Vorwort

Der 5. Tätigkeitsbericht des Thüringer Landesbeauftragten für den Datenschutz umfasst den Berichtszeitraum vom 1. Januar 2002 bis zum 31. Dezember 2003.

Der Bericht beinhaltet Schwerpunkte der Tätigkeit im Berichtszeitraum. Gemäß § 40 Abs. 1 ThürDSG sind Ergebnisse der Kontrolltätigkeit und Anregungen zu Verbesserungen des Datenschutzes enthalten. Über durchgeführte Kontrollen, die im Berichtszeitraum noch nicht abgeschlossen wurden, werde ich in meinem 6. Tätigkeitsbericht weiter berichten.
Der Bericht wurde im Beirat vorberaten.
Er steht im Internet unter www.datenschutz.thueringen.de zur Verfügung.

Erfurt, im Dezember 2003

Silvia Liebaug
Thüringer Landesbeauftragte für den Datenschutz

5. Tätigkeitsbericht des TLfD
Berichtszeitraum vom 01.01.2002 bis 31.12.2003

Inhaltsverzeichnis
Abkürzungsverzeichnis

Entschließungen der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 in Dresden

Entschließungen zwischen den Konferenzen 2003

Entschließungen der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig

Entschließungen zwischen den Konferenzen 2003/2004

Weitere Anlagen

Sachregister

Abkürzungsverzeichnis

Abkürz.	**Bedeutung**
4. StVollzÄndG	4. Strafvollzugsänderungsgesetz
Abl.	Amtsblatt
Abs.	Absatz
AD	Active Directory
AGB	Allgemeine Geschäftsbedingungen
AK	Arbeitskreis
AO	Abgabenordnung
AO-E	Abgabenordnung-Entwurf
Art.	Artikel
BAföG	Bundesausbildungsförderungsgesetz
BAT-O	Bundes-Angestelltentarif-Ost
BDSG	Bundesdatenschutzgesetz
BerRehaG	Gesetz über den Ausgleich beruflicher Benachteiligungen für Opfer politischer Verfolgung im Beitrittsgebiet
BfD	Bundesbeauftragter für den Datenschutz
BfF	Bundesamt für Finanzen
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BImSchVO	Bundesimmissionsschutzverordnung
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BMBF	Bundesministerium für Bildung und Forschung
BMF	Bundesministerium der Finanzen
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BTX	Bildschirmtext
BuStra	Bußgeld- und Strafsachenstelle
BVerfG	Bundesverfassungsgericht
BZR	Bundeszentralregister
bzw.	beziehungsweise
CC	Common Criteria
CN	Corporate Network
d. h.	das heißt
DA	Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden

DIN	Deutsches Institut für Normung
DNA-Analyse	Genetischer Fingerabdruck
DSB	Datenschutzbeauftragter/Datenschutzbeauftragte
DVBl.	Deutsches Verwaltungsblatt
DVD	Digital Versatile Disc
EAPoL	Extensible Authentication Protocol over LAN
EDV	Elektronische Datenverarbeitung
EFS	Encryption File System
EG	Europäische Gemeinschaft
E-Government	Elektronische Verwaltung
ELSTER	Elektronische Steuererklärung
E-Mail	Elektronic-Mail (elektronische Post)
EStG	Einkommenssteuergesetz
EStG-E	Einkommenssteuergesetz-Entwurf
EU	Europäische Union
Eurojust	Gemeinsame Stelle zur justiziellen Zusammenarbeit
Europol	Europäisches Polizeiamt
FeV	Verordnung über die Zulassung von Personen zum Straßenverkehr (Fahrerlaunisverordnung)
FGG	Freiwillige Gerichtsbarkeit-Gesetz
FTP	File Transfer Protocol
FVG	Finanzverwaltungsgesetz
G 10 Gesetz	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel-10-Gesetz)
GBV	Grundbuchverfügung
GC	Global Catalog
GG	Grundgesetz
ggf.	gegebenenfalls
ggü.	gegenüber
GKI	Gemeinsame Kontrollinstanz
GKV	Gesetzliche Krankenversicherung
GMG	Gesundheitsmodernisierungsgesetz
grds.	grundsätzlich
GVBl.	Gesetz- und Verordnungsblatt
HBCI	Home Banking Computer Interface
HTTP	Hyper Text Transfer Protocol
i. d. R.	in der Regel
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IABV	Integriertes Automatisches Besteuerungsverfahren

IDS	Intrusion-Detection-System
IEEE	Institut of Electrical and Electronic Engeneers
IEEE	Institut of Electrical and Electronic Engeneers
IfSG	Infektionsschutzgesetz
IMA-IT	Interministerieller Ausschuss für Informationstechnik
IN	Identifikationsnummer
INPOL	Informationssystem der Polizei
IPSec	Internet Protocol Security
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria
IuK	Informations- und Kommunikationstechnik
KAN	Kriminalaktennachweis
Kfz	Kraftfahrzeug
KitaG	Thüringer Gesetz über Tageseinrichtungen für Kinder als Landesausführungsgesetz zum Kinder- und Jugendhilfegesetz
LaDiVA	Landeseinheitliches Dialogverfahren Ausländerwesen
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LfD	Landesbeauftragter für den Datenschutz
Nr.	Nummer
o. g.	oben genannt
OBG	Ordnungsbehördengesetz
OFD	Oberfinanzdirektion
OH	Orientierungshilfe
OWiG	Ordnungswidrigkeitengesetz
PAG	Polizeiaufgabengesetz
PassG	Passgesetz
PC	Personal Computer
PD	Polizeidirektion
PDA	Personal Digital Assistant
PIN	Persönliche Identifikationsnummer
PStG	Personenstandsgesetz
PStV	Personenstandsverordnung
PUKs	Personal Unblocking Keys
RC4	Rivest Cipher 4
RegTP	Regulierungsbehörde für Post und Telekommunikation

RLAktenThürPol	Richtlinie zum Umgang mit dienstlichem Schriftgut sowie zur Akten- und Schriftgutaussonderung in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei
S.	Seite
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SMTP	Simple Mail Transfer Protocol
sog./sogen.	sogenannte/sogenannter
SSID	Service Set Identifier
StARoV	Staatliches Amt zur Regelung offener Vermögensfragen
StDAV	Steuerdaten-Abruf-Verordnung
StDÜV	Steuerdaten-Übermittlungsverordnung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVBG	Steuerverkürzungsbekämpfungsgesetz
StVergAbG	Steuervergünstigungsabbaugesetz
StVG	Straßenverkehrsgesetz
StVollzÄndG	Strafvollzugsänderungsgesetz
StVollzG	Strafvollzugsgesetz
TAN	Transaktions-Nummer
TB	Tätigkeitsbericht
TCPA	Trusted Computing Platform Alliance
TCSEC	Trusted Computer System Evaluation Criteria
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Telekommunikations-Datenschutzverordnung
TESTA	Trans European Services for Telematics between Administrations
TFM	Thüringer Finanzministerium
ThLARoV	Thüringer Landesamt zur Regelung offener Vermögensfragen
ThürArchivG	Thüringer Archivgesetz
ThürBG	Thüringer Beamtengesetz
ThürBO	Thüringer Bauordnung
ThürBVVG	Thüringer Gesetz über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid
ThürDSG	Thüringer Datenschutzgesetz

ThürGGO	Gemeinsame Geschäftsordnung für die Landesregierung sowie für die Ministerien und die Staatskanzlei des Freistaats Thüringen
Thüringer OLG	Thüringer Oberlandesgericht
ThürKHG	Thüringer Krankenhausgesetz
ThürKO	Thüringer Kommunalordnung
ThürLMG	Thüringer Landesmediengesetz
ThürMeldeG	Thüringer Meldegesetz
ThürPersVG	Thüringer Personalvertretungsgesetz
ThürPersVWO	Wahlordnung zum Thüringer Personalvertretungsgesetz
ThürPolPrüffristVO	Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung
ThürPsychKG	Thüringer Gesetz zur Hilfe und Unterbringung psychisch Kranker
ThürRettG	Thüringer Rettungsdienstgesetz
ThürSchulG	Thüringer Schulgesetz
ThürStrUBG	Thüringer Gesetz über die Unterbringung besonders rückfallgefährdeter Straftäter
ThürVSG	Thüringer Verfassungsschutzgesetz
ThürVwVfG	Thüringer Verwaltungsverfahrensgesetz
ThürZustVBezüge	Thüringer Verordnung über Zuständigkeiten für die Feststellung, Berechnung und Anordnung der Zahlung der Bezüge von Bediensteten und Versorgungsempfängern
TIM	Thüringer Innenministerium
TJM	Thüringer Justizministerium
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKM	Thüringer Kultusministerium
TKÜ	Telekommunikationsüberwachung
TLfD	Thüringer Landesbeauftragter für den Datenschutz
TLfV	Thüringer Landesamt für Verfassungsschutz
TLRZ	Thüringer Landesrechenzentrum
TLS	Thüringer Landesamt für Statistik
TLT	Thüringer Landtag
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
TPM	Trusted Platform Modul
TRH	Thüringer Rechnungshof
u. a.	unter anderem (und andere)
u. ä.	und ähnliches
UIG	Umweltinformationsgesetz
UPN	User Personality Network
USB	Universal Serial Bus
USt	Umsatzsteuer
UStG	Umsatzsteuergesetz
UVT	Unfallversicherungsträger
VerfThür	Verfassung des Freistaats Thüringen
VermG	Vermögensgesetz
VPN	Virtual Private Network
WaffG	Waffengesetz
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Array Network
z. B.	zum Beispiel
z. T.	zum Teil
z. Z.	zur Zeit
ZIV	Zentrum für Informationsverarbeitung
ZPO	Zivilprozessordnung

1. Vorbemerkung

Im Ergebnis der Kontrollbesuche in den öffentlichen Stellen des Freistaats Thüringen ist festzustellen, dass den Belangen des Datenschutzes und der Datensicherheit überwiegend eine angemessene Beachtung beigemessen wird und entsprechende technische und organisatorische Maßnahmen diesbezüglich eingeleitet wurden.
Aufgrund festgestellter Mängel beim Umgang mit personenbezogenen Daten wurden im Berichtszeitraum insgesamt 21 Beanstandungen ausgesprochen. In diesem Zusammenhang wurden auch die jeweiligen Aufsichtsbehörden der öffentlichen Stellen davon verständigt und eine Behebung der Mängel in angemessener Frist gefordert. Die beanstandeten Stellen kamen den datenschutzrechtlichen Forderungen, wenn auch mitunter erst nach entsprechender Anmahnung, nach.

Vorgetragene Bürgeranliegen oder -beschwerden werden in der Dienststelle mit höchster Priorität bearbeitet. Infolge vorliegender Anfragen wurden mitunter mehrmalige Kontrollbesuche in den öffentlichen Stellen durchgeführt, um eine umfassende datenschutzrechtliche Bewertung vornehmen zu können und den Petenten bestmöglich bei der Wahrnehmung seiner Datenschutzrechte unterstützen zu können.

Gemäß § 40 Abs. 7 ThürDSG gehört es auch zu den Aufgaben des Landesbeauftragten, die der Kontrolle unterliegenden Stellen zu beraten und Empfehlungen zur Verbesserung des Datenschutzes zu geben. Im Rahmen der vorhandenen Möglichkeiten wurden den Beratungsersuchen sowohl von mir selbst, als auch von den Mitarbeiterinnen und Mitarbeitern der Dienststelle, entsprechend Rechnung getragen. Leider wurde mir auch im Berichtszeitraum nicht die beantragte dringend erforderliche zusätzliche Stelle im Bereich Technik bereitgestellt. Ich werde auch weiterhin meine diesbezügliche Forderung an den Thüringer Landtag herantragen.

In den jeweiligen Konferenzen der Datenschutzbeauftragten (DSB) des Bundes und der Länder wurden aktuelle datenschutzrechtliche Themen und Gesetzentwürfe diskutiert. Die gemeinsam verabschiedeten Entschließungen sind in der Anlage zum Tätigkeitsbericht aufgenommen.

2. Europäischer und Internationaler Datenschutz

2.1 Datenschutzkolloquium in Montevideo

Auf Einladung des Goethe Instituts Inter Nations Montevideo nahm ich im Mai 2003 am Kolloquium zum Thema „Datenschutz“ in Uruguay teil.
In Uruguay existiert bislang kein Datenschutzgesetz und keine Datenschutzkontrollbehörde. Im Rahmen der Veranstaltung machte ich grundlegende Ausführungen zur Ausgestaltung des Grundrechts auf Datenschutz in Deutschland und Thüringen. Dem Schutz der Persönlichkeitsrechte und der Privatsphäre der Bürger kommt eine hohe Bedeutung zu, was durch die Verfassung des Freistaats Thüringen ausdrücklich garantiert wird. Artikel 69 der Landesverfassung bestimmt, dass zur Wahrung des Rechts auf Schutz der personenbezogenen Daten und zur Unterstützung bei der Ausübung der parlamentarischen Kontrolle beim Landtag ein DSB berufen wird.
Damit entspricht der Status des DSB seiner besonderen Verantwortung. Er ist in seiner Amtsausübung nämlich völlig unabhängig und dabei nur dem Gesetz unterworfen.
In Gesprächsrunden uruguayischer und ausländischer Experten standen die Themen „Datenschutz im Bereich Arbeit und Gesundheit“ sowie „Datenschutz im Bank- und Finanzbereich“ im Mittelpunkt. Es fand ein reger Erfahrungsaustausch dazu statt.

2.2 Europol

In vorangegangenen TB (1. TB, 7.9; 2. TB, 7.3; 3. TB, 2.3) habe ich bereits Ausführungen zum Aufgabenbereich von Europol gemacht. Die Gemeinsame Kontrollinstanz von Europol (GKI) hat zwischenzeitlich einen Tätigkeitsbericht für den Zeitraum von Oktober 1998 bis Oktober 2003 veröffentlicht. Dieser ist über die Internetpräsentation des Landesbeauftragten für den Datenschutz in Sachsen-Anhalt, der im Berichtszeitraum durch den Bundesrat im Oktober 2003 gemäß Art. 2 § 6 Abs. 2 und 4 EuropolG wiederum als Vertreter in der GKI benannt wurde, unter www.datenschutz.sachsen-anhalt.de abrufbar.

2.3 Eurojust

Der Beschluss über die Einrichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität (2002/187/JI) wurde am

28. Februar 2002 vom Rat der Europäischen Union angenommen und ist mit der Bekanntmachung im Amtsblatt der Europäischen Gemeinschaften am 6. März 2002 (Abl. EG Nr. L63 S. 1) in Kraft getreten. Die Bestimmungen dieses Beschlusses waren nach seinem Artikel 42 bis zum 6. September 2003 in innerstaatliches Recht umzusetzen.
Zur Umsetzung liegt nunmehr der Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Umsetzung des Beschlusses (2002/187/JI) des Rates vom 28. Februar 2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität (Eurojust-Gesetz - EJG) - Bundesrats-Drucksache 545/03 vom 15. August 2003 vor. Er enthält die sich zur Umsetzung aus dem Beschluss ergebenden Verpflichtungen, Regelungen insbesondere zur Ernennung und Abberufung des nationalen Mitglieds, der ihm unterstehenden Personen, zur Informationsübermittlung, zu den nationalen Anlaufstellen, zur gemeinsamen Kontrollinstanz und zu haftungsrechtlichen Fragen.
Der Gesetzentwurf sieht nach wie vor eine Pflicht der Strafverfolgungsbehörden vor, die angeforderten Informationen zu übermitteln. Auch haben Gerichte und Behörden, die nicht Aufgaben der Strafverfolgung wahrnehmen, weiterhin die Befugnis, auf Gesuch Informationen zu übermitteln. Dies ist jedoch nur insoweit zulässig, als es gegenüber einem Gericht oder einer Staatsanwaltschaft zur Durchführung eines Strafverfahrens zulässig wäre. Weiterhin haben alle öffentlichen Stellen die Möglichkeit so genannter Spontanmitteilungen, wobei unklar ist, in welchen Fällen Daten übermittelt werden dürfen. Die nationalen Anlaufstellen sollen das Recht haben, die Informationen in Arbeitsdateien zu verwenden, wobei dies im Gesetzentwurf nur unvollständig geregelt ist.
Einige der Anregungen der DSB des Bundes und der Länder (4. TB, 2.2) sind im Gesetzentwurf umgesetzt worden. So sind bspw. bei Übermittlungen nicht nur besondere bundesgesetzliche, sondern auch entsprechende landesgesetzliche Verwendungsregelungen zu beachten, die justizielle Sachleistungsbefugnis bleibt bei einer Übermittlung unberührt und Register im Sinne des Gesetzes sind automatisiert geführte Dateisammlungen, die nicht nur internen Zwecken der verantwortlichen Stellen dienen. Darüber hinaus ist Eurojust auch über den Abschluss eines Verfahrens zu unterrichten. Bei sogenannten Spontanmitteilungen müssen Anhaltspunkte für die Notwendigkeit der Kenntniserlangung durch Eurojust vorliegen. Es besteht die Verpflichtung, Eurojust bei der Übermittlung zu ersuchen, übermittelte personenbezogene Daten unverzüglich daraufhin zu überprüfen, ob sie für

die bezeichneten Zwecke erforderlich sind; nicht erforderliche Daten sind zu löschen. Der Gesetzentwurf wird in der parlamentarischen Beratung weiterhin begleitet, wobei zu berücksichtigen ist, dass es sich bei Eurojust um eine europäische Einrichtung handelt und insoweit die nationalen Anliegen abzustimmen sind.

3. Datenschutz im Parlament

Im 3. TB (3.2) wurde auf das Problem eingegangen, ob der Datenschutz dem Informationsrecht der Abgeordneten im Wege steht. Im Zusammenhang mit der Beantwortung parlamentarischer Anfragen wurde dort dargelegt, dass aufgrund des Verfassungsrangs sowohl des Informations- und Kontrollrechts des Parlaments als auch des Rechts auf informationelle Selbstbestimmung letztendlich anhand des konkreten Einzelfalls eine Güterabwägung vorgenommen werden muss. Nicht automatisch hat der Datenschutz Vorrang vor dem Auskunftsrecht der Abgeordneten. Auch in diesem Berichtszeitraum wurden im Rahmen der Beantwortung Kleiner Anfragen wiederum datenschutzrechtliche Aspekte aufgeworfen.
Die Antwort auf eine Kleine Anfrage enthielt den Hinweis, dass Angaben zur Besoldungsstufe bzw. Vergütungsgruppe von Bediensteten aus datenschutzrechtlichen Gründen nicht aufgeführt werden könnten, da es sich hierbei um ein Merkmal handelt, aus dem auf die jeweilige Mitarbeiterin bzw. den Mitarbeiter geschlossen werden könne. Bei der Abwägung zwischen dem Informations- und Kontrollrecht des Parlaments und dem Recht auf informationelle Selbstbestimmung der Betroffenen war ausschlaggebend, dass die konkret Betroffenen nicht erkennbar sein durften, zumal dies für die Beantwortung der Frage auch nicht relevant war. Eine datenschutzgerechte Beantwortung hat der TLfD auch für möglich angesehen, indem ohne die jeweilige Besoldungsgruppe anzugeben z. B. ein Hinweis auf die Anzahl der Beschäftigten im höheren Dienst in einer konkreten Dienststelle oder die Anzahl Beschäftigter im gehobenen Dienst in einer konkreten Dienststelle erfolgt, was allerdings voraussetzt, dass dort mehrere Bedienstete in den betreffenden Laufbahnen beschäftigt sind.
Im Kreise der DSB wurde auch die Frage aufgeworfen, ob die Landtagsverwaltung bei der Veröffentlichung personenbezogener Daten in Landtagsdrucksachen im Rahmen der Beantwortung Kleiner Anfragen durch die Landesregierung ein eigenständiges Prüfungsrecht im Hinblick auf deren datenschutzrechtliche Zulässigkeit hat.

Aus meiner Sicht ist die Rechtslage in Thüringen eindeutig. Nach §§ 2 Abs. 5 und 37 Abs. 1 ThürDSG besteht keine Kontrollkompetenz des TLfD bezüglich der Veröffentlichung personenbezogener Daten in Landtagsdrucksachen. Zwar finden gemäß § 2 Abs. 5 die Bestimmungen des ThürDSG entsprechende Anwendung, die Einhaltung des Datenschutzes in Wahrnehmung parlamentarischer Aufgaben wird jedoch durch den Ältestenrat des Landtags kontrolliert.

Nach Art. 69 VerfThür i. V. m. § 40 Abs. 3 ThürDSG hat der TLfD dem Beratungsersuchen des Landtags nachzukommen und entsprechende Gutachten und Berichte zu fertigen. Gemäß Art. 67 VerfThür trägt die Landesregierung die Verantwortung für die Entscheidung bezüglich der Veröffentlichung der Antworten auf Anfragen aus dem parlamentarischen Bereich. Von Seiten der Landtagsverwaltung sind ggf. Hinweise und Empfehlungen im Vorfeld möglich, der Abwägungsprozess im Einzelfall obliegt jedoch der Landesregierung.

4. Medien/Telekommunikation

4.1 Neue Medienordnung/Thüringer Landesmediengesetz (ThürLMG)

Die Koordinierung zwischen Bund und Ländern zur Neuordnung des Mediendatenschutzes über die schon berichtet worden war (4. TB, 4.6) ist bislang noch nicht abgeschlossen.
Die Thüringer Landesregierung hat, den Entwicklungen im Rundfunk- und Medienbereich Rechnung tragend, das Thüringer Rundfunkgesetz durch das Erste Gesetz zur Änderung des Thüringer Rundfunkgesetzes vom 6. Januar 2003 (GVBl. S. 1 ff.) novelliert und in Thüringer Landesmediengesetz (ThürLMG) umbenannt. Modernisiert wurde in diesem Zusammenhang auch der Abschnitt Datenschutz §§ 56 ff. So ist § 56 um datenschutzrechtliche Grundsätze wie die Zweckbindung der erhobenen personenbezogenen Daten, die Datensparsamkeit, die informierte Einwilligung in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Möglichkeit einer elektronischen Einwilligung erweitert worden. Die Regelung der technisch- organisa-

torischen Maßnahmen im Bereich des privaten Rundfunks wurde um eine Verpflichtung der Veranstalter, dem Nutzer die anonyme bzw. pseudonyme Bezahlung von Angeboten, unter der Maßgabe der technischen Realisierbarkeit, zu ermöglichen, ergänzt. In diesem Zusammenhang wurde festgeschrieben, dass Nutzungsprofile nur bei Verwendung von Pseudonymen zulässig sind. Auch wurden differenzierte Regelungen zum Auskunftsrechts des Nutzers und die Möglichkeit des Datenschutz- Audit in das Gesetz aufgenommen.

4.2 Novellierung des Telekommunikationsgesetzes (TKG)

Im Rahmen der Neuregelung des TKG beabsichtigt die Bundesregierung die Umsetzung der Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2002 (ABl. EG L201 vom 31. Juli 2002 S. 27) und die Integration der Telekommunikations-Datenschutzverordnung (TDSV).
Ein Referentenentwurf von Anfang 2003 enthielt daneben eine Reihe datenschutzrechtlich bedenklicher Neuregelungen. So sollte die Verpflichtung der TK-Unternehmen, Angaben zu Überwachungsmaßnahmen an die RegTP zum Zwecke einer Jahresstatistik zu melden, entfallen. Des weiteren war, entgegen der bisherigen Regelung, die eine informierte Einwilligung des Telekommunikationskunden voraussetzt, nunmehr vorgesehen, eine Nutzung von Bestandsdaten der TK für andere Zwecke, bspw. Werbung, schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Außerdem sollten Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation (wie z. B. PINs) schützen, der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich gemacht werden dürfen. Bisher ist das nur im Falle bestimmter schwerer Straftaten möglich. Diese Absenkung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, würde dem Urteil des Bundesverfassungsgerichts vom 12. März 2003 widersprechen. Mit der Neuregelung sollen beim Verkauf von Handys mit wiederaufladbarer Karte Daten zur Identifikation des Käufers erfasst und in der Folge für einen Zugriff der Sicherheitsbehörden auf Vorrat gespeichert werden. Hierdurch würde der aus datenschutzrechtlicher Sicht erwünschte anonyme Zugang zum Mobilfunk versagt. Zudem ist zu erwarten, dass ein Großteil der gespeicherten Kundendaten nicht zweckdienlich nutzbar sein wird, da häufig der

Erwerber nicht mit dem tatsächlichen Nutzer eines Prepaid-Angebotes übereinstimmt.
Hiergegen sprachen sich die DSB des Bundes und der Länder in der Entschließung „Transparenz bei der Telefonüberwachung“ (Anlage 13) anlässlich ihrer Konferenz vom 27./28. März 2003 sowie in der Entschließung „Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation“ (Anlage 16) vom 28. April 2003 aus.
In meiner Stellungnahme zum Referentenentwurf vom 30. April 2003 gegenüber dem TMWAI habe ich mich dafür ausgesprochen, die Nutzung von TK- Diensten auch weiterhin ohne den Zwang einer Offenbarung nicht erforderlicher personenbezogener Daten zu gewährleisten und kritisiert, dass für die Abrechnung der Diensteanbieter untereinander weder eine Frist zur Speicherung der Daten noch ein Hinweis, diese nur so lange wie erforderlich zu speichern, vorgesehen ist. Weiterhin wurde angeregt, die Nutzung von Jokerzeichen im automatisierten Abrufverfahren auf Ausnahmefälle zu beschränken, da ansonsten eine massenhafte Offenbarung von Daten Unbeteiligter nicht auszuschließen ist. Zum Verhältnis von § 93 Abgabenordnung (AO) zu § 89 Abs. 6 TKG-alt, welches die kontrovers diskutierte Zulässigkeit von Auskunftsersuchen der Finanzämter bei TK-Anbietern betrifft, habe ich um Unterstützung bei einer Klarstellung im Rahmen der weiteren Novellierung des TKG gebeten.
Da im derzeitigen Gesetzesentwurf, mit Ausnahme der Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen, wesentliche datenschutzrechtliche Kritikpunkte nicht ausgeräumt wurden, und zudem weitere Verschlechterungen des Datenschutzniveaus beabsichtigt sind, hat sich die Konferenz der DSB des Bundes und der Länder in der Entschließung vom 21. November 2003 „Gravierende Verschlechterung des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes“ (Anlage 22) gegen datenschutzrechtlich bedenkliche Neuregelungen, insbesondere gegen die vorgesehene Berechtigung zur unverkürzten Speicherung aller Verkehrsdaten, einschließlich der Zielrufnummern, bis zu sechs Monaten ausgesprochen. Dies würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen.

5. Innenverwaltung - Kommunales - Sparkassen

5.1 Innenverwaltung

5.1.1 Thüringer Gesetz zur Änderung verwaltungsverfahrensrechtlicher und anderer Vorschriften

Nachdem auf Bundesebene das Verwaltungsverfahrensgesetz (4. TB, 5.1.5) geändert worden ist, liegt nun auch für Thüringen der Gesetzentwurf zur Änderung verwaltungsverfahrensrechtlicher und anderer Vorschriften dem Landtag zur Beratung vor, an dessen Erarbeitung der TLfD frühzeitig beteiligt war. Mit dem Gesetz sollen die Rechtsgrundlagen für die elektronische Kommunikation zwischen den Bürgern und der Verwaltung des Landes geschaffen werden. Vom TLfD wurde darauf hingewiesen, dass im Falle der elektronischen Kommunikation die Identifizierung der Personen des Signaturschlüsselinhabers auch bei Verwendung eines Pseudonyms möglich sein müsse. Diesen Bedenken ist durch die Bezugnahme auf das Signaturgesetz des Bundes Rechnung getragen worden. Aufgegriffen wurde in dem Entwurf auch meine Anregung, § 4 Abs. 3 ThürDSG um eine Regelung zu ergänzen, die auch dem elektronischen Rechtsverkehr Rechnung trägt, indem bei der elektronischen Form der Einwilligung nunmehr eine qualifizierte elektronische Signatur für den Regelfall gefordert wird. Mein Hinweis auf die nähere Erläuterung zu datenschutzrechtlichen Aspekten bei der elektronischen Kommunikation mit Gemeinderatsmitgliedern wurde ebenfalls übernommen. Das Gesetzgebungsverfahren wird seitens des TLfD weiter begleitet.

5.1.2 Gewährleistung des Datenschutzes bei Bürgerantrag, Volksbegehren und Volksentscheid

Am 31. Dezember 2003 ist das Gesetz zur Änderung des Thüringer Gesetzes über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid und des Thüringer Verfassungsgerichtshofsgesetzes vom 4. Dezember 2003 (GVBl. S. 505) in Kraft getreten.
Zum Ende des letzten Berichtszeitraumes hatte die Landesregierung Gesetzentwürfe zur Änderung der Verfassung des Freistaats Thüringen sowie zur Änderung des Thüringer Gesetzes über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid (ThürBVVG) vorgelegt. Inhalt der Neuregelungen war insbesondere die Verringe-

rung des geforderten Unterstützungsquorums für den Antrag auf Zulassung eines Volksbegehrens mit der Maßgabe, dass künftig nur noch Amtssammlungen durchgeführt werden sollten. In diesem Zusammenhang war auch beabsichtigt, die bisherige Sammlung der Unterschriften je Unterzeichner auf einem gesonderten Bogen durch eine Listensammlung zu ersetzen. Diese Verfahrensänderung stieß auf datenschutzrechtliche Bedenken, da durch die Verwendung von Listen alle jeweils nachfolgenden Unterzeichner die Möglichkeit erhalten würden, Kenntnis davon zu nehmen, welche Personen unter Angabe der Vor- und Familiennamen, Anschriften und Geburtsdaten sich bereits in die Liste eingetragen haben und somit das Anliegen unterstützen. Unter Hinweis darauf, dass es sich bei politischen Meinungsäußerungen um sensible und gemäß § 4 Abs. 5 ThürDSG besonders schützenswerte Daten handelt, wurde empfohlen, von Listensammlungen abzusehen und weiterhin die Unterschriften auf Einzelbögen zu erfassen. Zur Begründung verwies ich u. a. auf die entsprechenden Regelungen in der Landeswahlordnung, wonach die Unterstützungsunterschriftensammlungen für Wahlkreisvorschläge nur auf Formblättern vorgenommen werden dürfen, die eine einzige Unterstützungsunterschrift enthalten. Die Notwendigkeit für die Verwendung von Einzelbögen ergibt sich im Besonderen aus der strengen und strafbewehrten Zweckbindung der Daten (§ 30 ThürBVVG), nach der sich jegliche Übermittlung von Daten an Privatpersonen verbietet. Da nach § 9 ThürDSG öffentliche Stellen verpflichtet sind, durch technische und organisatorische Maßnahmen eine Kenntnisnahme der personenbezogenen Daten durch unbefugte Dritte zu verhindern, ist faktisch einer Nutzung von Sammellisten durch öffentliche Stellen unmöglich.
Im Ergebnis wurde zunächst in den Gesetzentwurf eine Formulierung aufgenommen, wonach die Eintragenden, wenn sie das Volksbegehren unterstützen wollten, darin einwilligen müssen, dass ihre Daten von den an Zielen des Bürgerantrags/Bürgerbegehren interessierten Personen eingesehen werden können. Diese Regelung war aus datenschutzrechtlicher Sicht nicht akzeptabel, da fraglich ist, inwieweit hierbei eine freie „Willensentscheidung“ der Unterzeichner gegeben ist, wenn der Betroffene bei einer Nichteinwilligung sein verfassungsmäßiges Recht auf Mitgestaltung des politischen Lebens (Art. 9 der Thüringer Verfassung) nicht wahrnehmen kann. Offen blieb auch, welches dem informationellen Selbstbestimmungsrecht überwiegende öffentliche Interesse die Notwendigkeit der Sammlung in Listenform statt auf Einzelbögen begründet, zumal Einzelbögen nicht nur „datenschutzfreundlicher“ (keine Einsichtnahme durch nachfolgende Unterzeich-

ner, zeitliche Verkürzung der Möglichkeit für eine Kenntnisnahme der Unterschriftsleistung durch Dritte), sondern durchaus auch „bürgerfreundlicher“ (statt überwachter zeitaufwendiger Listeneintragung erfolgt nur eine Identitätsprüfung bei der Einzelbogenabgabe) sein dürfte.
In der parlamentarischen Beratung wurden alle datenschutzrechtlichen Hinweise berücksichtigt. So wurden bspw. auch im ThürBVVG die Bestimmungen zur Zweckbindung der Daten im Hinblick auf die neuen Begriffsbestimmungen im ThürDSG präzisiert.

5.1.3 Ungenügende Datensicherheitsvorkehrungen beim Umgang mit personenbezogenen Daten

Presseveröffentlichungen Mitte Oktober 2002 waren Anlass, das TIM um Auskunft zu bitten, ob unzulässigerweise personenbezogene Daten übermittelt worden sind.

Der damalige Innenminister erklärte im Rahmen einer Sondersitzung des Thüringer Landtags Ende Oktober, dass ein Datenträger derzeit nicht auffindbar sei.
Infolge dessen teilte der TLfD dem TIM mit, dass gemäß § 9 ThürDSG die öffentlichen Stellen verpflichtet sind, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, den Schutz personenbezogener Daten zu gewährleisten.
Mit der erklärten Nichtauffindbarkeit wurden nach § 9 Abs. 2 ThürDSG die erforderliche Vertraulichkeit, die Verfügbarkeit und insbesondere die Revisionsfähigkeit und Transparenz der Datenverarbeitung für nicht gewährleistet angesehen.
Diese Verletzung datenschutzrechtlicher Vorschriften wurde gemäß § 39 ThürDSG beanstandet. Für Datenträger, die besonderen Geheimschutzvorschriften unterliegen, müssen besondere Sicherheitsvorkehrungen durch die Daten verarbeitende Stelle getroffen werden. In der Stellungnahme des TIM wurde darauf verwiesen, dass die zuständigen Stellen im TIM nochmals belehrt und auf die Bestimmungen der Verschlusssachenanweisung hingewiesen worden sind.

5.1.4 Verarbeitung personenbezogener Daten im Verfahren LaDiVA in Auftragsdatenverarbeitung im ZIV

Im 3. TB (5.1.5) hatte ich über Kontrollen im Bereich des Ausländerwesens insbesondere der automatisierten Datenverarbeitung im Rahmen des Verfahrens LaDiVA (Landeseinheitliches Dialogverfahren Ausländerwesen) in Auftragsdatenverarbeitung auf der Grundlage von Nutzungsverträgen zwischen den jeweiligen Kommunen und dem TLRZ berichtet. Da das Programmsystem auf dem Großrechner im ZIV (Zentrum für Informationsverarbeitung der Thüringer Landesverwaltung), das zum Bereich der Oberfinanzdirektion Erfurt gehört, abgearbeitet wird, wurde im Berichtszeitraum auch dort eine Kontrolle durchgeführt. Ziel der Kontrolle war eine datenschutzkonforme Gestaltung der Verträge zwischen dem TLRZ und den Kommunen bzw. dem ZIV. Desweiteren sollten die vom ZIV ergriffenen technischen und organisatorischen Maßnahmen zur Absicherung des Verfahrens LaDiVA im Hinblick auf die eingesetzte Betriebsumgebung geprüft werden.
Das Verfahren LaDiVA ist eine Client-Server-Anwendung. Das ZIV stellt dazu im Rahmen des Unterauftragsverhältnisses mit dem TLRZ die rechentechnischen Ressourcen (Speicher- und Verarbeitungskapazität) als Server zur Verfügung. Die Ausländerbehörden rufen mit ihren Client (PC) über ein spezielles Verbindungsprogramm direkt, d. h. ohne Zugangskontrolle auf der Betriebssystemebene, die Anwendung LaDiVA auf dem Großrechner im ZIV auf. Nach einer Berechtigungsprüfung der zugreifenden Nutzer durch LaDiVA können diese auf ihre hier gespeicherten Daten zugreifen und die Sachbearbeitung vornehmen. Die anwendungstechnische Betreuung und die Benutzerverwaltung einschließlich der Rechtevergabe für das Verfahren LaDiVA wird durch die Anwendungsbetreuer des TLRZ im Auftrag der jeweiligen Kommune nach deren Vorgaben wahrgenommen. Im Hinblick auf die Einbindung des Verfahrens LaDiVA auf den Großrechner kann zwischen privilegierten Benutzern mit Zugang auf das Betriebssystem (Systemadministratoren, Auditoren, Bediener, Systemprogrammierer, LaDiVA-Administratoren) und Benutzern ohne Betriebssystemzugang (Endanwender-LaDiVA) unterschieden werden. Da die Sicherheitsmechanismen des eingesetzten Rechnerbetriebssystems keinen ausreichenden Schutz für die eingesetzten Anwendungen und deren zu verarbeitenden Daten bieten, wird vom ZIV zusätzlich ein leistungsfähiges Sicherheitssystem eingesetzt. Dieses übernimmt u. a. auf Betriebssystemebene die Zugangs- und Zugriffs-

kontrolle der Benutzer sowie die Protokollierung der Zugriffe und auftretender sicherheitstechnischer Ereignisse. Auch die Dateizugriffsrechte auf der Betriebssystemebene werden mit diesem Sicherheitsprogramm verwaltet und kontrolliert.
Der Rechner verfügt über einen Fernwartungsanschluss zur Hardware-Diagnose und für eine eventuelle Einleitung von Fehlerbehebungsmaßnahmen.
Bereits im vorangegangenen Tätigkeitsbericht war gefordert worden, dass die Nutzungsverträge zwischen TLRZ und den kommunalen Nutzern zu überarbeiten sind. Auch die Vereinbarung zwischen TLRZ und ZIV, das datenschutzrechtlich ein Unterauftragsverhältnis darstellt, musste entsprechend überarbeitet werden. Insbesondere gaben die Vereinbarungen zwischen den Ausländerbehörden und dem TLRZ bislang keinen Raum für das Unterauftragsverhältnis mit dem ZIV. Ausgehend von dem Gesetzestext (§ 8 ThürDSG) sind jeweils die Auftraggeber und damit die kommunalen Stellen verantwortlich für die Festlegungen insbesondere der technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes. Dies greift auch auf eventuelle Unterauftragsverhältnisse durch, die der Auftragnehmer befugt ist, einzugehen. Infolge der Forderungen des TLfD im Ergebnis der Kontrolle wurden die Verträge zwischen Ausländerbehörden und TLRZ sowie die Vereinbarung zwischen TLRZ und ZIV weitestgehend den datenschutzrechtlichen Forderungen entsprechend überarbeitet. Konkrete Maßnahmen nach § 9 ThürDSG im TLRZ sowie die Regelung zur Zulässigkeit weiterer Unterauftragsverhältnisse werden nach Mitteilung des TLRZ bei künftigen Vertragsergänzungen Berücksichtigung finden.
Für einen datenschutzkonformen Betrieb des Verfahrens LaDiVA auf dem Großrechner ist die Einbettung des Verfahrens in eine gesicherte, vor unbefugtem Zugriff abgeschottete Umgebung erforderlich. Insbesondere der Zugang über das Betriebssystem ist abzusichern, wobei auch die Zugriffsrechte privilegierter Systemnutzer auf das erforderliche Maß einzuschränken sind. Durch die eingesetzten technischen und organisatorischen Maßnahmen wird dies umgesetzt. Als ergänzende Maßnahme für die regelmäßig durchgeführten Kontrollen auf sicherheitsrelevante Vorkommnisse wurde gefordert, auch die in der Sicherheitssoftware eingestellten Zugriffsrechte anhand der legitimierten Vorgaben in die Kontrolle mit einzubeziehen, um auf diese Weise unzulässige oder zu weit reichende Rechte festzustellen. Die Forderung wurde erfüllt.

