicht die sichere Übertragung dieser personenbezogenen Daten und die rechtlichen Aspekte wie Inhalt, Form und Zugriff auf Einträge zu klären. Der Arbeitskreis Technik der DSB des Bundes und der Länder verabschiedete in seiner 35. Sitzung die o. g. Orientierungshilfe. Diese basiert auf

dem Betrieb eines Verzeichnisdienstes in einer definierten Netzwerkumgebung (Intranet) innerhalb der öffentlichen Verwaltung. In Verzeichnisdiensten wird in der Regel ein eindeutiger Teilnehmername definiert, welcher als Adresse im Verzeichnis, mit der die Person gefunden werden kann, dient. In Verbindung mit der Möglichkeit, beliebige Informationen zu einer Person zu speichern, erwachsen hieraus besondere datenschutzrechtliche Gefahren. Die einfache Zusammenführung bisher getrennt gespeicherter Daten ermöglicht die Erstellung von sehr detaillierten Profilen, deren Umfang nicht absehbar ist. Üblicherweise wird der Verzeichnisdienst als Unterstützungsfunktion in bestehende Verfahren integriert. Damit muss aber sichergestellt sein, dass der Zugriff auf Informationen in Einträgen nur auf das für die Aufgabenerledigung Notwendige beschränkt wird. Wird der Verzeichnisdienst als Basis von Personalinformationssystemen genutzt oder gar ausgebaut, ist der Personalrat aufgefordert, durch Nutzung seiner Mitbestimmungsrechte und Abschluss von Dienst- und Betriebsvereinbarungen die Zusammenführung von Daten zu unterbinden bzw. zu kontrollieren. Verzeichnisdienste, soweit sie nur im Intranet einer Daten verarbeitenden Stelle angeboten werden, unterliegen weder dem Telenoch dem Mediendienst, sondern den allgemeinen datenschutzrechtlichen Bestimmungen für Dienst- und Arbeitsverhältnisse. Soweit auf den Verzeichnisdienst nur Mitarbeiterinnen/Mitarbeiter der eigenen Verwaltung zugreifen können, dürfen die erforderlichen Angaben über sämtliche Mitarbeiterinnen/Mitarbeiter zur Verfügung gestellt werden. Erstreckt sich die Zugriffsmöglichkeit auch auf andere Stellen, dürfen Personen nur aus dienstlichen Gründen, bei denen die Erreichbarkeit zu ihrer dienstlichen Aufgabe gehört, in das Verzeichnis aufgenommen werden. Für Bedienstete, die in der Regel keinen unmittelbaren Kontakt außerhalb der eigenen Dienststelle haben, ist die Bekanntgabe ihrer Daten nicht erforderlich und somit nur mit Einwilligung zulässig. In der Orientierungshilfe werden aus datenschutzrechtlicher Sicht weiter zu beachtende Maßnahmen beim Betrieb eines Verzeichnisdienstes aufgeführt.

- Internetnutzung durch öffentliche Stellen

  Durch die Modernisierung von Verwaltungsdienstleistungen wird im zunehmenden Maße die Notwendigkeit der Zentralisie-

rung von Aufgaben bei den Stellen propagiert, in denen an einem Ort Verwaltungsleistungen verschiedener Art entgegengenommen werden können (Bürgerämter, Bürgerbüros o. ä.). In diesem Zusammenhang werden für die Mitarbeiter Zugriffe auf die verschiedensten Informationssysteme geschaffen.
Die DSB des Bundes und der Länder verabschiedeten auf der 60. DSB-Konferenz im Oktober 2000 eine entsprechende Entschließung „Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung“ (Anlage 10). Hier wiesen sie aus datenschutzrechtlicher Sicht darauf hin, dass es bei der Modernisierung der öffentlichen Verwaltung insbesondere bei der Dienstleistungs- und Serviceorientierung, Lösungen für eine sichere und vertrauliche Kommunikation zu schaffen gilt. Eine Arbeitsgruppe der DSB des Bundes und der Länder hat daraufhin Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung erarbeitet, welche den Verwaltungen helfen sollen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen sind auszugsweise in der o. g. Broschüre veröffentlicht, und beziehen die rechtlichen Voraussetzungen und die technischen und organisatorischen Maßnahmen bei der Ausgestaltung von Bürgerämtern, Kundencentern, Call-Centern, Informationsangebote öffentlicher Stellen im Internet, interaktive Verwaltung, der Bürgerkarte, der elektronischen Auskunft, Akteneinsicht und Bürgerbeteiligung und die Auslagerung von Verwaltungsfunktionen mit ein.

15.14 Datenschutzrechtliche Aspekte von Data Warehouse Systemen

Die maschinelle Speicherung auch sehr umfangreicher Datenbestände stellt gemäß dem Stand der Informationstechnik sowohl technologisch und als auch kostenmäßig kein nennenswertes Problem mehr dar. In allen gesellschaftlichen Bereichen werden hierzu i. d. R. Datenbanksysteme eingesetzt. Zumeist wurden bisher jedoch die Daten in separaten Datenbanken vorgehalten, die nicht oder nur teilweise miteinander verbunden waren und untereinander nur einen begrenzten Datenaustausch durchführten. Die Datenbanken selbst waren auf

ganz bestimmte administrative und organisatorische Zwecke ausgerichtet und zumeist nicht langfristig angelegt. Um für die unterschiedlichsten Aufgaben insgesamt eine verbesserte datenbankübergreifende Auswertung und Nutzung der vorhandenen Datenbestände zu erzielen, werden zunehmend Daten aus den vorhandenen Datenbanken extrahiert, nach einem einheitlichen System geordnet zusammengeführt und langfristig vorgehalten. Eine solche einheitliche und logisch zentrale Datenbasis, in der ein Nutzer relativ leicht und jederzeit verfügbar die von ihm gesuchten Informationen in gewünschter Kombination und Aufbereitung finden kann, wird als Data Warehouse (Daten-Lagerhaus) bezeichnet. Durch ein als Data Mining bezeichnetes Verfahren, können weiterhin die scheinbar zusammenhanglosen Daten des Data Warehouses nach bisher unbekannten, wissenswerten Zusammenhängen durchsucht werden. Hierzu werden u. a. Methoden der Heuristik und künstlichen Intelligenz eingesetzt. Damit werden auch Nichtexperten in die Lage versetzt, u. a. durch intelligente Menüführung Abfragen zu formulieren, um bisher nicht erkannte Zusammenhänge oder bestimmte Sachverhalte aufzudecken.