Da zur Kontrolle der Ablauf der Fernwartung, insbesondere die ergriffenen Sicherheitsmaßnahmen sowie der Umfang der Zugriffe des Auftragsnehmers bei der Einleitung von Fehlerbehebungsmaßnahmen, nicht ausreichend dargelegt werden konnten, wurde das ZIV gebeten, kurzfristig die diesbezüglichen Informationen nachzureichen und die Verfahrensweise der Fernwartung nachvollziehbar zu dokumentieren. Seitens des ZIV wurde dem nachgekommen.

5.1.5 Besucherdaten in Gemeinschaftsunterkünften/ Kontrollen

Den mit der Verarbeitung personenbezogener Daten von Besuchern in Gemeinschaftsunterkünften verbundenen datenschutzrechtlichen Fragen bin ich, wie im 4. TB (5.1.9) angekündigt, im Berichtszeitraum weiter nachgegangen. In den kontrollierten Fällen erfolgte die Verarbeitung personenbezogener Daten von Besuchern durch private Wachfirmen als Auftragsdatenverarbeitung und wurde mit erhöhtem Sicherheitsbedarf oder der Sicherstellung, dass die Besucher die Gemeinschaftsunterkunft auch wieder verlassen, begründet. Ein Träger einer betroffenen Gemeinschaftsunterkunft hatte sich auf den Standpunkt gestellt, durch die Beauftragung eines Privaten zum Betrieb der Gemeinschaftsunterkunft und zur Bewachung sei dieser auch für die Zulässigkeit der Verarbeitung und Nutzung personenbezogener Daten verantwortlich. Ein Blick in § 8 ThürDSG stellt allerdings klar, dass der Auftraggeber weiterhin verantwortlich bleibt und die erforderlichen Vorgaben, insbesondere aber auch die technischen und organisatorischen Maßnahmen in der Vereinbarung zur Auftragsdatenverarbeitung festzulegen hat. Soweit es zulässig war, personenbezogene Daten zu verarbeiten, waren darüber hinaus angemessene Aufbewahrungsfristen festzulegen. Die nicht den Anforderungen des § 8 ThürDSG entsprechenden Vereinbarungen wurden den Forderungen und Empfehlungen des TLfD folgend geändert. Ausweise von Besuchern werden nicht mehr einbehalten, es werden wenige erforderliche personenbezogene Daten im Besucherbuch festgehalten, die nach kurzen Aufbewahrungsfristen gelöscht werden. Die Besucher werden über den Zweck der Verarbeitung ihrer Daten entsprechend informiert.
Im Rahmen der durchgeführten Kontrollen wurden auch andere datenschutzrechtliche Probleme festgestellt.
In einer Einrichtung standen für die Bewohner keine Briefkästen oder Brieffächer zur Verfügung. Daher mussten sich die Bewohner zur Aushändigung ihrer Post bei der Heimleitung melden, die vom Post-

boten alle eingehenden Sendungen entgegennahm. Zu diesem Zweck wurde eine täglich aktualisierte Liste der Namen von Bewohnern ausgehängt, die Post abholen können. Briefe von Behörden oder Anwälten wurden sogar in ein eigens hierfür geführtes Postbuch eingetragen und nur gegen Unterschrift ausgehändigt. Diese Vorgehensweise sah man als erforderlich an, um eventuelle Rückfragen von Absendern beantworten zu können. Dies war weder durch den Betreibervertrag gedeckt noch rechtlich zulässig, da es weder die Aufgabe der Heimleitung ist, den Eingang nicht eingeschriebener Postsendungen an Bewohner zu dokumentieren noch auf Nachfragen von Absendern zu bestätigen. Nachdem es nach der Mitteilung des kommunalen Trägers nicht möglich ist, für die Bewohner jeweils eigene Briefkästen bereitzustellen, hielt ich es für akzeptabel, dass die Bewohner bei Aufnahme die Möglichkeit erhalten, entweder darin einzuwilligen, dass sie per Aushang über eingegangene Post informiert werden oder regelmäßig entsprechend nachfragen. Die Praxis, nicht eingeschriebene Behörden- oder Anwaltsschreiben in das Postbuch einzutragen, wurde aufgegeben.

Darüber hinaus wurde bei Aufnahme eines Bewohners ein Hausausweis gefertigt, den dieser bei der Wache zu hinterlegen hatte und nur bei Verlassen der Einrichtung ausgehändigt bekam. Als Zweck wurde angegeben, die Hausausweise dienten der Übersicht, welche Personen anwesend seien. Da aber die Einhaltung der Bestimmung in der Praxis nur teilweise erfolgte, war diese Verfahrensweise ungeeignet und wurde in der Folge aufgegeben. Gleichzeitig war bei der Wache auch die Kopie der Aufenthaltserlaubnisse der Betroffenen hinterlegt, die bei endgültigem Verlassen der Einrichtung auszusondern war. Dies sollte gegebenenfalls die Feststellung der Identität eines Bewohners durch das Wachpersonal erleichtern. Aufenthaltserlaubnisse enthalten aber personenbezogene Daten, die für die Aufgabenerfüllung des Objektschutzes nicht erforderlich waren. Die Kopien waren daher zu vernichten.

Im Rahmen einer Kontrolle wurde seitens der anderen kontrollierten Stelle auch die Gelegenheit genutzt, Empfehlungen des TLfD in die vorgesehene Installation einer Videoüberwachung des Eingangsbereichs einer Gemeinschaftseinrichtung einzubeziehen. Da nicht beabsichtigt war, das Kommen und Gehen von Bewohnern und Besuchern aufzuzeichnen, musste lediglich sichergestellt werden, dass der unmittelbar angrenzende öffentliche Verkehrsraum nicht erfasst wurde und damit gänzlich unbeteiligte Passanten durch die Videokameras auch

nicht auf die Monitore übertragen werden. Der Hinweis für die Betroffenen auf die Videoüberwachung wurde ebenfalls vorgenommen.

5.2 Kommunales

5.2.1 Neuregelungen im Melderecht

Am 3. April 2002 wurde das Gesetz zur Änderung des Melderechtsrahmengesetzes und anderer Gesetze vom 25. März 2002 (BGBl. I, S. 1343) in Kraft gesetzt. Es enthält umfassende Änderungen zum Umgang mit Meldedaten, insbesondere im Hinblick auf die Nutzung moderner Informations- und Kommunikationstechnologien. Danach wird es künftig nach Maßgabe des Landesrechts erlaubt sein, auch auf dem Weg des automatisierten Abrufs über das Internet Auskünfte an öffentliche und nicht öffentliche Stellen zu erteilen. Als Voraussetzung dafür sind geeignete Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, insbesondere zur Gewährleistung der Vertraulichkeit und Unversehrtheit der Meldedaten. Als technische Möglichkeiten stehen dafür vor allem moderne Verschlüsselungsverfahren sowie die qualifizierte elektronische Signatur nach dem Signaturgesetz zur Verfügung.
Bei der Novellierung des Gesetzes wurde die Forderung der DSB, dass die einfache Melderegisterauskunft an private Stellen über das Internet von der ausdrücklichen Einwilligung der Betroffenen abhängig gemacht werden sollte, nicht erfüllt. Statt dessen sieht das Gesetz nunmehr ein Widerspruchsrecht der Betroffenen vor. Keine Berücksichtigung fand gleichfalls die Forderung der DSB, die bestehende Widerspruchslösung für Melderegisterauskünfte an politische Parteien zu Wahlwerbezwecken dahingehend zu ändern, dass dies nur noch erlaubt wird, wenn der Betroffene dies wünscht.
Abgeschafft wurde die bisher normierte Nebenmeldepflicht des Wohnungsgebers. Statt dessen wurde jedoch eine Regelung aufgenommen, die es künftig erlaubt, den Eigentümern von Wohnungen bzw. den Wohnungsgebern die Namen der in seiner Wohnung gemeldeten Einwohner mitzuteilen. Voraussetzung hierfür ist die Glaubhaftmachung eines rechtlichen Interesses an der Kenntnis der Bewohnerdaten. Mit dieser Regelung wurde insbesondere einer häufig geäußerten Bitte von Eigentümern entsprochen, die bei der Durchsetzung ihrer Rechtsansprüche (z. B. im Rahmen der Umlegung von Müllgebühren bei der Betriebskostenabrechnung) von den Meldebehörden keine Gruppenauskünfte über die bei ihnen gemeldeten Personen erhielten.

Die vorgenannten Regelungen gelten derzeit in Thüringen noch nicht, da die Länder verpflichtet sind, innerhalb von zwei Jahren nach Inkrafttreten des geänderten Melderechtsrahmengesetzes ihr Melderecht den geänderten und neuen Vorschriften des Melderechtsrahmengesetzes anzupassen.

5.2.2 Umsetzung der Ersten Thüringer Meldedatenübermittlungsverordnung

Bereits im 4. TB (15.9) hatte ich darüber berichtet, dass aufgrund der Zentralisierung der automatisierten Datenverarbeitung der Landesverwaltung im ZIV die nach der Ersten Thüringer Meldedatenübermittlungsverordnung dem TLRZ übertragene Aufgabe der Verarbeitung von Meldedaten im Rahmen einer Auftragsdatenverarbeitung künftig vom ZIV wahrgenommen wird. Die hierzu bereits im letzten Berichtszeitraum im TLRZ vorgenommene Kontrolle wurde deshalb auf die Verarbeitung der Meldedaten im ZIV ausgedehnt. Hierbei wurden keine datenschutzrechtlichen Verstöße bei der praktischen Umsetzung der Ersten Thüringer Meldedatenübermittlungsverordnung festgestellt. Es erfolgten Hinweise, da die Programmdokumentationen teilweise unvollständig sind bzw. nicht dem aktuellen Stand entsprechen. Dies betrifft auch die Unterlagen zum polizeilichen Abrufverfahren. Das TLRZ wurde deshalb aufgefordert, die betreffenden Unterlagen zu überarbeiten und dafür Sorge zu tragen, dass die am Verfahren Beteiligten vollständige Unterlagen und Anweisungen zum Umgang mit den Meldedaten erhalten. Die Realisierung dieser Forderungen ist seitens des TLRZ für die nächsten Wochen angekündigt.

5.2.3 Wer zählt in Thüringen zu den Alters- und Ehejubilaren

Im vorangegangenen 4. TB (5.2.5) wurde darüber berichtet, dass mit dem Ersten Gesetz zur Änderung des Thüringer Meldegesetzes vom 21. November 2001 die (aus datenschutzrechtlicher Sicht umstrittene) Widerspruchslösung für die Auskunftserteilung über Alters- und Ehejubiläen an parlamentarische Körperschaften, die Presse und den Rundfunk eine Präzisierung erfahren hat. Der Landtag hatte, anderen Ländern folgend, die im Gesetz als Jubiläen bezeichneten Geburtstage über die die Öffentlichkeit informiert werden kann, solange der Betroffene nicht ausdrücklich widerspricht, im Meldegesetz konkret festgelegt (65., 70., 75., 80., 85., 90. und jeder spätere Geburtstag).

Bis zu diesem Zeitpunkt gab es lediglich in der amtlichen Begründung zum Thüringer Meldegesetz eine Anmerkung, wonach man bei Altersjubiläen vom 70. Geburtstag, bei Ehejubiläen mit der Goldenen Hochzeit beginnen könne. Obwohl aus datenschutzrechtlicher Sicht, wie auch Beschwerden Betroffener zeigten, eine Widerspruchslösung gegenüber einer Einwilligungslösung stets nur die zweitbeste ist, konnten durch diese Präzisierung der Jubiläen zumindest unterschiedliche Interpretationen und Missverständnisse bei den Beteiligten ausgeschlossen werden.
Im Rahmen der Änderung des Gesetzes zur Änderung der Thüringer Kommunalordnung und anderer Gesetze wurde eine Änderung des Thüringer Meldegesetzes (GVBl. 2002, S. 479) aufgenommen, wonach künftig der 65. und jeder nachfolgende Geburtstag als Jubiläum gilt. Ehejubilare sind nunmehr Einwohner, die die Goldene Hochzeit oder ein späteres Ehejubiläum begehen.

5.2.4 Einwohnermeldelisten für Gebührenbeauftragte

Im Berichtszeitraum gab es Anfragen von Meldeämtern, inwieweit Auskunftsverlangen des MDR zur Wahrung des Rundfunkgebühreneinzugs Rechnung zu tragen ist.
Im Rahmen eines Gesprächstermins mit den Verantwortlichen des MDR wurden deshalb die jeweiligen Rechtsstandpunkte ausgetauscht mit dem Ziel, eine datenschutzgerechte Verfahrensweise, die der Durchsetzung der Rundfunkgebührenpflicht und -gebührengerechtigkeit unter weitestgehender Gewährleistung des informationellen Selbstbestimmungsrechts der Bürger Rechnung trägt, in Anwendung zu bringen. Hierbei wurde festgestellt, dass die Rechtsauffassungen zur Auslegung der melderechtlichen Bestimmungen im Hinblick auf die Datenübermittlungen in den wesentlichen Punkten übereinstimmten. Bei der praktischen Durchführung mangelte es mitunter an notwendigen Informationen über Auswahlkriterien für die Auskunftsersuchen. Man verständigte sich deshalb darauf, dass den gesetzlichen Voraussetzungen für die gewünschten Gruppenauskünfte entsprechend hinreichende Anhaltspunkte dafür vorliegen müssen, dass bei dem ausgewählten Personenkreis eine unverhältnismäßig hohe Anzahl von Personen ihrer Gebührenpflicht nicht nachkommt. Betroffen können einzelne Wohnhäuser, Straßenzüge oder Wohngebiete, wie auch Ortsteile oder ganze Gemeinden sein. Eine Beschränkung auf Personen ab dem 18. Lebensjahr ist dabei vom Gesetzgeber nicht vorgesehen. Um ihr gesetzlich vorgesehenes Ermessen ausüben zu können,

sind den Gemeinden bei Datenanforderungen insbesondere die Gründe zur Gebietsauswahl durch Angaben über die derzeitige Rundfunkteilnehmerdichte mit Vergleichs- und Durchschnittswerten darzulegen. Hierzu hat der MDR ein Musteranschreiben an die Gemeinden zur Bereitstellung von Einwohnermeldelisten erarbeitet, in dem auch ein Hinweis auf die vorgesehene Speicherdauer beim MDR enthalten ist (maximal 1 Jahr).
Im Hinblick auf den angeforderten Datenumfang ist zu berücksichtigen, dass aus technischen Gründen dem MDR die Rundfunkteilnehmerdichte nicht für jede gewünschte territoriale Einheit zur Verfügung steht. Während eine Eingrenzung des Gebietes in größeren Städten i. d. R. unproblematisch ist, stehen häufig bei kleineren Gemeinden oder Verwaltungsgemeinschaften EDV-technisch begründet keine entsprechenden Vergleichswerte zur Verfügung, sodass auch weiterhin bei einer fehlenden Datenbasis eine Überprüfung der gesamten Gemeinde erforderlich ist.
Im Gespräch mit dem MDR verständigte man sich deshalb darauf, dass das Thüringer Landesverwaltungsamt als oberste Aufsichtsbehörde für die Meldebehörden zum Zwecke der Transparenz jährlich über die erfolgten Auskunftsersuchen vom MDR unterrichtet wird.

5.2.5 „Private Beauftragung“ eines Mitarbeiters eines Meldeamtes zur Übermittlung von Meldedaten an eine Bundesbehörde

Im Rahmen meiner Beratungsaufgaben wandte sich der Bürgermeister einer Gemeinde an mich mit der Bitte um eine datenschutzrechtliche Prüfung in nachfolgender Angelegenheit:
Eine Bundesanstalt hatte zur Durchführung eines Forschungsvorhabens beabsichtigt, die Anschriften bzw. Sterbedaten von Einwohnern einer Gemeinde auf der Grundlage eines privaten Honorarvertrags durch einen Mitarbeiter des Meldeamtes zu erheben. Ein offizielles, ordnungsgemäßes und begründetes schriftliches Auskunftsersuchen der Bundesanstalt war jedoch zu keinem Zeitpunkt an die Stadt gerichtet worden. Die Daten sollten lediglich im Ergebnis eines Telefonates von einem Mitarbeiter des Meldeamtes laut Vertrag aus dem Melderegister entnommen werden.
Ungeachtet der Tatsache, dass es die originäre Aufgabe von Meldebehörden ist, durch die unentgeltliche Bereitstellung von Meldedaten öffentliche Stellen bei der Erfüllung ihrer Aufgaben zu unterstützen, wurde bei dieser Verfahrensweise offensichtlich verkannt, dass allein

die Meldebehörde als Daten verarbeitende Stelle über die Zulässigkeit von Datenübermittlungen nach pflichtgemäßem Ermessen entscheidet. Insoweit war es dem Mitarbeiter als Privatperson unter den im Vertrag genannten Bedingungen eigentlich nicht möglich den Vertrag zu erfüllen, da er versichern sollte, dass er berechtigt sei über sämtliche Daten zu verfügen und dem Auftraggeber das Recht einräumen sollte, über die weitere Nutzung der bereitgestellten Daten allein zu befinden.
Ob und inwieweit eine öffentliche Stelle zur Erfüllung ihrer Aufgaben im Rahmen einer Auftragsdatenverarbeitung Personen oder Stellen mit der Erhebung von Daten beauftragt, bleibt, soweit keine gesetzliche Bestimmungen dem entgegenstehen, ihr überlassen. Die Entscheidungen, wann, in welchem Umfang und in welcher Form Daten übermittelt werden, trifft ausschließlich die Daten verarbeitende Stelle. Über die im Melderegister gespeicherten Daten verfügt auch nur die Meldebehörde, nicht aber auf privatrechtlicher Basis die dort beschäftigten Mitarbeiter.
Dies wurde der Gemeinde mitgeteilt, die den Vorgang in entsprechender Weise auswertete. Gleichzeitig wurde darüber auch der Bundesbeauftragte für den Datenschutz informiert, der in besagter Angelegenheit mit der Bundesanstalt Kontakt aufnahm.
In einer Stellungnahme wurde von der betreffenden Bundesanstalt erklärt, dass die kritisierte Verfahrensweise nur deshalb in Betracht gezogen worden war, weil ansonsten bei fehlenden Daten der Fortgang des Forschungsprojektes gefährdet gewesen wäre. Auf mündliche Anfrage im Meldeamt hatte der Mitarbeiter des Meldeamtes erklärt, dass eine Bearbeitung der angeforderten Daten aus personellen Gründen nicht innerhalb der regulären Arbeitszeit sondern nur durch eine entgeltliche Tätigkeit des Mitarbeiters im Amt außerhalb der Arbeitszeit möglich wäre. Von diesem Angebot habe man im Interesse des Forschungsvorhabens ausnahmsweise Gebrauch gemacht. Um rechtliche Bedenken auszuräumen, habe man den Vertrag an die dienstliche Anschrift des Mitarbeiters gesandt, damit zumindest sichergestellt wäre, dass die Angelegenheit den „üblichen“ Dienstweg der Verwaltung nimmt.
Meine Argumente und datenschutzrechtlichen Bedenken wurden von der Bundesanstalt im Ergebnis einer nochmaligen Prüfung der Vorgehensweise uneingeschränkt akzeptiert mit der Folge, dass das Vertragsangebot unverzüglich zurückgezogen und direkt der Kontakt mit der Gemeinde zur Erörterung der Möglichkeiten zur Datenbereitstellung aufgenommen wurde.

5.2.6 Meldedatenübermittlung an Wohnungsgesellschaften

Um dem teilweise sehr deutlichen Rückgang der Einwohnerzahl und dem damit verbundenen hohen Leerstand von Wohnungen entgegensteuern zu können, besteht auch seitens der kommunalen Wohnungsunternehmen für Analysezwecke ein nachhaltiges Interesse an Einwohner- und Mieterdaten. Um dieses Informationsbedürfnis zu befriedigen, treten mitunter Wohnungsunternehmen an die Meldeämter mit der Bitte heran, ihnen entsprechendes Datenmaterial zur Verfügung zu stellen. Dass hierbei nicht nur statistisches Material gefragt ist, zeigte z. B. das Auskunftsersuchen eines kommunalen Wohnungsunternehmens, welches vom Meldeamt unter Hinweis auf das öffentliche/städtische Interesse eine Liste über die Namen, das jeweilige Geburtsjahr, die Staatsbürgerschaft aller Bewohnern ihrer Häuser erbat.
Aufgrund berechtigter Zweifel der Verwaltung wurde ich hierzu um eine datenschutzrechtliche Bewertung gebeten. In meiner Stellungnahme habe ich der Stadtverwaltung mitgeteilt, dass das Unternehmen, obwohl es nach dem Thüringer Datenschutzgesetz zu den öffentlich-rechtlichen Wettbewerbsunternehmen zählt, im Sinne des Thüringer Meldegesetzes eine nicht öffentliche Stelle ist. Melderegisterauskünfte über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) an nicht öffentliche Stellen sind nach § 32 Abs. 3 Thüringer Meldegesetz nur zulässig, soweit sie im öffentlichen Interesse liegen. Das ist im vorliegenden Fall aber nicht gegeben. Hierzu heißt es in der amtlichen Begründung zum Thüringer Meldegesetz: Unter öffentlichem Interesse ist ein Interesse der Allgemeinheit zu verstehen. Rein oder überwiegend kommerzielles Interesse werde diesen Anspruch nicht erfüllen. Auch Unternehmen der Markt-, Meinungs- und Sozialforschung dürfen Gruppenauskünfte nur erteilt werden, wenn sie im öffentlichen Interesse liegen. Durch eine Vereinbarung der Länder wurde die Verfahrensweise einheitlich geregelt. Danach dürfen die Auskünfte nur erteilt werden, wenn der Beauftragte des Unternehmens eine gültige Unbedenklichkeitsbescheinigung vorlegt, die vom Innenministerium des Landes ausgestellt ist.
In diesem Zusammenhang sei darauf hingewiesen, dass es in absehbarer Zeit (nach ihrer Umsetzung in Landesrecht innerhalb der nächsten zwei Jahre) eine weitere Spezialregelung für „Gruppenauskünfte“ geben wird. Mit der Novellierung des Melderechtsrahmengesetzes im Jahr 2002 wurde eine Neuregelung aufgenommen, nach der die Eigentümer einer Wohnung bzw. der Wohnungsgeber bei der Glaubhaftmachung eines rechtlichen Interesses (z. B. im Rahmen der Aufschlüsse-

lung von Müllgebühren) Auskunft über die Vor- und Familiennamen sowie Doktorgrade der in seinen Wohnungen gemeldeten Einwohnern erhalten werden.
Diese Neuregelungen werden aber auf das beispielhaft genannte Auskunftsbegehren von Wohnungsunternehmen nach Meldedaten für Zwecke der Markt- und Bedarfsforschung auch künftig keine Auswirkungen haben. Hier bleibt den Wohnungsunternehmen wie bisher, als einzige Möglichkeit der Datenerhebung, die Mieter zur freiwilligen Mitwirkung zu gewinnen. Ebenso wie jedes private Unternehmen kann auch eine kommunale Wohnungsgesellschaft ihre Mieter auf freiwilliger Grundlage um Auskünfte bitten. Dabei ist zu gewährleisten, dass die Mieter ausdrücklich auf die Freiwilligkeit und die Zweckbestimmung der Daten hingewiesen werden und durch geeignete Maßnahmen die alsbaldige Anonymisierung der Daten erfolgt. Bei der Beurteilung des Datenumfangs sind die datenschutzrechtlichen Grundsätze insbesondere hinsichtlich der Erforderlichkeit zu beachten. Insoweit wurde bei der beabsichtigten Datenerhebung durch das Wohnungsunternehmen die Notwendigkeit und Zweckmäßigkeit für die Erhebung des konkreten Geburtsjahres (statt Altersgruppen) und der Staatsangehörigkeit allein für Analysezwecke bezweifelt. Ein Erfordernis für die Kenntnis des Alters oder der Staatsangehörigkeit von Mietern für eine ordnungsgemäße Verwaltung kommunaler Wohnungen dürfte in jedem Fall nicht gegeben sein.
Aufgrund der obigen datenschutzrechtlichen Bewertung wurde von der Übermittlung von Einzeldatensätzen an das Wohnungsunternehmen abgesehen und statt dessen auf bestimmte Wohngebiete bezogene Altersstatistiken bereitgestellt.

5.2.7 Datenerhebungen zur Ermittlung von Fahrzeugführern

Auch im Berichtszeitraum erreichten den TLfD erneut Anfragen zur Fahrerermittlung bei Verkehrsordnungswidrigkeiten. In einem Fall, in dem sich sowohl die Betroffene wie auch die Presse an den TLfD wandten, war ein Fahrzeug vom Ordnungsamt einer Stadtverwaltung beim zu schnellen Fahren „geblitzt“ worden. Da der vom Kfz-Bundesamt ermittelte Halter auf den Zeugenfragebogen nicht antwortete und der Halter eindeutig nicht der Fahrer sein konnte, weil es sich beim Fahrzeugführer um eine Frau handelte, wurden weitere Ermittlungen aufgenommen. Zu diesem Zweck wurden zunächst die Mitarbeiter der Meldebehörde unter Vorlage des Fahrerfotos nach einer

möglichen Identität der Fahrerin befragt. Hierbei ergab es sich, dass eine Mitarbeiterin der Meldebehörde glaubte, eine bestimmte Einwohnerin auf dem Foto erkennen zu können. Nach erfolgten Bildabgleich mit dem Personalausweisfoto im Meldeamt wurde die betreffende Person „mit hoher Wahrscheinlichkeit“ als die Gesuchte der Bußgeldstelle mitgeteilt. Darauf erhielt die betreffende Einwohnerin ein Verwarngeld in Höhe von 15 Euro für die Überschreitung der Höchstgeschwindigkeit um sieben Kilometer pro Stunde. Die Betroffene, die die Fahrereigenschaft bestritt und auch nicht im Besitz eines Führerscheines ist, machte daraufhin den ihrer Auffassung nach datenschutzrechtlich bedenklichen Vorgang öffentlich.
Im Ergebnis der Prüfung wurde dann durch den TLfD festgestellt, dass bei der Fahrerermittlung im vorliegenden Fall die einschlägigen datenschutzrechtlichen Bestimmungen und Grundsätze nicht beachtet worden waren. Gemäß § 24 StVG handelte es sich bei der festgestellten Überschreitung der gesetzlich bestimmten Höchstgeschwindigkeiten um eine Verkehrsordnungswidrigkeit, die gemäß §§ 55 ff von der zuständigen Verwaltungsbehörde im pflichtgemäßen Ermessen zu verfolgen ist. Zur Ermittlung des Täters hat dabei die Verfolgungsbehörde, soweit dies im OWiG nicht anders bestimmt ist, die selben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten (§ 46 Abs. 1 OWiG). Insoweit ist das Ordnungsamt, wenn dem keine gesetzlichen Bestimmungen ausdrücklich entgegenstehen, auch berechtigt, von anderen Behörden Auskunft zur Ermittlung des Täters einzuholen. Nach § 22 Abs. 3 Passgesetz (PassG) bzw. § 2 Abs. 2 Personalausweisgesetz ist eine Übermittlung von Pass- bzw. Personalausweisdaten zulässig, wenn die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, die ihr obliegende Aufgabe zu erfüllen und die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können. Demnach sind die Ordnungsämter grundsätzlich berechtigt, zur Durchführung eines Verkehrsordnungswidrigkeitsverfahrens das Lichtbild des vermutlichen Fahrers aus dem Personalausweisregister zum Zwecke eines Abgleichs anzufordern. Dabei gebieten nicht nur die Bestimmungen des Personalausweisgesetzes, sondern im Übrigen auch die Grundsätze des Datenschutzes (Erforderlichkeit, Verhältnismäßigkeit), dass zuvor ein hinreichender Verdacht für eine Identität des Täters mit der Person auf dem angeforderten Lichtbild besteht. Der Bildabgleich dient nur zur Bestätigung eines bestimmten Verdachts gegen den vermuteten Fahrer. Zuständige Stelle für eine Täterermittlung ist bei einer entsprechenden Aufgabenstellung das Ord-

nungsamt, welches bei der Verfolgung der Ordnungswidrigkeit das Fahrerfoto nicht anderen Personen oder Stellen (z. B. Meldebehörden, Führerscheinstellen) ohne vorherige konkrete Anhaltspunkte für den wahrscheinlichen Täter übermitteln oder ihnen gar Ermittlungsaufgaben (z. B. den Bildabgleich selbst) übertragen kann. Eine Fahrerermittlung wegen einer Verkehrsordnungswidrigkeit „ins Blaue hinein", wie sie im konkreten Fall erfolgt war, widerspricht insoweit den datenschutzrechtlichen Grundsätzen und ist auch wegen der großen Gefahr falscher Ergebnisse (wie im konkreten Fall bestätigt) als unzulässig zu bewerten. In diesem Zusammenhang sei auch unter Bezugnahme auf den konkreten Fall darauf hingewiesen, dass es hierbei keine Sonderregelungen bei Behörden mit verschiedenen Ämtern „unter einem Dach" (z. B. in kreisfreien Städten) gibt. Das TIM hat im Jahr 1998 eine Verwaltungsvorschrift über die Aufgaben der Polizei bei der Verfolgung von Verkehrsordnungswidrigkeiten erlassen, die insbesondere auch Hinweise für eine datenschutzkonforme Ermittlungsarbeit enthält. Danach sollten die Fahrzeughalter, soweit sie auf den Anhörungsbogen nicht reagieren, zunächst vorgeladen oder aufgesucht werden. Für den Fall, dass dies auch zu keinem Ergebnis führt, kann sich die Bußgeldbehörde bei dem zuständigen Meldeamt nach dem Ehegatten und den Kindern des Fahrzeughalters (ggf. auch nach Mitbewohnern in einem Einfamilienhaus) erkundigen, da erfahrungsgemäß Kraftfahrzeuge vor allem innerhalb der Familie von verschiedenen Personen genutzt werden. Stellt sich dabei heraus, dass hiervon einige Personen altersmäßig als Fahrer in Betracht kommen, können auch von diesen Personen Fotos aus dem Personalausweisregister für einen Bildabgleich angefordert werden. Unter Beachtung des Verhältnismäßigkeitsgrundsatzes wird als letzte Möglichkeit auch eine gezielte Befragung von Personen oder Stellen (z. B. Nachbarn des Halters) nicht grundsätzlich ausgeschlossen, wenn mit hoher Wahrscheinlichkeit davon ausgegangen werden kann, dass diesen der Fahrer bekannt sein müsste.

Die geschilderte zulässige Vorgehensweise, d. h. der Besuch eines Außendienstmitarbeiters des Ordnungsamtes beim Fahrzeughalter führte letztlich im konkreten Fall zur Fahrerermittlung, nachdem die Petentin nachdrücklich gegenüber der Bußgeldstelle zum Ausdruck gebracht hatte, dass sie nicht als Fahrerin in Frage kommt.

5.2.8 Datenübermittlung aus Personenstandsunterlagen des Standesamtes an nicht öffentliche Stellen

Ein Inkassounternehmen hatte sich an ein Standesamt mit der Bitte gewandt, ihm zur Durchsetzung eines vollstreckbaren Schuldtitels die beglaubigte Abschrift aus dem Standesamtsregister über die Namensänderung eines Schuldners zu übersenden. Dies ist zunächst nicht grundsätzlich ausgeschlossen, da gemäß § 61 PStG Personen zur Einsicht in Personenstandsbücher, auf Durchsicht dieser Bücher oder auf Erteilung von Personenstandsurkunden berechtigt sind, wenn sie ein rechtliches Interesse glaubhaft machen. Nach herrschender Ansicht ist es auch zulässig, im Fall einer Namensänderung eine bereits erteilte Vollstreckungsklausel durch einen Nachtrag entsprechend zu ergänzen, weshalb das rechtliche Interesse eines Gläubigers an dem Nachweis einer Namensänderung durchaus zu bejahen war. Durch die Beifügung entsprechender Nachweise zur Erforderlichkeit dieser Auskunft bestanden deshalb im konkreten Fall keine Zweifel darüber, dass damit das rechtliche Interesse der Firma an einer amtlichen Bestätigung über die vollzogene Namensänderung des Schuldners hinreichend glaubhaft gemacht wurde.
Da ein beglaubigter Auszug aus dem Familienbuch nicht nur Angaben zur Namensänderung sondern eine Vielzahl weiterer personenbezogener Daten sowohl über den Betroffenen als auch über dessen Ehegatten enthält, war aber das rechtliche Interesse an einem von dem Inkassounternehmen gewünschten Auszug aus dem Familienbuch über die erfolgte Eheschließung der Schuldnerin an die auskunftsersuchende Stelle nicht gegeben. Nach allgemeiner Rechtsauffassung ist den Grundsätzen des Datenschutzes entsprechend bei der Prüfung der Glaubhaftmachung des rechtlichen Interesses auf Einsicht in Personenstandsbücher nach § 61 zunächst regelmäßig zu prüfen, ob ein Verfahren, bei dem weniger personenbezogene Daten des Betroffenen an Dritte offenbart werden, zum selben Erfolg führt. Dies war im konkreten Fall dadurch gegeben, dass für den beabsichtigten Zweck auch eine entsprechende Auskunft über die vollzogene Namensänderung vom zuständigen Meldeamt auf der Grundlage des § 32 ThürMeldeG eingeholt werden konnte.
Selbst unter der Voraussetzung, dass vom Gericht eine erweiterte Melderegisterauskunft für die Titelumschreibung als nicht ausreichend betrachtet worden wäre - was angezweifelt wurde - hätte das Standesamt die Grundsätze der Verhältnismäßigkeit bei der Gewährung von Einsichtnahme, Durchsicht, Erteilung von Personenstandsurkunden

oder Auskünften beachten müssen. So ist es verpflichtet, grundsätzlich die Urkunde zu erteilen, welche die wenigsten Daten offenbart, wenn damit der Nutzungszweck erreicht werden kann. Um dies zu unterstreichen, enthält u. a. auch der § 87 der Dienstanweisung für Standesbeamte eine Regelung, die verhindern soll, dass aus Gründen der Arbeitsvereinfachung beglaubigte Abschriften durch Ablichtung erteilt werden. Hierzu heißt es im Kommentar zum Personenstandsgesetz: „Der Standesbeamte hat auch zu prüfen, ob statt einer Personenstandsurkunde eine formlose Auskunft oder eine Bescheinigung nach § 9 a PStV erteilt werden kann, weil nur einzelne Angaben (z. B. über eine Namensänderung) benötigt werden. Die Auskunft über einzelne Angaben eines Personenstandseintrags ist in § 61 PStG nicht ausdrücklich genannt, wird hiervon aber auch erfasst. Sie ist datenschutzrechtlich unbedenklich, da bei dieser Form der Übermittlung weniger Daten zur Kenntnis gegeben werden, als bei Einsicht, Durchsicht oder Erteilung von Personenstandsurkunden und stellt damit eine weniger einschneidende Maßnahme dar. § 68 Abs. 1 DA stellt daher die Erteilung von Auskünften neben die in § 61 PStG ausdrücklich genannte Form der Übermittlung von Personenstandsdaten. Unter Berücksichtigung der vorgenannten Rechtsauffassung wäre im konkreten Fall für die Titelumschreibung beim Amtsgericht, selbst für den Fall, dass vom Gericht ausdrücklich eine vom Standesamt gefertigte Bestätigung gefordert worden wäre, eine vom Standesamt bestätigte Mitteilung über die erfolgte Namensänderung ausreichend gewesen. Durch die Übersendung des Auszugs aus dem Familienbuch wurden aber im vorliegenden Fall ohne jedes Erfordernis weitere Daten insbesondere auch über Dritte (den Ehepartner) unnötiger- und damit unzulässigerweise an die auskunftsersuchende Stelle übermittelt. Hierbei war es auch gleichgültig, dass diese Daten der auskunftsersuchenden Stelle oder, wie im konkreten Fall, auf deren Wunsch dem Gericht unmittelbar zugeleitet wurden. Die Beurteilung der Zulässigkeit und das Verfahren für eine Datenübermittlung nach § 61 PStG ist letztlich ausschließlich nach der beim Standesamt auskunftsersuchenden Stelle zu beurteilen.

Aufgrund dessen war die vom Standesamt vorgenommene Übersendung der Eheschließungsurkunde zu beanstanden. Gleichzeitig wurde eine entsprechende Auswertung im betreffenden Standesamt gefordert, um künftig Wiederholungen bei der Bearbeitung von Auskunftsersuchen auszuschließen.

5.2.9 Datenschutz beim Rettungswesen

Während es Aufgabe des Datenschutzes ist, das informationelle Selbstbestimmungsrecht des Einzelnen bei der Verarbeitung oder Nutzung seiner personenbezogenen Daten zu schützen, geht es bei der Notfallrettung um die Durchführung lebensrettender oder sonstiger erforderlicher Maßnahmen bei Notfallpatienten, mit dem Ziel, die Transportfähigkeit herzustellen und sie zur weiteren Versorgung in eine geeignete Behandlungseinrichtung zu befördern. Bei genauerer Betrachtung zeigt sich jedoch, dass die Notfallrettung und der Datenschutz einige Berührungspunkte haben, die für die Betroffenen von entscheidender Bedeutung sein können.
Die Gewährleistung eines angemessenen Datenschutzes und Datensicherheit verlangt gerade im Rettungsdienstbereich von den Daten verarbeitenden Stellen, dass die erforderlichen personenbezogenen Daten der Patienten zeitnah und vollständig den verantwortlichen Stellen zur Verfügung stehen.

Ein schwer Verletzter wird sich in der akuten Notfallsituation keine Gedanken über die Wahrung seines Rechts auf informationelle Selbstbestimmung machen. Er wird sich, soweit er dazu überhaupt in der Lage ist, um die Wiederherstellung seiner Gesundheit sorgen. Und selbstverständlich geht es auch in der akuten Notfallsituation zunächst um nichts anderes, als dieser Sorge und der Gefahr für Leib und Leben des Betroffenen erfolgreich zu begegnen. Damit bei einem Notfalleinsatz möglichst nichts dem Zufall überlassen bleibt, wurde in Thüringen ein mehrschichtiges Regelungssystem zum Rettungswesen geschaffen. Grundlage ist das Thüringer Rettungsgesetz (ThürRettG), welches insbesondere die Aufgaben des Rettungsdienstes, die Aufgabenträgerschaft, rettungsdienstliche Organisationen und Einrichtungen sowie allgemeine Anforderungen und Pflichten des Leistungserbringers regelt. Aufgabenträger des Rettungsdienstes sind in Thüringen die Landkreise und die kreisfreien Städte. Untersetzt und ergänzt wird die Vorschrift durch den Landesrettungsdienstplan für den Freistaat Thüringen, in dem bspw. die Strukturen der Rettungsdienstbereiche oder konkrete Vorgaben für Hilfsfristen (Zeitraum vom Eingang der Notfallmeldung bis zum Eintreffen des Rettungsmittels am Notfallort) festgelegt sind. Weitere Präzisierungen hierzu erfolgen auf der Ebene der jeweiligen Rettungsdienstbereichspläne der Aufgabenträger, Detailfragen zum Rettungswesen werden in Rundschreiben der Aufsichtsbehörden behandelt.