Data Warehouse Systeme eignen sich insbesondere für eine nicht zweckgebundene Datenvorratshaltung. Enthält die Datenbasis personenbezogene Daten, weisen Data Warehousing- und Data Mining-Konzepte datenschutzrechtliche Relevanz auf. Die immensen Datenmengen und die Auswertungsmöglichkeiten solcher automatisierten Systeme können zu einer generellen Überwachungs- und Kontrollmöglichkeit sowie zur Bildung von umfangreichen Persönlichkeitsprofilen des Einzelnen (Betroffener) führen. So können Data Warehouse-Lösungen bspw. für Marketingzwecke genutzt werden, um alle verfügbaren Informationen über Kunden und Interessenten individuell und bedarfsgerecht zu verwerten.

So wäre auch in der öffentlichen Verwaltung denkbar, dass sämtliche Vorgänge der Organisationseinheiten einer Stelle personenbezogen recherchierbar gespeichert werden.

Die DSB des Bundes und der Länder wiesen auf Ihrer 59. Konferenz am 14./15.03.2000 in Hannover in einer Entschließung (Anlage 2) auf die mit dem Einsatz von Data Warehouse Systemlösungen und Data Mining verbundenen datenschutzrechtlichen Gesichtspunkte hin. Hier sind wesentliche datenschutzrechtliche Forderungen benannt, die bei der Planung und dem Einsatz solcher Systeme und

Verfahren zu beachten sind. So gilt u. a. auch für die Speicherung und Nutzung personenbezogener Daten mittels Data Warehouse Lösungen das grundrechtliche Gebot der Zweckbindung dieser Daten. Im öffentlichen Bereich ist eine für allgemeine und unbestimmte Zwecke erfolgende Speicherung von Daten auf Vorrat in einem Data Warehouse, wie auch in anderen informationsverarbeitenden Systemen, aufgrund der hier grundrechtlich geschützten Zweckbindung der Daten unzulässig.

15.15 Transparente Software

Die DSB des Bundes und der Länder setzen sich intensiv für die Nutzung datenschutzfreundlicher Technologien ein (2. TB, 15.6; 3. TB, 15.10). Unter anderem fordern sie die Hersteller von Informations- und Kommunikationstechnik auf, Software so zu entwickeln und herzustellen, dass Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.
Unter dem Motto „Transparente Software - eine Voraussetzung für datenschutzfreundliche Technologien“ hat der Arbeitskreis Technik auf Anforderung der 59. DSB-Konferenz des Bundes und der Länder ein entsprechendes Arbeitspapier erarbeitet.
Dieses Arbeitspapier, veröffentlicht unter www.lfd.m-v.de/ak_tech/dsfrtech/transoft/transoft.html, geht davon aus, dass ein viel versprechender Ansatz für die Transparenz, also der Nachvollziehbarkeit des ablaufenden automatisierten Verfahrens, das Entwicklungsmodell „Open Source“ darstellt. Unter Open-Source versteht man Software, deren Quelltext offen gelegt und für jeden frei verfügbar ist. Die vollständige Offenlegung des Quelltextes von Programmen stellt für die IT-Sicherheit und den Datenschutz eine große Chance dar, insbesondere um eventuell verdeckte Programmfunktionen besser erkennen zu können. Die Definition für die Open-Source-Software beinhaltet neun Kriterien, wie z. B. uneingeschränkte lizenzfreie Weitergabe an Dritte, keine Einschränkungen für bestimmte Anwendungsbereiche und keine Diskriminierung von einzelnen Personen oder Gruppen.
Open-Source-Programme besitzen aber nicht zwangsläufig eine höhere Sicherheit weil sie veröffentlicht wurden und theoretisch von jedem geprüft werden können. Die Verfügbarkeit des Quellcodes ist

zwar ein entscheidender Schritt in die Richtung Transparenz, allerdings nur eine notwendige, nicht aber hinreichende Bedingung, die Abwesenheit von Fehlern und versteckten Funktionalitäten zu gewährleisten.
Ein ergänzender Ansatz, ohne den auch das Open-Source-Modell kein berechtigtes Vertrauen erzeugen kann, stellt die Evaluierung und Zertifizierung von Software durch unabhängige Fachleute dar.
Die Sicherheit der Software soll in erster Linie durch Prüfung der Funktionalität und der Schadensfunktionsfreiheit garantiert werden. Die Funktionalität, Qualität, Vertrauenswürdigkeit und die implementierten Sicherheitsmechanismen der Software werden in einem umfangreichen Evaluierungsprozess festgestellt und in einer abschließenden Bewertung durch ein Zertifikat bestätigt. Eingehaltene Sicherheitsstandards wie DIN/ISO9000 als Norm für diese Qualitätssicherung bei den Herstellern, die Europäische „Information Technologie Security Evaluation Criteria“ (ITSEC) und die „Common Criteria“ (CC) als internationaler Standard für die Prüfung und Bewertung der Sicherheit der Informationstechnik ist auch für die öffentliche Verwaltung ein geeigneter Weg, das Vertauen in die Qualität und Sicherheit der eingesetzten Produkte zu stärken.

15.16 Das virtuelle Datenschutzbüro

Das virtuelle Datenschutzbüro ist ein gemeinsamer Service von Datenschutzinstitutionen aus aller Welt mit dem Ziel für Jedermann eine Online-Ansprechstelle im Internet zu Datenschutzfragen bereitzustellen. Unter der Web-Adresse www.datenschutz.de der deutschen Sektion können hier zahlreiche Informationen rund um den Datenschutz abgerufen werden. Neben allgemeinen und aktuellen Informationen zum Datenschutz und zur Datensicherheit finden sich im virtuellen Datenschutzbüro auch Diskussionsforen zu Datenschutzthemen. Als weltweite Plattform soll es den DSB eine gemeinsame wie auch arbeitsteilige effektive Bearbeitung von Themen und Projekten ermöglichen. Es versteht sich aber auch als zentrale Anlaufstelle für Anfragen und Beschwerden der Bürger in Sachen Datenschutz.
Das virtuelle Datenschutzbüro hat sich eine eigene Geschäftsordnung gegeben, die Fragen zur Verfahrensweise zwischen den Projektpartnern sowie Kooperationspartnern und Projektförderern regelt. Derzeit beteiligen sich unter Federführung Schleswig-Holsteins der BfD,

DSB der Länder sowie der norddeutschen Bistümer der katholischen Kirche, der Schweiz, den Niederlanden, Kanada, Slowakei und Polen. Die notwendige Technik für das virtuelle Datenschutzbüro wird vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein zur Verfügung gestellt und betreut.

Anlage 1

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 14./15. März 2000 in Hannover

Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o.ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.

- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind - es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann – zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden – nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollten bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.
  Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o. g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum – ausschließlich zum Zweck der Sicherung des Rechtsschutzes – aufzubewahren.

- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Betroffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung).
  Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.
  Damit sind Regelungen z.B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Ein-

griffes ausgeschlossen werden kann.
Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.

- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.

- Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.

- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung – bei Datenübermittlungen auch bei den Datenempfängern – erstrecken.

- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.

- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.

- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weiter gehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

Anlage 2

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 14./15. März 2000 in Hannover

Data Warehouse, Data Mining und Datenschutz

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im „Data Warehouse“ werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. „Data Mining“ bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem „Daten-Lagerhaus“ gesammelt werden.

- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden ist. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.

- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.

- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.

- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern“ rechtswidrig.

- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). „Data Mining“ ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von „Data Warehouse“- und „Data Mining“-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

Anlage 3

Entschließung

der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 14./15. März 2000 in Hannover

Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung „INPOL-neu“ eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur soweit eingegriffen wird, wie dies im Rahmen der Erforderlichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die „gesamte kriminelle Karriere“ jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereitgehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventi-

ven als auch im repressiven Bereich auf „Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung“. Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die „Straftaten“, nicht die einzelne Person und auch nicht das „Gesamtbild einer Person“. Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

Anlage 4

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 14./15. März 2000 in Hannover

Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluss des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,

- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, sodass sie uneingeschränkt zur Strafverfolgung genutzt werden können,

- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,

- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse“ Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

Anlage 5

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

am 14./15. März 2000 in Hannover

Für eine freie Telekommunikation in einer freien Gesellschaft

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

- **Erhebliche Zunahme der Telekommunikationsvorgänge**
  Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, e-mail und mail-boxen sowie das Internet genutzt.

- **Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten**
  - Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.
  - Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch e-mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.
  - Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.
  - Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.
  - Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

- **Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten**

Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

- **Entwicklung des Internets zum Massenkommunikationsmittel**
  Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

- **Schwer durchschaubare Rechtslage**
  Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: *1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802*

- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen – der Katalog wurde seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.

- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflich-

tung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.

- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen „ENFOPOL“, befasst sich u. a. mit der Frage, welchen Anforderungen die Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weiter gehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.

- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vor-

ratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.

- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.

- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.

- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.

- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.

- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhältnismäßig. Es muss deshalb ver-

bindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.

- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.

- Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

Anlage 6

Entschließung
der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 14./15. März 2000 in Hannover

Risiken und Grenzen der Videoüberwachung

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zur einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen
- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch video-technisch gewonnener – insbesondere biometrischer – Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.

   - Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. *Dafür kommen – **soweit nicht überwiegende schutzwürdige Be-***

lange von Betroffenen entgegenstehen *– unter Anderem in Betracht*[1]*:*

- *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.*
- *für die Verkehrslenkung nur Übersichtsaufnahmen,*
- *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.*

- Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
- Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.
- Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im Einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
- Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
- Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen

[1] Die kursiv gedruckte Passage wurde bei Stimmenthaltung der Datenschutzbeauftragten der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern und Nordrhein-Westfalen angenommen.

Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

Anlage 7

Entschließungen zwischen den Konferenzen 2000

Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

(Umlaufentschließung/ Juni 2000)

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten „Großen Lauschan-

griffe“ zu unterrichten. § 100e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufende parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll aufgrund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahme zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen umfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem „Großen Lauschangriff“ ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z. B. unverdächtigte Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn – wie in den „Wiretap-Reports“ der USA – die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräu-

me, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten „Großen Lauschangriffe".

Anlage 8

Entschließungen zwischen den Konferenzen 2000

Auftragsdatenverarbeitung durch das Bundeskriminalamt
(Umlaufentschließung/ Oktober 2000)

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises II und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern dazu auf, die für die Datenverarbeitung beim Bundeskriminalamt gesetzlich gezogenen Grenzen strikt zu beachten. Sie appellieren an die Innenminister/ -senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlose Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

Anlage 9

Entschließung
der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 12./13. Oktober 2000 in Braunschweig

Datensparsamkeit bei der Rundfunkfinanzierung

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das „Bereithalten eines Rundfunkempfangsgerätes“ anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbst-

bestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.

Anlage 10

Entschließung
der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 12./13. Oktober 2000 in Braunschweig

Vom Bürgerbüro zum Internet
- Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung –

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauf-

tragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personenbezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

Anlage 11

Entschließung
der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 12./13. Oktober 2000 in Braunschweig

Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Einblick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung“ bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestimmung“ vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.
Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.

2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrekken. Im Falle eines Widerrufs sind die gewonnen Informationen zu löschen oder an den Betroffenen herauszugeben.

3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u.a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwer wiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.

Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur – wie bisher – Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

Anlage 12

Entschließung
der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 12./13. Oktober 2000 in Braunschweig

Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz - § 3a E-BDSG) und die Einführung des Daten-

schutzaudit (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in die bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

Anlage 13

Entschließung
der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 08./09. März 2001 in Düsseldorf

Novellierung des Melderechtsrahmengesetzes

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht der Bundesregierung, das Melderechtsrahmengesetz im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen.

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hin-

nehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.

2. Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf - wie in seiner Begründung ausdrücklich betont wird – nunmehr vorsieht, einfache Melderegisterauskünfte mit Hilfe des Internet durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim Internet-gestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsrecht oder mindestens ein Widerspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.

3. Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betroffenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.

4. Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbeauftragten treten angesichts des in diesen Fällen bestehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.

5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen Auskunft über Daten von

Gruppen von Wahlberechtigten erteilen, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

6. Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist.

Bei Enthaltung Thüringens zu Ziffer 6.

Anlage 14

Entschließung
der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 08./09. März 2001 in Düsseldorf

Informationszugangsgesetze

Die Konferenz verfolgt mit Interesse die Bestrebungen des Bundes, ein Informationszugangsgesetz zu schaffen und dem Bundesbeauftragten für den Datenschutz die Aufgaben zur Sicherung des Informationszugangs zu übertragen. Die Bundesregierung nimmt damit die Überlegungen auf, die in Artikel 255 EU-Vertrag und Artikel 42 EU-Grundrechte-Charta zum Ausdruck kommen. Die Konferenz betont, dass das Recht auf informationelle Selbstbestimmung der Einzelnen dem freien Zugang zu behördeninternen, amtlichen Informationen nicht entgegen steht, wenn die Privatssphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben. Die Berichte aus den Ländern Berlin, Brandenburg und Schleswig-Holstein zeigen, dass die datenschutzrechtlichen Gewährleistungen für die informationelle Selbstbestimmung sich mit dem erweiterten Zugangsrecht zu den Informationen öffentlicher Stellen unter der

Voraussetzung entsprechender Schutzmechanismen vereinbaren lassen. Die Zusammenführung von Datenschutz- und Informationszugangskontrolle kann diese Gewährleistung institutionell absichern.