Mit dem Eingang des Notrufs werden bereits die ersten personenbezogenen Daten über Zeit, Ort und Notfallsituation erhoben und verarbeitet. Vor Ort trifft sodann der Notarzt eine Vielzahl medizinischer Feststellungen, erhebt damit Daten über den Zustand des Patienten, die erfolgten Untersuchungen und Behandlungen, um sie zum einen als unmittelbare Grundlage für die weiteren Rettungsmaßnahmen zu nutzen, zum anderen, um seiner Dokumentationspflicht gemäß § 10 Abs. 1 der Berufsordnung der Landesärztekammer Thüringen nachzukommen. Es versteht sich von selbst, dass die ärztlichen Aufzeichnungen nicht zuletzt im Interesse des Notfallpatienten umfassend und richtig sein müssen, bilden sie doch eine bedeutende Informationsgrundlage zur Weiterbehandlung für die aufnehmende medizinische Einrichtung. Dementsprechend regelt § 20 Abs. 3 Satz 1 ThürRettG, dass über jeden Einsatz in der Notfallrettung ein Bericht zu fertigen ist, „der zusammen mit dem Patienten der zu dessen Weiterbehandlung bestimmten Einrichtung zu übergeben ist“. Weiter heißt es in der Vorschrift, dass die Durchführenden verpflichtet sind, den Aufgabenträgern einen Abdruck des Berichts in anonymisierter Form für Zwecke der Qualitätssicherung zu überlassen (§ 20 Abs. 3 Satz 2 ThürRettG). Die Vorschrift wird präzisiert durch ein Rundschreiben des Thüringer Innenministeriums aus dem Jahre 1994, in welchem Regelungen zur Notarzteinsatzprotokollierung in Thüringen getroffen werden. In der Praxis wird die Dokumentation auf einem Formularvordruck, dem so genannten Notarzteinsatzprotokoll, durchgeführt. Das o. g. Rundschreiben sieht dafür einen bestimmten Vordruck vor und regelt ausdrücklich, dass das Original zur weiterbehandelnden Einrichtung, die erste Durchschrift (Kopie genannt) für den Verbleib beim Notarzt und die zweite Kopie anonymisiert für Zwecke der Qualitätssicherung zu verwenden ist. Unter dem datenschutzrechtlichen Blickwinkel stellt der durch das Rundschreiben ergänzte § 20 Abs. 3 ThürRettG eine Spezialregelung dar, welche die Übermittlung notfallmedizinischer und rettungstechnischer Daten vorsieht und den Aufgabenträger in die Lage versetzt, Maßnahmen zur Qualitätskontrolle und Qualitätssicherung einleiten zu können.

Neben § 20 Abs. 3 ThürRettG gelten beim Umgang mit den Notfallpatientendaten auch die allgemeinen datenschutzrechtlichen Bestimmungen und die in § 9 ThürDSG niedergelegten Grundsätze zur Gewährleistung der Datensicherheit. Demzufolge sind bspw. notfallmedizinische personenbezogene Daten vollständig an den vorgesehenen Empfänger zu übermitteln.

Überprüfungen durch den TLfD haben aber ergeben, dass den gesetzlichen Vorgaben nicht in jedem Falle entsprochen wird.

So wurde in einem Rettungsdienstbereich festgestellt und beanstandet, dass dort generell nicht das Original des Notarzteinsatzprotokolls mit dem Patienten der medizinischen Einrichtung übergeben wurde, sondern eine Kopie. Das Original sowie die erste Kopie verblieb beim Notarzt selbst. Diese Praxis widerspricht nicht nur der im genannten Rundschreiben vorgesehenen Regelung, sie kann auch für die Weiterbehandlung des Patienten durch die aufnehmende medizinische Stelle von nicht unerheblicher Bedeutung sein. Wie sich herausstellte, kann nicht ausgeschlossen werden, dass die Daten auf dem Original und der im Durchschriftverfahren erstellten Kopie nicht vollkommen übereinstimmen. In einem Fall, der vom TLfD aufgrund einer Eingabe bearbeitet wurde, war ein medizinischer Befund auf der mit dem Patienten übergebenen Kopie signiert worden. Der Befund war auf dem Original des Notarztprotokolls nicht zu finden. Erklärt wurde dies vom Aufgabenträger mit dem Prinzip des Durchschreibesatzes, da das Durchdrücken von Markierungen oder Schriftzeichen aus möglicherweise anderen darüberliegenden Unterlagen nie mit völliger Sicherheit ausgeschlossen werden könne. Umgekehrt hatte zudem der Notarzt auf dem Original nachträglich Eintragungen vorgenommen, die auf der dem Patienten mitgegebenen Kopie nicht erschienen. Der Aufgabenträger hat das Verfahren nach eingehender Diskussion zwischenzeitlich den Anforderungen des Rundschreibens entsprechend umgestellt.
Dass im vorliegenden Fall die Kontrolle durch den TLfD noch nicht abgeschlossen werden konnte, weil ihm vom Aufgabenträger bislang nicht die geforderte Einsicht in alle vorhandenen Unterlagen gemäß § 37 Abs. 2 ThürDSG gewährt wurde, sei an dieser Stelle noch vermerkt. Weder die Beanstandung dieses Verhaltens gemäß § 39 ThürDSG noch die eindeutige Unterstützung des TLfD durch die Kommunalaufsicht haben hieran bislang etwas ändern können. Das infolgedessen eingeleitete kommunalaufsichtliche Verfahren dauert noch an.
Probleme zeigten sich auch im Hinblick auf die gemäß § 20 Abs. 3 ThürRettG dem Aufgabenträger zu überlassende zweite Kopie in anonymisierter Form für Zwecke der Qualitätssicherung. Bei meinen Kontrollen, die ich aufgrund der festgestellten Unzulänglichkeiten in dem genannten Rettungsdienstbereich auf alle Aufgabenträger im Freistaat Thüringen ausdehnte, ergab sich insbesondere im Hinblick auf die anonymisierte Kopie keine einheitliche Verfahrensweise beim

Umfang der vorzunehmenden Anonymisierung, d. h. zur Frage, welche Protokollfelder konkret zu schwärzen bzw. welche für die vorgesehene Qualitätssicherung des Protokolls unentbehrlich sind. Ich habe daher mit den zuständigen Aufsichtsbehörden Kontakt aufgenommen, um hierzu gesetzeskonforme und einheitliche Vorgaben beim Ausfüllen und Verteilen des Notarzteinsatzprotokolls zu treffen.

5.2.10 Änderungen datenschutzrechtlicher Bestimmungen in der Thüringer Kommunalordnung

Im Berichtszeitraum stand im Thüringer Landtag u. a. auch ein Entwurf eines Gesetzes zur Änderung der Thüringer Kommunalordnung und anderer Gesetze auf der Tagesordnung.
Regelungsinhalt der Gesetzesänderung waren u. a. auch neue Vorgaben zur Verfahrensweise bei der Durchführung von Bürgeranträgen/Bürgerbegehren in den Kommunen. U. a. wurde festgeschrieben, dass künftig zur Sammlung der Unterstützungsunterschriften nur noch Unterschriftslisten genutzt werden. Da hierbei zumindest im Rahmen der Unterschriftsleistung alle nachfolgenden tatsächlichen oder vorgeblichen Unterschriftswilligen die Möglichkeit erhalten, Kenntnis zu nehmen, welche Personen sich bereits in die Liste eingetragen haben und das Anliegen unterstützen, wurde ebenso wie zunächst auch im Rahmen der Gesetzesänderung über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid vorgesehen, eine neue Regelung in § 17 Abs. 4 ThürKO aufgenommen. Danach müssen künftig alle Unterschriftsleistenden, wenn sie den Bürgerantrag/das Bürgerbegehren unterstützen wollen, darin einwilligen, dass ihre Daten „von an den Zielen des Bürgerantrags/Bürgerbegehren interessierten Personen eingesehen werden können“. Während aufgrund meiner hierzu geäußerten datenschutzrechtlichen Bedenken bei der Beratung der Gesetzesänderung über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid meine Hinweise berücksichtigt wurden, indem man dort von dieser Regelung Abstand nahm und die Unterschriftssammlungen künftig auf Einzelbögen erfolgen (sh. hierzu 5.1.2), verblieb diese datenschutzrechtlich problematische Bestimmung in der Kommunalordnung. Meiner Empfehlung im Rahmen der parlamentarischen Beratung § 17 Abs. 4 Satz 2 ersatzlos zu streichen, ist man nicht gefolgt.
Eine weitere Änderung in der Kommunalordnung betraf eine Präzisierung der Vorschrift zum Umgang mit Niederschriften über nicht öffentliche Sitzungen. Durch mehrere Anfragen im Rahmen meiner

Kontrolltätigkeit habe ich festgestellt, dass in Kommunen mit Niederschriften über nicht öffentliche Sitzungen in einer Weise verfahren wird, die nicht den gesetzlichen Vorgaben entspricht. Mit der Begründung, dass insbesondere bei sehr großen Gebietseinheiten die jeweiligen Kommunalvertreter nicht ausreichend Gelegenheit hätten, sich mit Niederschriften eingehend zu befassen bzw. deren Richtigkeit zu prüfen, bevor hierüber der Beschluss gefasst wird, wurden entgegen § 42 Abs. 3 ThürKO nicht nur Niederschriften über öffentliche Sitzungen sondern auch die über nicht öffentliche Sitzungen den Mitgliedern der Kommunalvertretungen zur Kenntnisnahme und weiteren Verwendung übergeben. Bezüglich der Frage, ob und inwieweit eine Erforderlichkeit besteht, den Kommunalvertretern auch Kopien von Niederschriften aus nicht öffentlichen Sitzungen zur Verfügung zu stellen, wurde auch die Kommunalaufsicht eingebunden. Im Ergebnis ihrer Prüfung führte sie aus, dass der Versand und Verbleib von Entwurfsexemplaren oder Kopien der Niederschriften ein nicht unwesentliches Risiko berge hinsichtlich einer möglichen Verletzung der Geheimhaltungspflichten. Desweiteren wurde darauf verwiesen, dass auch die Kommentare zur Thüringer Kommunalordnung nachdrücklich auf die Unzulässigkeit der Übergabe von Niederschriften über nicht öffentlicher Sitzungen hinweisen und ein überwiegendes Erfordernis hierfür nicht besteht. Da in der Vergangenheit dennoch einige Kommunalvertretungen in ihren Geschäftsordnungen Regelungen aufgenommen hatten, die eine Übergabe von Niederschriften über nicht öffentliche Sitzungen an die Gemeinderatsmitglieder vorsahen, wurde um Missverständnisse künftig auszuschließen, im Rahmen des Gesetzes zur Änderung der Thüringer Kommunalordnung und anderer Gesetze eine Ergänzung des § 42 Abs. 3 ThürKO beschlossen: „Die Geschäftsordnung kann neben der Einsichtnahme in die Niederschriften die Übersendung von Abschriften der Niederschriften über öffentliche Sitzungen an alle Mitglieder des Gemeinderates vorsehen.“ (GVBl. 2002, S. 472)

5.2.11 Offenbarung personenbezogener Daten in einer Ratsinformationsvorlage

Durch eine Pressemitteilung erhielt ich Kenntnis darüber, dass in einer Informationsvorlage zum Rettungsdienst für die Ratsmitglieder einer kreisfreien Stadt eine Übersicht über Beschäftigtendaten eines Leistungserbringers aufgenommen war, deren Zulässigkeit aus datenschutzrechtlicher Sicht angezweifelt wurde. Zur Aufklärung des Sach-

verhaltes erfolgte deshalb unverzüglich ein Kontrollbesuch. Dabei bestätigte sich, dass die Offenbarung der Mitarbeiterdaten für die Information nicht erforderlich und daher unzulässig war. Aufgrund eines Hinweises hatte die Verwaltung diesen Umstand aber bereits unmittelbar nach Verteilung der Unterlagen erkannt, mit der Folge, dass alle Empfänger benachrichtigt wurden, die entsprechenden Aufstellungen nicht zu verwenden und sie unverzüglich zurück zu geben. Unter Berücksichtigung, dass die Unterlagen ausschließlich an Mitglieder des Stadtrates bzw. seiner Ausschüsse zur Kenntnis gelangt waren und diese gemäß § 12 Abs. 3 ThürKO zur Verschwiegenheit verpflichtet sind, wurde diese Entscheidung als die geeignete Maßnahme zur weiteren Sicherstellung des Datenschutzes gewertet und von einer förmlichen Beanstandung nach dem Thüringer Datenschutzgesetz abgesehen.

5.2.12 Umgang mit personenbezogenen Daten in öffentlichen und nicht öffentlichen Sitzungen

Auch im letzten Berichtszeitraum musste sich der TLfD erneut mit Fragen der Behandlung von Sachverhalten mit Personenbezug in öffentlichen Sitzungen von Kommunalvertretungen sowie Inhalten von Bekanntmachungen hierüber beschäftigen (4. TB, 5.2.9). In den Bemühungen, die Einwohner umfassend zu informieren bzw. diese soweit wie möglich, in die Entscheidungsprozesse einzubeziehen, treten jedoch in Einzelfällen auch datenschutzrechtliche Probleme auf, was mitunter auch beanstandet wurde. Dies drückt sich u. a. darin aus, dass z. B. in Einladungen für öffentliche Sitzungen statt der konkreten Bezeichnung des Beratungsgegenstandes lediglich Name von Personen/Antragstellern genannt werden. Ebenso werden Sachverhalte (wie Baumaßnahmen jeglicher Art, Anträge auf Steuerermäßigung) in öffentlicher Sitzung erörtert, deren Umgang teilweise auch besonderen Regelungen zur Geheimhaltung unterfallen. Bei entsprechenden Feststellungen wurden die betreffenden Stellen aufgefordert, künftig die jeweiligen datenschutzrechtlichen Bestimmungen, insbesondere auch das Datengeheimnis und die Verschwiegenheitspflichten der Gemeinderats- und Kreistagsmitglieder, strikt einzuhalten und hierzu geeignete Maßnahmen zu treffen. In diesem Zusammenhang wurde auch mit der obersten Kommunalaufsicht Einvernehmen darüber erzielt, dass z. B. bei der Frage, ob Bauanträge in öffentlicher oder nicht öffentlicher Sitzung erörtert werden sollen oder dürfen, schutzwürdige Belange der Antragsteller zu berücksichtigen sind. Hierzu stellt die Wil-

lensbekundung des Betroffenen im Bauantrag, ob er mit einer Veröffentlichung der Daten bzw. deren Weiterleitung z. B. an Baustelleninformationsdienste einverstanden ist, ein nicht unwesentliches Entscheidungskriterium dar. Soweit dieses Einverständnis nicht erklärt wird, ist die Beratung über einen Bauantrag nur dann in öffentlicher Sitzung angezeigt, wenn hierfür durch ein überwiegendes öffentliches Interesse für die Notwendigkeit einer öffentlichen Beratung begründet werden kann.

5.2.13 Unzulässige Datensammlungen und deren Offenbarungen im Rahmen der Öffentlichkeitsarbeit

Es fällt nicht in die Zuständigkeit des TLfD, zu beurteilen, ob von Bürgern berechtigte oder unberechtigte Anliegen oder Kritiken gegenüber der Verwaltung geäußert werden. Bei der öffentlichen Auseinandersetzung darüber sind jedoch der öffentlichen Verwaltung auch datenschutzrechtliche Grenzen gesetzt, die nicht überschritten werden dürfen.
So wurde der TLfD in nachfolgender Angelegenheit um eine datenschutzrechtliche Bewertung bzw. Unterstützung gebeten, weil nach Auffassung des betreffenden Bürgers über ihn unzulässige Datensammlungen angelegt und veröffentlicht wurden. Im vorliegenden Fall hatte der betreffende Bürger seit einem längeren Zeitraum mehrfach verschiedene, nach seiner Auffassung kritik- oder veränderungswürdige, Zustände in der Gemeinde bei Vorsprachen in der Verwaltung, Wortmeldungen in den Gemeindevertreterversammlungen oder über die Presse namhaft gemacht und sich auch bei entsprechenden Bürgerinitiativen engagiert. Dies führte dazu, dass sich der Bürgermeister auch persönlich angegriffen sah und sich im Amtsblatt „dagegen“ zur Wehr setzte. Hierzu wurden jedoch im Amtsblatt keine Sachargumente zu den aufgeworfenen Problemen vorgebracht, sondern die Einwohner lediglich darüber „informiert“, dass der betreffende Mitbürger durch seine Aktivitäten unter Mitwirkung der örtlichen Presse die Gemeinde und ihre gewählten Vertreter diffamieren und Zwietracht und Missgunst unter die Einwohner bringen würde. Gleichzeitig erstellte der Bürgermeister eine Übersicht über alle bisherigen „Aktivitäten“ des Bürgers bzw. der Gemeinde, die aufgrund von Anträgen, Anfragen des Bürgers durch die Gemeinde erfolgten. Darin waren ebenso „Vier-Augen-Gespräche“ mit dem Bürgermeister, Wortmeldungen in den Gemeinderatssitzungen wie Presseartikel, bis hin zu Beratungsinhalten nicht öffentlicher Sitzungen, vermerkt. Diese Liste hatte der Bürgermeister allen Gesprächsteilnehmern einer vom Bür-

germeister initiierten Beratung im Vorfeld übergeben, zu der neben den Gemeinderatsmitgliedern der Kommunalaufsicht und der Betroffenen auch zwei Redakteure der örtlichen Presse eingeladen waren. Ziel der Aussprache sollte es nach Auffassung der Gemeinde sein, dem Bürger die Möglichkeit zu geben, seine vermeintlichen Anschuldigungen zu belegen oder diese gegenüber der Presse zurückzunehmen.
Diese Verfahrensweise wurde vom TLfD gemäß § 39 Abs. 1 ThürDSG beanstandet. In der Begründung dazu wurde der Gemeinde mitgeteilt, dass es selbstverständlich einer Gemeindeverwaltung zusteht, sich gegen mögliche nach ihrer Auffassung ungerechtfertigte und falsche Behauptungen zu wehren. Dies kann jedoch neben einer gerichtlichen Klärung nur in Form einer sachlichen Auseinandersetzung mit den öffentlich vorgebrachten Behauptungen erfolgen. Hierzu hat der Gesetzgeber in § 11 Thüringer Pressegesetz ausdrücklich den so genannten Gegendarstellungsanspruch aufgenommen, von dem im vorliegenden Fall jedoch kein Gebrauch gemacht wurde. Die von der Gemeindeverwaltung aufgestellte undifferenzierte „chronologische" Zusammenstellung von „Aktivitäten und Veröffentlichungen des Bürgers" stellt eine unzulässige Datensammlung dar, da es keine Aufgabe der Gemeindeverwaltung ist, entsprechende Übersichten zu führen. Darüber hinaus sind gemäß § 16 Abs. 1 ThürDSG personenbezogene Daten zu löschen, wenn deren Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist, wovon bei einer Vielzahl der aufgelisteten Daten auszugehen war. Desweiteren ist eine Offenbarung von Verwaltungsdaten an Dritte (wie z. B. den Vertretern der Presse) nur zulässig, soweit es eine Rechtsvorschrift erlaubt oder anordnet oder der Betroffene eingewilligt hat. Diese Voraussetzungen lagen für die in der Übersicht aufgelisteten „Aktivitäten" lediglich für die öffentlich zugänglichen Informationen (wie Wortmeldungen in öffentlichen Gemeinderatssitzungen bzw. Leserbriefe) vor. Für die darüber hinaus offenbarten „Verhaltensdaten" bestand auch keine Erforderlichkeit für eine Kenntnisnahme durch die an dem betreffenden Gespräch teilnehmenden Personen und Stellen.
Da die betreffende Gemeindeverwaltung zunächst meiner Aufforderung zur Stellungnahme trotz mehrfacher Mahnungen nicht folgte, bedurfte es erst einer weiteren Beanstandung, in dessen Folge die Kommunalaufsicht um Unterstützung gebeten wurde, die Löschung der unzulässig erhobenen und gespeicherten Daten durchzusetzen.

5.2.14 Das „gläserne Rathaus“ im lokalen Fernsehen

Von einem Einwohner einer Kleinstadt wurde ich auf eine mir bisher unbekannte Form der Öffentlichkeitsarbeit einer Kommune aufmerksam gemacht. Hierbei nahm der Bürgermeister die Forderung nach Transparenz der Verwaltung und einem „gläsernen Rathaus“ allzu wörtlich, indem er die Einwohner täglich im lokalen Fernsehen über den „Terminkalender“ des Bürgermeisters bzw. die Aktivitäten der Verwaltung sowie sonstige Neuigkeiten in der Stadt informierte. Dabei wurden nicht nur Beratungsinhalte und die handelnden Personen genannt, sondern darüber hinaus auch noch unter der Überschrift aus der „Gerüchteküche“ Stellung aus der Sicht der Verwaltung zu vermeintlichen „Ortsgesprächen“ (z. B. über bestehende Pachtrückstände eines Einwohners) gezogen.
Auf die Intervention des TLfD hin reagierte der Bürgermeister, indem er die Veröffentlichungen sofort einstellte. Gleichzeitig übergab er dem TLfD den Entwurf einer „Einwilligungserklärung“ für die Einwohner, um künftig auf dieser Grundlage die bisherige Informationspolitik fortzusetzen. Darin sollten sich diese bei einem jederzeitigen Widerrufsrecht gegenüber der Stadt schriftlich damit einverstanden erklären, „dass im Rahmen der allgemeinen Bürgerinformation im regionalen Stadtkanal, dem Amtsblatt der Stadt sowie in öffentlichen Schaukästen personenbezogene Daten seiner Person erhoben, gespeichert, verarbeitet und genutzt werden.“
In seiner Stellungnahme hat der TLfD der Stadt mitgeteilt, dass nach § 15 Abs. 1 ThürKO die Gemeinde die Einwohner über wichtige Gemeindeangelegenheiten in geeigneter Form zu unterrichten hat. Ziel ist es dabei, durch umfassende und weit reichende Information und Publizität die Entscheidungsprozesse in der Gemeinde offen zu legen und die Arbeit der Gemeindeorgane durchsichtig und verständlich zu machen, um so die Einwohner für das Gemeindegeschehen zu interessieren und zur Mitwirkung anzuregen. Wesentliche Voraussetzung für die Informationspflicht ist somit, dass die Nachrichten für die Einwohner wichtig sind. Das bedeutet hinsichtlich der Veröffentlichung personenbezogener Daten im besonderen Maße die Beachtung des Erforderlichkeitsgrundsatzes, wonach es in jedem Einzelfall unter Abwägung mit dem Recht auf informationelle Selbstbestimmung nachvollziehbarer Gründe für die Notwendigkeit der Bekanntgabe dieser Daten bedarf. Diese Gründe waren bei dem überwiegenden Teil der bisherigen Informationen nicht erkennbar.

Darüber hinaus haben die öffentlichen Bediensteten das Datengeheimnis gemäß § 6 ThürDSG zu beachten, nach dem es den bei den Daten verarbeitenden Stellen beschäftigten Personen untersagt ist, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen. Für ehrenamtlich Tätigen gilt in entsprechender Weise § 12 Abs. 3 ThürKO, der sie verpflichtet, über die ihnen bei der Ausübung des Ehrenamts bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren, soweit nicht diese Tatsachen offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.
Eine Befugnis zur Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen liegt gemäß § 4 Abs. 1 ThürDSG nur dann vor, wenn dies eine Rechtsvorschrift erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat. Nach § 4 Abs. 2 ThürDSG muss der Betroffene, soweit eine Einwilligung bei ihm eingeholt wird, auf den Zweck der Speicherung und die vorgesehene Übermittlung der jeweiligen Daten hingewiesen werden.
Diesen vorgenannten Anforderungen wurde die vorgelegte Einwilligungserklärung in keiner Weise gerecht. Sie stellte bei näherer Betrachtung eine aus datenschutzrechtlicher Sicht unzulässige Generalvollmacht dar, mit der sich die Verwaltung einen Freibrief zur Veröffentlichung bei „Bedarf“ aller in der Verwaltung gespeicherten Daten über den Betroffenen verschaffen wollte.
Es wurde deshalb gefordert, soweit von der Stadt künftig beabsichtigt sei, personenbezogene Daten wegen ihrer Wichtigkeit für die Gemeindebevölkerung öffentlich bekannt zu machen und hierfür keine gesetzliche Ermächtigung vorliegt, von den Betroffenen zuvor eine auf den konkreten Sachverhalt bezogene Einwilligungserklärung einzuholen. Dabei müssen die Betroffenen über den Inhalt der vorgesehenen Veröffentlichung informiert werden, damit diese ihre Entscheidung frei und unabhängig und in Kenntnis der Tragweite treffen können. Andernfalls dürften ohne Einwilligung des Betroffenen regelmäßig das Recht auf informationelle Selbstbestimmung wie auch die Wahrung von Dienst- und Geschäftsgeheimnissen einer umfassenden öffentlichen Darlegung dienstlichen Aktivitäten von Behörden einschließlich der Bekanntgabe der handelnden Personen entgegenstehen.

5.2.15 Preisgabe der Identität eines Informanten durch eine öffentliche Stelle

In einem Landkreis hatte ein Mitbürger das zuständige Veterinär- und Lebensmittelüberwachungsamt darüber informiert, dass ein Tierhalter des Kreises gegen das Tierschutzgesetz verstoße. Der Informant bat, im Interesse des Tieres unverzüglich dagegen einzuschreiten und hinterließ für einen möglichen Rückruf seine dienstliche sowie seine private Telefonnummer. Umso überraschter war der Betreffende, als sich am folgenden Abend telefonisch der Tierhalter bei ihm meldete und auf Nachfrage erklärte, dass er die Telefonnummer vom betreffenden Veterinäramt erhalten habe.
Auf Anfrage des TLfD beim Veterinär- und Lebensmittelüberwachungsamt wurde dies bestätigt. Als Begründung für die Bekanntgabe der Identität des Informanten wurde erklärt, dass sich die Richtigkeit der Anzeige hinsichtlich der vermeintlichen Tierquälerei nach Prüfung vor Ort nicht bestätigt habe. Aufgrund dessen sei man, durch entsprechende Erfahrungen geprägt, davon ausgegangen, dass es sich im vorliegenden Fall auch um eine Verleumdung handeln könnte. Zur Aufklärung des „Irrtums“ und um dem Tierhalter die Möglichkeit einer gezielten Strafanzeige wegen falscher Beschuldigungen/Verleumdung zu geben, habe man ihm die Telefonnummer des Informanten genannt.
Diese Vorgehensweise der Übermittlung der Telefonnummer des Informanten an den Tierhalter wurde vom TLfD als schwer wiegender Verstoß gegen datenschutzrechtliche Bestimmungen gemäß § 39 Abs. 1 ThürDSG beanstandet. Begründet wurde dies damit, dass die Erhebung und Speicherung der Daten des Informanten zur Dokumentation des Sachverhaltes gehört, mit dem Zweck, bei Erforderlichkeit spätere Rückfragen zu ermöglichen bzw. die betreffende Person ggf. als Zeugen im weiteren Verfahren benennen zu können. Eine Einsichtnahme in bzw. eine Auskunftserteilung aus Unterlagen, die im Rahmen der Verfolgung von Ordnungswidrigkeiten angelegt sind, können einem Beteiligten (hier: Tierhalter) nur dann gewährt werden, soweit nicht überwiegende schutzwürdige Interessen Dritter entgegenstehen (§ 49 OWiG). Eine entsprechende Abwägung hatte im vorliegenden Fall nicht stattgefunden. Darüber hinaus war auch nicht ersichtlich, dass und inwieweit die Preisgabe der Identität des Informanten gegenüber dem Tierhalter zur Durchführung des Verwaltungsverfahrens erforderlich war. Auch wenn im vorliegenden Fall seitens der Behörde nicht ausgeschlossen werden konnte oder gar die (unbegrün-

dete) Vermutung bestand, dass es sich um falsche Beschuldigungen bzw. vorsätzliche Verleumdungen handelte, kann dies nicht zu einer uneingeschränkten Offenbarung von Daten über einen Informanten führen. Letztlich bleibt dem Angeschuldigten hierzu immer der Rechtsweg (Strafanzeige wegen Verleumdung) offen. In diesem Fall wären die Ermittlungsbehörden befugt, entsprechende Auskünfte über den Informanten von der betreffenden Stelle einzuholen.
Diese Rechtsauffassung wurde von der beanstandeten Stelle akzeptiert und dort mit den Mitarbeitern in entsprechender Weise ausgewertet, um künftig in vergleichbaren Fällen die Einhaltung der datenschutzrechtlichen Bestimmungen zu gewährleisten.

5.2.16 Anforderungen an Einwilligungserklärungen

Ein Petent wandte sich an den TLfD mit der Bitte um Prüfung, inwieweit eine Kommune berechtigt sei, in einer Grundstücksangelegenheit Dritten Daten aus einem Kaufvertrag zu übermitteln bzw. Kontakt mit seiner „Hausbank“ aufzunehmen. Im Rahmen von Verhandlungen in einer Grundstücksangelegenheit zum Erwerb einer Teilfläche zwecks Einrichtung einer Grundstückszufahrt war in einem persönlichen Gespräch zwischen der den Erwerber unterstützenden Gemeindeverwaltung und dem Eigentümer vom letztgenannten zum Ausdruck gebracht worden, dass sein das Grundstück finanzierende Kreditinstitut keine Zustimmung für einen Verkauf erteilen würde. Dabei war nach Darlegung der Gemeindeverwaltung in diesem Zusammenhang einer Kontaktaufnahme durch die Gemeinde mit der Finanzierungsbank vom Petenten zugestimmt worden.
Die Prüfung des TLfD in der Gemeindeverwaltung ergab, dass für eine Einwilligungserklärung des Petenten keine Nachweise vorlagen. Auch wenn nach § 4 Abs. 3 ThürDSG wegen besonderer Umstände eine andere als die Schriftform für die Erteilung einer Einwilligung zulässig ist, hätte im vorliegenden Fall zumindest ein schriftlicher Vermerk über den Gesprächsverlauf gefertigt werden und damit Zweifel an der Einwilligung ausschließen können. Dies wurde gegenüber der Gemeinde unmissverständlich zum Ausdruck gebracht und gefordert, dass der Vorgang diesbezüglich ausgewertet und künftig die Abgabe von Einwilligungserklärungen in geeigneter Weise dokumentiert wird.

5.2.17 Computerdiebstahl als Anlass für eine datenschutzrechtliche Prüfung

Datenschutzrechtliche Kontrollen bei öffentlichen Stellen werden sowohl anlassbezogen als auch anlassunabhängig durchgeführt. Anlässe können dabei Hinweise auf mögliche Verletzungen datenschutzrechtlicher Bestimmungen beim Umgang mit den personenbezogenen Daten sein. Da bei Verlusten oder Diebstählen von Computern stets davon ausgegangen werden muss, dass die darauf befindlichen gespeicherten Daten durch Unbefugte zur Kenntnis genommen werden können, wird dies regelmäßig zum Anlass genommen, die Gewährleistung von Datenschutz und Datensicherheit in der jeweiligen öffentlichen Stelle zu überprüfen.
In einem Fall von Computerdiebstahl in einer Kommune wurde dabei festgestellt, dass sich auf dem gestohlenen PC noch Lohn- und Gehaltsdaten befanden, deren Speicherung zum Zeitpunkt des Diebstahls nicht mehr erforderlich war. Darüber hinaus war die vorliegende Sicherheitskonzeption nicht fortgeschrieben worden und entsprach insoweit nicht mehr dem aktuellen Stand der Entwicklung der Informationstechnik. Auch die Räumlichkeiten, in denen die Daten verarbeitet wurden, erfüllten nur unzureichend die Sicherheitsanforderungen. Durch die kurzfristige Einleitung geeigneter Baumaßnahmen sowie einer Reihe auf der Grundlage eines überarbeiteten Sicherheitskonzepts abgeleiteter Datensicherungsmaßnahmen wurden, wie vom TLfD gefordert, von der kontrollierten Stelle die notwendigen Voraussetzungen dafür geschaffen, dass künftig beim Umgang mit den personenbezogenen Daten den sicherheitstechnischen Erfordernissen entsprochen wird.

5.2.18 Neue Regelungen im Waffenrecht

Ziel des Gesetzes zur Neuregelung des Waffenrechtes vom 11. Oktober 2002 (BGBl. I S. 3970) war es auch, unter Berücksichtigung eines angemessenen Ausgleichs zwischen den grundrechtlich geschützten Freiheits- und Persönlichkeitsrechten der Antragsteller und dem Gefahrenabwehrinteresse des Staates bzw. dem Schutzanspruch der Allgemeinheit, den missbräuchlichen Umgang mit Waffen stärker einzuschränken. Ein wesentliches Instrument hierfür stellt die behördliche Genehmigung, ebenso wie die mindestens nach Ablauf von drei Jahren vorgesehene erneute Prüfung der Zuverlässigkeit und persönlichen Eignung im Rahmen der Verlängerung der waffenrecht-

lichen Erlaubnis dar. Mit dem Gesetz zur Neuregelung des Waffenrechts wurden deshalb die Voraussetzungen für die Erteilung und Verlängerung einer waffenrechtlichen Erlaubnis neu bestimmt. Danach hat die Waffenerlaubnisbehörde nunmehr im Rahmen der Zuverlässigkeitsprüfung mindestens eine unbeschränkte Auskunft aus dem Bundeszentralregister (BZR), eine Auskunft aus dem zentralen staatsanwaltschaftlichen Verfahrensregister hinsichtlich der im Waffengesetz genannten Straftaten sowie eine Stellungnahme der örtlichen Polizeidienststelle über dort bekannte Tatsachen, die Bedenken gegen die Zuverlässigkeit begründen können, einzuholen. Weitere konkrete Vorgaben zur Informationsgewinnung für die Zuverlässigkeitsprüfung enthält das Waffengesetz nicht, schließt diese aber auch nach der (nicht völlig eindeutigen) Formulierung im Gesetzestext nicht aus.

Zur Prüfung der praktischen Umsetzung des neuen Waffenrechts erfolgte zwischenzeitlich auch eine Kontrolle des TLfD in einer Waffenbehörde. Dabei stellte sich heraus, dass bisher von der Waffenerlaubnisbehörde die nach § 5 Abs. 1 Waffengesetz (WaffG) vorgesehene Regelanfrage beim zentralen staatsanwaltschaftlichen Verfahrensregister im Rahmen der Prüfung zur Erteilung oder Verlängerung einer Waffenerlaubnis noch nicht praktiziert wird. Hierzu teilte das TIM auf Anfrage mit, dass z. Zt. alle Länder aus technischen und organisatorischen Gründen noch nicht in der Lage sind, online auf das elektronische Verzeichnis zuzugreifen und andere geeignete Alternativen nicht zur Verfügung stehen. An einer bundesweiten Lösung werde gearbeitet.
Bei der Kontrolle in der Waffenerlaubnisbehörde wurde desweiteren festgestellt, dass dort wie bisher alte Vordrucke für die Antragstellung auf eine waffenrechtliche Erlaubnis verwendet werden, obwohl diese auf nicht mehr geltende Rechtsvorschriften verweisen. Weiter enthalten sie Fragestellungen für die unterschiedlichen Erlaubnisverfahren, ohne dass es für den einzelnen Antragsteller erkennbar ist, welche Angaben zur Bearbeitung des jeweiligen Antrags erforderlich sind. Schließlich werden sogar Eintragungen gefordert, obwohl eine Kenntnis der Daten aufgrund der Neufassung des Waffenrechts für keines der Erlaubnisverfahren erforderlich ist.
Diese Verfahrensweise wurde bemängelt und die Waffenerlaubnisbehörde aufgefordert, künftig nur noch der aktuellen Rechtslage entsprechende Vordrucke zu verwenden.

5.2.19 Videoüberwachung in kommunalen Einrichtungen

Aufgrund der Anfragen öffentlicher Stellen im Berichtszeitraum ist festzustellen, dass der Einsatz von Videoüberwachungstechnik weiter zunimmt. Durch Beratungsersuchen öffentlicher Stellen und Kontrollen wurde der TLfD mit verschiedenen Einsatzgebieten konfrontiert, für die z. T. unterschiedliche Rechtsgrundlagen Anwendung finden. Sofern es sich um öffentliche Stellen handelt, die dem Wettbewerb unterliegen, gelten über § 26 ThürDSG die Vorschriften des Bundesdatenschutzgesetzes (BDSG), d. h. hier § 6 b BDSG (Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen). Das betrifft z. B. die Videoüberwachung von Bussen und Bahnen durch kommunale Verkehrsbetriebe, Geldautomaten von Sparkassen oder die Überwachung kommunaler Sportstätten. Daneben gibt es im Polizeiaufgaben- und Ordnungsbehördengesetz besondere Ermächtigungsnormen (§ 33 PAG und § 26 OBG) für die Überwachung öffentlich zugänglicher Plätze zur Abwehr einer Gefahr für die öffentliche Sicherheit und Ordnung, z. B. bei rechtswidrigen Müllablagerungen. Ein datenschutzrechtliches Problem liegt hier darin, dass in der Sicherheitsrechtsnovelle von 2002 zwar § 33 PAG, nicht jedoch § 26 OBG geändert worden ist. Da sowohl das PAG als auch das OBG mit der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung im Wesentlichen dieselben Zielstellungen haben (in der überwiegenden Mehrzahl der Bundesländer sind die polizeirechtlichen Grundlagen für die Vollzugspolizei und die kommunalen Ordnungsbehörden in einem einheitlichen Gesetz geregelt), stellen sich die datenschutzrechtlichen Rahmenbedingungen für die Videoüberwachung im Bereich der Ordnungsbehörden als nicht ausreichend dar. Die derzeitige Rechtslage führt zu dem unbefriedigenden Ergebnis, dass für den Einsatz von Videoüberwachung durch die Vollzugspolizei restriktivere Voraussetzungen (Kriminalitätsschwerpunkte, Anhaltspunkte für Straftaten) gelten als bei den Ordnungsbehörden, die bereits zur Verfolgung von Ordnungswidrigkeiten zum Mittel der Videoüberwachung greifen dürfen. Darin ist ein Wertungswiderspruch zu sehen, der vom Gesetzgeber aufgelöst werden sollte. Zudem gibt es bei einer beabsichtigten Videoüberwachung der Ordnungsbehörden auch keine dem § 33 PAG entsprechenden verfahrenssichernden Regelungen (Hinweispflicht, Datensparsamkeit, Löschverpflichtung, Information des TLfD). Auch insoweit besteht gesetzgeberischer Handlungsbedarf, der die rechtlichen Rahmenbedingungen in § 26 OBG denen des § 33 PAG angleicht.

Bislang nicht ausdrücklich geregelt ist die Videoüberwachung außerhalb des Anwendungsbereichs der genannten Normen. Betroffen ist in erster Linie die Videoüberwachung zur Wahrnehmung des Hausrechts durch öffentliche Stellen.
Setzen öffentliche Wettbewerbsunternehmen Videoüberwachung ein, so ist dies nach § 6 b Abs. 1 BDSG nur zulässig, soweit dies zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Bereits im Vorfeld einer beabsichtigten Videoüberwachung sind diese Voraussetzungen durch die Stelle genau zu prüfen und auch im laufenden Betrieb regelmäßig einer Revision zu unterziehen, wobei die Überwachung einzustellen ist, wenn die Voraussetzungen nicht mehr vorliegen.
So wurde bei der datenschutzrechtlichen Kontrolle eines städtischen Verkehrsbetriebs von diesem nachvollziehbar dargestellt, dass es in der Vergangenheit Sachbeschädigungen in Bussen und Straßenbahnen von erheblichem Umfang gegeben hat, die durch die Überwachungskameras künftig vermieden bzw. deren Verursacher ermittelt werden sollen. Durch die kurzzeitige Speicherung der Aufnahmen von 24 Stunden, wenn kein die Auswertung erforderlich machendes Ereignis (z. B. festgestellte Sachbeschädigungen) vorliegt, konnten hier die schutzwürdigen Interessen der Betroffenen nicht als überwiegend angesehen werden, sodass sich diese Überwachung im zulässigen Rahmen hält. Allerdings sind neben diesen materiellen Voraussetzungen bei der Durchführung von Videoüberwachung eine Reihe organisatorischer Maßnahmen zum Datenschutz einzuhalten. Hierzu zählt insbesondere die Herstellung von Transparenz, um dem Betroffenen die Ausübung seines Rechts auf informationelle Selbstbestimmung überhaupt zu ermöglichen. So schreibt § 6 b Abs. 2 BDSG vor, dass der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Auch bei dem kontrollierten Verkehrsbetrieb gab es hierbei Defizite. Die vorgesehene Kennzeichnung, dass in dem Verkehrsmittel eine Videoüberwachung stattfindet, war nicht auffällig genug gestaltet und wurde aufgrund meiner Forderung so verändert, dass zusätzlich zu den Hinweisen im Fahrgastraum auch ein entsprechendes Piktogramm an den Eingangstüren zu den Bussen und Straßenbahnen mit Videoüberwachungstechnik angebracht wurde. Von Bedeutung ist zudem die Pflicht nach § 6 b Abs. 5 BDSG zur unverzüglichen Löschung der Daten, wenn sie

zur Erreichung des Zwecks nicht mehr erforderlich sind. Das bedeutet, dass die Aufzeichnungen durchaus auch länger zu Zwecken der Beweisführung gespeichert bleiben dürfen. Bei dem Verkehrsunternehmen konnte ich durchsetzen, dass jeweils nur die betreffenden Sequenzen nicht jedoch die ganzen Bänder länger als erforderlich aufbewahrt werden. Um sicherzugehen, dass die rechtlichen Grenzen der Videoüberwachung nicht überschritten werden, wurde empfohlen, die für den konkreten Einsatz von Videoüberwachungstechnik relevanten Maßnahmen schriftlich zu dokumentieren und von Anfang an den internen DSB einzubeziehen. Der Verkehrsbetrieb hat die von mir empfohlenen Ergänzungen und Konkretisierungen in seiner hierzu erlassenen Unternehmensanweisung umgesetzt.

Ausgelöst durch Medienberichte wurde der TLfD auf bereits praktizierte Videoüberwachungen durch kommunale Ordnungsbehörden zur Verhinderung bzw. Verfolgung von Ordnungswidrigkeiten (z. B. Schmierereien, unzulässiges Hundebaden etc.) aufmerksam. Die Kommunen stützen sich dabei auf den bereits o. g. § 26 Abs. 1 Nr. 1 OBG, wonach Bild- und Tonaufnahmen auch zur Erfüllung der sonstigen Aufgaben der Ordnungsbehörden zulässig sind, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen. Damit ist vom Wortlaut her eine relativ weite Ermächtigungsgrundlage zum Einsatz von Videoüberwachung durch Ordnungsämter zur Erfüllung ihrer Aufgaben vorhanden. Wie bei allen Grundrechtseingriffen ist auch hier der Grundsatz der Verhältnismäßigkeit zu wahren und diese Ermächtigungsnorm verfassungskonform und damit einschränkend auszulegen. Das bedeutet vereinfacht, dass z. B. die Gefahr des Wegwerfens von Zigarettenkippen auf einem Platz keine Videoüberwachung rechtfertigen kann, weil dabei mit „Kanonen auf Spatzen geschossen“ würde. Differenzierter stellt es sich dar, wenn - wie praktiziert - zeitweise Videoüberwachungsanlagen eingesetzt werden, um unerlaubte Müllablagerungen auf Wertstoffsammelhöfen zu vermeiden bzw. zu verfolgen und alle anderen Maßnahmen zuvor erfolglos geblieben sind. Hier kann auch unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes § 26 Abs. 1 Nr. 1 OBG zum Zuge kommen.
Wie sich bei der datenschutzrechtlichen Kontrolle in einer Stadt herausstellte, wurden dort seit geraumer Zeit öffentliche Straßen und Plätze bzw. Einrichtungen durch das Ordnungsamt überwacht. Dabei kam sowohl stationäre als auch mobile Videotechnik zum Einsatz. Bei einigen stationären Kamerastandorten konnte das zuständige Ord-

nungsamt aber keine tatsächlichen Anhaltspunkte dafür anführen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen und somit die Voraussetzungen des § 26 Satz 1 Nr. 1 OBG vorliegen. Bei anderen überwachten Räumen waren zwar Anzeigen über festgestellte Verunreinigungen oder Sachbeschädigungen dokumentiert, dies allein erlaubte aus meiner Sicht allerdings noch nicht die permanente Videoüberwachung und -aufzeichnung dieser Bereiche. Vor der Entscheidung zur Videoüberwachung hätte anhand der konkreten Erkenntnisse deutlich werden müssen, dass für einen begrenzten Zeitraum keine „milderen Mittel“ zur Durchsetzung von Ordnung und Sicherheit einsetzbar sind und ansonsten sich die festgestellten Rechtsverstöße mit einer hohen Wahrscheinlichkeit fortsetzen werden. Im Ergebnis hat die Stadtverwaltung in einem Bereich die Videoüberwachung eingestellt und an einem anderen Standort den Einsatz auf die Nachtstunden und das Wochenende reduziert, also in Zeiten, in denen die Verwaltung über keine anderen Eingriffsmöglichkeiten verfügt. Im letztgenannten Fall kam die Stadtverwaltung meiner Aufforderung nach, aufgrund fehlender Geeignetheit und Angemessenheit der Maßnahme die stationäre Videoüberwachung in einem Stadtpark einzustellen bzw. mit Schildern darauf hinzuweisen, dass eine Videoüberwachung nur während der Schließzeiten des Geländes erfolgt. Darüber hinaus wurde eine Dienstanweisung erstellt, in der die erforderlichen Regelungen zum Einsatz der Videotechnik getroffen sind. Da die Stadtratsbeschlüsse zur Videoüberwachung jeweils auf ein halbes Jahr begrenzt sind, werde ich mich über den jeweils aktuellen Stand auch weiterhin unterrichten lassen.

Ebenfalls aufgrund einer Pressemitteilung wurde ich darauf aufmerksam, dass durch ein Landratsamt zwei Wertstoffcontainerstellplätze mit einer Videoanlage überwacht wurden. Ich wandte mich an die verantwortliche Stelle mit der Bitte um Mitteilung, welche Art von Videoüberwachung zur Anwendung kommt und ob die gemäß § 26 Satz 1 Nr. 1 OBG erforderlichen Voraussetzungen für eine Videoüberwachung überhaupt erfüllt sind. In diesem Fall konnte das Landratsamt durch das Vorlegen von Protokollen und Fotos von den stark verunreinigten Containerstandplätzen ausreichend darlegen, dass grundsätzlich eine Videoüberwachung als zulässig zu erachten war. Nach Angaben des Landratsamts wurde die Videoüberwachung nur vier bzw. sechs Wochen lang durchgeführt und danach eingestellt. Da sich mit der Abnahme der Verunreinigungen auf beiden Plätzen ein deutlicher Erfolg eingestellt hätte, war das Ziel der Videoüberwachung erreicht worden und ein weiterer Einsatz daher nicht geplant.

Durch die Eingabe eines Bürgers wurde ich darauf aufmerksam gemacht, dass über mehrere Monitoren in der Eingangshalle eines Freizeitbades zur allgemeinen Beobachtung das Badegeschehen übertragen wird. Darüber hinaus übertrage auch ein Privat-TV Sender zeitweise solche Aufnahmen.
Bei der von mir daraufhin durchgeführten Kontrolle in dem Schwimmbad stellte ich fest, dass auf dem gesamten Badegelände eine größere Anzahl von Videokameras installiert waren, wobei nach Angaben des Schwimmbadbetreibers dies der Überwachung von bestimmten Gefahrenbereichen dient, in denen es vermehrt zu gefährlichen Situationen oder Unfällen von Badegästen kommt. Einige Kameras erstellen darüber hinaus Übersichtsaufnahmen um die „Stimmung im Bad“ für die sich noch im Eingangsbereich aufhaltenden Badegäste zu übertragen. Wie sich zeigte, war die Qualität der Übersichtsaufnahmen ausreichend, um eine Identifizierung der erfassten Personen zu ermöglichen. Da eine Erforderlichkeit für die Übertragung der Videoaufnahmen in das Badefoyer nicht ersichtlich war, forderte ich die Badleitung zu einer Einstellung des Verfahrens. In diesem Zusammenhang stellte der Geschäftsführer des Bades klar, dass zu keinem Zeitpunkt eine Übertragung von Live-Bildern in den lokalen TV-Sender erfolgt sei. Es wurde lediglich einmalig ein Werbefilm über das Freizeitbad gedreht, der in diesem Sender ausgestrahlt wurde. Weiterhin werden im Büro des Bademeisters automatisch im Wechsel alle 15 Sekunden die Bilder einer der Videokameras auf 2 Monitoren übertragen, wobei eine Aufzeichnung der Bilder nicht erfolgt. Da dies ausschließlich der Sicherheit der Badegäste dient, bestehen hiergegen keine datenschutzrechtliche Bedenken. An einem weiteren Monitor werden diejenigen örtlichen Gegebenheiten gleichzeitig übertragen, an denen sich die meisten Badeunfälle ereignen. Nur hiervon werden während des gesamten Badebetriebs Aufzeichnungen erstellt, die grundsätzlich einer Löschungsfrist von einem Monat unterliegen. Begründet wurde die Erforderlichkeit der permanenten Aufzeichnungen und der monatlichen Aufbewahrung mit einer Beweissicherung in Fällen von Schadensersatzforderungen gegenüber dem Badbetreiber. Meine Forderung um nochmalige Überprüfung der Verfahrensweise führte zu dem Ergebnis, dass die Geschäftsleitung des Bades die Aufzeichnungen nur noch an einem Unfallschwerpunkt durchführt und die Videobänder nunmehr i. d. R. täglich überspielt werden. Nur in Fällen von angezeigten Sach- und Körperschäden werden die Aufnahmen ausgewertet und zur weiteren Klärung aufbewahrt. Die von mir geforderten technischen und organisatorischen Regelungen zum Einsatz der

Videotechnik wurden in einer Dienstanweisung schriftlich fixiert. Darüber hinaus wurde auch das Anbringen von Hinweisschildern, die auf die Videoüberwachung aufmerksam machen, veranlasst.
In diesem Zusammenhang ist noch auf die Problematik des Einsatzes von Kameraattrappen durch öffentliche Stellen hinzuweisen. Die erforderliche Transparenz ist insbesondere beim Einsatz von nicht funktionstüchtigen Videokameras nicht hergestellt. Dem Betroffenen wird hier durch die Aufstellung von Attrappen und Hinweisschildern eine scheinbare Sicherheit vorgetäuscht und er könne sich zur Geltendmachung seines Auskunftsanspruchs an die beobachtende Stelle wenden, obwohl dieser Anspruch von vornherein ins Leere läuft. Außerdem kann sich der Betroffene subjektiv in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt fühlen, obwohl faktisch weder eine Verarbeitung oder Nutzung seiner personenbezogenen Daten erfolgt. Denkbar ist hier, soweit eine zeitweise Überwachung vorgesehen und möglich ist, auf diese entsprechend hinzuweisen.

Die vorgenannten Regeln gelten jedoch nicht für öffentliche Stellen, die weder Wettbewerbsunternehmen sind noch Polizei- oder Ordnungsrecht vollziehen. Daher hat der TLfD bereits 2001 bei der Beratung zur Novellierung des ThürDSG die Aufnahme einer dem § 6 b BDSG entsprechenden Norm angeregt. Damit könnte Rechtsklarheit insbesondere auch beim Einsatz von Überwachungskameras zur Wahrnehmung des Hausrechts hergestellt werden.

5.3 Sparkassen

5.3.1 Vervielfältigung von notariellen Testamenten bei Kontenauflösungen

In einer gemeinsamen Eingabe beschwerten sich zwei Betroffene darüber, dass zwecks der Kontenauflösung einer verstorbenen Verwandten, die dort ebenfalls Kundin gewesen war, zwei von den Erben vorgelegte Testamente von der Sparkasse, ohne das Einverständnis der Beschwerdeführer einzuholen, kopiert worden sein sollen. Den Petenten sei weder Auskunft gegeben worden, wie viele Kopien erstellt wurden, noch seien ihnen diese Kopien auch nach ausdrücklicher Aufforderung zunächst nicht ausgehändigt worden. Darüber hinaus soll ihnen auch nicht die Rechtsgrundlage genannt worden sein, die eine Erforderlichkeit der Erstellung von Testamentskopien bei der Kontoauflösung von verstorbenen Kunden begründet.

Zu einem ähnlichen Sachverhalt wandte ich mich bereits in der Vergangenheit in dieser Frage an den Sparkassen- und Giroverband Hessen-Thüringen (4. TB, 5.3.1). Gemäß Nr. 5 der Sparkassen-AGB verlangt die Sparkasse grundsätzlich zur Klärung der Verfügungsberechtigung einen Nachweis durch die Vorlegung des Erbscheines. Die Sparkasse kann allerdings auf diese Unterlage verzichten und sich mit der Vorlegung der öffentlichen Testamentsurkunde und Eröffnungsurkunde begnügen. Dem Verfügungsberechtigten steht es somit frei, ob er mit dem Erbschein ein Dokument vorlegt, in dem ausschließlich die zur Erfüllung der Geschäftszwecke der Sparkasse erforderlichen personenbezogenen Daten enthalten sind oder dieser aber zum Nachweis die öffentliche Testamentsurkunde und die Eröffnungsurkunde vorlegt, auf der dann allerdings weiter gehende personenbezogene Daten vorhanden sind. Kopien der vorgelegten Urkunden werden von der Sparkasse grundsätzlich zu den Akten genommen, da nicht abzuschätzen sei, welche personenbezogenen Daten bei späteren Streitigkeiten hinsichtlich der Nachlassabwicklung von Belang sein könnten. Die Sparkassen wollen in diesen Fällen einen Beweis in den Händen halten, auf welcher Grundlage sie ihre Entscheidung getroffen haben.
Die datenschutzrechtliche Beurteilung, ob ein Vorlegen der erforderlichen Urkunden ausreicht oder aber diese Urkunden in Kopie bei der Sparkasse zur Aufgabenerfüllung verbleiben dürfen, lässt Nr. 5 der AGB offen, da es sich bei der „Vorlegung“ um einen unbestimmten Rechtsbegriff handelt. Bei der Berücksichtigung aller Umstände in dem konkreten Fall bin ich jedoch davon ausgegangen, dass die Sparkasse aus Beweisgründen im Fall einer möglichen Erbauseinandersetzung eine Kopie der vorgelegten Urkunde anfertigt und zu deren Akten nimmt, aus datenschutzrechtlicher Sicht nicht zu beanstanden ist.
Wie sich aufklärte, wurde in dem konkreten Vorgang lediglich eine Kopie des Testaments erstellt und später an die Beschwerdeführer zurückgegeben. Der Sparkasse reichte es in diesem Fall aus, eine Kopie der von den Petenten später vorgelegten Generalvollmacht zum Konto der Verstorbenen als Nachweisführung zu den Akten zu nehmen. Einen datenschutzrechtlichen Verstoß von Seiten der Sparkasse konnte ich letztlich nicht feststellen.

5.3.2 Datenschutzgerechte Gestaltung von Kundenschalterbereichen in Sparkassen

In einer Eingabe beschwerte sich ein Kunde einer Sparkassenfiliale über die erfolgte Neugestaltung des Kundendienstbereichs. Durch die

geänderte Anordnung der einzelnen Kundenbereiche seien die Diskretionszonen entfallen und somit könne neben dem Bankmitarbeiter sowie seinem Kunden auch ein Dritter ohne Schwierigkeiten in die Computermonitore einsehen und personenbezogene Bankdaten zur Kenntnis nehmen. Ich wandte mich daher an die betroffene Sparkassenfiliale und wies auf § 9 Satz 1 BDSG hin, wonach öffentliche und nicht öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen haben, die erforderlich sind, um die Ausführung der Vorschriften des Datenschutzgesetzes, insbesondere die in der Anlage zum Gesetz genannten Anforderungen, zu gewährleisten. Die Sparkasse vertrat in ihrer Stellungnahme die Auffassung, dass gerade durch die Umgestaltung des Kundenraumes datenschutzrechtliche Anforderungen in diesem Konzept Vorrang eingeräumt wurde, indem z. B. Warte- und Sichtflächen neu angeordnet und großzügige Diskretionszonen geschaffen wurden.
Zwar reichen erfahrungsgemäß solche Maßnahmen nicht in jedem Fall aus, um eine unbefugte Kenntnisnahme von personenbezogenen Daten durch Dritte zu verhindern, aus datenschutzrechtlicher Sicht habe ich das neue Konzept trotzdem für akzeptabel angesehen, weil denjenigen Kunden, die sich durch die offene räumliche Gestaltung in ihrem Recht auf Diskretion gestört fühlen, von der Sparkasse die Möglichkeit angeboten wird, ihr Anliegen auf Wunsch in separaten Räumen vorzutragen. In diesem Sinne wurde der Beschwerdeführer von mir unterrichtet.

5.3.3 Aufzeichnungen von Kundengesprächen durch die Sparkasse

In einer Pressemitteilung wurde berichtet, dass viele Banken und Sparkassen beim sog. „Telefonbanking“ Telefongespräche ohne Wissen des Kunden aufzeichnen würden. Dies war für mich Anlass beim Sparkassen- und Giroverband Hessen-Thüringen um eine Stellungnahme zu diesem Sachverhalt zu bitten. Der Sparkassen- und Giroverband startete daraufhin eine Umfrage bei den Thüringer Sparkassen und teilte mir als Ergebnis mit, dass ein generelles Mitschneiden von Kundengesprächen, abgesehen von Aufzeichnungen mittels Anrufbeantworter außerhalb der Geschäftszeiten nicht stattfindet. Wenn allerdings Sparkassenkunden die Möglichkeit des Telefonbanking nutzen wollen, so müssen diese zuvor eine vertragliche Vereinbarung unterzeichnen und die Bedingungen für das Telefonbanking der Sparkassen

akzeptieren. Die unter Nr. 5. drucktechnisch fett hervorgehobene Klausel lautet dabei wie folgt: „Ich bin damit einverstanden, dass Telefongespräche im Rahmen des Sparkassen Telefon-Bankings über die unter Nr. 2. genannte Rufnummer von der Sparkasse aufgezeichnet werden. Mit der Aufzeichnung soll sichergestellt werden, dass in Reklamationsfällen Zweifelsfragen über den Inhalt eines Auftrags sowie die Person des Auftraggebers ausgeräumt werden können." Da für das Telefonbanking dem Kunden eine bestimmte, nur hierfür genutzte Telefonnummer zugewiesen wird, ist eine Aufzeichnung von Telefongesprächen, die unmittelbar mit der kontoführenden Geschäftsstelle geführt werden, ausgeschlossen. Da für diese Gesprächsmitschnitte beim Telefonbanking regelmäßig eine Einwilligung der teilnehmenden Kunden vorliegt, bestehen gegen die Verfahrensweise aus datenschutzrechtlicher Sicht keine Bedenken.

5.3.4 Veröffentlichung von Kunden-Mail-Adressen durch eine Sparkasse

Ein Sparkassenkunde teilte mir in seiner Beschwerde mit, dass im Anhang einer über das Internet versandten, monatlich erscheinenden Informationsbroschüre des Geldinstituts die Mail-Adressen einer größeren Anzahl von Kunden enthalten waren. Dadurch war seine eigene Mail-Adresse ebenfalls gegenüber Dritten bekannt gegeben worden. Außerdem habe er die Einstellung dieses Informationsdienstes an ihn verlangt, was allerdings ignoriert worden sei. Ich teilte daraufhin der Sparkasse mit, dass es sich bei einer E-Mail-Adresse weder um ein allgemein zugängliches, personenbezogenes Datum handelt noch die Übermittlung der Erfüllung ihrer eigenen Geschäftszwecke dient. Da die Versendung von Kunden-Mail-Adressen im Anhang der Informationsschrift eine unzulässige Übermittlung personenbezogener Daten darstellt, forderte ich die Sparkasse zu einer kurzfristigen Einstellung dieser Verfahrensweise auf.
Die Sparkasse erklärte hierzu, dass es sich um einen Systemfehler gehandelt habe, was allen reklamierenden Kunden mitgeteilt worden sei. Da die Fehlersuche keinen Erfolg zeigte, wechselte die Sparkasse den Dienstleister, der im Auftrag für die Versendung der Informations-E-Mail verantwortlich war. Ebenfalls wurde eine neue Software installiert. Somit konnte die E-Mail Versendung des „Newsletter" ohne die Übermittlung von E-Mail-Adressen anderer Kunden im Anhang sichergestellt werden. Hinsichtlich der Frage, aus welchen Gründen ein Widerspruchsersuchen des Kunden zum Newsletterversand

nicht beachtet wurde, ließ sich nicht mehr aufklären, ob die Filiale einen solchen Widerspruch auf elektronischem Wege erhalten hatte. Die Sparkasse versicherte mir aber die Beachtung jedes ihr vorliegenden Widerspruchs. Dies teilte ich dem Petenten abschließend mit.

6. Personal

6.1 Einführung eines einheitlichen Personalinformationssystems

Im Berichtszeitraum informierte das TMWFK über ein Vorhaben zur Einführung eines einheitlichen Personalinformationssystems für die Verwaltung des Freistaats Thüringen. Dem TMWFK wurde im Rahmen des Maßnahmekatalogs zur Umsetzung des eGovernment-Konzeptes des Landes für die Bewertung eines einheitlichen Personalmanagementsystems die Federführung und Leitung der hierzu erstellten Projektgruppe übertragen. Schon frühzeitig sollte der TLfD in die Projekterarbeitung mit eingebunden werden, um datenschutzrechtliche Vorgaben und Erfordernisse rechtzeitig berücksichtigen zu können. Dem TLfD wurde der Auftrag sowie das vorläufige Ergebnis der Projektgruppe vorgestellt. Das Ziel ist, die bisher im Einsatz befindlichen unterschiedlichen Personalverarbeitungssysteme im Land mittelfristig abzulösen, sodass künftig nur noch ein einheitliches Personalinformationssystem in der Landesverwaltung zum Einsatz kommt. Beginnen soll die Einführung zunächst auf der Ebene der obersten Landesbehörden. Das vorgesehene Konzept basiert auf der angestrebten zentralen Datenhaltung aller Ministerien. Das Personalinformationssystem ist als eine Web-Applikation konzipiert, um kompatibel zu technischen Anforderungen der eGovernment-Plattform des Freistaats Thüringen zu sein. Es soll auf einem zentralen System im ZIV installiert und ausgeprägt als Applikationsserver und Datenbankserver vorgehalten werden. Die jeweiligen Personalbearbeiter sollen von ihrem Arbeitsplatz mit einem Web-Browser über das Landesverwaltungsnetz (CN) auf die Applikation zugreifen und die Personaldatenverarbeitung vornehmen.
In Anbetracht der datenschutzrechtlichen Relevanz, die ein Personalinformationssystem aufweist, wurde das Projekt bis zum derzeitigen Stand (Erstellung eines Pflichtenheftes) datenschutzrechtlich begleitet. Da mir zunächst noch keine konkreten Unterlagen zu dem vorgesehenen Projekt zur Verfügung gestellt werden konnten, zeigte ich in einer grundsätzlichen Stellungnahme zunächst wesentliche datenschutz-

rechtliche und sicherheitstechnische Aspekte auf, die bei der Konzeption und dem Betrieb eines solchen Systems zu beachten sind. Nach dem vom TLfD empfohlenen Schutzstufenkonzept (1. TB, 15.3) gehören Personaldaten zur Schutzstufe 2, die einen hohen Schutzbedarf erfordert. Es handelt sich hierbei um personenbezogene Daten, deren Verarbeitung erhebliche Auswirkungen auf das informationelle Selbstbestimmungsrecht insofern erwarten lässt, als der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. Insofern sind gemäß § 9 Abs. 2 ThürDSG auf der Grundlage eines Sicherheitskonzepts die hier vorgegebenen Sicherheitsziele, nämlich die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Authentizität der personenbezogenen Daten sowie die Revisionsfähigkeit und Transparenz der Verarbeitung dieser Daten, uneingeschränkt zu gewährleisten. Eine Erfüllung dieser Sicherheitsziele erfordert die Implementierung und den Einsatz von Sicherheitsfunktionen und -mechanismen. Wesentliche Maßnahmen hierfür sind u. a.:

- Durch ein Mandantenkonzept ist abzusichern, dass jedes Ressort nur Zugriff auf seine Personaldaten erhält.
- Die Zugangskontrolle ist durch sichere Identifizierungs- und Authentifizierungsverfahren vorzunehmen.
- Für jeden Benutzer (Personalbearbeiter) ist die Vergabe differenzierter Zugriffsrechte gemäß seiner Aufgaben vorzusehen. Neueinträge und Änderungen von Daten sind zu protokollieren, um im Zweifelsfall feststellen zu können, wer wann auf welche Datenobjekte zugegriffen hat und welche inhaltlichen Veränderungen vorgenommen wurden.
- Personenbezogene Daten sind verschlüsselt in der Datenbank vorzuhalten.
- Die elektronische Datenübertragung zwischen der jeweiligen personalführenden Stelle und der zentralen Applikation muss in verschlüsselter Form über das CN erfolgen.
- Administratoren dürfen kein Zugriffsrecht auf die Personaldaten besitzen. Soweit erforderlich, ist das Vier-Augen-Prinzip hier zu beachten. Grundsätzlich ist auf eine personelle Trennung von Systemadministration (Betriebssystem) und Datenadministration abzustellen. Die Aktivitäten dieser Funktionsträger sind zu protokollieren.
- Die Einführung und der Betrieb eines Personalinformationssystems bedarf eines IT-Sicherheitskonzeptes.

Aus datenschutzrechtlicher Sicht sind weiter insbesondere die zu verarbeitenden Datenarten im Hinblick auf ihre Erforderlichkeit abschließend zu definieren.
Die vorgesehene Form der Datenverarbeitung ist eine Auftragsdatenverarbeitung. Im ZIV werden die Daten vorgehalten und maschinell verarbeitet. Das TLRZ übernimmt technisch die Administration des Systems. Die fachlich inhaltliche Bearbeitung der Daten erfolgt durch die jeweilige Personalstelle der Ressorts. Letztere müssen als Auftraggeber unter Beachtung von § 8 ThürDSG mit dem Auftragnehmer (TLRZ/ZIV) jeweils eine vertragliche Vereinbarung zur Datenverarbeitung treffen. Ein Vorschlag zur Ausgestaltung solcher Verträge ist unter Anlage 23 aufgezeigt.
In Form eines Workshops, an dem auch der TLfD teilnahm, wurden im Hinblick auf die Erstellung eines Pflichtenheftes die notwendigen Funktionalitäten des Systems und Datenarten herausgearbeitet und benannt. Im zu erstellenden Pflichtenheft sind die datenschutzrechtlichen und sicherheitstechnischen Anforderungen darzulegen. Konkrete Hinweise und Empfehlungen, die im Laufe der bisherigen Projektbegleitung den Projektverantwortlichen gegeben wurden, sind zu berücksichtigen.
Auch die Umsetzung des Projektes wird vom TLfD datenschutzrechtlich begleitet werden.

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

Bereits in meinen vorangegangenen Tätigkeitsberichten (1. TB, 6.3.1; 2. TB, 6.7; 3. TB, 6.7; 4. TB, 6.12) hatte ich auf eine ausstehende Verwaltungsvorschrift zum Umgang mit den Bezügeakten, die bei der OFD - Zentrale Gehaltsstelle - geführt werden, hingewiesen.
Nach Auskunft des TFM sind die Arbeiten am Entwurf der Ablöseverordnung der ThürZustVBezüge derzeit noch nicht abgeschlossen.

6.3 Bewerbungen per E- Mail

Auch im vergangenen Berichtszeitraum befasste sich der TLfD mit der Frage des Versandes von Bewerbungen per E-Mail. Nach vorherrschender Auffassung wird der E-Mail-Verkehr dem Bereich der Tele-

kommunikation zugeordnet, sodass nach § 87 Abs. 1 TKG angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten von dem Betreiber der Telekommunikationsanlagen zu treffen sind. Bewerberdaten haben ein hohes Schutzbedürfnis, sodass nach § 9 Abs. 1, 2 ThürDSG hierfür die notwendigen technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes zu treffen sind. Wenn daher eine Dienststelle das Angebot, Bewerbungsunterlagen per E-Mail entgegennehmen zu wollen, macht, hat sie ein Verschlüsselungsverfahren anzubieten. Auch ist darauf hinzuweisen, dass ein unverschlüsselter E-Mail-Verkehr mit Risiken für die personenbezogenen Daten verbunden ist, falls der Bewerber von der angebotenen Verschlüsselung keinen Gebrauch machen will.

6.4 Einsichtnahme in Personalakte und weitere Akten

Ein Bediensteter beschwerte sich bei mir darüber, dass er bei der ihm gewährten Einsichtnahme in seine Personalakte einerseits das Fehlen von wichtigen Dokumenten und Unterlagen festgestellt hatte, andererseits aber nicht erforderliche Unterlagen darin enthalten waren.
Die von mir angefragte Stelle erklärte, dass die nicht in die Personalakte verfügten Vorgänge als Sachakten geführt würden und der Petent auch hierin zwischenzeitlich Einsicht nehmen konnte.
Ich wies sowohl den Beschwerdeführer als auch die Stelle darauf hin, dass ein Angestellter im öffentlichen Dienst gemäß § 13 Abs. 1 BAT-O ein Recht auf Einsicht in seine vollständige Personalakte hat. Dort hinein gehören alle Unterlagen, die den Bediensteten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen; andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden. In der Praxis finden beim Umgang mit Personalakten der Angestellten die beamtenrechtlichen Vorschriften entsprechende Anwendung. Nach § 100 Abs. 4 ThürBG hat der Beamte auch ein Recht auf Einsicht in andere Akten, die personenbezogene Daten über ihn enthalten und für sein Arbeitsverhältnis verarbeitet oder genutzt werden. Darüber hinaus besteht ein Auskunftsrecht gegenüber der speichernden Stelle nach § 13 Abs. 1 ThürDSG zu allen anderen zu seiner Person verarbeiteten Daten. Nach Abs. 3 muss dem Betroffenen allerdings nur dann Auskunft erteilt werden, soweit Angaben gemacht werden, die das Auffinden der Daten ermöglichen und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informations-

interesse steht. Der Sinn der Regelung liegt darin, den Arbeitsaufwand der Verwaltung in Grenzen zu halten. Es soll verhindert werden, dass die Daten verarbeitende Stelle alle vorhandenen Aktenbestände durchsuchen muss.
Die Stelle musste nach Prüfung der Unterlagen einräumen, dass bestimmte Unterlagen, die mit dem Dienstverhältnis des Angestellten in einem unmittelbaren Zusammenhang stehen, zum Zeitpunkt der Einsichtnahme durch den Bediensteten nicht in seiner Personalakte vorhanden waren. Ich habe die Stelle aufgefordert, zukünftig solche Unterlagen zeitnah zur Personalakte zu verfügen. Hinsichtlich der nicht in einem unmittelbaren Zusammenhang stehenden Vorgänge, wurde die Entfernung der entsprechenden Schriftstücke aus der Personalakte verlangt. So ist bspw. der Antrag auf Akteneinsicht kein Bestandteil der Personalakte und daher hieraus zu entfernen.

6.5 Datenerhebung zur Ortszuschlagsberechnung (Formblatt F, O, S, A)

Im 3. TB (6.5) wurde über die Bereitschaft der OFD berichtet, in einem überarbeiteten Formular den Hinweis aufzunehmen, dass Angaben zum Arbeitgeber des Ehegatten nur auszufüllen sind, soweit der Ehegatte im öffentlichen Dienst beschäftigt ist, um nicht erforderliche Datenerhebungen zu vermeiden. In der Folgezeit war allerdings festzustellen, dass es zu der Verwendung des überarbeiteten Formblatts nicht gekommen war. Auf Nachfrage wurde von der OFD erklärt, das geänderte Formblatt entspreche nach nochmaliger Prüfung nicht einer korrekten Anwendung besoldungs- und tarifrechtlicher Konkurrenzvorschriften. Die Entscheidung, ob es sich bei einer Stelle um eine dem öffentlichen Dienst gleichgestellte Stelle handelt, obliege der nach § 40 Abs. 6 Bundesbesoldungsgesetz, § 29 Abschnitt B Abs. 7 BAT/BAT-O zuständigen Stelle, also der OFD. Darüber hinaus falle es den Bezügeempfängern oftmals schwer, die Tätigkeit des Ehegatten zuzuordnen. Insoweit wurden die Bedenken des TLfD zurückgezogen. Erneut hat sich allerdings eine Bedienstete des Freistaats in diesem Zusammenhang an den TLfD gewandt. Ihr wurde turnusgemäß die Erklärung F, O, S, A zur Ausfüllung zugeleitet. Da sie geschieden ist und allein das Kindergeld für die aus der geschiedenen Ehe hervorgegangenen Kinder erhält, stellte sich die Frage, inwieweit sie verpflichtet ist, die Angaben zu ihrem geschiedenen Ehegatten zu machen. Der Arbeitgeber des früheren Ehegatten war ihr nicht konkret bekannt, sie hätte diesbezüglich Nachforschungen anstellen müssen. Von der OFD

wurde dazu mitgeteilt, dass bei dieser Fallgestaltung eine Auskunft über den früheren Gatten zur Festsetzung des kinderbezogenen Familienzuschlags nicht erforderlich ist und Betroffene somit auch keine Nachforschungen über den Arbeitgeber des geschiedenen Ehegatten anstellen müssen. Die Betroffene hat unabhängig davon, ob der frühere Ehegatte im öffentlichen Dienst beschäftigt ist, vorrangig Anspruch auf den kinderbezogenen Familienzuschlag, wenn ihr das Kindergeld gewährt wird. Es wurde zugesagt, in den Vordruck einen entsprechenden Hinweis aufzunehmen.

6.6 Auslegung von Wählerverzeichnissen zu Personalratswahlen

Im Vorfeld der Vorbereitung von Personalratswahlen werden an den TLfD periodisch wiederkehrend aus verschiedenen Bereichen Fragen zum Inhalt und der Form der Auslegung von Wählerverzeichnissen gestellt, die mich bereits 1998 veranlasst hatten, die obersten Landesbehörden, die Landratsämter und kreisfreien Städte sowie das Thüringer Landesverwaltungsamt auf einige datenschutzrechtliche Probleme bei der Erstellung und Auslegung von Wählerverzeichnissen hinzuweisen. Dennoch zeigte sich auch im letzten Berichtszeitraum, dass nicht bei allen Stellen der Datenschutz bei der Anfertigung und Auslegung von Wählerverzeichnissen ausreichend Beachtung findet. Gemäß § 2 Abs. 2 Wahlordnung zum Thüringer Personalvertretungsgesetz (ThürPersVWO) hat der Wahlvorstand zu Personalratswahlen ein Verzeichnis der Wahlberechtigten (Wählerverzeichnis) getrennt nach Gruppen der Beamten, Angestellten und Arbeiter aufzustellen. Mangels näherer Regelungen bestimmt sich der Inhalt des Wählerverzeichnisses in der Wahlordnung den Grundsätzen des Datenschutzes folgend nach der Erforderlichkeit (§§ 19 ff ThürDSG). Die Aufnahme in das Wählerverzeichnis ist die formelle Voraussetzung für die Wahlberechtigung des Beschäftigten, sodass darin alle für deren Prüfung maßgeblichen Angaben enthalten sein müssen. Gemäß § 1 Abs. 2 ThürPersVWO hat die Dienststelle dem Wahlvorstand zur Aufstellung des Wählerverzeichnisses die erforderlichen Unterlagen und Auskünfte zu erteilen. Dies betrifft insbesondere die Übergabe von Übersichten mit den Namen und den Beschäftigungsstellen aller Beschäftigten und Wahlberechtigten unter Angabe des jeweiligen Geschlechts und der Gruppenzugehörigkeit. Darüber hinaus ist die Dienststelle verpflichtet, Auskünfte zu erteilen, die dem Wahlvorstand die Prüfung der Wahlberechtigung nach § 13 ThürPersVG insbesondere hinsicht-

lich des Alters, der einzelnen Beschäftigten und des Beschäftigungsverhältnisses ermöglicht. Weitere Angaben wie Doktor- und Dienstgrade, Amtstitel oder Funktionsbezeichnungen können, soweit dies als zweckmäßig und zur eindeutigen Identifikation der betreffenden Mitarbeiter in der Dienststelle geboten erscheint, in das Verzeichnis aufgenommen werden. Darüber hinausgehende Daten, wie insbesondere Geburtsdaten (soweit nicht das Hinzufügen des Geburtsjahres im Einzelfall aufgrund von Namensgleichheit und gleicher Beschäftigungsstellen als Unterscheidungsmerkmal zweckmäßig ist) oder Privatanschriften sind regelmäßig zur Durchführung des Wahlverfahrens entbehrlich. Etwas anderes gilt für die Aufnahme der Privatanschriften für den Fall, dass z. B. wegen der besonderen Gegebenheiten einer Dienststelle die schriftliche Stimmabgabe angeordnet wird und der Wahlvorstand deshalb den Wahlberechtigten die Wahlunterlagen zuzustellen hat. Ebenso steht der Aufnahme einer Anschrift z. B. als Urlaubsanschrift in das beim Wahlvorstand geführte Wählerverzeichnis nichts entgegen, wenn der Beschäftigte die Übersendung der Wahlunterlagen nach § 17 Abs. 1 ThürPersVWO verlangt. Selbst wenn die Erforderlichkeit der Aufnahme des Geburtsdatums oder der Privatanschrift in das Verzeichnis für den Wahlvorstand begründet ist und dies als unabdingbare Voraussetzung für dessen ordnungsgemäße Aufgabenerfüllung festgestellt wird, steht das Recht des Beschäftigten auf informationelle Selbstbestimmung einer Aufnahme dieser Angaben zumindest in dem Exemplar des Wählerverzeichnisses, das zur Einsicht nach § 2 Abs. 3 ThürPersVWO bestimmt ist, entgegen. Entscheidend für den Inhalt des Wählerverzeichnisses ist ausschließlich, dass darin die Identifizierung des einzelnen Beschäftigten und die Prüfung seiner Wahlberechtigung durch die zur Einsichtnahme Berechtigten möglich ist. Anders als in den Bestimmungen in § 1 Abs. 3 ThürPersVWO, wonach der Wahlvorstand die Namen seiner Mitglieder und Ersatzmitglieder durch Aushang in der Dienststelle bekannt zu geben hat, ist das Wählerverzeichnis oder eine Abschrift davon nach Einleitung der Wahl bis zum Abschluss der Stimmabgabe gemäß § 2 Abs. 3 ThürPersVWO an einer geeigneten Stelle auszulegen. Dies soll allen Beschäftigten, gleichgültig ob sie wahlberechtigt sind oder nicht, die Einsichtnahme in das Wählerverzeichnis nach § 3 Abs. 1 ThürPersVWO ermöglichen. Zu beachten ist dabei aber, dass das Wählerverzeichnis nur für den innerdienstlichen Betrieb bestimmt ist und deshalb eine Einsichtnahme durch Dritte auszuschließen ist. Insoweit ist es unzulässig, Wählerverzeichnisse in Räumlichkeiten un-

beaufsichtigt auszulegen, die Dritten (z. B. Besuchern der Behörde) zugänglich sind.