Anlage 15

Entschließung
der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 08./09. März 2001 in Düsseldorf

Äußerungsrecht der Datenschutzbeauftragten

Die Datenschutzbeauftragten des Bundes und der Länder sind verpflichtet, Einzelne – wie es die Rechtsprechung des Bundesverfassungsgerichts und die Richtlinie der Europäischen Gemeinschaft zum Datenschutz von 1995 vorsehen – vor rechtswidrigem Umgang mit ihren personenbezogenen Daten wirksam zu schützen. Die damit verbundenen Beratungs- und Kontrollaufgaben verleihen den Datenschutzbeauftragten ein öffentliches Wächteramt, das die Befugnis einschließt, Behördenverhalten auch im Detail und, soweit der Bedeutung der Sache angemessen, auch unter Bezeichnung der Amtsträgerinnen und Amtsträger öffentlich zu rügen.

Aus gegebenem Anlass wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder energisch gegen Versuche im Land Sachsen, durch gesetzgeberische Maßnahmen dieses Recht zu beschneiden und die Arbeit des Sächsischen Datenschutzbeauftragten zu behindern.

Anlage 16

Entschließung
der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 08./09. März 2001 in Düsseldorf

Datenschutz bei der Bekämpfung von Datennetzkriminalität

Der Europarat entwirft gegenwärtig zusammen mit anderen Staaten, insbesondere den USA und Japan, eine Konvention über Datennetzkriminalität (Cyber-crime-Konvention), die über ihren Titel hinaus auch die automatisierte Speicherung von Daten im Zusammenhang mit anderen Straftaten regeln soll.[2]

Die Datenschutzbeauftragten des Bundes und der Länder verkennen nicht, dass das Internet – ebenso wie andere technische Hilfsmittel – für Straftaten missbraucht wird. Sie teilen daher die Auffassung des Europarats, dass der Kriminalität auch im Internet wirksam begegnet werden muss. Allerdings ist zu beachten, dass sich die weit überwiegende Anzahl der Nutzenden an die gesetzlichen Vorgaben hält. Insoweit stellt sich die Frage der Verhältnismäßigkeit von Maßnahmen, die alle Nutzenden betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder teilen die Auffassung der Europäischen Kommission, dass zur Schaffung einer sichereren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden und anonyme wie pseudonyme Nutzungsmöglichkeiten erhalten bleiben müssen; über Fragen der Bekämpfung der Datennetzkriminalität sollte ein offener Diskussionsprozess unter Einbeziehung der Betreiberinnen und Betreiber, Bürgerrechtsorganisationen, Verbraucherverbände und Datenschutzbeauftragten geführt werden. [3]

Die Konferenz regt eine entsprechende Debatte auch auf nationaler Ebene an und bittet die Bundesregierung, hierfür den erforderlichen Rahmen zu schaffen.

[2] European Committee on Crimes Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), Draft Convention on Cyber-crime (PC-CY (2000) Draft No. 25)

[3] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 26.01.2001 – KOM (2000) 890 endgültig

Die Konferenz der Datenschutzbeauftragten fordert die Bundesregierung auf, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass

- Maßnahmen zur Identifikation von Internet-Nutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,

- der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,

- der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,

- Daten von Internet-Nutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

Anlage 17

Entschließung
der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 08./09. März 2001 in Düsseldorf

Novellierung des G 10-Gesetzes

Die Datenschutzbeauftragten des Bundes und der Länder sehen mit großer Sorge, dass die Empfehlungen des Rechts- und des Innenausschusses des Bundesrates erhebliche Einschränkungen der Persönlichkeitsrechte der Bürgerinnen und Bürger zur Folge hätten, die über den Gesetzentwurf der Bundesregierung teilweise weit hinaus-

gehen. Die Datenschutzbeauftragten wenden sich insbesondere entschieden dagegen, dass

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u.a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften,

- der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein und

- die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

Darüber hinaus kritisieren die Datenschutzbeauftragten des Bundes und der Länder, dass die Bundesregierung mit der Gesetzesnovelle über die Vorgaben des BVerfG hinaus weitere Änderungen im G 10-Bereich erreichen will, die neue grundrechtliche Beschränkungen vorsehen:

- Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G 10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.

- Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G 10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Art. 87 Abs. 1 Satz 2 GG weiter infrage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung durchzuführen, weitet die Ge-

fahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.

- Alle Neuregelungen wie z.B. zum Parteienverbotsverfahren, zur Verwendung von G 10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen worden.

- Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G 10-E genannten Straftaten genutzt werden dürfen.

- Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen, begegnen schwerwiegenden datenschutzrechtlichen Bedenken.

- Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G 10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.

- Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.

- Dem BND wird nicht mehr nur die „strategische Überwachung" des nicht-leitungsgebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.

- Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G 10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei „strategischen Überwachung“ nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

Anlage 18

Entschließung
der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 08./09. März 2001 in Düsseldorf

Datenschutz beim elektronischen Geschäftsverkehr

Die Konferenz wendet sich mit Entschiedenheit gegen Anträge, die gegenwärtig dem Bundesrat zum Entwurf eines Gesetzes zum elektronischen Geschäftsverkehr (BR-Drs. 136/01) vorliegen. Danach sollen Bestands- und Nutzungsdaten bei Telediensten nicht nur an Strafverfolgungsbehörden, sondern auch an Verwaltungsbehörden zur Verfolgung von Ordnungswidrigkeiten und an Nachrichtendienste übermittelt werden. Darüber hinaus sollen die Anbieterinnen und Anbieter zur Speicherung von Nutzungsdaten auf Vorrat für eine mögliche spätere Strafverfolgung verpflichtet werden.

Die Datenschutzbeauftragten weisen darauf hin, dass sich anhand dieser Daten nachvollziehen lässt, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen nachgeht. Eine pauschale Registrierung jeder Inanspruchnahme von Telediensten zur staatlichen Überwachung greift tief in das Persönlichkeitsrecht der betroffenen Nutzerinnen und Nutzer ein und berührt auf empfindliche Weise deren Informationsfreiheit. Der Bundesrat wird daher aufgefordert, diese Anträge abzulehnen.

Anlage 19

Entschließungen zwischen den Konferenzen 2001

Anlasslose DNA-Analyse aller Männer verfassungswidrig
(Umlaufentschließung/ 12. März 2001)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist entschieden den Vorschlag zurück, den „genetischen Fingerabdruck“ aller Männer zu erheben und rein vorsorglich zu speichern. Die Erhebung personenbezogener Daten ist auch im Rahmen der Strafverfolgung an rechtsstaatliche Grundsätze gebunden. Eine Datenerhebung auf Vorrat, die die Hälfte der Bevölkerung als potenzielle Straftäter behandelt, ist verfassungsrechtlich unzulässig. Darüber hinaus erscheint der erwartete Abschreckungseffekt äußerst fragwürdig.