6.7 Umgang mit dem personenbezogenen Datum der Gewerkschaftsmitgliedschaft von Beschäftigten

Es wurde an mich die Anfrage gerichtet, ob die Personalabteilung einer Stadtverwaltung berechtigt ist, Auskunft darüber zu geben, ob auf einer Liste aufgeführte Gewerkschaftsmitglieder noch bei der Stadtverwaltung beschäftigt sind.
Grundsätzlich gilt, dass ein Arbeitnehmer nicht verpflichtet ist, dem Arbeitgeber Auskunft über seine Gewerkschaftsmitgliedschaft zu geben. Die Gewerkschaftsmitgliedschaft eines Beschäftigten im öffentlichen Bereich ist ein personenbezogenes Datum, das für die Personalverwaltung und -bewirtschaftung nicht erforderlich ist, es sei denn, es wird z. B. Sonderurlaub für gewerkschaftliche Zwecke beantragt.
Die zur Stellungnahme aufgeforderte Stadtverwaltung hatte mitgeteilt, es habe sich in der Tat um eine Liste mit Angabe der Adressen von Beschäftigten gehandelt. Eine Gewerkschaftsmitgliedschaft sei jedoch nicht erkennbar gewesen. Die Personalverwaltung habe lediglich geprüft, ob noch ein Beschäftigungsverhältnis bestehe. Im Übrigen seien diese Adressen im Einwohnermeldeamt ebenso erhältlich oder im Adressbuch der Stadt nachzulesen.
Ich habe daraufhin in der Stadtverwaltung eine Kontrolle nach § 37 ThürDSG durchgeführt. Dabei wurde festgestellt, dass die Personalverwaltung eine Liste von Gewerkschaftsmitgliedern mit Namen, Adressen, Geburtstag, Beschäftigungsbeginn, Datum des Eintritts in die Gewerkschaft erhalten hatte, um diese zu aktualisieren, damit die Mitglieder zu einer Gewerkschaftsversammlung eingeladen werden konnten. Diese Liste war von einer Beschäftigten der Stadtverwaltung in ihrer Eigenschaft als Gewerkschaftsbeauftragte, und somit in dieser Rolle als Dritte zu behandeln, dem Personalamt übergeben worden. Eine Auskunft an Dritte, ob eine bestimmte Person dort beschäftigt ist, stellt nach § 3 Abs. 4 Nr. 3 ThürDSG eine Datenübermittlung dar, die nach § 4 Abs. 1 ThürDSG nur dann zulässig ist, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Mangels Einwilligung des Bediensteten und fehlender Rechtsvorschrift war eine Weitergabe der Beschäftigtendaten vom Personalamt an die Beschäftigte zur Erfüllung seiner dienstlichen Aufgaben der Personalverwaltung oder der Personalbewirtschaftung nicht erforder-

lich. Auch in entsprechender Anwendung des § 101 Abs. 2 ThürBG ergab sich kein anderes Ergebnis. Hierzu ist nachdrücklich festzustellen, dass der Schutzzweck der Einschränkung der Auskünfte für die Personalverwaltung auch in den Fällen nicht entfällt, in denen die Daten anderweitig erlangt werden könnten. Ich habe die Auskunftserteilung daher als datenschutzrechtlichen Verstoß gemäß § 39 ThürDSG beanstandet und die Stadtverwaltung aufgefordert, den Vorgang auszuwerten und Festlegungen zu treffen, die künftig jede unzulässige Übermittlung von Personaldaten ausschließen. Die Stadtverwaltung ist meiner Wertung zunächst nicht gefolgt. Es wurde die Auffassung vertreten, dass bei der Auskunftserteilung der Personalabteilung an Dritte regelmäßig eine Abwägung der berechtigten Interessen des Empfängers gegen die schutzwürdigen Interessen des Betroffenen im Anschluss der Übermittlung zu erfolgen habe. Beamtenrechtliche Vorschriften seien hier nicht anwendbar. Dies konnte nicht hingenommen werden. Nach Einbeziehung der Aufsichtsbehörde hat die beanstandete Stadtverwaltung dann mitgeteilt, dass in der Personalverwaltung der Datenschutz über eine Belehrung der Mitarbeiter sowie interne organisatorische Regelungen abgesichert wurde. Zukünftig sollen Auskünfte aus Personalunterlagen an Mitarbeiter der Stadtverwaltung, auf entsprechende Ersuchen von Behörden und sonstigen öffentlichen Institutionen sowie privaten Organisationen ausnahmslos nur nach vorheriger Kontaktierung der für datenschutzrechtliche Belange zuständigen Mitarbeiterin im Rechtsamt herausgegeben werden dürfen. Dies entspricht jedoch nur dann den datenschutzrechtlichen Vorgaben, wenn grundsätzlich für die Bearbeitung der Auskunftsersuchen das Personalamt zuständig bleibt und eine Einbeziehung des Rechtsamts nur im Einzelfall oder nicht personenbezogen erfolgt.

6.8 Dürfen Beihilfestellen Personaldaten zugänglich gemacht werden?

Von einer Kommune wurde die Frage an mich herangetragen, ob und in welchem Umfang einer Beihilfestelle zur Prüfung der Beihilfeberechtigung ihrer Bediensteten und deren Angehörigen Daten aus Personalunterlagen zur Verfügung gestellt werden können. Hintergrund war die zufällige Feststellung der Beihilfestelle über eine nicht erfolgte Veränderungsmeldung der im Familienzuschlag berücksichtigten und beihilfeberechtigten Kinder mit der Folge, dass dies bei Unkenntnis der Beihilfestelle zu einer Überzahlung der Beihilfe geführt hätte.

Im Ergebnis meiner Prüfung wurde in Abstimmung mit dem für das Dienstrecht federführende Referat des TIM hierzu folgende Auffassung vertreten:
Gemäß § 98 ThürBG sind Beihilfeakten als Teilakten in einer von der übrigen Personalverwaltung getrennten Organisationseinheit zu bearbeiten. Nach § 97 Abs. 3 ThürBG dürfen nur Beschäftigte Zugang zu Personalakten haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur, soweit dies zu Zwecken der Personalverwaltung oder der Personalbewirtschaftung erforderlich ist. Hieraus lässt sich auch im Hinblick auf § 19 Abs. 2 Nr. 3 ThürDSG aber kein absolutes Verbot für einen Zugang von Beihilfestellen auf Personaldaten ableiten. Aus der Tatsache, dass die Beihilfestelle im konkreten Fall ein gesonderter, abgeschotteter Teil der Personalverwaltung ist, folgt die Anwendbarkeit der Vorschriften der §§ 97 ff ThürBG auch auf die Beihilfeakten, soweit sie sachlich in Betracht kommen und nicht in § 98 ThürBG Abweichendes vorgeschrieben ist. § 98 ThürBG enthält indes „nur“ ein Zugangsverbot für die allgemeine Personalverwaltung auf die Beihilfevorgänge, was sich aus dem besonderen Schutzbedürfnis der Beamten im Hinblick auf ihre höchstpersönlichen Angaben zu ihrem Gesundheitszustand und der dazu gehörigen Heilbehandlung in den Beihilfeanträgen und den beigefügten Belegen ergibt. Umgekehrt besteht dieses besondere Schutzbedürfnis zur Geheimhaltung bestimmter, beihilferelevanter Personaldaten gegenüber der Beihilfestelle nicht, vielmehr ist die Beihilfestelle ebenso personalaktenführende Stelle wie das Personalamt selbst. Dies ergibt sich gerade aus § 98 Satz 1 ThürBG, wonach die Beihilfeakte eine Teilakte der Personalakte darstellt. Selbstverständlich ist der Beihilfestelle ein Zugang zur Personalakte bzw. sind Informationen daraus nach § 97 Abs. 3 ThürBG nur insoweit zu gewähren bzw. zur Verfügung zu stellen, als sie für Zwecke der Beihilfebearbeitung benötigt werden. Dies betrifft Angaben des Beamten, seines Ehepartners sowie der im Familienzuschlag berücksichtigten Kinder, aus denen sich ein Anspruch auf Beihilfe sowie zu deren Höhe ergeben. Im Übrigen ist strikt darauf zu achten, dass die Beihilfebearbeitung von der übrigen Personalverwaltung getrennt erfolgt und der Informationsfluss ausschließlich in einer Richtung, d. h. von der Personalverwaltung zur Beihilfestelle und nicht umgekehrt, erfolgen darf.
Werden von der Beihilfestelle regelmäßig Daten aus den Personalunterlagen genutzt (Angaben zur Verbeamtung, zum Ehepartner oder den im Familienzuschlag berücksichtigten Kinder), ist konsequenter-

weise auf eine Verpflichtung der Beihilfeberechtigten zur Abgabe von Änderungsmitteilungen zu verzichten.

6.9 Beihilfebearbeitung

Wie bereits im 3. und 4. TB (6.4/6.5) erörtert, wird von einem großen Teil der Kommunen die Beihilfebearbeitung durch private Versicherungsunternehmen im Rahmen einer Auftragsdatenverarbeitung durchgeführt. Der zwischenzeitlich vom zuständigen Ministerium erarbeitete Entwurf einer gesetzlichen Regelung dazu ist aus datenschutzrechtlicher Sicht in der vorliegenden Form nicht zufriedenstellend.
Nach der derzeit vorgesehenen Ergänzung des § 87 Abs. 2 ThürBG sollen die Gemeinden, Verwaltungsgemeinschaften, Zweckverbände und Landkreise berechtigt werden, sich zur Erfüllung ihrer Verpflichtung aus Abs. 1 der genannten Vorschrift der Dienstleistungen geeigneter Unternehmen zu bedienen und hierzu die erforderlichen Daten nach Maßgabe von § 8 des ThürDSG übermitteln. Die beabsichtigte Neuregelung enthält in sich Widersprüche, die einer Klärung bedürfen. Zunächst schließen die Begriffe Übermittlung und Auftragsdatenverarbeitung einander aus. Hierzu heißt es in den Hinweisen zum Thüringer Datenschutzgesetz des Thüringer Innenministeriums: „Datenverarbeitung im Auftrag im Sinne des § 8 ThürDSG umfasst jene Fälle, in denen die tatsächliche Verarbeitung personenbezogener Daten für eine andere Stelle erfolgt, der Auftraggeber aber für die Verarbeitung und deren Ergebnis nach außen verantwortlich bleibt. Die Weitergabe an die Auftragnehmer stellt keine Datenübermittlung dar. Abzugrenzen von der Datenverarbeitung im Auftrag ist die so genannte Funktionsübertragung, bei der nicht lediglich die Durchführung, Verarbeitung oder Nutzung, sondern die Aufgabe selbst, zu deren Wahrnehmung die Verarbeitung oder Nutzung dient, auf eine andere Stelle übertragen wird (z. B. die Übertragung einer Aufgabe auf ein beliehenes Unternehmen). Eine solche Funktionsübertragung - auch Outsourcing genannt - bedarf einer Rechtsgrundlage.“ Entscheidende Voraussetzung für die Anwendung des § 8 ThürDSG ist, dass der Datenempfänger lediglich eine technisch geprägte Hilfstätigkeit wahrnimmt, während die auftraggebende öffentliche Stelle auch weiterhin für die Wahrnehmung der eigentlichen Verwaltungsaufgabe verantwortlich bleibt. Insoweit scheidet nach § 8 ThürDSG die Übertragung eines vollständigen Aufgabenbereichs bzw. eines separaten Aufgabenteilbereichs auf den Auftragnehmer aus. Es bedarf deshalb einer ein-

deutigen Klärung, ob künftig die Wahrnehmung der Beihilfebearbeitung von privaten Versicherungsunternehmen lediglich im Rahmen einer Auftragsdatenverarbeitung im Sinne des § 8 ThürDSG oder als Outsourcing einer Verwaltungsaufgabe erlaubt werden soll. Entscheidend dabei ist, dass bei einer Auftragsdatenverarbeitung keine funktionelle Privatisierung stattfindet und in der Vertragsgestaltung konkrete Vorgaben und Grenzen zum Umgang mit den Beihilfedaten aufzunehmen sind. Insbesondere muss deutlich werden, dass der Auftraggeber ohne Einschränkungen in der Lage ist, die vertragsgerechte Auftragsdatenverarbeitung unter datenschutzrechtlichen Aspekten zu prüfen und dass dem Auftragnehmer bei der Datenverarbeitung kein eigener Beurteilungs- und Entscheidungsspielraum gewährt wird. Es sind Regelungen zu treffen, die die bestehenden Rechte der Beihilfeberechtigten nach § 103 Abs. 3 ThürBG zur jederzeitigen Einsichtnahme in die vollständige Beihilfeakte, die unverzügliche Rückgabe von Unterlagen (aus denen die Art einer Erkrankung ersichtlich ist, wenn sie für den Zweck, für den sie vorgelegt wurden, nicht mehr benötigt werden) bzw. die Vernichtung von Unterlagen über Beihilfe nach Ablauf von 5 Jahren nach Abschluss des Beihilfevorganges vertraglich gewährleisten. Ansprechpartner der Beamten zur Durchsetzung dieser Rechte sind dabei stets die Behörden als Auftraggeber. Bei einem Outsourcing, d. h. bei einer Aufgabenübertragung, sind die entsprechenden Vorgaben in das Gesetz aufzunehmen, die gewährleisten, dass die Beamten in den betreffenden Kommunen datenschutzrechtlich nicht schlechter gestellt werden, als Beamte öffentlicher Stellen mit eigener Beihilfebearbeitung. Im Hinblick darauf, dass für private Stellen das BDSG und dies nur insoweit gilt, als dort personenbezogene Daten in automatisierten Dateien verarbeitet werden bedarf es bei einer Privatisierung der Bearbeitung von besonders schützenswerten Beihilfedaten zur Gewährleistung der Gleichbehandlung der Beamten zwingend einer gesetzlichen Vorgabe zur Fortgeltung der Regelung des § 100 und § 103 ThürBG. Desweiteren sollte die Dienstleistung nicht allgemein von „geeigneten Unternehmen“, wie im Gesetzentwurf vorgesehen, sondern wie bereits derzeit praktiziert, ausschließlich von geeigneten Stellen wie z. B. von Krankenversicherungsunternehmen wahrgenommen werden. Aufgrund der besonderen Schutzwürdigkeit von Gesundheitsdaten sollten diese auch nur besonders vertrauenswürdigen Stellen anvertraut werden.

6.10 Datenverarbeitung bei Personalkostenzuschüssen

Bereits in meinem 2. TB (6.11) habe ich mich mit der Frage befasst, in welchem Umfang personenbezogene Daten der Mitarbeiter freier Träger der Jugendhilfe im Zusammenhang mit der Beantragung und Bewilligung von Fördermitteln des Landes von den zuständigen Stellen erhoben werden dürfen. Die Thematik ist auch weiterhin aktuell und muss in jedem Einzelfall geprüft werden, wie bspw. die Eingabe eines Trägers der freien Jugendhilfe zeigt. Danach forderte ein Jugendamt im Zusammenhang mit den Verhandlungen um eine Anpassung des Regelleistungsentgelts verschiedene personenbezogene Daten der bei dem Träger beschäftigen pädagogischen Mitarbeiter, obwohl dies in dem zugrunde liegenden Rahmenvertrag nach § 78 f SGB VIII nicht ausdrücklich vorgesehen war. Es stellte sich jedoch heraus, dass im Rahmen der Verhandlungen Unterlagen eingereicht worden waren, die Personalkosten in nicht nachvollziehbarer Größenordnung enthielten. Die Datenerhebung diente damit dem Zweck, Zweifel an einer möglichen Doppelfinanzierung auszuräumen. Diese Verfahrensweise sah ich als gerechtfertigt an, da hierbei in einem konkreten Einzelfall personenbezogene Daten im erforderlichen Umfang zur Aufgabenerfüllung erhoben wurden. Dennoch habe ich das Jugendamt ausdrücklich darauf hingewiesen, dass über diesen Einzelfall hinaus die Erhebung und weitere Verarbeitung von personenbezogenen Daten von Mitarbeitern der Einrichtungsträger sich eng an der Erforderlichkeit für die Bewilligung und Rechnungsprüfung zu orientieren habe.

6.11 Personalverwaltungssystem PERSOS-PT-O

Im Berichtszeitraum setzte mich das TIM von dem Vorhaben in Kenntnis, im Unterschied zur bisherigen dezentralen Verarbeitung der Personaldaten auf abgeschotteten Computersystemen nunmehr auf einem Server des TLRZ/ZIV die zentrale Verarbeitung als Datenverarbeitung im Auftrag nach § 8 ThürDSG durchführen lassen zu wollen. Nachdem hierzu das Betreiberkonzept vorgelegt worden war, habe ich einer ausführlichen Stellungnahme auf erforderliche Ergänzungen und insbesondere auf die Notwendigkeit der Erstellung eines Sicherheitskonzeptes verwiesen. Der Entwurf des Sicherheitskonzeptes wird nach Aussagen des TIM frühestens im Januar 2004 zur Verfügung stehen.

6.12 Berufung und Abberufung von Datenschutzbeauftragten

Im Berichtszeitraum wurde an den TLfD die Frage der Verfahrensweise bei der Berufung und Abberufung von DSB herangetragen. Bei der Beantwortung ist zunächst davon auszugehen, dass die öffentlichen Stellen die Ausführung des Thüringer Datenschutzgesetzes sowie anderer Rechtsvorschriften über den Datenschutz gemäß § 34 ThürDSG sicherzustellen haben. In diesem Zusammenhang sind sie nach § 10 a ThürDSG verpflichtet, soweit personenbezogene Daten mit Hilfe automatisierter Verfahren verarbeitet oder genutzt werden, schriftlich einen Beschäftigten zum Beauftragten für den Datenschutz zu bestellen. Der Beauftragte muss über die notwendige Fachkenntnis in Fragen des Datenschutzes und der Datensicherheit verfügen und durch diese Tätigkeit keinem unüberwindbaren Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt sein. Er ist in dieser Funktion dem Leiter der Daten verarbeitenden Stelle unmittelbar zu unterstellen und muss insoweit weisungsfrei und unabhängig, d. h. ohne Berücksichtigung weiterer Unterstellungsverhältnisse und Dienstwege den Leiter bei der Ausführung von Rechtsvorschriften zum Datenschutz unterstützen und auf deren Einhaltung hinwirken. Bezüglich der Rechtsstellung eines behördlichen Datenschutzbeauftragten wurde auf Anfrage vom TIM ausgeführt, dass auch bei der Bestellung eines Beauftragten für den Datenschutz die Daten verarbeitende Stelle für die Sicherstellung des Datenschutzes verantwortlich bleibt. Nicht vorgesehen ist nach dem Thüringer Datenschutzgesetz die Bestellung externer Personen zu Beauftragten für den Datenschutz, ebenso können Gemeinderats- oder Stadtratsmitglieder nicht zum Beauftragten für den Datenschutz bestellt werden, da sie keine Beschäftigten der Gemeinde sind. Die Auswahl des Beauftragten für den Datenschutz sowie dessen Bestellung und Widerruf erfolgt allein durch den Leiter der Daten verarbeitenden Stelle, da diesem originär die Sicherstellung des Datenschutzes und der Datensicherheit obliegt und der Beauftragte ihm in seiner Funktion unmittelbar unterstellt ist. Die Bestellung und Abberufung stellen sich sowohl in einem datenschutzrechtlichen als auch in einem arbeits- bzw. dienstrechtlichen Vorgang dar und können wechselseitige Wirkungen hervorrufen. Dies kann zur Folge haben, dass eine im Verhältnis zur beauftragten Tätigkeit überwiegend anderweitig ausgeübte und damit das Beschäftigungsverhältnis prägende Tätigkeit bei Wegfall ein wichtiger Grund für die Beendigung auch der Beauftragtentätigkeit sein kann. Das im Rahmen der Organi-

sationshoheit bestehende Direktionsrecht der Behörde wird Restriktionen unterworfen sein, die sich an den Anforderungen des § 626 BGB messen lassen müssen.

6.13 Umfang zu erhebender Personaldaten in Personalbögen

In ihrer Stellungnahme zum 4. TB hatte die Landesregierung ausgeführt, die in 6.7 zum Ausdruck kommende Auffassung, dass Personaldaten nur insoweit erhoben werden dürften, als sie Relevanz für das Dienstverhältnis haben, werde geteilt. Im Übrigen wurde der Bericht zum Anlass genommen, in den Geschäftsbereichen der Thüringer Ministerien eine Überprüfung einschlägiger Fragebögen hinsichtlich der Frage des Umfangs der dort erfragten personenbezogenen Daten durchzuführen und die einschlägigen Frage- und Personalbögen unter dem Aspekt der Notwendigkeit der erhobenen Daten für das Beschäftigungsverhältnis zu prüfen.
Für den Geschäftsbereich des TIM wurde zwischenzeitlich mitgeteilt, dass Fragebögen in Bewerbungsverfahren im Vorfeld einer Einstellungsentscheidung nicht verwendet werden. Lediglich im Auswahlverfahren für den allgemeinen Polizeivollzugsdienst wird als Ergänzung der individuellen Bewerbungsunterlagen ein ausgefüllter Vordrucksatz verlangt. Der bisher allgemein verwandte Personalbogen für Angehörige des öffentlichen Dienstes des Landes Thüringen wird bis zum Neudruck dahingehend modifiziert werden, dass Angaben bspw. zum Getrenntleben, zur Wiederverheiratung, zum Kindschaftsverhältnis (z. B. ehelich), zur Schul- und Berufsausbildung von Kindern, ob diese verheiratet oder versorgt sind, zu den Eltern der Beschäftigten sowie zur Teilzeitbeschäftigung, Beurlaubung ohne Dienstbezüge, zur Beendigung der Laufbahn, zur Angabe der Betriebsratsmitgliedschaft sowie zu den Strafen geschwärzt werden. Freiwillig sollen zukünftig Angaben hinsichtlich der beruflichen Tätigkeit bezogen auf öffentlicher Dienst-Staatsapparat, Besoldungs-, Vergütungs-, Lohn- und Gehaltsgruppen sein. Diejenigen Angaben, die jedoch ständig aktualisiert werden müssen, werden künftig auf einem gesonderten Blatt als Bestandteil der Personalakte aufgenommen und ggf. anlassbezogen fortgeführt. Dabei kann es sich durchaus auch um die zunächst als zu schwärzen dargestellten Daten handeln, soweit sie für die Personalverwaltung und Personalwirtschaft von Bedeutung sind.
Datenschutzrechtliche Bedenken gegen die geschilderte beabsichtigte Vorgehensweise bestehen nicht.

7. Polizei

7.1 Änderung des Polizeiaufgabengesetzes (PAG)

Mit dem Thüringer Gesetz zur Änderung des Polizei- und Sicherheitsrechtes vom 20. Juni 2002 (GVBl. S. 247) wurde insbesondere auch das Polizeiaufgabengesetz novelliert. Nach der Neufassung kann die Polizei auch an einem öffentlich zugänglichen Ort, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Straftaten verabredet, vorbereitet oder verübt werden sollen, zur Gefahrenabwehr mittels Bildübertragung offen beobachten oder Bildaufzeichnungen von Personen anfertigen. Hierzu habe ich die Auffassung vertreten, dass sich mittels Videoüberwachung schwerlich feststellen lassen wird, ob potenzielle Straftäter möglicherweise Straftaten verabreden oder vorbereiten und zu erwarten steht, dass möglicherweise eine Verlagerung der Kriminalität an andere örtliche Bereiche stattfindet. Nach § 33 Abs. 3 Satz 3 PAG bedarf die polizeiliche Videoüberwachung der Zustimmung des für die Polizei zuständigen Ministeriums, was als verfahrenssichernde Maßnahme zu begrüßen ist. Auch ist in § 33 Abs. 3 Satz 4 vorgesehen, dass der TLfD zu informieren ist.
Zu § 34 Abs. 3 habe ich im Rahmen der Anhörung zum Gesetzentwurf bei der Neuformulierung erhebliche Bedenken dagegen geäußert, dass nicht klar definiert ist, in welcher Weise vermeintliche Kontakt- und Begleitpersonen zur Zielperson in Kontakt stehen, da kein strafrechtsrelevanter Kontakt vorausgesetzt wird, sodass aus meiner Sicht die vorliegende Fassung zu weitgehend ist, zumal nicht gleichzeitig verlangt wird, dass Tatsachen die Annahme rechtfertigen müssen, dass die Verbindung in einer Weise bestehen muss, die erwarten lässt, dass die Maßnahme zur Verhütung von Straftaten beitragen wird. Erhebliche datenschutzrechtliche Bedenken habe ich auch gegenüber der in § 34 Abs. 3 Satz 2 neu eingeführten Regelung erhoben, wonach so genannte Strukturermittlungen „im bisher der Polizei nicht zugänglichen Vorfeld zur Beobachtung von organisierter Kriminalität“ ermöglicht werden. Hierdurch soll die Möglichkeit geschaffen werden, schon im Vorfeld etwaiger Straftaten Daten zu erheben, wenn tatsächliche Anhaltspunkte für die Begehung künftiger Straftaten von erheblicher Bedeutung und organisierter Form vorliegen, ohne dass diese bereits bestimmten Personen zuzurechnen sind. Dieser als Strukturermittlung definierte Ermittlungsansatz wird nur dadurch begrenzt, dass die Maßnahmen nur dann durchgeführt werden sollen, wenn sie zwingend erforderlich und die Aufgliederung der Strukturen auf andere

Weise aussichtslos wäre. Nicht erkennbar wird hier, wie die Grenzen für derartige tatsächliche Anhaltspunkte gefunden werden können, wenn diese Maßnahmen zwingend erforderlich sind und eine Aufklärung der so genannten Strukturen auf andere Weise aussichtslos wäre, ist nach meiner Auffassung schon der Bereich zureichender tatsächlicher Anhaltspunkte gegeben, die die Staatsanwaltschaft nach § 152 Abs. 2 i. V. m. § 163 Abs. 1 StPO zu Strafverfolgungsmaßnahmen ermächtigen. Herr des Ermittlungsverfahrens ist die Staatsanwaltschaft, sodass Ermittlungen außerhalb der Kontrolle der Staatsanwaltschaft im Hinblick darauf, dass vor der Einleitung eines eigentlichen Ermittlungsverfahrens den Betroffenen die Rechte eines förmlich Beschuldigten vorenthalten werden, problematisch sind. Die nach der Neuregelung vorgesehenen Ermittlungen im Vorfeld einer Gefahr im Sinne des Polizeiaufgabengesetzes sollen dazu dienen, einen Verdacht erst einmal zu gewinnen. Ich sehe es für problematisch an, dass nur im Hinblick darauf, dass es sich um organisierte Kriminalität handelt, ohne konkrete Vorstellung, was geklärt werden soll, Ermittlungen durchgeführt werden. Bedenkt man, dass eine derartige Anordnung, die auf höchstens drei Monate zu befristen ist, um jeweils weitere drei Monate verlängert werden kann, kann die Möglichkeit nicht ausgeschlossen werden, dass über einen längeren Zeitraum breit angelegte Ermittlungen zu Datenerhebungen über völlig Unbeteiligte führen. Aus datenschutzrechtlicher Sicht habe ich mich bei der Anhörung im Innenausschuss des Thüringer Landtags gegen eine derartige Regelung ausgesprochen.

Gesetzliches Neuland hat Thüringen mit der Vorschrift des § 34 a betreten.

Mit den Regelungen in § 34 a wurde eine Ermächtigungsnorm für Datenerhebungen zur Telekommunikation für präventiv-polizeiliche Zwecke in das PAG aufgenommen. Nach Art. 7 Abs. 1 VerfThür sind das Briefgeheimnis, das Post- und Fernmeldegeheimnis und das Kommunikationsgeheimnis unverletzlich. Beschränkungen dürfen nur aufgrund eines Gesetzes angefordert werden. Auch sind Beschränkungen dem Betroffenen gegenüber grundsätzlich nach Abschluss der Maßnahmen mitzuteilen. Ich habe im Rahmen der Anhörung zum Gesetzentwurf deutlich gemacht, dass aus datenschutzrechtlicher Sicht eine derartige Rechtsgrundlage im PAG höchsten Anforderungen hinsichtlich der Erforderlichkeit, Unausweichlichkeit, Verhältnismäßigkeit sowie Geeignetheit genügen muss, um einen Eingriff in Grundrechte der Bürger rechtfertigen zu können. Insbesondere an die Eingriffsschwelle in das Recht auf Privatsphäre und das Recht auf

informationelle Selbstbestimmung nach Art. 6 VerfThür müssen hinreichend bestimmte normenklare Tatbestandsvoraussetzungen gesetzlich bestimmt sein. Ich habe ausgeführt, dass ein Eingriff in das Fernmeldegeheimnis im Zuge der Abwehr einer dringenden Gefahr für Leben, Gesundheit und Freiheit einer Person für vertretbar erscheint. Wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter und Teilnehmer Straftaten nach § 100 a StPO begangen hat oder zu begehen versucht oder mit Vorbereitungen begriffen ist, habe ich das bestehende rechtliche Instrumentarium für ausreichend erachtet. Meiner Empfehlung, § 34 a Abs. 1 Nr. 1 aus dem Gesetzentwurf zu streichen, ist man jedoch nicht nachgekommen. Datenerhebungen über Kontakt- und Begleitpersonen, nach § 34 a Abs. 1 Ziff. 3 habe ich für unverhältnismäßig angesehen.
Kritisiert habe ich im Gesetzentwurf auch den Umstand, dass eine Anordnung eines Behördenleiters außer Kraft tritt, wenn sie nicht unverzüglich, spätestens binnen drei Tagen durch den Richter bestätigt wird. Das halte ich für problematisch. Im Gesetz finden sich keine Regelungen dazu, was mit den Daten passiert, die ohne richterliche Anordnung erhoben wurden. Weiter ist damit auch nicht sichergestellt, dass kurzzeitige Anordnungen überhaupt dem Richter vorgelegt werden.

Im Rahmen meiner Kontrollzuständigkeit habe ich mich an das TIM gewandt und um ergänzende Auskünfte gebeten. Die Kontrollen sind noch nicht abgeschlossen. Über meine datenschutzrechtlichen Bewertungen werde ich den Innenausschuss im Thüringer Landtag in Kenntnis setzen.

7.2 INPOL-neu

Am 16. August 2003 ist das Verfahren INPOL-neu, über das in vorausgegangenen Tätigkeitsberichten (3. TB, 7.5; 4. TB, 7.2) eingehend berichtet wurde, in Betrieb gegangen. Die zunächst vorgesehene Auftragsdatenverarbeitung der Daten der Länder beim BKA (4. TB, 7.2) erfolgt nun nicht mehr, was zu begrüßen ist. Mit der Inbetriebnahme von INPOL-neu wurden die Länder, wie dies nach § 34 Abs. 1, 2 BKAG vorgesehen ist, um Zustimmung zu Errichtungsanordnungen zu automatisierten Dateien mit personenbezogenen Daten gebeten. Seitens der DSB hat man sich bei der Datei „Kriminalaktennachweis (KAN)“ dagegen ausgesprochen, den kriminellen Werdegang in die

Datei aufzunehmen (4. TB, Anlage 3), da nach dem Wortlaut von § 2 Abs. 1 BKAG die Zuständigkeit des BKA sowohl im präventiven als auch im repressiven Bereich auf „Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung“ begrenzt ist. Diese rechtliche Bewertung wird seitens der Innenministerien nicht geteilt und sieht auch die Speicherung von Daten vor, wenn lediglich die Annahme besteht, dass dies zur Verhütung von keinen relevanten Straftaten beitragen kann, ohne dass eine der Straftaten die Erheblichkeitsschwelle nach § 2 Abs. 1 BKAG erreicht haben muss. Auch hat man sich nicht der Auffassung der DSB angeschlossen, dass alle Abrufe aus dem System automatisch protokolliert werden sollen. Die DSB des Bundes und der Länder haben die Einführung von INPOL-neu im Berichtszeitraum zum Anlass genommen, eine Arbeitsgruppe zu bilden, die sich mit weiteren Detailfragen zu INPOL-neu befassen wird.

7.3 Rasterfahndung

Im vorangegangenen 4. TB (7.8) habe ich darüber informiert, dass ich die Verarbeitung personenbezogener Daten auf der Grundlage der angeordneten Rasterfahndungsmaßnahme im Herbst 2001 unter dem Gesichtspunkt der Einhaltung der gesetzlichen Bestimmungen in diesem Zusammenhang kontrollieren werde.

Im Berichtszeitraum haben mehrere Kontrollen stattgefunden. Beanstandet wurde, dass Datenübermittlungsersuchen der Polizei an einzelne Studieneinrichtungen bezüglich personenbezogener Studentendaten über die in der Rasterfahndungsanordnung vorgegebenen Rasterkriterien hinausgingen.
Kritisiert habe ich auch den Umstand, dass die ergänzenden konkretisierten Anordnungen gemäß § 44 Abs. 4 PAG von Ende September 2001 und Anfang Oktober 2001 mir nicht umgehend zur Kenntnis gegeben wurden, obwohl dies ausdrücklich erbeten wurde.
Die in diesem Zusammenhang aufgestellten Forderungen waren auch Gegenstand der parlamentarischen Beratung im Innenausschuss des Thüringer Landtags. Mit Erlass des Thüringer Innenministeriums wurde sichergestellt, dass die datenschutzrechtlichen Forderungen zukünftig Beachtung finden. Auch die Löschung der so genannten „Trefferfälle“ wurde im Berichtszeitraum vorgenommen. Im Berichtszeitraum wurden nach dem Kenntnisstand des TLfD keine weiteren Rasterfahndungsanordnungen erlassen.

7.4 Polizeiliche Videoüberwachung an öffentlichen Plätzen in Weimar

Mit der Novellierung des PAG im Berichtszeitraum (7.1) wurde u. a. der Polizei die Befugnis eingeräumt, gemäß § 33 Abs. 2 an Kriminalitätsschwerpunkten und an gefährdeten Anlagen oder Objekten Videoüberwachung einzusetzen.
Im Gesetz sind die Rahmenbedingungen dafür festgelegt. Die Videoüberwachung ist danach eine offene polizeiliche Maßnahme die durch geeignete Hinweise erkennbar zu machen ist. Die Maßnahme bedarf gemäß § 33 Abs. 3 PAG der Zustimmung des TIM. Dieses unterrichtet den TLfD. Im § 33 Abs. 4 PAG ist weiter bestimmt, dass die Aufzeichnungs- und Übertragungsgeräte mit technischen Vorkehrungen ausgestattet sein sollen, die insbesondere durch Aufnahme-, Löschungs-, Sperrungs- und Berechtigungssysteme eine hohe Datensicherheit und einen hohen Datenschutz gewährleisten.
Mitte des Jahres 2003 erhielt ich von Seiten des TIM die Information, dass ein Pilotprojekt zur polizeilichen Videoüberwachung im öffentlichen Raum in Weimar - Theaterplatz/Goetheplatz - vorbereitet wird. Es wurde ein Konzeptionsentwurf mit der Bitte zur datenschutzrechtlichen Bewertung zugeleitet. Zu diesem wurden vom TIM ergänzende Unterlagen angefordert. Im Rahmen der darauf folgenden Gespräche machte ich deutlich, dass eine datenschutzrechtliche Bewertung des Vorhabens erst nach Vorlage aller Unterlagen, so auch der diesbezüglichen Dienstanweisung der PD, möglich ist. Es wurde darauf aufmerksam gemacht, dass nicht nur Festlegungen zu Kamerastandorten wichtig sind, sondern auch bezüglich des zu überwachenden Bereichs. Zum zugeleiteten Entwurf der „Dienstanweisung zur polizeilichen Videoüberwachung in Weimar“ wurde Stellung genommen und Änderungshinweise gegeben.
Nachdem durch Pressemitteilung des TIM auf den technischen Testbetrieb für Videoüberwachung in Weimar hingewiesen und die überarbeitete Dienstanweisung zugeleitet wurde, beauftragte ich Mitarbeiter der Dienststelle sich von den technischen Rahmen-bedingungen ein Bild zu verschaffen und den Änderungs- und Ergänzungsbedarf zur Dienstanweisung darzulegen. Auch machten die Beauftragten des TLfD zu diesem vor Ort Termin deutlich, dass noch die Übersichtszeichnung über die Schwenkbereiche der Kameras ausstehen.
Die aktuelle Dienstanweisung zur Videoüberwachung wurde mir unmittelbar vor dem öffentlichen Start des Pilotprojekts zugeleitet.

Daraus war nicht zu entnehmen, dass Lokalredaktionen von Zeitungen oder andere sensible Bereiche tangiert sein könnten.
Auf nachfolgende Presseanfragen bezüglich der Einbeziehung von Gebäuden der Lokalredaktion von Zeitungen habe ich dargelegt, dass ich darüber keine Erkenntnisse habe und hier ein Klärungsbedarf besteht. Während der öffentlichen Vorstellung des Pilotprojekts Ende Oktober war das Gebäude der Lokalredaktionen auf dem Bildschirm in Form einer schwarzen Maske teilweise je nach Zoomfunktion ausgeblendet. Ich habe sowohl schriftlich als auch im Rahmen eines nachfolgenden vor Ort Termins in Weimar deutlich gemacht, dass die Kameraeinstellungen nicht den gesetzlichen Voraussetzungen genügen und unverzüglich Abhilfe zu schaffen ist, da dieser Umstand beanstandungswürdig ist. Vier Tage nach dem Start des Pilotprojekts wurde es insgesamt abgeschaltet, die Daten wurden gelöscht. Dadurch waren weiter gehende datenschutzrechtliche Forderungen entbehrlich.
Gegenwärtig ist kein weiteres Vorhaben in Thüringen gemäß § 33 Abs. 2 Punkt 1 PAG bekannt.

7.5 Automatische Gesichts- und Kennzeichenerfassung

Im Berichtszeitraum wurde im Kreise der DSB des Bundes und der Länder die Thematik diskutiert ob und unter welchen Bedingungen und Rechtsgrundlagen durch die Polizei Systeme zur automatischen Gesichts- und Kennzeichenerfassung eingesetzt werden können.
Es wurde berichtet, dass verschiedene Überlegungen z. B. von Gesichtserkennungssystemen im Bereich der Grenzkontrollstellen oder im Rahmen der Kennzeichenerfassung bestehen, indem vorbeifahrende Fahrzeuge vollautomatisch mit dem Fahndungsbestand abgeglichen und Trefferfälle an die Polizei gemeldet werden sollen.
Dies nahm der TLfD zum Anlass, im TIM nachzufragen, ob auch derartige Überlegungen zur Durchführung bestehen. Man teilte mit, dass die Absicht besteht, ein automatisches Kennzeichenerkennungssystem zu testen. Nachdem konkrete Informationen zum vorgesehenen Projekt vorlagen, teilte der TLfD mit, dass für derartige Datenverarbeitungen im PAG keine Rechtsgrundlage gegeben sei und auch die Anwendung der Regelungen der StPO bezüglich der Datenerhebung Unbeteiligter problematisch erscheine. In diesem Zusammenhang wurde mitgeteilt, dass, wenn man ein solches Verfahren, nach einem Pilotversuch zum Einsatz bringen will, es einer Rechtsänderung bedarf.

Es wurde von Seiten des TIM ein Entwurf einer Konzeption zur „Automatischen Kennzeichenerfassung“ mit der Bitte um eine datenschutzrechtliche Stellungnahme zugeleitet. Noch bevor diese Stellungnahme erfolgte, lag zwischenzeitlich die Information vom TIM vor, dass vom Pilotprojekt Abstand genommen wird und die Ergebnisse der bundesweiten Arbeitsgruppe zur rechtlichen Bewertung entsprechend zugrunde gelegt werden sollen.
Dass Kameras zur „Automatischen Kennzeichenerfassung“ in Thüringen im Einsatz gewesen sein sollen, habe ich aus Pressemeldungen erfahren. Dies war mir Anlass, den Sachverhalt umfassend zu kontrollieren. Es wurde festgestellt, dass im Rahmen der Installation der technischen Ausrüstung kurzzeitig unzulässigerweise außer Kfz-Kennzeichen der Polizei auch Kfz-Kennzeichen anderer öffentlicher Verkehrsteilnehmer auf einem Server gespeichert waren. Dass für das Testverfahren gemäß § 34 ThürDSG keine Freigabe vorlag, habe ich beanstandet. Es wurde die Forderung erhoben, die unzulässig gespeicherten Kfz-Kennzeichen öffentlicher Verkehrsteilnehmer unwiederbringlich zu löschen, was durch ein physisches Löschen des Datenbestandes vollzogen wurde.
Der Vorgang konnte im Berichtszeitraum noch nicht abgeschlossen werden.

7.6 Einhaltung der Prüffristenverordnung

Die am 28. April 2000 in Kraft getretene Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (ThürPolPrüffristVO) schreibt detailliert vor, nach welchen Fristen regelmäßig zu überprüfen ist, ob eine weitere Speicherung von Polizeidaten erforderlich ist. Seitens des TLfD wurde hierzu eine Kontrolle in einer PD durchgeführt, die sich auch darauf erstreckte, wie bei der Aussonderung der zugrunde liegenden Aktenbestände verfahren wird. Das Verfahren gestaltet sich so, dass vom Landeskriminalamt monatlich Prüflisten übersandt werden, anhand deren eine Überprüfung durchgeführt wird, ob entweder eine Verlängerung der Aufbewahrungsfristen erfolgt oder aber die Akten zu löschen sind. Bei Durchsicht der Vorgänge, die am Tag der Datenschutzkontrolle zur Überprüfung anstanden, stellte sich heraus, dass in einem Fall nach einer Dienstanweisung aus dem Jahr 1992 verfahren wurde, obwohl nach der Frist der ThürPolPrüffristVO vorzugehen gewesen wäre. Seitens der PD wurde dann im weiteren Verfahren die zutreffende Prüffrist zugrunde gelegt. Bei der stichprobenhaften Kontrolle der Kriminalakten in der Registratur

war in einem Fall festzustellen, dass der Abschluss des Verfahrens aus der Akte nicht zu entnehmen ist, sodass eine weitere Speicherung nicht mehr angezeigt war. Die PD hat meine Feststellung zum Anlass genommen, diese Kriminalakte zu löschen. Die Archivanbietungspflichten werden beachtet. Als nicht datenschutzgerecht stellte sich das Verfahren der Vernichtung von Akten dar. Die PD hatte mit einer Privatfirma einen Vertrag zur Aktenentsorgung abgeschlossen. Die Leistungsbedingungen des Vertrags enthielten keine detaillierten Regelungen zur Auftragsdatenverarbeitung, wie dies nach § 8 Abs. 2 ThürDSG erforderlich ist. Die datenschutzrechtlichen Defizite des Vertrages wurden als so schwer wiegend angesehen, dass eine Beanstandung nach § 39 Abs. 1 ThürDSG ausgesprochen wurde und die Empfehlung gegeben wurde, den gesamten Vertrag im Hinblick auf die aufgezeigten datenschutzrechtlichen Mängel zu überarbeiten. Die PD wollte zunächst an dem Vertrag festhalten, hat aber nach einer erneuten Intervention des TLfD mitgeteilt, dass bis zu einem zu erarbeitenden Mustervertrag das Schriftgut geschreddert wird und größere Aktenbestände zugangssicher auf dem Gelände der PD in verschlossenen Räumlichkeiten verwahrt würden. Das TIM nahm einen Hinweis des TLfD zum Anlass, das Verfahren auch in den anderen PDs zu überprüfen und hat zwischenzeitlich einen Mustervertrag vorgelegt, an dessen Ausarbeitung der TLfD beteiligt war. Der kritisierte Vertrag in der kontrollierten PD ist zwischenzeitlich in datenschutzgerechter Weise ergänzt worden. Da in der Praxis beim Abschluss von Verträgen nach § 8 ThürDSG immer wieder Mängel festgestellt werden, soll das in der Anlage 23 beigefügte Muster einer Vereinbarung zur Auftragsdatenverarbeitung als Orientierung dazu dienen, welche wesentlichen datenschutzrelevanten Vereinbarungen Gegenstand dieser Verträge zu sein haben.

Noch während dieses Verfahrens setzte das TIM eine Richtlinie zum Umgang mit dienstlichem Schriftgut sowie zur Akten- und Schriftgutaussonderung in den Behörden, Einrichtungen und Dienststellen der Thüringer Polizei (RLAktenThürPol) in Kraft, die zum Teil in datenschutzgerechter Weise den Umgang mit auszusonderndem Schriftgut regelte. Da die Richtlinie zur Sensibilität der Daten bei der Vernichtung von Polizeidaten den Vorgaben zum Datenschutz und der Datensicherheit nicht Rechnung trug, wurde auch sie gemäß § 39 Abs. 1 ThürDSG beanstandet. So war nicht eindeutig sichergestellt, dass ausgesondertes Schriftgut möglicherweise auch von unberechtigten Dritten zur Kenntnis genommen werden konnte und bei Aufträgen zur Übernahme und Vernichtung ausgesonderten Schriftguts nicht die

strikte Einhaltung der Regelungen von § 8 ThürDSG vorgegeben. Meine Vorschläge zur Änderung der Richtlinie wurden zwischenzeitlich vom TIM umgesetzt, sodass die Beanstandung als ausgeräumt angesehen werden kann.

7.7 Unzulässige Anfrage beim Arbeitgeber durch die Polizei

Eine Petentin hatte sich an mich gewandt, weil ein von ihr verfasster Leserbrief mit kritischen Äußerungen zur Darstellung der Polizei in der Presse dazu führte, dass vom Leiter der PD Kontakt zu ihrem Dienstvorgesetzten aufgenommen wurde. Sie bat um Prüfung, woher der PD Leiter die persönlichen Daten erhalten hat bzw. welche Datenermittlungen in diesem Zusammenhang angestellt worden sind.
Nach mehrmaligem Anmahnen teilte der PD Leiter in seiner Stellungnahme mit, dass der Hinweis auf die Dienststelle der Petentin sich aus der „e-mail“ ergeben habe, die einem Leserbrief der Petentin zugrunde lag. Zwischenzeitlich nahm ich auch Kontakt mit dem TIM auf, um den vorliegenden Sachverhalt zu klären.
Gegenüber der PD habe ich infolge eine Beanstandung gemäß § 39 ThürDSG ausgesprochen, da es sich bei der Kontaktaufnahme zum Arbeitgeber der Petentin bezüglich des Inhalts eines privaten Leserbriefes an die Presse um eine unzulässige Datenverarbeitung gehandelt hat.
Zunächst wurde von Seiten der PD ein Verstoß gegen datenschutzrechtliche Bestimmungen nicht anerkannt. Das TIM legte dar, dass die Rechtsauffassung geteilt wird und der Vorfall mit dem PD Leiter auch in datenschutzrechtlicher Hinsicht ausgewertet wird. Auch der betreffende PD Leiter brachte schließlich sein Bedauern über den Vorfall zum Ausdruck, verbunden mit dem Hinweis, dass eine Wiederholung auszuschließen ist.

8. Verfassungsschutz

8.1 Sicherheitsüberprüfungsgesetz

Nachdem ich in den vorangegangenen Tätigkeitsberichten darauf verwiesen hatte, dass für die Durchführung von Sicherheitsüberprüfungen in Thüringen eine gesetzliche Grundlage zu schaffen ist, wurde in diesem Berichtszeitraum das Thüringer Gesetz über die Vorausset-

zungen und das Verfahren von Sicherheitsüberprüfungen und zur Änderung verfassungsschutzrechtlicher Bestimmungen vom 17. März 2003 (GVBl. S. 185 ff) beschlossen.
Im Rahmen des Gesetzgebungsverfahrens wurde ich gemäß §§ 20, 21 ThürGGO beteiligt. In den Stellungnahmen habe ich einige Änderungsvorschläge unterbreitet, die auch teilweise im Gesetzentwurf berücksichtigt wurden. Die noch nicht umgesetzten Punkte wurden im Rahmen der Anhörung im Thüringer Landtag vorgetragen. Dies betraf unter anderem die Formulierung im Gesetzentwurf, dass sich ein Sicherheitsrisiko bei der betroffenen Person auch aufgrund sicherheitserheblicher Erkenntnisse „zu anderen Personen“ ergeben kann, was eine zu weit gehende Formulierung darstellt, weil hier möglicherweise Erkenntnisse zu Personen, die mit der betroffenen Person in keinerlei verwandtschaftlicher oder familiärer Beziehung stehen, ein Sicherheitsrisiko bei der betroffenen Person ergeben könnten. Dabei war nicht einmal ein längerer Zeitraum des Bekanntseins der betroffenen zur anderen Person als Voraussetzung festgelegt. Das Sicherheitsrisiko aufgrund sicherheitserheblicher Erkenntnisse zu anderen Personen wurde in der parlamentarischen Beratung dahingehend modifiziert, dass diese anderen Personen mit der betroffenen Person insbesondere als Ehegatte oder Lebenspartner in enger persönlicher Beziehung stehen.
Ein weiterer Punkt war, das Widerspruchsrecht gegen die Einsichtnahme des TLfD in Sicherheitsüberprüfungsakten nach § 37 Abs. 2 ThürDSG auf Referenz- und Auskunftspersonen auszudehnen. Das Widerspruchsrecht von Auskunfts- und Referenzpersonen wurde gestrichen. Im Ergebnis ist festzustellen, dass die Anregungen und Hinweise des TLfD insgesamt im Gesetz umgesetzt wurden.

Im 5. Abschnitt des Gesetzes bestehen Sonderregelungen bei Sicherheitsüberprüfungen für nicht öffentliche Stellen. Auch hier kommt dem TLfD die Zuständigkeit als datenschutzrechtliche Kontrollbehörde zu. Dies lässt sich daraus ableiten, dass die Vorschriften des 5. Abschnitts anwendbar sind, soweit sie von den übrigen Abschnitten abweichende Regelungen betreffen. Im Übrigen gelten die sonstigen Vorschriften des Sicherheitsüberprüfungsgesetzes, die die Zuständigkeit des TLfD festlegen. Insoweit ist eine einheitliche Kontrollzuständigkeit des TLfD im gesamten Sicherheitsüberprüfungsbereich gegeben.

8.2 Änderungen zum Verfassungsschutzgesetz

Die Änderungen zum Verfassungsschutzgesetz, über die zum Teil schon berichtet wurde (4. TB, 8.1), gingen im Berichtszeitraum in die parlamentarische Beratung. Ich habe darauf hingewiesen, dass es einer normenklaren Abgrenzung der Aufgaben des Verfassungsschutzes zu den Aufgaben von Justiz und Polizei und deren notwendiger Koordinierung bedarf und eine Richtlinie hierfür aus meiner Sicht nicht ausreicht. Gleichwohl sieht das Gesetz vor, dass eine Koordinierung aufgrund einer Richtlinie erfolgen soll. Diese liegt noch nicht vor. Ich habe darum gebeten, mir diese zur datenschutzrechtlichen Bewertung zuzuleiten, was mir auch in Aussicht gestellt wurde. Bedenken habe ich gegen die Neufassung von § 7 Abs. 2 Thüringer Verfassungsschutzgesetz (ThürVSG) geltend gemacht, der den verdeckten Einsatz besonderer technischer Mittel zur Informationsgewinnung im Schutzbereich des Art. 13 GG vorsieht. Da der Kreis der Delikte um weniger gravierende Delikte wie z. B. Urkundenfälschung und Untreue erweitert wird, habe ich den Einsatz besonderer technischer Mittel bei Delikten dieser Art als Eingriff in das Recht auf Unverletzlichkeit der Wohnung und das Recht auf informationelle Selbstbestimmung als unverhältnismäßig angesehen. Das Gesetz sieht vor, dass derartige Maßnahmen erfolgen können, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert würde. Ich habe mich dafür ausgesprochen, den Halbsatz „oder wesentlicher erschwert wäre“ zu streichen, da im Hinblick auf den vorgesehenen Grundrechtseingriff dann eine gerechtfertigte Hürde bestünde. Bei den neuen Eingriffsbefugnissen nach § 7 ThürVSG habe ich vorgeschlagen, diese auf einen Zeitraum von 5 Jahren zu befristen. Gefordert wurde auch bei der nach § 7 Abs. 8 ThürVSG vorgesehenen Unterrichtung des Landtags durch die Landesregierung konkrete Vorgaben aufzunehmen, damit der Bericht auch aussagefähig ist. Angeregt worden war im Hinblick auf das Thüringer Archivgesetz, eine Klarstellung zur Anbietungspflicht ausgesonderter Unterlagen des TLfV. Dies erschien erforderlich, da nach § 11 Abs. 2 ThürArchivG auch „Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder über den Datenschutz unterworfen sind“ vor einer Löschung zur Feststellung der Archivwürdigkeit und ggf. die Übernahme dem zuständigen Archiv anzubieten sind. Der Gesetzgeber ist meinen Anregungen nicht gefolgt.

Im Kreise der DSB wurde im Berichtszeitraum auch die Frage erörtert, inwieweit Regelungen zum Schutz von Berufsgeheimnisträgern

beim verdeckten Einsatz besonderer technischer Mittel erforderlich sind. Ich habe gegenüber dem TIM in Anlehnung an Vorschriften anderer Länder einen entsprechenden Vorschlag unterbreitet. Regelungsbedarf sehe ich auch aufgrund der Änderung in § 15 Abs. 5 Artikel 10-Gesetz - G 10, durch den die Kontrollbefugnis für die gesamte Erhebung und Verarbeitung der Nutzung nach diesem Gesetz erlangten personenbezogenen Daten der G 10-Kommission des Bundes übertragen wurde. Eine Umsetzung dieser aufgrund eines Urteils des Bundesverfassungsgerichts eingeführten Regelung in das Thüringer Landesrecht ist bisher noch nicht erfolgt, sodass sich die Frage nach der zu gewährleistenden Datenschutzkontrolle in diesem Bereich stellt. Dies gilt insbesondere deshalb, weil nach § 16 Abs. 2 Artikel 10-Gesetz - G 10 personenbezogene Daten des Bundesamtes für Verfassungsschutz nur dann an Landesbehörden übermittelt werden dürfen, wenn die Kontrolle ihrer Verarbeitung und Nutzung durch den Landesgesetzgeber geregelt ist. Gegenüber dem TIM habe ich die Auffassung vertreten, dass ich insofern von einer Kontrollzuständigkeit des TLfD ausgehe. Nach § 37 Abs. 3 ThürDSG sind der Kontrolle des DSB nämlich nur die personenbezogenen Daten entzogen, die ausdrücklich der Kontrolle der G 10-Kommission unterliegen. Eine Stellungnahme hierzu steht noch aus.

8.3 Kontrollen im Thüringer Landesamt für Verfassungsschutz

Auch im vergangenen Berichtszeitraum fanden Kontrollen im Thüringer Landesamt für Verfassungsschutz (TLfV) statt. Diesen lagen Anfragen Betroffener zugrunde, die geklärt haben wollten, ob es zu ihnen Datenspeicherungen gab. Im Rahmen der durchgeführten Kontrollen konnte im Ergebnis in keinem Fall festgestellt werden, dass Verstöße gegen das ThürVSG vorlagen.

9. Finanzen - Steuern

9.1 Gesetz zum Abbau von Steuervergünstigungen und Ausnahmeregelungen (Steuervergünstigungsabbaugesetz - StVergAbG)

Im Ende 2002 vorgelegten Entwurf eines StVergAbG der Bundesregierung (BT-Drucksache 15/119) war vorgesehen, durch einen Abbau von Steuervergünstigungen und Ausnahmeregelungen die Steuerehr-

lichkeit und die Einnahmen der öffentlichen Haushalte zu verbessern. In datenschutzrechtlicher Hinsicht enthielt der Gesetzentwurf eine Reihe bedenklicher Neuregelungen, die zu wirksameren Überprüfungsmöglichkeiten von Kapitaleinkünften führen sollten. So war einerseits durch einen Wegfall von § 30 a Abs. 2 AO und eine Neuregelung des § 23 a EStG-E vorgesehen, Kreditinstitute zu verpflichten, einmal pro Jahr Kontrollmitteilungen zu Veräußerungsgeschäften mit Wertpapieren und aus Termingeschäften an das BfF unter Angabe eines Identifikationsmerkmals (§ 139 a AO-E) zu melden. Zum anderen sollten durch die Streichung des § 30 a Abs. 3 AO und die Neuregelung des § 194 Abs. 3 AO-E Verhältnisse anderer Personen als der zu prüfende Steuerpflichtige, bei einer Außenprüfung eines Kreditinstitutes festgestellt, und soweit diese für deren Besteuerung von Bedeutung sein könnten, zwecks Steuerprüfung ausgewertet werden dürfen.
Ich habe im Kreise der DSB des Bundes und der Länder den datenschutzrechtlich relevanten Regelungsgehalt des Gesetzentwurfes kritisiert und das TFM über meine Auffassung in Kenntnis gesetzt. Da der Gesetzesbegründung nicht zu entnehmen war, wie eine Abwägung zwischen der beabsichtigten Erhöhung der Steuergerechtigkeit und dem Grundrecht der Steuerbürger auf informationelle Selbstbestimmung vorgenommen wurde und ob weniger einschneidende Maßnahmen in Betracht gezogen wurden, habe ich die beabsichtigte umfassende Überwachung privater Kapitaleinkünfte im Hinblick auf das Verhältnismäßigkeitsprinzip als bedenklich angesehen. Die mit § 139 a AO-E vorgesehene Einführung eines Identifikationsmerkmals wurde damit begründet, dass die in rechtlicher und tatsächlicher Hinsicht gebotene gleichmäßige Besteuerung eine bessere Prüfbarkeit der Angaben des Steuerpflichtigen erfordere. Dazu sei die Zusammenarbeit der Finanzbehörden zu verbessern, was eine eindeutige Identifizierung des Steuerpflichtigen auf der Grundlage eines eindeutigen, dauerhaften und unveränderlichen Identifikationsmerkmals voraussetze. Da der Text des Gesetzentwurfs eine eindeutige Regelung zu Zweckbindung und Beschränkung hinsichtlich der Nutzung des Identifikationsmerkmals vermissen ließ, war seine Verwendung im Sinne einer allgemeinen Personenkennzahl nicht auszuschließen. Die im Entwurf vorgesehene Regelung der Verwendung des Identifikationsmerkmals mittels Rechtsverordnung habe ich im Hinblick auf das verfassungsrechtliche Bestimmtheitsgebot für bedenklich gehalten und gefordert, den Gesetzestext zum Mindesten um Regelungen zur Verwendung und Nutzungsbeschränkung des Identifikationsmerkmals zu ergänzen.

Angesichts vergleichbarer Sensibilität von personenbezogenen Daten im Steuer- und Sozialbereich, habe ich eine an §§ 18 f, 18 g SGB IV (u. a. Zweckbindung und Beschränkungen der Erhebung, Verarbeitung und Nutzung der Versicherungsnummer) angelehnte Regelung im Falle des vorgesehenen steuerlichen Identifikationsmerkmals angeregt.
Die DSB des Bundes und der Länder haben sich in einer gemeinsamen Stellungnahme vom 13. Dezember 2002 „Entwurf des Steuervergünstigungsabbaugesetz lässt sorgfältige Abwägung zwischen Steuergerechtigkeit und informationellem Selbstbestimmungsrecht vermissen“ (Anlage 24) gegen datenschutzrechtlich bedenkliche Neuregelungen im Entwurf des StVergAbG ausgesprochen. Nachfolgend habe ich die gemeinsame Stellungnahme der DSB des Bundes und der Länder zum StVergAbG dem TFM zur Kenntnis gegeben.
Im weiteren Gesetzgebungsverfahren wurden sämtliche datenschutzrechtlich bedenklichen Neuregelungen aufgegeben. Der Bundestag hat das StVergAbG (BGBl. I Nr. 19 S. 660 ff) am 16. Mai 2003 beschlossen.

9.2 Entwurf eines zweiten Gesetzes zur Änderung steuerlicher Vorschriften

Im Rahmen des Entwurfes eines zweiten Gesetzes zur Änderung steuerlicher Vorschriften (Steueränderungsgesetz 2003) beabsichtigt die Bundesregierung durch Änderungen der AO und des Melderechts, jedem Steuerpflichtigen zum Zwecke der eindeutigen Identifizierung im Steuerverfahren eine bundeseinheitliche lebenslange Identifikationsnummer (IN) für steuerliche Zwecke zuzuordnen, was zu einer Erhöhung der Effizienz der Steuerverwaltung führen soll. Um die IN erstmals bilden zu können, sollen alle Meldebehörden dem BfF für jeden Einwohner - auch für Neugeborene - Daten aus dem Melderegister übermitteln. Das BfF speichert diese Daten mit den zugeteilten IN in einem zentralen Register und teilt den Meldebehörden anschließend die IN zur Speicherung im Melderegister mit. Ebenso ist eine Datenübermittlung an das BfF bei Änderungen der Daten im Melderegister vorgesehen. Des weiteren berechtigt der Entwurf neben Finanzbehörden auch andere öffentliche und nicht öffentliche Stellen die IN zu erheben und zu verwenden.
Im Kreise der DSB des Bundes und der Länder wurde dieses Gesetzgebungsvorhaben kritisch diskutiert. So hat der BfD gegenüber dem Finanz- und Innenausschuss des Deutschen Bundestages und dem

BMF darauf hingewiesen, dass der mit der Einführung einer einheitlichen IN einher gehende Aufbau eines zentralen Registers mit allen aktuellen Adressen aller Einwohner beim BfF erfahrungsgemäß über den ursprünglichen Verwendungszweck hinaus Begehrlichkeiten anderer Stellen wecken wird. Die Vorschläge, Zugriffsmöglichkeiten und Auskunftsrechte von Stellen außerhalb der Finanzverwaltung für andere Zwecke gesetzlich auszuschließen haben in den Neuregelungen der §§ 139 b und 139 c AO des derzeit vorliegenden Gesetzentwurfs Berücksichtigung gefunden.
Darüber hinaus besteht Diskussionsbedarf zur vorgesehenen Umsetzung der Rechtsverordnung gemäß der Verordnungsermächtigung des § 139 d AO. In diesem Zusammenhang erscheint es im Hinblick auf die gebotene Datensparsamkeit fraglich, ob es erforderlich ist, jedem Neugeborenen eine IN zu geben, oder ob es datenschutzgerechter wäre, die IN erst zu vergeben, nachdem der Betroffene erstmals steuerlich in Erscheinung getreten ist. Auch sollten Sanktionsmöglichkeiten bei Verstößen gegen unrechtmäßige Auskunftserteilung in Betracht gezogen werden.

9.3 Entwurf eines Gesetzes zur Förderung der Steuerehrlichkeit

Im Rahmen eines Gesetzentwurfs zur Förderung der Steuerehrlichkeit (BT-Drucksache 15/1309) beabsichtigt die Bundesregierung bisher unentdeckten Steuersündern einen Anreiz zu bieten, in die Steuerehrlichkeit zurückzukehren. Gleichzeitig sollen durch Neuregelungen der AO Überprüfungsmöglichkeiten der Finanzverwaltung verbessert werden, um künftige Steuerhinterziehung zu erschweren. In diesem Zusammenhang erlaubt § 93 Abs. 7 und 8 AO-neu Finanzbehörden für sich selbst oder auf Ersuchen anderer Behörden oder Gerichte bei Kreditinstituten über das BfF Kontoinformationen abzurufen, wenn ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht. Hierzu haben die Kreditinstitute Dateien auch zum automatisierten Abruf bereitzuhalten. Laut Gesetzesbegründung soll den betroffenen Steuerpflichtigen im Einzelfall nach pflichtgemäßen Ermessen der Finanzbehörde Auskunft darüber erteilt werden, ob in ihrem Fall ein Abruf stattgefunden und zu welchem Ergebnis er geführt hat.
Aus datenschutzrechtlicher Sicht wird es für erforderlich angesehen, dass den Steuerpflichtigen ein vom Ermessen der Finanzbehörde unabhängiger Auskunftsanspruch bzw. ein Akteneinsichtsrecht zu dem

erfolgten Abruf von Daten über ihre Konten eingeräumt wird. Auch sollte der Abruf der Kontendaten nur in Einzelfällen erfolgen und sichergestellt werden, dass vor einem Abruf beim Kreditinstitut zumindest erst versucht wurde, die Daten beim Steuerpflichtigen selbst zu erheben. Des Weiteren sollten die Informationsbefugnisse im Rahmen dieses Gesetzesvorhabens auf Finanzbehörden beschränkt werden.

9.4 Offenbarung der Steuernummer leistender Unternehmen durch Neuregelungen im Umsatz- und Einkommenssteuergesetz (StVBG)

Durch das StVBG (BGBl. 2001 I S. 3922) wurde das Umsatzsteuergesetz dahingehend geändert, dass der leistende Unternehmer gemäß § 14 Abs. 1 a UStG ab 1. Juli 2002 in der Rechnung die vom Finanzamt erteilte Steuernummer anzugeben hat. Des Weiteren sind gemäß § 48 b Abs. 3 EStG in der Freistellungsbescheinigung u. a. Name, Anschrift und Steuernummer des leistenden Unternehmens anzugeben.
Da aufgrund dieser Regelungen die Steuernummer des Leistenden gegenüber Außenstehenden offenbart wird, habe ich gegenüber dem TFM angeregt, die Beschäftigten in den Finanzämtern auf eine mögliche Durchbrechung des Steuergeheimnisses gegenüber unberechtigten Anrufern hinzuweisen und um Mitteilung der getroffenen Maßnahmen gebeten.
Nach Auskunft des TFM sind die Beschäftigten der Finanzämter laut einer Verfügung der OFD Erfurt darauf hingewiesen worden, sich vor einer Auskunftserteilung von der Berechtigung des Anfragenden zu überzeugen. Im Zweifel sei, insbesondere bei telefonischen Anfragen, die Auskunft zu verweigern bzw. auf eine schriftliche Anfrage oder persönliche Vorsprache zu orientieren.

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

Zum Entwurf der StDAV vom August 2002 hatte ich eine Reihe datenschutzrechtlich problematischer Formulierungen kritisiert. So habe ich wie DSB des Bundes und der Länder gefordert, die Formulierung in der Begründung des Entwurfs, die AO stelle eine Datenschutzvor-

schrift mit abschließendem Charakter dar und lasse für andere Datenschutzvorschriften keinen Raum, zu streichen. Weiterhin war zu bemängeln, dass zwar in § 7 die erforderlichen Sicherheitsfunktionen als Zielstellung benannt werden, für deren Umsetzung aber nur wenige konkrete Mechanismen vorgegeben werden und zu wichtigen Sicherheitsmechanismen wie Verschlüsselung und elektronische Signatur keine Regelungen enthalten sind. Wegen der raschen technischen Entwicklung sollte auf die Vorgabe technischer Details verzichtet und statt dessen die konkreten Sicherungsmechanismen in einem IT-Sicherheitskonzept, dass dem Fortschritt der Technik jederzeit angepasst werden kann, verankert werden. Des weiteren sollte auch eine Regelung in Betracht gezogen werden, die ähnlich wie im Entwurf der StDÜV von November 2002 (9.7), eine Abstimmung zwischen den federführenden Bereichen der Steuerverwaltung und dem BSI in Fragen der IT-Sicherheit vorsieht. Da der Entwurf automatisierte Aufzeichnungen der Abrufe ausdrücklich vorschreibt, aber dem gegenüber in seiner Begründung Handaufzeichnungen, soweit automatisierte Aufzeichnungen mit vertretbarem Aufwand nicht möglich sind, als zulässig betrachtet werden, habe ich im Hinblick auf die gebotene Rechtsklarheit gebeten, die Begründung dem Regelungstext anzupassen. Da für das im Begründungstext beispielhaft genannte Verfahren ZAUBER (9.7) derzeit m. E. eine Rechtsgrundlage nicht ersichtlich ist, sollte auf eine Bezugnahme zum Verfahren ZAUBER verzichtet werden.
In dem derzeit gültigen Verordnungsentwurf von April 2003 wurde der Aspekt zum Sicherheitskonzept in die Begründung des § 1 einbezogen. Unberücksichtigt blieben dagegen die Bedenken zur Darstellung des Verhältnisses von AO und den Datenschutzgesetzen. Zur Formulierung in § 5 des aktuellen StDAV-Entwurfs, wonach Amtsträger auch „... zur Bearbeitung sonst zugewiesener Aufgaben des Besteuerungsverfahrens ...“ berechtigt sind Daten eines Finanzamts abzurufen, habe ich mich der Kritik des Bundesministeriums der Justiz angeschlossen und eine Streichung der kritisierten Formulierung bzw. eine Präzisierung der Zugriffsvoraussetzungen gefordert.

9.6 Elektronische Steuererklärung (ELSTER) über Internet

Seit dem 1. Januar 2000 ist das Verfahren ELSTER bundesweit im Einsatz.
Für die jeweiligen Veranlagungszeiträume werden unter www.elster.de sowohl das „ElsterFormular 2001“ als auch das „ElsterFormular 2002“ zur Verfügung gestellt.
Bislang sind bundesweit über 2 Millionen Einkommenssteuererklärungen und über 21 Millionen Steueranmeldungen elektronisch eingegangen. Rund 40 % der ELSTER-Erklärungen stammen von Bürgern, 60 % von Lohnsteuer Hilfevereinen und kleineren Steuerberatungs-Büros.
Seit 1. Januar 2002 werden in Thüringen die elektronisch übermittelten Einkommensteuererklärungen bevorzugt bearbeitet.

Bereits in den vorangegangenen Tätigkeitsberichten (3. TB, 9.3; 4. TB, 9.4) stellte ich den Verfahrensablauf von ELSTER und die hier enthaltenen technischen organisatorischen Maßnahmen zur Datensicherheit dar. Zur Nutzung der zentralen Clearingstellen durch die Länder bedarf es einer Verwaltungsvereinbarung, die im Entwurf vorliegt, aber nach Angaben des TFM immer noch nicht in Kraft gesetzt wurde.

Gegenwärtig wird für das Verfahren ELSTER die qualifizierte elektronische Signatur eingeführt. Die rechtliche Grundlage für die Gleichstellung der elektronischen Signatur bei elektronischen Steuererklärungen ergibt sich aus § 150 und § 87 a AO i. V. m. der Steuerdaten-Übermittlungsverordnung (StDÜV). Die qualifizierte elektronische Signatur dient der Authentifizierung des Nutzers und der Überprüfung der Datenintegrität. Sie ist somit ein wichtiger Schritt auf dem Weg zu einer sicheren papierlosen Steuererklärung. Eine elektronische Übermittlung der Einkommenssteuererklärung in Verbindung mit einer nach dem SigG zugelassenen qualifizierten elektronischen Signatur ist der handschriftlichen Unterschrift auf den amtlichen Vordrucken gleichgestellt.
Problematisch ist allerdings, dass gemäß § 87 a AO i. V. m. § 7 StDÜV bis zum 31. Dezember 2005 auch eine „qualifizierte elektronische Signatur mit Einschränkungen“, also nur eine fortgeschrittene Signatur (4. TB, 15.7), eingesetzt werden darf.

Die DSB des Bundes und der Länder lehnen die gesetzliche Einschränkung der qualifizierten elektronischen Signatur im Finanzbereich ab, zumal administrative und technische Voraussetzungen für eine qualifizierte elektronische Signatur nach dem SigG inzwischen weitgehend vorhanden sind. Weiterhin bietet die „qualifizierte elektronische Signatur mit Einschränkungen“ bspw. keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit der elektronischen Dokumente.
Vor diesem Hintergrund empfahl die Konferenz der DSB des Bundes und der Länder auf der Datenschutzkonferenz am 27./28. März 2003 (Anlage 12) der Bundesregierung u. a., dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden und das Verfahren ELSTER zu nutzen, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Zurzeit wird für das Verfahren ELSTER an der Umsetzung der qualifizierten elektronischen Signatur unter Verwendung von beliebigen Signaturkarten im Pilotverfahren gearbeitet. Aufgrund der bisher nur unzureichenden Verbreitung von Signaturkarten wurde im April 2003 ein Signaturbündnis gegründet, dem neben dem Bundesministerium der Finanzen auch die Partner verschiedener Banken beigetreten sind. Weiterhin ist die Einbindung von Mitarbeiterkarten größerer Arbeitgeber geplant.
Ziel ist es, dass zukünftig Signaturkomponenten (Chipkarte, Chipkartenleser, Zertifikat und Treiber usw.) beliebiger Hersteller innerhalb der elektronischen Steuererklärung verwendet werden können, soweit sie die Anforderungen des Signaturgesetzes bzw. der Signaturverordnung erfüllen.
Die Referenzliste der derzeit im Verfahren ELSTER unterstützten Chipkarten und Kartenlesegeräte einschließlich der Angaben, ob es sich zurzeit um eine „qualifizierte elektronische Signatur mit Einschränkung“ oder eine gemäß dem SigG handelt, ist unter www.elster.de/ssl/index-projekt.htm im Internet einsehbar.
Die Anwendung der elektronischen Signatur, die sich noch in der Pilotierungsphase befindet, ist ab ElsterFormular 2002 möglich und wird bisher von einigen Steuerverwaltungen der Länder praktiziert. Nach Angaben der Oberfinanzdirektion Erfurt ist die Teilnahme Thüringens von der weiteren Entwicklung des Verfahrens und der Akzeptanz der Signaturkarten abhängig.

9.7 Das Verfahren ZAUBER - Zentrale Datenbank zur Speicherung und Auswertung von Umsatzsteuer-Betrugsfällen und Entwicklung von Risikoprofilen

Ende 2001 hatte das TFM gemäß § 7 Abs. 3 ThürDSG informiert, dass in Thüringer Finanzämtern das Verfahren ZAUBER eingesetzt wird, welches den Zugriff auf eine beim BfF geführte Datenbank von Umsatzsteuerbetrugsfällen ermöglicht. Im Rahmen des Kontrollbesuchs in der Bußgeld - und Strafsachenstelle (BuStra) eines Thüringer Finanzamts wurde das Verfahren ZAUBER vor Ort kontrolliert.
Ziel der Datenbank ist es, durch einen direkten Zugriff der Landesfinanzbehörden auf die Datenbank mit bundesweiter Erfassung von Betrugsfällen im Bereich der Umsatzsteuer eine effektive Bekämpfung von Umsatzsteuerdelikten bzw. die Sicherung des Umsatzsteueraufkommens zu ermöglichen.
In der Datenbank werden Angaben von natürlichen und juristischen Personen, Personenzusammenschlüsse aus folgenden Fällen gespeichert:

- unabhängig vom späteren Ausgang eingeleitete Strafverfahren wegen einfacher und gewerbsmäßiger oder bandenmäßiger Steuerhinterziehung sowie eingeleiteter Bußgeldverfahren wegen Schädigung des Steueraufkommens,
- Scheinunternehmen,
- Scheinrechnungen,
- Kraftfahrzeuge, d. h. alle bei Außenprüfungen festgestellten Fälle von grenzüberschreitenden Kfz-Lieferungen mit Ausnahme von Lieferungen des Herstellers oder bei Fahrzeugeinzelbesteuerung ab 5.000 pro Fahrzeug,
- Fälle mit einem festgestellten umsatzsteuerlichen Mehrergebnis ab 125.000.