Anlage 20

Entschließungen zwischen den Konferenzen 2001

Veröffentlichung von Insolvenzinformationen im Internet
(Umlaufentschließung/ 24. April 2001)

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen – vor allem in Verbraucherinsolvenzverfahren – künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirt-

schaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, aufgrund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigen Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und die Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichts im Beschluss vom 09.03.1988 – 1 BvL 49/86 – zu einem vergleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.

Bevor die geplante Änderung des § 9 InsO verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z. B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil ins Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entschieden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich, wie von der Bundesregierung erwartet, einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

Anlage 21

Entschließungen zwischen den Konferenzen 2001

Entwurf der Telekommunikations-Überwachungsverordnung

(Umlaufentschließung/ 10. Mai 2001)

Das Bundesministerium für Wirtschaft hat Ende Januar 2001 den Entwurf für eine Telekommunikations-Überwachungsverordnung

(TKÜV) vorgelegt, der in Kürze dem Bundeskabinett zugeleitet wird. Der Entwurf basiert auf dem Telekommunikationsgesetz, das den Begriff der Telekommunikation weit fasst. Da er technikneutral formuliert ist, werden von den Überwachungsmaßnahmen nicht nur die Sprachtelefonie und der Telefaxverkehr, sondern auch alle anderen elektronischen Kommunikationsplattformen und damit insbesondere auch das Internet erfasst.

Sobald ein Internet-Provider einen E-Mail-Dienst anbietet, muss er technischen Einrichtungen zur Umsetzung der Überwachungsmaßnahmen vorhalten, obwohl die Vermittlung des Zugangs zum Internet als anmelde- und zulassungsfreier Teledienst nicht zu den Telekommunikationsdiensten gehört. Diese Verpflichtung der Internet-Provider macht es technisch möglich, künftig den gesamten Internet-Verkehr, also auch das bloße „Surfen“ zu überwachen. Dies ist aber nach deutschem Recht so nicht vorgesehen. Bedenklich ist in diesem Zusammenhang, dass das European Telecommunications Standards Institute (ETSI) gegenwärtig an einem technischen Standard arbeitet, der den Lauschangriff auf IP-Netze (Internet) und die Überwachung des gesamten Internet-Verkehrs europaweit vereinheitlichen soll.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden dagegen, eine technische Infrastruktur zu schaffen, die jederzeit eine umfassende Überwachung des Internet-Verkehrs möglich macht. Eine derartige Überwachung würde einen unverhältnismäßigen Eingriff in das Grundrecht auf Persönlichkeitsschutz darstellen und darüber hinaus den im Teledienstedatenschutzgesetz und im Mediendienstestaatsvertrag normierten Grundsätzen der Datenvermeidung und der Datensparsamkeit zuwiderlaufen.

Es muss sichergestellt werden, dass die zunehmende Nutzung von Telediensten zu Alltagsgeschäften auch künftig generell überwachungsfrei bleibt. Die bestehenden materiellen Befugnisse zur Telekommunikationsüberwachung im Strafprozessrecht, G 10-Gesetz und im Außenwirtschaftsgesetz bedürfen zudem insgesamt dringend einer kritischen Evaluation und Bereinigung, die die Bundesregierung durch eine wissenschaftliche Untersuchung der Effektivität bisheriger Überwachungsanordnungen bereits eingeleitet hat.

Die Datenschutzbeauftragten des Bundes und der Länder fordern ebenso eine Evaluation der Telekommunikations-Überwachungsverordnung, die im Lichte der Ergebnisse der Untersuchung über die Effektivität von Telekommunikations-Überwachungsmaßnahmen vorzunehmen ist.

Anlage 22

Entschließung

Sondertreffen der Datenschutzbeauftragten des Bundes und der Länder zur Terrorismusbekämpfung
(1. Oktober 2001)

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z.B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

Anlage 23

Entschließung
der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 24. - 26. Oktober 2001 in Münster

Datenschutzrechtliche Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte)

Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines „Arzneimittelpasses“ in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Bisher ist nicht ansatzweise belegt, dass die bekannt gewordenen Gefahren für die Patientinnen und Patienten dadurch entstanden sind, dass verschiedene Ärztinnen und Ärzte

ohne Kenntnis voneinander unverträgliche Medikamente verordnet hätten. Deswegen ist auch nicht ersichtlich, dass die aufgetretenen Probleme mit einem Arzneimittelpass hätten verhindert werden können.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als **Pflichtkarte**. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

Die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über Einsatz und Verwendung der Karte muss gewährleistet werden (**Grundsatz der Freiwilligkeit**).

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 zum freiwilligen Einsatz von Chipkarten im Gesundheitswesen Stellung genommen; deren Zulässigkeit wird dort von verschiedenen Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten abhängig gemacht. Grundlegende Voraussetzung ist vor allem die freie Entscheidung der Betroffenen (auch als Versicherte). Sie müssen entscheiden können,

- ob ihre Daten auf einer Chipkarte gespeichert werden,
- welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,
- welche ihrer Daten auf der Karte wieder gelöscht werden,
- ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und

- welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Die Verantwortung für die Wahrung der Arzneimittelsicherheit tragen grundsätzlich die Ärztinnen und Ärzte sowie die Apothekerinnen und Apotheker. Sie darf nicht auf die Betroffenen abgewälzt werden. Dies gilt auch, wenn sie von dem „Arzneimittelpass“ keinen Gebrauch machen.

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Patientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den „Arzneimittelpass“ auf der **Krankenversichertenkarte** gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die „Funktion Krankenversichertenkarte“ von der „Funktion Arzneimittelpass“ informationstechnisch getrennt würde, so dass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offenlegen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

Die Betroffenen müssen ferner das Recht und die Möglichkeit haben, ihre auf der Chipkarte gespeicherten Daten vollständig zu lesen.

Die Verwendung der Karte außerhalb des medizinischen Bereichs, z.B. durch Arbeitgeberinnen und Arbeitgeber oder Versicherungen, muss gesetzlich verboten und sanktioniert werden.