In Abstimmung unter den obersten Finanzbehörden des Bundes und der Länder wurde dem BfF die Pflege der Datenbank, die Auswertung der Daten und die Entwicklung von Risikoprofilen übertragen.
Vor Ort im Finanzamt war festzustellen, dass von den Mitarbeitern neben dem Abruf von Daten aus der Datenbank auch Daten aus den zu bearbeitenden Ermittlungsverfahren eingegeben werden können, sodass es sich bei dem Verfahren nicht - wie es aufgrund der mir zunächst zur Verfügung gestellten Unterlagen schien - um ein reines automatisiertes Abrufverfahren handeln konnte.
Insoweit stellte sich die Frage nach der Rechtsgrundlage für die Führung einer solchen Datei. Die Auffassung der Finanzverwaltung, § 5

Abs. 1 Nr. 13 FVG und § 88 a AO als Rechtsgrundlagen des Verfahren anzusehen, wird nicht geteilt. Gemäß § 5 Abs. 1 Nr. 13 FVG ist das BfF mit der Aufgabe, der zentralen Sammlung und Auswertung der von den Finanzbehörden der Länder übermittelten Informationen über Umsatzsteuer im Bereich der USt betraut. Demgegenüber mangelt es jedoch an einer Befugnis für die Bereitstellung dieser Daten zum Abruf durch andere Behörden. Nach § 88 a AO dürfen die Finanzbehörden nach § 30 AO geschützte Daten auch für Zwecke künftiger Verwaltungsverfahren, Rechnungsprüfungsverfahren, gerichtlicher Verfahren in Steuersachen, Strafsachen wegen einer Steuerstraftat oder Bußgeldverfahren wegen einer Steuerordnungswidrigkeit insbesondere zur Gewinnung von Vergleichswerten in Dateien oder Akten sammeln und verwenden, soweit es zur Sicherstellung einer gleichmäßigen Festsetzung und Erhebung der Steuern erforderlich ist. Zweck des Verfahrens ZAUBER ist aber nicht die Sicherstellung einer gleichmäßigen Festsetzung und Erhebung der Steuern, sondern die Bekämpfung von Umsatzsteuerdelikten und die Sicherung des Umsatzsteueraufkommens. Darüber hinaus bietet § 88 a AO nach meiner Auffassung auch keine Rechtsgrundlage für einen bundesweiten Zugriff auf die beim BfF gespeicherten Daten aller Finanzämter der Länder.

Das Verfahren ist vielmehr als eine beim BfF geführte Verbunddatei anzusehen, wobei die Verantwortlichkeit für die Daten bei den einzelnen Finanzämtern aller teilnehmenden Bundesländer als speichernde Stellen verbleibt. Insoweit bedarf es einer normenklaren, gesetzlichen Grundlage für den Betrieb der Datenbank ZAUBER, die bislang nicht vorliegt. Die diesbezüglichen Bedenken werden auch vom Bundesbeauftragten für den Datenschutz geteilt.

Darüber hinaus war zu bemängeln, dass es an normenklaren differenzierten Regelungen fehlt, zu welchen Fallgruppen Daten zu speichern sind, zur Verantwortlichkeit für die gespeicherten Daten sowie zur Löschung der Daten.

Einvernehmen konnte mit der Steuerverwaltung darüber erzielt werden, dass die Daten verarbeitenden Stellen in Thüringen für die Auskunftserteilung nach § 13 ThürDSG für die von ihnen eingestellten Daten zuständig sind und ihnen gegenüber die Betroffenenrechte auf Löschung, Sperrung und Berichtigung bestehen.

Es sind detaillierte Regelungen zu Pflichtfeldern und freien Feldern erforderlich, damit es den Mitarbeitern nicht freigestellt ist, welche personenbezogenen Daten eingegeben werden.

Die Einstellung von Daten aus allen Ermittlungsverfahren, unabhängig von deren Ausgang erscheint als datenschutzrechtlich bedenklich. Insbesondere ist eine fortgesetzte Speicherung in Fällen, in denen sich ein Tatverdacht nicht bestätigt hat oder das Verfahren gegen eine geringe Auflage eingestellt wurde, als unverhältnismäßig anzusehen. Die undifferenzierte Speicherfrist von 10 Jahren für alle Daten ohne Differenzierung hinsichtlich des Ausgangs des Verfahrens stößt auf erhebliche Bedenken.
Meiner Anregung, die Passwortmindestlänge von 5 auf 8 Stellen zu erhöhen, wurde durch Weisung der OFD entsprochen.
Seitens des TFM wurde angekündigt, das Erfordernis einer einheitlichen Regelung beim BMF vorzutragen und wegen der grundsätzlichen Bedeutung des Verfahrens infolge seiner bundesweiten Nutzung die Problematik an die entsprechenden Gremien des Bundes und der Länder weiterzuleiten.

9.8 Kontrolle in einer Bußgeld- und Strafsachenstelle bei einem Thüringer Finanzamt

Die Finanzbehörden sind bei dem Verdacht einer Steuerstraftat zuständig für die Ermittlung des Sachverhalts. Sie führen das Ermittlungsverfahren aufgrund des § 386 Abs. 2 AO selbständig durch und nehmen die Rechte und Pflichten wahr, die der Staatsanwaltschaft im Ermittlungsverfahren zustehen(§ 399 AO). Die Finanzbehörden sind auch zuständige Verwaltungsbehörde im Bußgeldverfahren bei Steuerordnungswidrigkeiten nach §§ 377 ff AO. Für diese Aufgaben sind in Finanzämtern Bußgeld- und Strafsachenstellen (BuStra) eingerichtet. Die Arbeit dieser Stellen beginnt i. d. R. mit Eingang einer Verdachtsanzeige durch den Innendienst oder der Anzeige eines bei einer Außenprüfung eingeleiteten Ermittlungsverfahrens, aber auch bspw. bei Eingang einer Selbstanzeige, wie vor Ort bei der Kontrolle in einer BuStra bei einem Finanzamt festgestellt werden konnte.
Bei Eingang von Verdachtsanzeigen oder eingeleiteten Ermittlungsverfahren zu Steuerstraftaten werden in der BuStra Karteikarten zu den Beschuldigten und Betroffenen angelegt. Nach den Aufbewahrungsbestimmungen der Finanzverwaltung sind Karteikarten nach Ablauf der Aufbewahrungsfrist von 5 Jahren nach Ablauf des Kalenderjahres, in dem die letzte Eintragung vorgenommen wurde, auszusondern bzw. zu löschen. Da bisher noch keine Aussonderung vorgenommen wurde, wurde gefordert, die Karteikarten aller Beschuldigten

und Betroffenen unverzüglich zur zulässigen Aufbewahrungsfrist zu überprüfen und ggf. Aussonderungen vorzunehmen.
Bei der stichprobenmäßigen Einsicht in Ermittlungsakten war festzustellen, dass diese grundsätzlich Abfragen zum BZR enthielten. In Anbetracht einer vorgefundenen hohen Anzahl von ergebnislosen Abfragen (keine Eintragungen) zu letztendlich eingestellten Ermittlungsverfahren wurde angeregt zu prüfen, ob beim BZR erst dann angefragt werden sollte, wenn abzusehen ist, dass das betreffende Verfahren zumindest nicht nach § 170 Abs. 2 StPO eingestellt wird.
In einer Handakte zu einer Ermittlungsakte wurde eine Auflistung aus dem Verfahren IABV vorgefunden, die neben Angaben zum Beschuldigten auch solche zu Personen gleichen Nachnamens enthielt. Es wurde veranlasst, die Daten Dritter zu schwärzen. Eine andere Handakte enthielt eine Mitteilung der Staatsanwaltschaft, die neben Angaben zu dem im betreffenden Ermittlungsverfahren Beschuldigten auch Daten Unbeteiligter enthielt. Es wurde der Vorschlag aufgenommen, mit der zuständigen Staatsanwaltschaft zu vereinbaren, künftig in Übernahmefällen nur Angaben zu den jeweiligen Betroffenen zu übersenden.
Der Forderung, die OFD-Verfügung an die geänderten Richtlinien für das Strafverfahren und das Bußgeldverfahren anzupassen, wurde ebenfalls entsprochen.
Darüber hinaus wurde festgestellt, dass eine unbefugte Kenntnisnahme personenbezogener Daten aufgrund der Regelung, dass Reinigungskräfte im Rahmen des Reinigungsvertrags Unterlagen zur Vernichtung durch den Hausmeister transportieren sollten, nicht ausgeschlossen werden konnte. Dies wurde eingestellt und im Nachgang eine Firma mit der datenschutzgerechten Aktenvernichtung beauftragt, was als geeignete Maßnahmen zur Einhaltung datenschutzrechtlicher Bestimmungen anzusehen ist.
Meiner Forderung, das Verfahrensverzeichnis nach § 10 ThürDSG gemäß den Vorgaben des novellierten ThürDSG zu ergänzen, wurde ebenfalls entsprochen.

9.9 Datenschutz in einem Thüringer Finanzamt

Bei einer datenschutzrechtlichen Kontrolle in einem Thüringer Finanzamt im Berichtszeitraum wurde die Hebelschubanlage des Archivraums unverschlossen vorgefunden. Zu diesem Zeitpunkt war keine Registraturkraft anwesend. Da sich im gleichen Raum auch das Zwischenarchiv einer anderen Dienststelle befindet, konnte aufgrund

der Zugangsmöglichkeit für die im Bereich des Finanzamts unzuständigen Mitarbeiter der anderen Dienststelle eine Durchbrechung des Steuergeheimnisses nach § 30 AO durch unbefugte Einsichtnahme in Steuerakten nicht ausgeschlossen werden. Meiner Forderung, umgehend dafür Sorge zu tragen, dass die Hebelschubanlage nach jeder Benutzung unverzüglich verschlossen wird, wurde entsprochen.
Der Forderung, die Reinigung der Diensträume entweder in Anwesenheit der Mitarbeiter des Finanzamtes durchzuführen oder ausreichende Möglichkeiten für den Verschluss der Arbeitsunterlagen nach Dienstende zu schaffen, wurde dadurch entsprochen, dass die Reinigung künftig in der Dienstzeit in Anwesenheit der Bediensteten des Finanzamtes durchgeführt wird.

9.10 Kontrolle in einem Thüringer Finanzamt

Bei einer Kontrolle anlässlich einer Zeitungsmeldung wurden in einem Finanzamt datenschutzrechtliche Verstöße festgestellt, weshalb eine Beanstandung gemäß § 39 ThürDSG auszusprechen war.
Um eine Offenbarung personenbezogener Daten gegenüber Unbefugten während der Reinigung der Diensträume auszuschließen, war sicherzustellen und im Reinigungsvertrag zu fixieren, die Reinigung künftig nur noch während der Dienstzeit in Anwesenheit der Mitarbeiter vorzunehmen. Da bei technischen Störungen ein Zugang Dritter erforderlich ist, wurde empfohlen, ausreichende Möglichkeiten für eine Verschlusssicherheit der Akten zu schaffen. Für eine Übergangszeit wurde eine Verpflichtung des Hausmeisters, eines Mitarbeiters einer anderen Stelle, auf das Steuergeheimnis nach § 30 AO als ausreichend angesehen.
Da eine Schlüsselordnung nicht vorlag, habe ich gefordert, umgehend eine schriftliche Schlüsselordnung zu erarbeiten. Dem wurde Rechnung getragen.
Vor Ort war außerdem festzustellen, dass die Tür des Lieferanteneingangs ungesichert offen stand. Meiner Forderung, den Zugang von Lieferanten umgehend zu regeln, um zu gewährleisten, dass ein unkontrollierter Zugang Unbefugter weitestgehend ausgeschlossen ist, wurde nachgekommen.
Da auch bei Transport und Vernichtung von Akten eine Kenntnisnahme personenbezogener Daten durch Unbefugte nicht auszuschließen war und lediglich eine mündliche Weisung bestand, habe ich gefordert, dem abzuhelfen. Im Nachgang wurde eine Fremdfirma mit der Aktenvernichtung beauftragt. Um die Einhaltung der datenschutz-

rechtlichen Bestimmungen beurteilen zu können, habe ich um Übersendung der zu Grunde liegenden Vereinbarung zur Auftragsdatenverarbeitung nach § 8 ThürDSG gebeten.

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

Bei einer Kontrolle in einer Außenstelle des StARoV wurde festgestellt, dass die Telefongebührendaten von Mitarbeitern der Außenstelle durch das Finanzamt als Betreiber der Telefonanlage in Auftragsdatenverarbeitung verarbeitet werden. Meiner Forderung, die hierfür erforderliche Dienstvereinbarung mit dem Personalrat gemäß § 74 Abs. 3 Nr. 18 ThürPersVG abzuschließen, wurde entsprochen.
Laut Hausverfügung ist innerhalb eines Sachgebiets ein Zugriffsprofil vorgeschrieben, welches das Lesen von Dateien anderer Mitarbeiter erlaubt, jedoch schreibenden und löschenden Zugriff ausschließt. Dem gegenüber wurde üblicherweise ein Zugriffsprofil verwendet, das auch schreibenden und löschenden Zugriff auf Dateien anderer Mitarbeiter erlaubt. Da diese Praxis ungeeignet ist, die Integrität, Verfügbarkeit und Authentizität der Daten zu gewährleisten, wurde der verantwortliche Mitarbeiter zur Umsetzung der Hausverfügung verpflichtet.
Die zur Identifikation der Nutzer verwendeten Passworte sind aufgrund der eingeschränkten Funktionalität der verwendeten Software zeitlich nicht zu begrenzen. Meiner Anregung, künftig alle Mitarbeiter durch die Systembetreuung an einen bevorstehenden Wechsel der Passworte zu erinnern und dies in der Hausverfügung zu fixieren, wurde entsprochen.
Da eine Schlüsselordnung für die vom StARoV im Gebäude des Finanzamtes genutzten Räume nicht vorlag, habe ich eine Regelung zum Zugangsrecht zu den Diensträumen und den Umgang mit Schlüsseln gefordert. Der Forderung wurde nachgekommen.
Auf eine mögliche Kenntnisnahme personenbezogener Daten durch Unbefugte bei der Aktenvernichtung angesprochen, wurde zugesagt, die Vernichtung von Akten künftig ausschließlich durch Mitarbeiter der Außenstelle in einem eigenen Aktenvernichter vorzunehmen. Mit Umsetzung dieser Zusage wurden geeignete Maßnahmen zur Einhaltung datenschutzrechtlicher Bestimmungen getroffen.
Weiterhin wurde gefordert, eine mögliche unbefugte Kenntnisnahme personenbezogener Daten im Zusammenhang mit Reinigungsarbeiten zu verhindern. Dem ist durch Verlegung der Reinigungszeiten in die

Dienstzeiten der Außenstelle Rechnung getragen worden, wodurch die Reinigung in Anwesenheit der Mitarbeiter erfolgt.
Das Zwischenarchiv der Außenstelle des StARoV befindet sich gemeinsam mit dem Zwischenarchiv des Finanzamtes in einem Kellerraum. Zugangsberechtigt sind sowohl Mitarbeiter des StARoV als auch des Finanzamtes. Die Akten sind in einer Hebelschubanlage untergebracht. Zum Zeitpunkt der Kontrolle wurde diese Anlage unverschlossen vorgefunden. Durch die Zugangsmöglichkeit auch der jeweils unzuständigen Mitarbeiter des Finanzamtes bzw. des StARoV ist die Vertraulichkeit i. S. v. § 9 Abs. 2 Ziffer 1 ThürDSG nicht gewährleistet. Meiner Forderung, umgehend dafür Sorge zu tragen, dass die Anlage nach jeder Benutzung unverzüglich verschlossen wird und die diesbezügliche Anweisung zu dokumentieren, wurde Rechnung getragen. Da derzeit ein Teil der Hebelschubanlage aufgrund baulicher Besonderheiten nicht verschließbar ist, kann eine Kenntnisnahme personenbezogener Daten durch Unbefugte aber weiterhin nicht ausgeschlossen werden. Daher habe ich gefordert, geeignete technisch-organisatorische Maßnahmen zu ergreifen um diesem Zustand abzuhelfen. Diese Forderung soll nach Auskunft des StARoV mit der Auflösung der Außenstelle umgesetzt werden.

9.12 Kontrolle in der Staatskasse

Wie bereits im 3. TB (9.8) berichtet, wurde in der Staatskasse Erfurt das Verfahren zur Aufrechnung von Forderungen Steuerpflichtiger mit Ansprüchen aus deren Steuerschuldverhältnis kontrolliert.
Hierbei wurde u. a. festgestellt, dass eine programmgesteuerte Protokollierung der Abfragen auf das Integrierte Automatische Besteuerungsverfahren der Thüringer Steuerverwaltung (IABV) zu Nachweiszwecken im Sinne der Steuerdaten-Abruf-Verordnung (StDAV) nicht realisiert war. Statt dessen wurde zum damaligen Zeitpunkt die Protokollierung in manueller Form vorgenommen. Wegen der fehlenden programmgesteuerten Protokollierung war die Zulässigkeit des Abrufs als nicht uneingeschränkt gegeben zu beurteilen.
Mit dem Nachfolgeprojekt „UNIX im Finanzamt“ (UNIFA) wird eine umfassende programmgesteuerte Protokollierung der Nutzerzugriffe ermöglicht.
Nachdem von Seiten der OFD im Berichtszeitraum die Einführung der programmgesteuerten Protokollierung in der Staatskasse zur Kenntnis gegeben wurde, konnte der Vorgang abgeschlossen werden.

9.13 Behandlung von personenbezogenen Daten durch das Thüringer Landesamt zur Regelung offener Vermögensfragen

Zu einem Verwaltungsverfahren nach §§ 30 ff Vermögensgesetz (VermG) hat mir ein Petent folgendes datenschutzrechtliches Problem vorgetragen: Die an den Bürger gerichtete Mitteilung der beabsichtigten Entscheidung war seitens des Thüringer Landesamtes zur Regelung offener Vermögensfragen (ThLARoV) in vollem Umfang auch an Personen versandt worden, die nur hinsichtlich eines der beantragten Grundstücke des Petenten als Verfügungsberechtigte anzusehen waren, wodurch diese Personen auch über die ihre Interessen nicht berührende Grundstücke des Beschwerdeführers Kenntnis erhielten.
Gemäß § 32 Abs. 1 Satz 3 VermG sind bei der Vorbereitung einer Verwaltungsentscheidung die in ihren Rechten Betroffenen am Verfahren zu beteiligen. Dabei ist jedoch dafür Sorge zu tragen, dass personenbezogene Daten nur gegenüber den Verfahrensbeteiligten in dem jeweils erforderlichem Umfang offenbart werden.
Nach Auskunft des ThLARoV seien die Mitarbeiter des Amtes um eine Wiederholung eines solchen Vorkommnisses zu vermeiden, nach einer Auswertung der Angelegenheit angewiesen worden, grundsätzlich in jedem Einzelfall zu prüfen, in welchem Umfang ein Bescheid den Verfahrensbeteiligten zuzustellen ist.

9.14 Fehlerhafte Adressierung durch das Finanzamt

Ein Bürger wandte sich gemäß § 11 ThürDSG an die Dienststelle des TLfD und teilte mit, dass er von einem Finanzamt versandte Unterlagen für seinen vor zwei Monaten verzogenen Vormieter in einem geöffneten A4-Umschlag steckend, in seinem Briefkasten vorgefunden habe.
Um Stellungnahme gebeten, teilte das Finanzamt mit, dass die Postsendung versehentlich mit der alten Anschrift adressiert worden sei. Weshalb die Zustellung durch das beauftragte Unternehmen in den nicht mehr mit dem Namen des Vormieters gekennzeichneten Briefkasten erfolgte und aus welchem Grunde der Umschlag geöffnet war, konnte nicht mehr festgestellt werden. Nach Auskunft das Finanzamtes werden die zum Versand bestimmten Briefe maschinell verschlossen, sodass die Versendung unverschlossener Briefe ausgeschlossen ist. Der Vorfall wurde im Finanzamt ausgewertet und die Mitarbeiter

auf ihre Sorgfaltspflicht hingewiesen, um eine Wiederholung zu vermeiden.

In einem weiteren Beschwerdefall hatte der Betroffene Kopien von Unterlagen verschiedener Gesellschaften, bei denen er versichert war, als Anlage der Einkommenssteuererklärung an ein Finanzamt übersandt. Nachfolgend wurden ihm diese Unterlagen, von einer der Versicherungsgesellschaften, mit denen er in vertraglicher Beziehung stand, ohne gesondertes Anschreiben zurückgesandt.
Da eine Versicherungsgesellschaft hier Einsicht in sämtliche Versicherungsverhältnisse des Betroffenen bei anderen Versicherern nehmen konnte, war von einem Verstoß gegen das Steuergeheimnis nach § 30 AO auszugehen. Daher habe ich das Finanzamt um Auskunft gebeten, aus welchem Grunde die Unterlagen nicht an den Betroffenen zurückgesandt wurden, sondern an die unbeteiligte Versicherungsgesellschaft gelangten.
Nach Auskunft des Finanzamtes ist zur Rücksendung der Unterlagen anstelle eines Schreibens mit der Adresse des Steuerpflichtigen versehentlich ein Versicherungsschein mit der Anschrift des Versicherers in einen Umschlag mit Sichtfenster kuvertiert worden, wodurch es zur fehlerhaften Versendung an die Adresse des Versicherers kam.
Der Vorfall wurde im Finanzamt ausgewertet, wobei die Mitarbeiter auf die ordnungsgemäße Adressierung und die Einhaltung ihrer Sorgfaltspflicht hingewiesen wurden.

9.15 Transport von Unterlagen durch den Thüringen-Courier in der Landesverwaltung

Der Presse war zu entnehmen, dass Akten einer Staatsanwaltschaft mit personenbezogenen Daten, die für ein Amtsgericht bestimmt waren, unverschlossen im Hof eines Landratsamtes abgestellt waren. Den Transport hatte der unter Aufsicht des TFM stehende Thüringen-Courier der OFD durchgeführt. Meine Nachfragen ergaben, dass es sich um eine postübliche Versandkiste handelte, die mit einem einrastenden Deckel verschließbar ist. Das Amtsgericht selbst wurde jedoch vom Thüringen-Courier nicht angefahren. Die Sendung wurde daher zum Landratsamt gebracht, das als „Relaisstation“ fungiert, weil von dort aus eigene Fahrer die Kisten weiter transportieren konnten. In diesem Fall kam es jedoch nicht direkt zum Weitertransport der Kiste. Der Landrat fand sie abends ungesichert im Hof des Landratsamts auf und nahm sie in Gewahrsam.

Dies war datenschutzrechtlich wie folgt zu bewerten:
Gemäß § 9 ThürDSG haben öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, den Datenschutz zu gewährleisten. Bei den zum Transport vorgesehenen Unterlagen der Staatsanwaltschaft lag ein hoher Schutzbedarf vor. Die Gewährleistung eines angemessenen Datenschutzes ist während des gesamten Datenverarbeitungsprozesses von der Datenerhebung bis zur Löschung der Vernichtung der Daten erforderlich. Im Rahmen der Weitergabekontrolle ist zu gewährleisten, dass personenbezogene Daten während des Transports nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Insoweit ist eine Versandart bzw. das Transportmittel so auszuwählen, das dem vorliegenden Schutzbedarf der personenbezogenen Daten ausreichend und angemessen Rechnung trägt.
In den Stellungnahmen des TFM und der Staatsanwaltschaft wurde mitgeteilt, dass die betreffende Postkiste verschlossen war. Eine Inaugenscheinnahme von Postkisten, die für den Transport vorgesehen sind, ergab, dass eine vergleichbare Postsendung in dem stabilen Transportbehältnis durch Einrasten des Deckels sowie durch Klebeband verschlossen war. Nach den Bestimmungen für den Transport durch den Thüringen-Courier sind die Absender dafür verantwortlich, die Postsendung entsprechend zu verpacken. Die Fahrer des Kurierdienstes waren dahingehend unterwiesen, dass das Kuriergut vor dem Zugriff durch Unbefugte zu schützen ist und keinesfalls unbeaufsichtigt abgestellt oder offen liegen gelassen werden darf. Nach der Sachverhaltsermittlung war dem auch nachgekommen worden. Bei der Abgabe der Kiste im Landratsamt war darauf hingewiesen worden, dass sie zur Abgabe beim Amtsgericht bestimmt ist. Ein Fahrer des Landratsamtes hatte den Angaben zufolge den Auftrag auch erhalten.
Eine Anfrage beim TJM hat ergeben, dass die für das Amtsgericht bestimmten Unterlagen letztendlich vollständig den Empfänger erreicht haben. In Auswertung des Vorkommnisses wurden die zuständigen Mitarbeiter des Landratsamts per Dienstanweisung über den Umgang mit Kuriergut belehrt. Die OFD hat zwischenzeitlich auf die Inanspruchnahme der Landratsämter als „Relaisstationen“ verzichtet. Post wird seither nur noch für Dienststellen transportiert, die im Gesamtverzeichnis der vom Kurierdienst anzufahrenden Stellen aufgeführt sind. Das Kuriergut ist ausschließlich bei Poststellen, Wachen oder Pförtnern persönlich abzugeben. Für besondere Sendungen wurde ein Lieferscheinsystem als geeignete Maßnahme zur Transportkon-

trolle eingeführt. In Anbetracht der veranlassten und eingeleiteten Maßnahmen der zuständigen Stellen waren daher weiter gehende datenschutzrechtliche Forderungen entbehrlich.

9.16 Zulässigkeit der Verarbeitung von Telefonverbindungsdaten

Des öfteren wird der TLfD hinsichtlich der Zulässigkeit der Verarbeitung von Telefonverbindungsdaten in den Behörden um seine datenschutzrechtliche Bewertung gebeten (1. TB, 15.7; 4. TB, 6.10). In meinen Stellungnahmen habe ich stets darauf hingewiesen, dass bezüglich der Verarbeitung und Nutzung von Gesprächsverbindungsdaten zunächst zwischen privaten und dienstlichen Gesprächen unterschieden werden muss. Während sich jede weitere Speicherung und Nutzung von Verbindungsdaten über Privatgespräche nach der Gebührenzahlung durch den betreffenden Mitarbeiter verbietet, bestehen aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken für einen überschaubaren Zeitraum noch die Verbindungsdaten der dienstlich deklarierten Telefongespräche für Stichprobenprüfungen weiterhin vorzuhalten und ggf. zu nutzen, soweit dies insbesondere in Dienstvereinbarungen vorgesehen ist. Zu beachten ist lediglich, dass die Prüfungen insbesondere bei sensiblen Bereichen nur durch die jeweiligen fachlich zuständigen Vorgesetzten erfolgen, um zu verhindern, dass unzuständige und somit unbefugte Mitarbeiter gegenüber offenbart wird, mit welchen Ferngesprächsteilnehmern dienstliche Gespräche geführt werden mussten.

Im Berichtszeitraum wurden vom TFM Landesdienststellen gebeten, zum Zweck des Abgleichs von Daten der TK-Anlagen von Landesdienststellen mit Rechnungsdaten und Einzelverbindungsnachweisen der Deutschen Telekom AG, alle bei ihnen aktuell vorhandenen Daten aus der/den TK-Anlage(n) und ggf. noch älteren Datenbeständen auf vorhandenen Sicherheitskopien der Staatskasse zu übersenden. Die Überlegungen waren, dass mit dem Abschluss der technischen Vorbereitung permanent Daten aus den einzelnen TK-Anlagen abgefordert werden sollten und durch eine spezielle Software für Rechnungsprüfungszwecke aufbereitet werden sollten. Einige Dienststellen hatten aus datenschutzrechtlichen Erwägungen oder wegen technischer Schwierigkeiten Datenübermittlungen abgelehnt. Bei einer Kontrolle in der Staatskasse war feststellbar, dass die erfolgten Datenübermittlungen EDV-mäßig aufbereitet zur Verfügung standen. Datenschutz-

rechtlich relevant in diesem Zusammenhang war der Umstand, dass Dienststellen in ihren Datensätzen u. a. alle Verbindungen einer konkreten Nebenstelle zugeordnet, angegeben haben. Auch wurden dienstliche und sogar private Verbindungen zum Teil vollständig (also ungekürzt) mitgeteilt. Die mitunter vorliegenden langen Speicherzeiträume verschärften die datenschutzrechtliche Problematik noch erheblich.
Die Datenanforderungen des TFM waren nach Auffassung des TLfD zu weit gehend und darüber hinaus ungeeignet, dem geschilderten Prüfgegenstand Rechnung zu tragen. Im Ergebnis waren alle Daten, die von den angeschriebenen Dienststellen übermittelt wurden und die über die zulässigen Angaben hinaus gingen, zu löschen.
Die Kontrollfeststellungen wurden zum Anlass genommen, mit den jeweiligen Dienststellen in Verbindung zu treten und die Verarbeitung von Telekommunikationsdaten anhand der vorliegenden Dienstvereinbarungen zu kontrollieren. Ich habe erklärt, dass der Umgang mit Telefondaten auf der Basis von Vereinbarungen der Dienststelle mit den Personalräten zu erfolgen habe. Auf den Hinweis, dass nicht jede kleine Dienststelle über das entsprechende Know-how verfüge, wurde erklärt, dass es denkbar erscheine, über eine Auftragsdatenverarbeitung nach § 8 ThürDSG dies zu regeln. Die Aufforderung an verschiedene Behörden um Übersendung der Dienstanweisungen und Festlegungen zur Verarbeitung von Telefondaten hat ergeben, dass teilweise keine Vereinbarungen mit dem zuständigen Personalrat als Rechtsgrundlage für die Speicherung der Daten vorlagen, die angegebenen Höchstfristen für die Speicherungen, die sich an der Erforderlichkeit zu Abrechnungszwecken orientieren müssen, teilweise nicht eingehalten wurden bzw. Telefondaten versehentlich nicht gelöscht worden waren.

10. Justiz

10.1 Parlamentarische Kontrolle der akustischen Wohnraumüberwachung

10.1.1 Akustische Wohnraumüberwachung im strafrechtlichen Ermittlungsverfahren (repressiver Bereich)

In Fortführung der bisherigen Darlegungen zur parlamentarischen Kontrolle der akustischen Wohnraumüberwachung (4. TB, 10.2) ist zu

berichten, dass mit der Drucksache 14/9860 vom 9. August 2002 des Deutschen Bundestags eine Unterrichtung durch die Bundesregierung über die durchgeführten Maßnahmen für das Jahr 2001 vorliegt. In Thüringen fand danach keine akustische Wohnraumüberwachung im repressiven Bereich statt.
Mit der Bundestags-Drucksache 14/8155 vom 30. Januar 2002 liegt der Erfahrungsbericht der Bundesregierung zu den Wirkungen der Wohnungsüberwachung durch Einsatz technischer Mittel (Art. 13 Abs. 3 bis 5 GG, §§ 100 c bis 100 f StPO) vor. Dieser enthält nähere Informationen und Hintergründe zu den ab dem Jahr 2002 erweiterten Angaben in den jährlichen Berichten der Bundesregierung. In diesem ist ausgeführt, dass in den bundeseinheitlichen Erhebungsrastern, als Grundlage der Länderberichte, lediglich knappe Informationen zu Anlass, Umfang, Dauer, Ergebnis und Kosten der Überwachungsmaßnahmen sowie über die erfolgte Benachrichtigung der Beteiligten oder der Gründe, aus denen die Benachrichtigung bislang unterblieben ist, enthalten sind. Die jährlichen Berichte liefern daher bislang vorwiegend statistische Aussagen über die genannten Wohnraumüberwachungsmaßnahmen. Aus diesem Grund habe das vom Bundestag gewählte Gremium nach Art. 3 Abs. 6 Satz 2 GG, das auf der Grundlage des Berichts der Bundesregierung nach Art. 13 Abs. 6 Satz 1 GG, § 100 e Abs. 2 StPO die parlamentarische Kontrolle ausübt, mehrfach die Aussagekraft der jährlichen Berichte beanstandet. Infolge dessen liegt nunmehr im Strafrechtsausschuss der Justizministerkonferenz der Beschluss zu einigen Präzisierungen der Erhebungsbögen sowie Hinweise zu diesen Erhebungsbögen vor. Der neue Erhebungsbogen enthält daher eine Frage nach dem OK-Bezug der der Wohnraumüberwachungsmaßnahme zugrunde liegenden Verdachtstaten, eine Unterscheidung des Objektes der Maßnahme der Privatwohnung und anderen dem Schutzbereich des Art. 13 GG unterfallenden Räumlichkeiten sowie eine Differenzierung nach technischen und inhaltlichen Gründen für eine mögliche fehlende Relevanz der aus der Wohnraumüberwachung gewonnenen Erkenntnisse für das Verfahren. Diese Präzisierungen wurden bereits ab dem Berichtsjahr 2002 relevant. Nach der Unterrichtung des Bundestags (DS 15/1504) vom 28. August 2003 sind aber ebenfalls für Thüringen keine akustischen Wohnraumüberwachungen zu verzeichnen. Auch nach den aufgrund des Beschlusses des Landtags in seiner 36. Plenarsitzung am 20. Januar 2001 dem Justizausschuss zu erstattenden Bericht über akustische Wohnraumüberwachungen zum Zwecke der Strafverfolgung in Thüringen für die Jahre 2002 und 2003 sind keine entsprechenden Maßnahmen erfolgt.

Insoweit bestand auch kein Anlass für weiter gehende datenschutzrechtliche Kontrollen in diesem Bereich.

10.1.2 Akustische Wohnraumüberwachungen im Bereich der polizeilichen Gefahrenabwehr (präventiver Bereich)

Nach § 35 Abs. 5 PAG unterrichtet die Landesregierung den Landtag jährlich über den nach Absatz 1 und, soweit richterlich überprüfungsbedürftig, nach Absatz 3 erfolgten Einsatz technischer Mittel. Die Parlamentarische Kontrollkommission übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus. Vom TIM wurde mitgeteilt, dass entsprechende Berichte nicht allgemein dem Landtag, sondern direkt der Parlamentarischen Kontrollkommission zugeleitet werden. Aus Sicht des TLfD wäre es zu empfehlen, gemäß vorliegendem Gesetzeswortlaut dem Thüringer Landtag den Bericht zuzuleiten. Damit wäre auch die Möglichkeit für den TLfD gegeben, entsprechende Informationen zu erhalten, um im Rahmen seiner Kontrollzuständigkeit tätig werden zu können.

10.2 Überwachung der Telekommunikation

Das im 4. TB (10.3) angesprochene Gutachten zum Thema „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO“ liegt seit Mai 2003 nunmehr vor. Die DSB des Bundes und der Länder haben dies zum Anlass genommen, auf der 66. Konferenz der DSB des Bundes und der Länder die Entschließung „Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation“ (Anlage 20) zu fassen. In dem im Auftrag des Bundesministeriums der Justiz erstellten Gutachten wurde festgestellt, dass sich die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, im Zeitraum von 1996 bis 2001 um 80 % erhöht hat, sich die Zahl der jährlich Betroffenen im Zeitraum von 1994 bis 2001 fast verdreifacht hat, immer mehr Gespräche abgehört worden sind und der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf 14 % angestiegen sind. Darüber hinaus haben sich die Maßnahmen tatsächlich in der Mehrzahl nicht über das gesetzliche Maximum von drei Monaten erstreckt, lediglich ca. ¼ der Beschlüsse waren substanziell begründet, nur in 17 % der Fällen lagen Ermittlungserfolge vor, die sich direkt auf den die Telefonüberwachung begründeten Verdacht bezogen und

73 % der Betroffenen Anschlussinhaberinnen und -inhaber wurden nicht unterrichtet. Die Konferenz der DSB des Bundes und der Länder hat daher den Gesetzgeber und die zuständigen Behörden aufgefordert, entsprechende Konsequenzen zu ziehen und insbesondere den gesetzlichen Richtervorbehalt nicht aufzulockern. Sie hat sich dafür ausgesprochen, die Qualität der richterlichen Entscheidungen zu verbessern und den Umfang des seit Einführung der Vorschrift regelmäßig erweiterten Straftatenkatalogs des § 100 a StPO zu reduzieren. Auch sollen zur umfassenden Kontrolle der Entwicklung der TKÜ-Maßnahmen zeitnahe aussagekräftige Berichte erstellt und der Umfang der Benachrichtigungspflichten im Gesetz näher definiert werden. Für wichtig angesehen wird auch zum Schutz persönlicher Vertrauensverhältnisse Regelungen zu schaffen, nach der Gespräche zwischen Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen, die Höchstdauer der Maßnahmen zu reduzieren und auch die Fortführung der wissenschaftlichen Evaluation sicherzustellen.
Nach den Berichten des TJM für die Jahre 2001 und 2002 war ein Rückgang der Anzahl der angeordneten Telefonüberwachungsmaßnahmen in Thüringen zu verzeichnen. Das TJM wurde gebeten, zu den im Berichtsjahr 2002 stattgefundenen Verfahren mitzuteilen, ob die Betroffenen nach § 101 StPO benachrichtigt worden sind bzw. in wie viel Fällen dies mit welcher Begründung noch nicht erfolgt ist. Die noch ausstehende Antwort wird in die weitere datenschutzrechtliche Begleitung der gesamten Diskussion zur Thematik einzubeziehen sein.
Da die Überwachung der Telekommunikation zu Strafverfolgungszwecken nicht zuletzt auch für die Allgemeinheit transparent sein muss, war mit der Entschließung der DSB des Bundes und der Länder anlässlich ihrer 65. Konferenz am 27./28. März 2003 in Dresden (Anlage 13) gefordert worden, dass die Jahresstatistiken, die die Betreiber von Telekommunikationsanlagen nach derzeit geltendem Recht zu erstellen haben, keinesfalls abgeschafft werden dürfen, wie dies nach aktuellen Plänen von der Bundesregierung geplant ist. Die Statistiken sollten nicht nur beibehalten, sondern außerdem auch auf die Zahl der Auskünfte über Telekommunikationsverbindungsdaten erstreckt werden.

10.3 DNA-Analyse - genetischer Fingerabdruck

Nachdem im Berichtszeitraum mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken

für die DNA-Analyse nach § 81 g StPO abzusenken, bekannt geworden sind, haben die DSB des Bundes und der Länder mit der Entschließung vom 16. Juli 2003 (Anlage 18) darauf hingewiesen, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt. Auch wenn sich die DNA-Analyse als Erleichterung bei der Aufklärung von Straftaten von erheblicher Bedeutung erwiesen hat und wegen des besonders hohen Aufklärungspotenzials der Analyse von DNA-Spuren in kriminalistischer Arbeit eine besondere Bedeutung zukommt, muss bei der Anwendung dieses Instruments angesichts der in der Entschließung dargelegten Wirkungen und Gefahrenpotenziale die Erweiterung des Einsatzes der DNA-Analyse kritisch gesehen werden. Die DSB des Bundes und der Länder haben daher an die Regierungen und Gesetzgeber des Bundes und der Länder appelliert, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Das TJM stimmt grundsätzlich mit dem Anliegen, Augenmaß zu bewahren, überein und prüft unter Berücksichtigung der Hinweise des BVerfG auf weitere Aspekte der Anwendung der DNA-Analyse die Möglichkeiten einer Erweiterung.
Gesetzesvorhaben, die die DNA-Analyse in weiteren Fällen zulassen sollen und vorsehen, dass über die bereits zu speichernden Merkmale hinaus Erkenntnisse aus der DNA-Analyse gezogen und gespeichert werden können, werden auch weiterhin kritisch begleitet.