Anlage 24

Entschließung
der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 24. - 26. Oktober 2001 in Münster

Gesetzliche Regelung von genetischen Untersuchungen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder konkretisiert ihre Forderungen an Bundestag und Bundesrat, genetische Untersuchungen am Menschen gesetzlich zu regeln. Geboten sind besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken. Außer dem „genetischen Fingerabdruck“ für Zwecke der Strafverfolgung – in der Strafprozessordnung bereits normiert – sind typische Anwendungsfelder für genetische Untersuchungen zu regeln. Von besonderer Bedeutung sind das Informations- und Entscheidungsrecht der betroffenen Personen. Die Kernanliegen der Datenschutzbeauftragten sind:

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;
- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;
- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;
- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;
- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;

- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung, individuell bedeutsame Untersuchungsergebnisse mitzuteilen;
- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen fordert die Konferenz der Datenschutzbeauftragten eine grundlegende Strafnorm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder ohne die grundsätzlich nur für Zwecke der medizinischen Behandlung oder Forschung wirksame Einwilligung der betroffenen Person zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder verstehen ihre Vorschläge als Anregungen zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

Anlage 25

Entschließung
der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 24. - 26. Oktober 2001 in Münster

Lkw-Maut auf Autobahnen und zur allgemeinen Maut auf privat errichteten Bundesfernstraßen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, bei der technischen Realisierung und bei der anstehenden internationalen Normierung elektronischer Mautsysteme datenschutzrechtliche Anforderungen durchzusetzen.

Das Bundeskabinett hat am 15. August 2001 den Gesetzentwurf für die Einführung eines solchen Mautsystems beschlossen. Ab 2003 ist neben der manuellen Erfassung der Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Autobahnbenut-

zungsgebühr (Maut) für Lastkraftwagen erhoben werden soll. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen prüft zurzeit Angebote, die im Ergebnis einer europaweiten Ausschreibung eingegangen sind.

Für das automatische System sollen das Satellitennavigationssystem GPS und die Mobilfunktechnologie genutzt werden. Dadurch werden stationäre Erfassungseinrichtungen entbehrlich. Relativ einfach könnte so das mautpflichtige Straßennetz beispielsweise auf den Bereich der Bundesstraßen ausgedehnt werden. Selbst ein grenzüberschreitender Einsatz derartiger Systeme wäre aus technischer Sicht leicht zu realisieren. Entsprechendes Interesse aus dem benachbarten Ausland ist bereits bekundet worden.

Die verfügbare, im Gesetzentwurf nicht festgeschriebene Technik ermöglicht es prinzipiell, den Fahrweg der Mautpflichtigen detailliert zu dokumentieren und zu archivieren und auf diese Weise exakte Bewegungsprofile zu erstellen. Damit würden die Voraussetzungen geschaffen, dass Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Die Datenschutzbeauftragten des Bundes und der Länder halten es deshalb für unverzichtbar, elektronische Mautsysteme datenschutzgerecht auszugestalten. Insbesondere ist dafür Sorge zu tragen, dass die Erhebung und Speicherung ausschließlich für Abrechnungszwecke verwendet werden.

Weiterhin ist bei Gestaltung und beim Betrieb der erforderlichen Erfassungs- und Kontrollsysteme das im Bundesdatenschutzgesetz normierte Prinzip der Datensparsamkeit sicherzustellen. Das erfordert den Einsatz von Verfahren, bei denen Mautgebühren vorab entrichtet werden können, ohne dass dafür die Erhebung und Speicherung personenbeziehbarer Daten erforderlich ist.

Insbesondere ist sicherzustellen, dass damit keine oder so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Soweit personenbezogene Daten beispielsweise für Abrechnungs- oder Kontrollzwecke gespeichert werden, sind sie zum frühestmöglichen Zeitpunkt, spätestens jedoch nach Entrichtung der Straßenbenutzungsgebühr beziehungsweise nach Abschluss eines Mauterstattungsverfahrens zu löschen, wenn sie nicht mehr für die

Abwicklung des Mautverfahrens oder für erforderliche Kontroll- oder Prüfverfahren benötigt werden.

Bereits 1995 haben die Datenschutzbeauftragten des Bundes und der Länder Anforderungen an Systeme zur automatischen Erhebung von Straßennutzungsgebühren formuliert. Insbesondere die folgenden Aspekte sind nach wie vor aktuell:

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.
- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.
- Es ist sicherzustellen, dass anfallende personenbezogenen Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

Außerdem liegt ein Gesetzentwurf vor, der zur Erhebung von Mautgebühren an Brücken, Tunneln und Gebirgspässen im Zuge von Bundesautobahnen und Bundesstraßen sowie an mehrspurigen Bundesstraßen mit getrennten Fahrbahnen berechtigt, soweit sie von Privaten errichtet sind. Die Mautpflicht gilt für alle Kraftfahrzeuge. Deshalb muss an der im Entwurf vorgesehenen Barzahlungsmöglichkeit ohne Verarbeitung personenbezogener Daten unbedingt festgehalten werden. Ihre Ausgestaltung sollte kundenfreundlich erfolgen. Diese Zahlungsweise vermeidet die weitergehende Datenerfassung für alle Mautpflichtigen (Kennzeichen und Bilder der Fahrzeuge). In der zu erlassenden Rechtsverordnung muss deshalb insbesondere sichergestellt werden, dass keine Datenerfassung bei Personen erfolgt, die die Gebühr unmittelbar entrichten.

Anlage 26

Entschließung
der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 24. - 26. Oktober 2001 in Münster

„Neue Medienordnung“

Bund und Länder beraten gegenwärtig über die Grundzüge einer neuen Medienordnung. Zu den dabei zu beachtenden verfassungsrechtlichen Rahmenbedingungen gehören neben den Gesetzgebungskompetenzen von Bund und Ländern auch die Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten, Meinungsfreiheit und Vertraulichkeit der Kommunikation. Diese Rechte müssen in einer neuen Medienordnung durchgängig gewährleistet bleiben.

Angesichts der technischen Entwicklung und der Konvergenz der Medien darf der Grad der Vertraulichkeit nicht mehr allein davon abhängig sein, ob ein Kommunikationsvorgang der Telekommunikation, den Tele- oder den Mediendiensten zugeordnet wird. Vielmehr muss für alle Formen der Kommunikation und der Mediennutzung ein angemessen hoher Schutz gewährleistet werden.

Aus diesem Grund fordert die Konferenz, das Fernmeldegeheimnis nach Art. 10 GG zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter zu entwickeln und einfachgesetzlich abzusichern.

Die Konferenz tritt in diesem Zusammenhang dafür ein, die einschlägigen Rechtsvorschriften inhaltlich stärker einander anzugleichen, klarer zu strukturieren und für Nutzende und Anbietende verständlicher zu gestalten.

Anlage 27

Entschließung

der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 24. - 26. Oktober 2001 in Münster

Grundsätze zur Übermittlung von Telekommunikations-verbindungsdaten

Die Bundesregierung hat den Gesetzentwurf für eine Nachfolgeregelung zu § 12 FAG vorgelegt, der eine Reihe datenschutzrechtlich positiver Ansätze enthält. Der Bundesrat hat sich demgegenüber in seiner Stellungnahme für eine Regelung ausgesprochen, die wesentlichen datenschutzrechtlichen Anforderungen nicht gerecht wird. Die Datenschutzbeauftragten des Bundes und der Länder lehnen den Vorschlag des Bundesrates entschieden ab.

Sie halten es für nicht vertretbar, Auskünfte über zurückliegende Aktivmeldungen von Mobiltelefonen auch bei reinem Stand-by-Betrieb zu erteilen und Diensteanbieter zur Aufzeichnung von Telekommunikationsverbindungsdaten eigens für Zwecke der Strafverfolgung zu verpflichten.

Auch die vom Bundesrat vorgeschlagene Regelung des § 18a BVerfSchG zur Übermittlung von Telekommunikationsverbindungsdaten an die Verfassungsschutzbehörden halten die Datenschutzbeauftragten des Bundes und der Länder für nicht akzeptabel. Sie fordern eine deutliche Klarstellung im Wortlaut des Gesetzes, dass Verbindungsdaten an den Verfassungsschutz nur dann übermittelt werden dürfen, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine in § 3 Abs. 1 G 10 genannte Straftat plant, begeht oder begangen hat oder sonst an gewalttätigen Bestrebungen oder sicherheitsgefährdenden Tätigkeiten teilnimmt. Eine Übermittlung der Verbindungsdaten für den gesamten Aufgabenbereich des Verfassungsschutzes ginge dagegen erheblich zu weit.

Ferner halten es die Datenschutzbeauftragten für geboten, hinsichtlich der Kennzeichnung und Zweckbindung der Daten, der Mitteilungen an Betroffene und der parlamentarischen Kontrolle einen dem G 10 möglichst gleichwertigen Standard zu gewährleisten.

Die Bundesregierung und der Deutsche Bundestag werden gebeten, diese datenschutzrechtlichen Mindestanforderungen im weiteren Gesetzgebungsverfahren zu berücksichtigen.

Anlage 28

Entschließung
der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 24. - 26. Oktober 2001 in Münster

Biometrische Merkmale in Personalausweisen und Pässen

Im Entwurf eines Terrorismusbekämpfungsgesetzes ist vorgesehen, die Möglichkeit zu eröffnen, in deutschen Personalausweisen und Pässen neben dem Lichtbild und der Unterschrift weitere biometrische Informationen wie zum Beispiel Fingerabdrücke, Handgeometrie, Gesichtsgeometrie u.a. aufzunehmen. Auch die Verwendung genetischer Daten wird nicht ausgeschlossen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass diese Maßnahme schon allein wegen des technischen und zeitlichen Aufwandes, der mit der Einführung derartiger Dokumente verbunden wäre, keinen kurzfristigen Beitrag zur Lösung der mit dem internationalen Terrorismus derzeit verbundenen Probleme leisten kann, zumal Ausländerinnen und Ausländer, die sich in Deutschland aufhalten, nicht erfasst werden.

Die Nutzung biometrischer Merkmale in Personalausweisen und Pässen sowie die damit verbundenen Folgeprobleme (zum Beispiel Art und Ort der Speicherung von Referenzdaten; Vermeidung von Überschussinformationen) werfen eine Vielzahl schwieriger Fragen auf, die einer ausführlichen Diskussion bedürfen. Die zuständigen Stellen werden hierzu aufgefordert, die Notwendigkeit und die rechtlichen und technischen Einzelheiten einer Realisierung dieser Maßnahmen darzulegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist bereit, sich unter diesen Voraussetzungen mit der Frage zu befassen, ob und wie es möglich ist, mit Hilfe geeigneter zusätzlicher Merkmale in Identifikationspapieren deren Missbrauch zu verhindern, ohne dabei die Grundsätze des Datenschutzes zu verletzen.

Anlage 29

Entschließung
der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 24. - 26. Oktober 2001 in Münster

Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass zahlreiche Vorschläge in der gegenwärtigen Debatte um notwendige Konsequenzen aus den Terroranschlägen vom 11. September 2001 die erforderliche sachliche und verantwortungsbewusste Abwägung mit den grundgesetzlich geschützten Freiheits- und Persönlichkeitsrechten der Einzelnen vermissen lassen.

Der Entwurf eines Terrorismusbekämpfungsgesetzes und der Antrag der Länder Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (BR-Drs. 807/01) übertreffen die in der Entschließung der Konferenz vom 1. Oktober 2001 geäußerte Befürchtung, dass übereilt Maßnahmen ergriffen werden sollen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger unangemessen einschränken.

Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist. Außerdem müsste der Frage nachgegangen werden, ob es nicht in den Geheimdiensten und in der Strafverfolgung Vollzugsdefizite gibt. Dabei müsste auch

untersucht werden, welche Resultate die vielen Gesetzesverschärfungen der letzten Jahre gebracht haben.

Persönlichkeitsrechte haben über ihre grundrechtssichernde Wirkung hinaus – mit den Worten des Bundesverfassungsgerichts – auch Bedeutung als „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert daher sehr eindringlich an alle Beteiligten, nicht Persönlichkeitsrechte vorschnell und ohne die gebotene sorgsam abwägende Prüfung über die bereits bestehenden Eingriffsmöglichkeiten hinaus dauerhaft einzuschränken und so den Ausnahmezustand zur Norm zu erheben.

Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte so überlagern, dass es in unserem Land zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.

Wesentliche im BMI-Entwurf eines Terrorismusbekämpfungsgesetzes enthaltene Eingriffsmöglichkeiten führen zwangsläufig dazu, dass eine Vielzahl völlig unbescholtener Einzelpersonen zentral erfasst oder verdeckt in Datenerhebungen einbezogen werden, ohne dass eine konkrete Verdachts- oder Gefahrenlage verlangt wird. Zugleich werden Auskunftspflichten und Ermittlungskompetenzen in einer Weise ausgedehnt, dass Eingrenzungen verloren gehen, die aus rechtsstaatlichen Gründen unverzichtbar sind.

Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post – und Telekommuni-

kationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahren gespeichert werden.

Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der StPO zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwischen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen. Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.

Auch die Vorschläge der Länder enthalten unvertretbare Einschränkungen von grundgesetzlich geschützten Rechtspositionen. So soll die Gefahrenschwelle für den verdeckten Einsatz technischer Mittel in Wohnungen übermäßig abgesenkt werden. Telekommunikationsunternehmen und Internetprovider sollen gesetzlich verpflichtet werden, Verbindungsdaten (zum Beispiel über den Besuch einer Website oder einer Newsgroup) länger zu speichern, als diese zu Abrechnungszwecken benötigt werden, um sie Sicherheitsbehörden zur Verfügung zu stellen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden. Eine unabhängige Evaluierung nach festgelegten Fristen ist unerlässlich, um Geeignetheit und Erforderlichkeit für die Zukunft sachgerecht beurteilen zu können.

Anlage 30

Entschließung

der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 24. - 26. Oktober 2001 in Münster

EUROJUST - Vorläufer einer künftigen europäischen Staatsanwaltschaft?

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sachgerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden auf dem Gebiet der Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als Grundlage für EUROJUST nur eine Konvention in Betracht, da für künftige Grundrechtseingriffe durch EUROJUST eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsanspruch des Betroffenen sowie zu einer Kontrollinstanz von EUROJUST enthalten.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sind folgende datenschutzrechtliche Anforderungen an EUROJUST zu stellen:

- Informationsaustausch mit Partnern
  Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und –stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EUROJUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Nur in absoluten Ausnahmefällen, die einer restriktiven Regelung bedürfen, sollte eine Datenübermittlung auch bei Fehlen einer solchen Vereinbarung zulässig sein.

- Verarbeitung personenbezogener Daten
  Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Eine zusätzliche Öffnungsklausel, die letztlich die Speicherung aller Daten zulassen würde, ist abzulehnen. Eine Verarbeitung der Daten von Opfern und Zeugen darf, wenn überhaupt erforderlich, nur unter einschränkenden Bedingungen vorgenommen werden.

- Ermittlungsindex und Dateien
  Der Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt. Sofern zusätzlich Arbeitsdateien geführt werden, sind sie genau zu bezeichnen.

- Auskunftsrecht
  Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein eigener Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Für den Fall, dass im Strafverfolgungsinteresse oder aus sonstigen Gründen des Gemeinwohls von einer Auskunft an den Be-

troffenen abgesehen werden soll, muss eine Abwägung mit den Interessen des Betroffenen an einer Auskunftserteilung vorangegangen sein.

- Änderung, Berichtigung und Löschung
  Es sollte auch eine Regelung zur Sperrung von Daten ausgenommen werden, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden.

- Speicherungsfristen
  Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z.B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Speicherungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Die Prüffristen sollten zwei Jahre betragen und auch für Folgeprüfungen nicht länger sein.

- Datensicherheit
  Erforderlich sind konkrete Vorschriften zur Datensicherheit. Um den Text des Beschlusses nicht zu überfrachten, könnte eine Regelung entsprechend Art. 22 der Verordnung EG 45/2001 oder § 9 BDSG vorgesehen werden.

- Gemeinsame Kontrollinstanz
  Die Erforderlichkeit einer gemeinsamen Kontrollinstanz für EUROJUST muss außer Frage stehen. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die EUROJUST-Mitglieder als auch das Kollegium müssen die Entscheidungen der gemeinsamen Kontrollinstanz bindender Charakter haben.

- Rechtsschutz
  Dem Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren. Es sollte festgelegt werden, welche nationale oder supranationale Gerichtsbarkeit für Klagen auf

Auskunft, Löschung, Berichtigung und Schadensersatz zuständig ist.

- Rechtsetzungsbedarf
  Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben.
  Darüber hinaus bedarf der Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

Anlage 31

Rundschreiben des TLfD Nr. 1/2000

Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

Mit Schreiben des TLfD Nr. 2/98 erhielten Sie die o. g. Orientierungshilfe mit Stand September 1998. Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diese wieder überarbeitet und dem derzeitigen Stand der Technik angepasst.

Neu aufgenommen wurden datenschutzrechtliche Hinweise zur Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall. Die entsprechenden Aussagen im Kapitel 4 der Orientierungshilfe hierzu beziehen sich anhand der in der Praxis vorkommenden Fallkonstellationen sowohl auf die Kontrolle von Inhaltsdaten bei der E-Mail-Kommunikation wie auch zur Protokollierung von Zugriffen in bzw. aus dem Internet über eine Firewall. Von einer solchen Kontrolle sind neben Dritten insbesondere die Bediensteten betroffen.

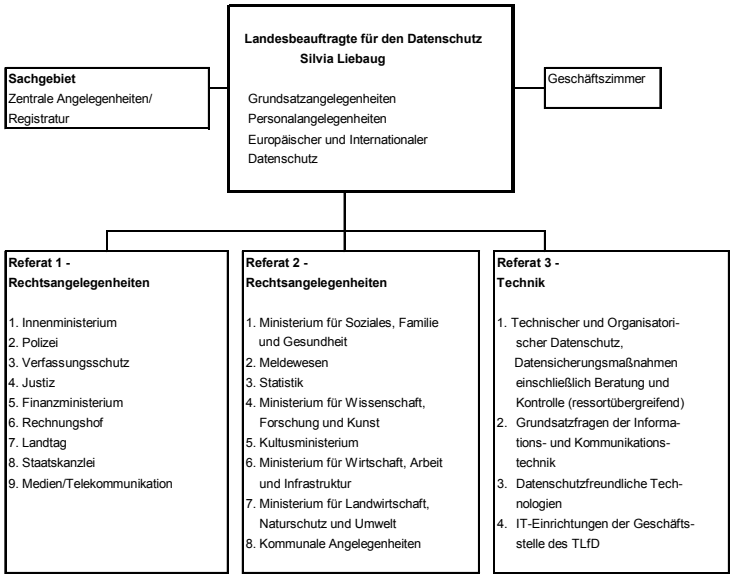
Es wird deshalb angeraten, in Abstimmung mit dem Personalrat, die hiermit zusammenhängenden Fragen eindeutig zu regeln.
Der TLfD weist im Zusammenhang mit der Internetnutzung auch auf seine diesbezüglichen Ausführungen im 3. Tätigkeitsbericht unter Punkt 15.8 hin.

Diesem Anschreiben liegt eine Diskette bei. auf der Ihnen die überarbeitete Orientierungshilfe mit Stand Mai 2000 als Winword 6.0 Datei unter dem Namen or-inter.doc zur weiteren Verwendung zur Verfügung steht.

Die o. g. Orientierungshilfe sowie der 3. Tätigkeitsbericht des TLfD sind auch über die Internetpräsentation des TLfD unter der Web-Adresse www.datenschutz.thueringen.de (Rubriken: Technischer Datenschutz/Internet - die Mutter der Netze bzw. Veröffentlichungen) verfügbar.

Anlage 32

Thüringer Landesbeauftragter für den Datenschutz (TLfD)



Anschrift
Johann-Sebastian-Bach-Str. 1
99096 Erfurt

Postanschrift
PF 10 19 51
99019 Erfurt

Tel. 0361/3771900
Fax 0361/3771904
E-Mail:poststelle@datenschutz.thueringen.de

Sachregister