10.4 Elektronisches Grundbuch

Im 4. TB (10.3) wurde über einen Informationsbesuch bei einem Grundbuchamt berichtet. Kritisiert worden war, dass eine nach § 65 Grundbuchverfügung (GBV) vorgeschriebene Dienstanweisung zur Regelung der Zugangssicherung und Datensicherungsverfahren sowie eine nach § 8 ThürDSG Rechnung tragende Vereinbarung zur Datenverarbeitung im ZIV nicht vorlag. Im Nachgang wurde durch das TJM der konkrete Umfang der Datenverarbeitung im Auftrag durch das ZIV dargelegt. Die Leistung des ZIV beschränkt sich danach ausschließlich auf die Bereitstellung von Räumlichkeiten, technischen

Vorkehrungen sowie den Wechsel der Sicherungsdatenträger und deren Aufbewahrung. Insoweit erschien die Kooperationsvereinbarung mit dem ZIV als ausreichend. Auch die allgemeine Dienstanweisung für den Umgang mit EDV-gestützten Arbeitsplätzen im Geschäftsbereich des Thüringer OLG genügte insoweit den Anforderungen der nach § 65 Abs. 1 Satz 3 GBV erforderlichen Dienstanweisung.
Im Berichtszeitraum wurde der Einsatz des elektronischen Grundbuchs in Thüringen zunächst im Rahmen eines Informationsbesuchs im Thüringer OLG hinsichtlich der datenschutzrechtlichen und datensicherheitsrechtlichen Aspekte unter Einbeziehung der Schulungsversion des Verfahrens weiter überprüft.
Zu bemängeln war, dass zu dem Verfahren kein konkretes Sicherheitskonzept vorlag. Es gab lediglich ein Konzept, in dem Möglichkeiten zur Umsetzung von Sicherheitsmaßnahmen dargelegt wurden. Gemäß § 9 Abs. 2 ThürDSG haben öffentliche Stellen die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage eines Sicherheitskonzepts zu ermitteln und je nach Art der zu schützenden Daten zu gewährleisten, dass die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und die Transparenz gewährleistet wird. Die Wirksamkeit dieser Maßnahmen ist unter Berücksichtigung sich verändernder Bedingungen und der Entwicklung der Technik zu überprüfen. Es bedürfte daher einer grundlegenden Istanalyse zur Umsetzung des Vorliegens des Konzeptes einschließlich verbindlicher Regelungen. Ziel des zu erstellenden Sicherheitskonzeptes muss es sein, die tatsächlich getroffenen technischen und organisatorischen Maßnahmen aufgrund einer Risikoanalyse wiederzuspiegeln.
Zu dem Verfahren von Online-Abrufen aus dem elektronischen Grundbuch wurde Folgendes festgestellt: Durch die Zulassung zum automatisierten Abrufverfahren von externen Nutzern, wobei das Zulassungsverfahren und die entsprechenden Unterlagen für alle Interessierten aus dem Internet abrufbar sind, wird offenbar davon ausgegangen, dass die letztendlich zugelassenen Nutzer generell ein berechtigtes Interesse zur Einsicht in alle Daten des zentralen Grundbuchs haben. Eine Erforderlichkeit, als Nutzer des Abrufverfahrens alle Daten des zentralen Grundbuchs anzuzeigen, wird jedoch seitens des TLfD grundsätzlich nicht gesehen. Wie bislang bei der Einsicht in das Grundbuch in Papierform müsste eine Differenzierung dahingehend erfolgen, dass lediglich die Grundstücke und zu diesen auch nur die Abteilungen, zu denen ein berechtigtes Interesse besteht, zur Einsicht

zur Verfügung stehen können. Da das Grundbuchamt bspw. bei Notaren ein berechtigtes Interesse als gegeben ansehen kann und dieses nicht dargelegt werden muss, sollte jedoch aufgrund der erleichterten Einsicht durch das automatisierte Abrufverfahren bei der Zulassung darauf hingewiesen werden, dass bei einer Weitergabe von auf diesem Weg erlangten Ausdrucken zu prüfen ist, inwieweit der Empfänger ein berechtigtes Interesse an der Kenntnis der Daten haben kann.
Gemäß § 83 Abs. 1 Satz 2 GBV sind Protokolldateien neben der Rechtmäßigkeit der Abrufe und der Erhebung der Kosten auch für die Sicherstellung der ordnungsgemäßen Datenverarbeitung zu verwenden. Da die GBV eine derartige Protokollierung vorsieht, besteht zur Sicherstellung der datenschutzrechtlichen Vorschriften die Verpflichtung, sich über die volle Funktionstüchtigkeit dieser Protokolldateien zu informieren und mindestens stichprobenweise eine Richtigkeit der eingerichteten Zugriffsrechte und des Abrufverfahrens aus sicherheitstechnischer Sicht zu prüfen. Bislang geht man seitens des TJM davon aus, dass die eingerichtete Protokolldatei nur zur Erhebung der Kosten dient, eine darüber hinausgehende Auswertung wird nicht für erforderlich erachtet.
Das Verfahren wird weiterhin begleitet.

10.5 Umzug in der Justiz

Im 4. TB (10.10) war dargelegt, wie wichtig es ist, die datenschutzrechtlichen Vorschriften bei der Vorbereitung und Durchführung von Behördenumzügen zu berücksichtigen und einzuhalten. Ungenügende Sicherheitsvorkehrungen beim Umzug mit der Folge, dass eine Vielzahl von Akten der Staatsanwaltschaft ungesichert in einer Tiefgarage zwischengelagert wurden, hatten zu einer Beanstandung nach § 39 ThürDSG geführt. Zur Feststellung, ob bei dem Umzug aufgrund der datenschutzrechtlichen Mängel Akten abhanden gekommen waren, hatte ich mich über die Durchführung einer aussagefähigen Stichprobenkontrolle, die zügig abgeschlossen wurde, verständigt. Umzugsbedingte Fehlbestände haben sich dabei nicht ergeben. In Anbetracht der eingeleiteten Maßnahmen von Seiten der Generalstaatsanwaltschaft zur Umsetzung der Forderungen und Empfehlungen konnte der Kontrollvorgang abgeschlossen werden.

10.6 Aufbewahrung des Schriftguts der Gerichte und Staatsanwaltschaften - Aktenaufbewahrungsgesetz

Nachdem die DSB des Bundes und der Länder bereits in mehreren Entschließungen (4. TB, 10.9) darauf hingewiesen hatten, dass die Dauer der Aufbewahrung personenbezogener Daten einer klaren und deutlichen gesetzlichen Grundlage bedarf, deren Notwendigkeit auch und gerade für Datenspeicherungen im Bereich der Justiz - Gerichte, Staatsanwaltschaften -, besteht, in dem oftmals Daten von besonderer Sensibilität vorgehalten werden und bislang keine Gesetzgebungsmaßnahmen bekannt geworden sind, haben die DSB des Bundes und der Länder auf ihrer 64. Konferenz am 24./25. Oktober 2002 in Trier den Beschluss gefasst, die unverzügliche Schaffung eines Aktenaufbewahrungsgesetzes für die Justiz zu fordern. Der so genannte Übergangsbonus konnte nach 19 Jahren nach den eindeutigen Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil nicht mehr länger als tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung angesehen werden. Der Gesetzgeber sollte darüber hinaus Sorge tragen, dass die Aufbewahrungsfristen vom Verordnungsgeber so kurz wie möglich bemessen und anlassbezogen überprüft werden.
Anfang Mai 2003 wurde im Kreise der DSB der Referentenentwurf eines Gesetzes über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz - JKomG) bekannt. In diesem Artikelgesetz war auch ein Artikel einem Gesetz zur Regelung der Aufbewahrung von Gerichtsakten nach Beendigung des Verfahrens (Gerichtsaktenaufbewahrungsgesetz - GAAG) gewidmet. Danach sollen gerichtliche Verfahrensakten unbeschadet anderweitiger anderer gesetzlicher Bestimmungen nach Beendigung des Verfahrens nur solange aufbewahrt werden, wie schutzwürdige Interessen der Verfahrensbeteiligten oder sonstiger Personen oder öffentlicher Interessen dies erfordern. Die eigentlichen konkreten Bestimmungen sollen per Verordnungsermächtigung der Bundesregierung und Landesregierungen jeweils für ihren Geschäftsbereich durch Rechtsverordnung bestimmen, welche Gerichtsakten zu welchen Aufbewahrungsfristen aufzubewahren sind.
Im Grundsatz ist der Gesetzentwurf zu begrüßen, jedoch reicht er den Anforderungen an eine konkrete gesetzliche Regelung nicht aus. Es müssten zumindest weitere Vorgaben für den Verordnungsgeber, wie mit besonders sensiblen Aktenteilen umzugehen ist, aus welchen konkreten Anlässen Aufbewahrungsfristen verringert werden können und

in welchen Fällen Sperrregelungen zum Zuge kommen aufgenommen werden.

10.7 Versendung von Unterlagen durch Justizbehörden

Zu der Versendung von Unterlagen durch Staatsanwaltschaften und Gerichte an kommunale Behörden habe ich mich bereits im 2. TB (10.16) geäußert. Dem datenschutzrechtlichen Anliegen wurde Rechnung getragen, indem im Geschäftsbereich der Justiz festgelegt wurde, dass Postsendungen mit personenbezogenen Daten an die jeweils zuständigen Ämter der Verwaltungsbehörden in gesonderten und verschlossenen Briefumschlägen versandt werden. Die Umsetzung dieser Maßnahmen wurde mir auch bestätigt.
In diesem Berichtszeitraum wandte sich ein Beschwerdeführer an mich, weil ihm von einem Amtsgericht nach seiner Darlegung Ladungen, Beschlüsse und andere Schriftstücke in unverschlossenen Briefumschlägen zugesandt worden waren. Erschwerend kam nach seiner Auffassung dazu, dass Briefe per Zustellungsurkunde in den Fällen, in denen der Empfänger vom Zusteller nicht angetroffen wird, in einer von der Post bestimmten Stelle hinterlegt werden, wobei der Zugriff Unbefugter nicht auszuschließen sei. Mangels Zuständigkeit des TLfD für die Deutsche Post AG, die nach § 181 Abs. 1 Nr. 2 ZPO Stellen bestimmen kann, bei denen nicht direkt zustellbare Post hinterlegt wird, konnte nur dem Vorwurf des unverschlossenen Versands von Schriftstücken durch das Amtsgericht nachgegangen werden. Ich habe dies zum Anlass genommen, einen Besuch vor Ort durchzuführen. Die vom Beschwerdeführer zur Verfügung gestellten Briefumschläge ließen keine Schlussfolgerung auf eine ursprüngliche Nichtverschlossenheit zu, obwohl sie augenscheinlich ohne Beschädigungen geöffnet worden waren. Hinweise darauf, dass die Sendungen auf dem Postweg geöffnet worden waren, lagen nicht vor. Insoweit konnte insgesamt nicht davon ausgegangen werden, dass keine erforderlichen technischen und organisatorischen Maßnahmen getroffen waren, um die unbefugte Kenntnisnahme durch Dritte in den vom Beschwerdeführer monierten Fällen auszuschließen. Ein datenschutzrechtlicher Verstoß konnte daher nicht festgestellt werden.

10.8 Thüringer Gesetz über die Unterbringung besonders rückfallgefährdeter Straftäter (ThürStrUBG)

Im Berichtszeitraum wurde der Entwurf eines Thüringer Gesetzes über die Unterbringung besonders rückfallgefährdeter Straftäter (Drucksache 3/2493) diskutiert. Dieser regelt die befristete oder unbefristete Unterbringung von Straftätern nach Verbüßung einer zeitigen Freiheitsstrafe auf Antrag der Justizvollzugsanstalt durch gerichtliche Entscheidung. Voraussetzung ist, dass aufgrund von Tatsachen davon auszugehen ist, dass von dem Betroffenen eine erhebliche gegenwärtige Gefahr für das Leben, die körperliche Unversehrtheit, die persönliche Freiheit oder die sexuelle Selbstbestimmung anderer ausgeht, insbesondere, weil er im Vollzug der Freiheitsstrafe beharrlich die Mitwirkung an der Erreichung des Vollzugsziels verweigert, namentlich eine rückfallvermeidende Psycho- oder Sozialtherapie ablehnt oder abbricht. Hierzu hat das Gericht alle Umstände zu ermitteln, die für die Entscheidung von Bedeutung sind und zur Gefährlichkeit des Betroffenen die Gutachten von zwei Sachverständigen einzuholen. Diese im Bereich des Polizeirechts liegende Regelung findet nur dann Anwendung, wenn gegen den Betroffenen keine Maßregelung der Besserung und Sicherung nach §§ 63 und 66 StGB angeordnet ist, in einem anhängigen Verfahren angeordnet werden kann oder die Anordnung nach § 66 a StGB nicht vorbehalten wurde.

Im Rahmen der parlamentarischen Beratung waren auch datenschutzrechtliche Fragen zu klären:
Es stellte sich zum einen die Frage, ob von der Justizvollzugsanstalt zum Zweck der Antragstellung zur Anordnung einer weiteren Unterbringung personenbezogene Daten, die im Strafvollzug dem besonderen Berufsgeheimnis eines Arztes oder Therapeuten anvertraut wurden, verarbeitet werden dürfen. Hierzu habe ich dargelegt, dass die Vollzugsbehörde nach § 180 Abs. 1 StVollzG personenbezogene Daten verarbeiten und nutzen darf, soweit dies für den ihr nach dem Strafvollzugsgesetz aufgegebenen Vollzug der Freiheitsstrafe erforderlich ist. § 180 Abs. 2 StVollzG zählt die Tatbestände auf, unter denen die Verarbeitung und Nutzung personenbezogener Daten für andere Zwecke zulässig ist, insbesondere auch zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwer wiegenden Beeinträchtigung der Rechte einer anderen Person. Mitarbeiter des Sozialdienstes und des psychologischen Dienstes sowie der Anstaltsarzt unterfallen

grundsätzlich einer besonderen Verschwiegenheitspflicht, die nach § 203 Abs. 1 Nr. 1, 2 und 5 StGB strafbewehrt ist. Um Unterlagen, die sich ausschließlich in der Obhut dieser Person befinden, nutzen zu können, bedarf es für die Durchbrechung der Verschwiegenheitsverpflichtung einer besonderen Rechtsgrundlage. Eine solche bietet § 182 StVollzG. Damit hängt die Frage nach einer Durchbrechung der Schweigepflicht oder auch der Offenbarungspflicht/Offenbarungsbefugnis für personenbezogene Daten davon ab, ob die Kenntnis der Daten zur Aufgabenerfüllung der Vollzugsbehörde oder zur Abwehr von erheblichen Gefahren für Leib und Leben des Gefangenen oder Dritten erforderlich ist. Die Offenbarungspflicht zur Abwehr von erheblicher Gefahr für Leib und Leben des Gefangenen oder Dritten dient dem Schutz höherrangiger Rechtsgüter des Einzelnen und ist aus Gründen der Verhältnismäßigkeit auf das unerlässliche Maß zu beschränken. Unterlagen, die sich beim Arzt, Anstaltspsychologen oder beim Sozialarbeiter oder Sozialpädagogen in der Anstalt befinden und weitere personenbezogene Daten des Gefangenen enthalten, die im Vertrauen auf die Schweigepflicht offenbart wurden, sind gesondert aufzubewahren. Ein Zugriff der Anstaltsleitung auf diese Unterlagen zum Zweck der Antragstellung nach § 4 Abs. 1 des Gesetzentwurfs besteht nicht. Die Anstaltsleitung ist somit auf die Nutzung der Daten beschränkt, die ihr von den dem Berufsgeheimnis unterliegenden Personen in Erfüllung ihrer Offenbarungsbefugnis oder Offenbarungspflicht zur Kenntnis gebracht wurden.
Die weitere Frage war, ob ein Gutachter, der Mitarbeiter der Justizvollzugsanstalt ist, personenbezogene Daten, die ihm aus der Gefangenenpersonalakte, der Gesundheitsakte oder aus anderen Karteien bekannt geworden sind bzw. die ihm vom Gefangenen anvertraut worden sind, für das Gutachten verarbeiten darf. Der Gesetzentwurf schloss nicht aus, dass auch ein Mitarbeiter der Justizvollzugsanstalt, der den Gefangenen behandelt, als Gutachter berufen werden könnte. Ob ein Gutachter, der Mitarbeiter der Justizvollzugsanstalt ist und mit dem Gefangenen befasst war, Daten, die ihm in dieser Funktion anvertraut worden sind, für das Gutachten verarbeiten kann, ist differenziert zu sehen. Befinden sich in seiner Obhut Daten, die der Schweigepflicht unterliegen, unterliegen diese auch gegenüber dem Gericht der Schweigepflicht, sofern der Sachverständige vom Gefangenen davon nicht entbunden ist. Insoweit wäre ein solcher der Schweigepflicht unterliegende Sachverständige einem Interessenskonflikt ausgesetzt, da er im Falle der Erstellung eines Gutachtens streng unterscheiden müsste, welche personenbezogene Daten in das Sachverständigengut-

achten einfließen dürften und welche nicht. Meine Hinweise in diesem Zusammenhang wurden umgesetzt. Das Gesetz enthält nunmehr die Regelung, dass einer der Sachverständigen zwar ein sachverständiger Mitarbeiter der Justizvollzugsanstalt, in die der Betroffene eingewiesen ist, sein kann, keiner der Sachverständigen darf jedoch im Rahmen des Strafvollzugs mit einer therapeutischen Behandlung des Betroffenen befasst gewesen sein.

10.9 Auskünfte aus Gefangenenpersonalakten an Gefangene

Im 4. TB hatte ich darüber informiert, dass seit Inkrafttreten des 4. StVollzÄndG Gefangene einen Auskunftsanspruch, bei besonderem rechtlichen Interesse auch Anspruch auf Akteneinsicht, haben.
Ein Gefangener hatte sich an mich gewandt, weil sein Antrag gemäß § 185 StVollzG auf Auskunft aus seiner Gefangenenpersonalakte bzw. Einsicht abgelehnt worden war. Seinen Antrag hatte er damit begründet, er benötige bestimmte Angaben um ggf. gegen einen ablehnenden Bescheid gerichtlich vorgehen zu können.
Ich habe von der Justizvollzugsanstalt gemäß § 185 StVollzG i. V. m. § 19 Abs. 6 BDSG Auskunft erbeten, die mir auch erteilt wurde. Ausreichende Gründe, dem Betroffenen die begehrten Auskünfte zu verweigern, waren allerdings nicht erkennbar. Nach einer datenschutzrechtlichen Kontrolle vor Ort konnte mit der Anstaltsleitung Einvernehmen dahingehend erzielt werden, dass den begehrten Auskünften keine Gründe entgegenstehen. Die Anstalt hat nach ihren Informationen die Auskünfte gewährt.

Bei einem Gefangenen bestand die Vermutung, dass in seiner Gefangenenpersonalakte Kopien von angehaltenen Schreiben abgeheftet wurden. Nach § 31 Abs. 3 Satz 2 StVollzG werden angehaltene Schreiben an den Absender zurückgegeben oder, sofern dies nicht möglich oder aus besonderen Gründen untunlich ist, behördlich verwahrt. Aus dem Gesetzestext ergeben sich keine Hinweise darauf, dass angehaltene Schreiben in die Gefangenenpersonalakte abgeheftet werden. Die Vollzugsgeschäftsordnung sieht dies allerdings für den Fall vor, dass die amtliche Aufbewahrung über den Zeitpunkt der Entlassung hinaus erforderlich ist. Liegen Gründe für eine amtliche Verwahrung von angehaltenen Schreiben vor, sind technische und organisatorische Maßnahmen gegen unbefugten Zugang und unbefugten Gebrauch gemäß § 183 Abs. 1 Satz 1 StVollzG zu treffen. Dies

bedeutet, dass die betreffenden Schreiben in einem verschlossenen Umschlag in der Gefangenenpersonalakte aufzubewahren wären. Für Kopien von Schreiben gilt nichts anderes, da sie den vollständigen Inhalt des Originals widerspiegeln.
Bei den in Kopie abgehefteten Schreiben führte eine nochmalige Prüfung zur Erforderlichkeit der Aufbewahrung durch die Anstaltsleitung zur Entfernung.

11. Gesundheits- und Sozialdatenschutz

11.1 Gesundheitsmodernisierungsgesetz (GMG)

Im Berichtszeitraum wurde von der Bundesregierung der Entwurf eines GMG vorgelegt. Die datenschutzrelevanten Probleme wurden unter den DSB des Bundes und der Länder eingehend diskutiert. Im Rahmen der Datenschutzkonferenzen wurden zwei Entschließungen (Anlage 15, Anlage 21) gefasst. Das GMG vom 14. November 2003 ist am 1. Januar 2004 in Kraft getreten.
Die Datenschutzkonferenz hat anerkennend zur Kenntnis genommen, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass durch strenge Zweckbindungsregelungen der Datenverarbeitung Versichertenprofile bei den Krankenkassen verhindert werden. Dass dies bei der Umsetzung der Regelungen in der Praxis auch umfassend beachtet wird, wird auch Gegenstand der Kontrolltätigkeit der DSB zu sein haben.

11.2 Gesetz zur Einführung der Meldepflicht an das Gemeinsame Krebsregister

Zusammen mit der Novellierung des Thüringer Krankenhausgesetzes ist das Gesetz zur Einführung der Meldepflicht an das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt sowie der Freistaaten Sachsen und Thüringen verabschiedet worden. Bislang stand in Thüringen den Ärzten nach dem Staatsvertrag über das Gemeinsame Krebsregister ein Melderecht und den Patienten ein Widerspruchsrecht gegen die Meldung zu. Mit der geänderten Rechtslage folgte Thüringen dem Beispiel der Länder Mecklenburg-Vorpommern und Sachsen-Anhalt sowie des Freistaats Sachsen und führte die Pflicht der Ärzte zur Meldung von Krebserkrankungen an das Gemeinsame Krebsregister ein. Den Patienten wird dabei kein Widerspruchsrecht gegen diese Mel-

dung eingeräumt. § 2 des Gesetzes sieht vor, dass der Patient jedoch über die erfolgte bzw. beabsichtigte Meldung seiner Krebserkrankung zu informieren ist. Zur Begründung der Einführung einer Meldepflicht wurde von der Landesregierung auf die niedrige Meldequote in Thüringen, die bei 53 % lag sowie die Erforderlichkeit von einer Meldequote von über 90 % hingewiesen, um zuverlässige wissenschaftliche Aussagen treffen zu können. Dieser Argumentation hat sich der Gesetzgeber angeschlossen und die Meldepflicht zum 28. Februar 2003 in Kraft gesetzt.

11.3 Änderung des Thüringer Krankenhausgesetzes (ThürKHG)

Im Rahmen der Änderung des ThürKHG habe ich bereits in meinem 4. TB (11.3) Ausführungen zu datenschutzrechtlich relevanten Problemen gemacht. Im Berichtszeitraum wurde die Novellierung des ThürKHG abgeschlossen, das Gesetz ist am 28. Februar 2003 in Kraft getreten (GVBl. S. 99). Neu aufgenommen wurden in einem § 27 a Bestimmungen zur Datenverarbeitung für Forschungszwecke außerhalb des Krankenhauses. Weiter wurden die Bestimmungen zur Auftragsdatenverarbeitung im § 27 b dahingehend geändert, dass die konkreten Anforderungen an eine Verarbeitung von Patientendaten durch Dritte gesetzlich festgelegt wurden.

Gegen eine ursprünglich im § 27 a vorgesehene personenbezogene Datenverarbeitung für Zwecke der „Krankenhausplanung“ habe ich erhebliche datenschutzrechtliche Bedenken geltend gemacht. Für eine bereichsspezifische Regelung im ThürKHG, die eine Offenbarung von Patientendaten für Zwecke der Krankenhausplanung ermöglicht, habe ich keine Erforderlichkeit gesehen, da für Planungszwecke regelmäßig nur aggregierte Daten benötigt werden. Im Ergebnis der parlamentarischen Beratung, unter Einbeziehung der Stellungnahmen der Anzuhörenden, wurde eine Lösung dahingehend gefunden, dass im § 7 die Auskunftspflichten der Krankenhäuser auf das erforderliche Maß beschränkt wurden und die Wahrung der ärztlichen Schweigepflicht und des Datenschutzes zu berücksichtigen sind.
Bei den Regelungen im § 27 a bezüglich der Datenverarbeitung für Forschungszwecke außerhalb des Krankenhauses wurden ebenfalls meine datenschutzrechtlichen Forderungen umgesetzt. So hat nunmehr das TMSFG als zuständige oberste Aufsichtsbehörde festzustellen, ob Patientendaten ohne Einwilligung des Patienten für bestimmte

Forschungsvorhaben verarbeitet und genutzt werden dürfen, sofern das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Patienten erheblich überwiegt. Festgelegt wurde in diesem Zusammenhang auch, dass die Patientendaten zu anonymisieren sind, soweit es der Forschungszweck zulässt und der DSB des Krankenhauses zu beteiligen ist.
Da es sich bei der Verarbeitung von Patientendaten um sehr sensible personenbezogene Daten handelt, mussten entsprechende Anforderungen an eine Verarbeitung dieser Daten durch Stellen außerhalb des Krankenhauses festgelegt werden, um den Schutz dieser Daten vor unbefugter Verwendung angemessen zu gewährleisten. So müssen kumulativ drei Voraussetzungen für die Zulässigkeit einer solchen Auftragsdatenverarbeitung vorliegen. Die Verarbeitung durch einen Dritten muss erheblich kostengünstiger vorgenommen werden können als die Verarbeitung durch das Krankenhaus oder es müssen hierdurch Störungen im Betriebsablauf vermieden werden können (§ 27 b Abs. 1 Satz 1 Nr. 1). Außerdem muss die Einhaltung der Datenschutzbestimmungen des ThürKHG sowie eine den Voraussetzungen des § 203 des Strafgesetzbuches entsprechende Schweigepflicht beim Auftragnehmer sichergestellt sein (§ 27 b Abs. 1 Satz 1 Nr. 2). Schließlich muss der Auftraggeber der Krankenhausaufsichtsbehörde nach § 32 Abs. 2 ThürKHG rechtzeitig vor der Auftragserteilung Art, Umfang sowie die technischen und organisatorischen Maßnahmen der beabsichtigten Datenverarbeitung im Auftrag anzeigen. Im § 27 b Abs. 3 wurde auch bestimmt, dass die gleichen Voraussetzungen für die Wartung oder Fernwartung automatisierter Datenverarbeitungsanlagen entsprechend gelten, soweit ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

11.4 Thüringer Verordnung über die Anpassung der Meldepflicht für Infektionskrankheiten (Thüringer Infektionskrankheitenmeldeverordnung - ThürIfKrMVO -)

Am 27. Februar 2003 ist auf der Grundlage des Infektionsschutzgesetzes (IfSG) die Thüringer Infektionskrankheitenmeldeverordnung (GVBl. S. 107) in Kraft getreten. Sie beinhaltet eine Erweiterung der Pflicht zur namentlichen Meldung von Erkrankungen und Todesfällen über die in § 6 IfSG genannten Krankheiten hinaus. Weiter ist nunmehr auch der Nachweis bestimmter, zusätzlich zu den in § 7 Abs. 1 IfSG aufgeführten, Krankheitserreger namentlich zu melden. Diese

Ausdehnung der namentlichen Meldepflicht greift in das informationelle Selbstbestimmungsrecht der Betroffenen ein, was nach § 15 Abs. 3 i. V. m. Abs. 1 IfSG dann gerechtfertigt ist, wenn die epidemische Lage dies zulässt oder erfordert. Dies zu beurteilen ist allerdings in erster Linie eine fachspezifische Frage.
Wegen des nicht unerheblichen Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen hat der Bundesgesetzgeber in § 15 Abs. 1 IfSG bestimmt, Meldepflichten für die auf Bundesebene vorgesehenen Meldungen auf dem Verordnungsweg aufzuheben oder einzuschränken, wenn die epidemische Lage dies zulässt. Ich habe daher das TMSFG gebeten, nach einer gewissen Zeit zu überprüfen, ob die festgelegten zusätzlichen Meldepflichten ganz oder teilweise aufgehoben werden können oder für die vorgesehenen Zwecke eine nicht namentliche Meldung ausreichend ist. Die Geltungsdauer der Verordnung wurde auf zwei Jahre befristet.

11.5 Datenerhebungen im Rahmen der Schulgesundheitspflege

Am 27. September 2003 trat die Thüringer Verordnung über die Schulgesundheitspflege (GVBl. S. 365) in Kraft. Damit liegen, wie vom TLfD in den vergangenen Tätigkeitsberichten mehrfach angemahnt, für alle Betroffenen (Eltern und Schüler) und den beteiligten Stellen normenklare Regelungen für die Verarbeitung und Nutzung schulmedizinischer Daten im Rahmen der Schulgesundheitspflege vor. Gleichzeitig wurde dies von der Aufsichtsbehörde zum Anlass genommen, den Umfang der Datenerhebung bei den Sorgeberechtigten im Rahmen der Pflichtuntersuchungen unter datenschutzrechtlichen Aspekten zu präzisieren und hierzu landesweit einheitliche Vordrucke zu erarbeiten.

11.6 Nutzung von Totenscheinen

In meinem 1. TB hatte ich bereits darüber informiert, dass in Thüringen eine erhebliche Rechtsunsicherheit beim Umgang mit Totenscheinen besteht, da eine entsprechende Rechtsvorschrift nicht existiert und die Vorschriften der ehemaligen DDR als fortgeltendes Recht auf diese Frage keine Antwort geben. Unzweifelhaft ist jedoch, dass Totenscheine nicht nur für die Standesämter oder statistische Zwecke benötigt werden, sondern darüber hinaus auch die Notwendigkeit besteht, Auskünfte daraus an Dritte zu erteilen. Dies zeigen die immer

wiederkehrenden Anfragen beim TLfD insbesondere auch von wissenschaftlichen Einrichtungen zur Durchführung von Forschungsvorhaben. Da die Daten aufgrund ihres Inhalts der ärztlichen Schweigepflicht unterliegen und eine unbefugte Offenbarung unter Strafe steht, bedarf es dringend einer gesetzlichen Regelung. Der gemeinsame Runderlass des TMSFG und des TIM zur Verwendung, Auskunftserteilung und Aufbewahrung von Totenscheinen aus dem Jahr 1994 stellte bestenfalls eine Übergangslösung dar und wurde auch von allen beteiligten Stellen so verstanden. Insoweit ist zu begrüßen, dass nunmehr im letzten Jahr von den zuständigen Ministerien der Entwurf eines Thüringer Gesetzes über das Bestattungswesen erarbeitet wurde. Die darin aufgenommenen Regelungen sind jedoch teilweise noch sehr allgemein und sollen in einer nachfolgenden Verordnung erst präzisiert werden. Problematisch ist aus datenschutzrechtlicher Sicht eine beabsichtigte Übermittlungsbefugnis, wonach Antragstellern künftig schon bei Glaubhaftmachung eines berechtigten Interesses soweit kein Grund zur Annahme besteht, dass durch die Offenbarung schutzwürdige Belange des Betroffenen oder seiner Angehörigen bestehen, Einsichtnahmen in Totenscheine erlaubt bzw. Ablichtungen davon ausgehändigt werden können. Dies erscheint insbesondere unter dem Aspekt, dass Totenscheine auch sensible medizinische Daten des Verstorbenen enthalten, nicht gerechtfertigt. Hier sollten Übermittlungsbefugnisse auf Fälle beschränkt bleiben, bei denen ein rechtliches Interesse besteht, da für den Zugang für wissenschaftliche Zwecke ohnehin eine spezielle Regelung vorgesehen ist.
Es bleibt zu hoffen, dass nunmehr die weiteren Beratungen zum Gesetzentwurf sowie die Vorlage eines Entwurfes für die Verordnung zügig fortgesetzt werden, damit dem gegenwärtigen unbefriedigenden Zustand der Rechtsunsicherheit in diesem Bereich baldmöglichst abgeholfen wird.

11.7 Datenschutzrechtliche Anforderungen an medizinische Netze

Nicht zuletzt aus Kostengründen werden im medizinischen Bereich zunehmend Informationstechnologien sowohl in der ambulanten als auch in der stationären Behandlung eingesetzt. Die eingesetzten IT-Verfahren sind komplex und ermöglichen eine verteilte Informationsverarbeitung. Aus datenschutzrechtlicher Sicht muss auch mit der Vernetzung der vorhandenen Strukturen und des damit einhergehen-

den wachsenden Informationsaustausches eine unbefugte Offenbarung der medizinischen Daten der Patienten verhindert werden.

Der zunehmende Einsatz einer elektronischen Kommunikation zwischen niedergelassenen Ärzten und Krankenhäusern erfordert insbesondere die Beachtung datenschutzrechtlicher Aspekte. Die Arbeitskreise „Soziales und Gesundheit“ sowie „Technik“ der DSB des Bundes und der Länder befassten sich intensiv mit dieser Thematik. Im Ergebnis wurde eine Orientierungshilfe (OH) zum datenschutzgerechten Umgang mit der elektronischen Kommunikation und der automatisierten Datenverarbeitung im Gesundheitswesen erarbeitet, die von den DSB des Bundes und der Länder am 24./25. Oktober 2002 in Trier zustimmend zur Kenntnis genommen wurde.

In der OH sind aus datenschutzrechtlicher Sicht grundlegende rechtliche, technische und organisatorische Anforderungen an medizinische Netze formuliert. Insbesondere bietet sie eine Hilfestellung zur Formulierung und Umsetzung einer datenschutzgerechten Sicherheitspolitik für die elektronische Kommunikation und Datenverarbeitung im Gesundheitswesen. Ausgehend von dem rechtlichen Rahmen, an dem sich die medizinische Datenverarbeitung zu orientieren hat, werden die grundlegenden Sicherheitsanforderungen für patientenbezogene Datenverarbeitungssysteme definiert. Neben einer Vielzahl zu treffender technischer und organisatorischer Sicherheitsmaßnahmen, die abhängig von den jeweiligen technischen Ausprägungen der eingesetzten Systeme sehr unterschiedlich sein können, ergeben sich aufgrund des hohen Schutzbedarfs der zu verarbeitenden Daten allerdings auch spezielle Sicherheitsmaßnahmen, die als unabdingbar anzusehen sind. Hierzu gehören bspw. Maßnahmen zur Verschlüsselung der gespeicherten und zu übertragenden Daten sowie zum Einsatz der elektronischen Signatur, um die Zurechenbarkeit von Dokumenten zum Urheber und den Nachweis der Unversehrtheit des Dokumenteninhaltes sicherzustellen. Die Ausführungen enthalten desweiteren Aussagen zur Sicherstellung der Verfügbarkeit der Daten, zur Gewährleistung der Revisionsfähigkeit der Verarbeitungsprozesse, zur Validität der Daten (Aktualität und Darstellungsqualität), zur Nichtabstreitbarkeit von Datenübermittlungen (Revisionsfähigkeit) sowie zu einer abgestuften Rechteverwaltung für die Nutzer.
Auch wird eine Kategorisierung von medizinischen Datenverarbeitungssystemen zur einrichtungsübergreifenden Kommunikation anhand der vier grundlegenden Organisationsformen zur Vorhaltung der

Daten (dezentrale Datenhaltung, zentrale Datenhaltung, verteilte Datenhaltung, dezentrale Datenhaltung mit zentraler Komponente) vorgenommen. Die hierzu enthaltenen Aussagen lassen sich weitgehend auf alle in der Praxis vorkommenden Organisationsformen übertragen.

Die Orientierungshilfe ist unter www.bfd.bund.de/technik/telemed.pdf abrufbar.

11.8 Undifferenzierte Gesundheitsdatenanforderung durch einen Unfallversicherungsträger bei einer Krankenkasse

Die Unfallversicherungsträger (UVT) benötigen für die Prüfung zur Entscheidung von Leistungen aufgrund von Berufsunfällen häufig eine Vielzahl z. T. sensibler Gesundheitsdaten der Betroffenen. Das SGB VII stellt ihnen dabei eine Reihe von speziellen Erhebungsmöglichkeiten bei anderen Stellen (Durchgangsärzten, Krankenkassen, Arbeitgeber etc.) zur Verfügung. Gleichzeitig sind mit der Eingliederung des Unfallversicherungsrechts als siebentes Buch in das Sozialgesetzbuch zum 01.01.1997 auch datenschutzrechtliche Vorkehrungen in das Gesetz aufgenommen worden, die absichern sollen, dass der Betroffene jederzeit nachvollziehen kann, welche seiner Gesundheitsdaten im Rahmen der Prüfung der Leistungsgewährung durch den UVT verarbeitet und mit anderen Stellen ausgetauscht werden sowie dass nur die zur Aufgabenerfüllung erforderlichen Daten verarbeitet werden. Eine dieser Vorschriften ist § 188 SGB VII. Sie regelt die Auskunftspflicht der Krankenkassen gegenüber dem UVT über frühere Erkrankungen. Weil es sich hierbei um sensible Daten handelt, ist eine Übermittlung nur zulässig soweit es für die Feststellung des Versicherungsfalls erforderlich ist. In § 188 Satz 2 SGB VII werden die UVT verpflichtet, ihr Auskunftsverlangen auf solche Erkrankungen oder solche Bereiche von Erkrankungen zu beschränken, die mit dem Versicherungsfall in einem ursächlichen Zusammenhang stehen können. Damit soll bereits bei der Anfrage vermieden werden, dass die Krankenkassen mehr Daten als erforderlich an den UVT übermitteln. Dem Betroffenen wird mit § 188 Satz 3 SGB VII die Möglichkeit gegeben, vom UVT zu erfahren, welche Daten die Krankenkasse dem UVT übermittelt hat. Zudem ist der UVT nach § 188 Satz 4 SGB VII verpflichtet, auf dieses Recht hinzuweisen. Dadurch soll beim Versicherten Transparenz bzgl. der Verarbeitung seiner Daten hergestellt werden.

Aufgrund einer Eingabe wurde ich darauf aufmerksam, dass die Beachtung dieser Vorschriften durch einen meiner Kontrolle unterliegenden UVT nicht gewährleistet war. Nach einem Arbeitsunfall hat der UVT die Krankenkasse eines Versicherten unter Verwendung eines Musterschreibens angeschrieben und um Übersendung aller dort dokumentierten Arbeitsunfähigkeitszeiten einschließlich der jeweiligen Diagnosen und Anschriften der jeweils behandelnden Ärzte gebeten, ohne diese Anforderungen auf bestimmte Erkrankungen oder Bereiche von Erkrankungen zu beschränken. Die Krankenkasse hat daraufhin eine entsprechende Liste aus dem gesamten Versicherungszeitraum (ca. 8 Jahre) an den UVT übermittelt. Diese Liste, die sämtliche Erkrankungen mit Arbeitsunfähigkeitszeiten enthielt, entdeckte der Petent erstmals bei einer Einsicht in seine Prozessakte. Er war der Auffassung, dass derart umfangreiche Übermittlungen eine Verletzung seiner Persönlichkeitsrechte darstellen. Meine Überprüfung des Vorgangs hat ergeben, dass es der UVT in diesem Fall unterlassen hatte, dem Betroffenen ein Eröffnungsschreiben zuzusenden, in dem er gem. § 188 Satz 4 SGB VII auf sein Recht nach § 188 Satz 3 SGB VII, auf Verlangen über die von den Krankenkassen übermittelten Daten unterrichtet zu werden, hingewiesen wird. Die nach § 188 Satz 2 SGB VII vorgeschriebene und hier unterbliebene Einschränkung der Datenanforderung bei der Krankenkasse habe ich gegenüber dem UVT beanstandet.
Die Überprüfung hat weiter ergeben, dass die Anforderung der Vorerkrankungen bei der Krankenkasse zu einem Zeitpunkt erfolgte, als die Zahlung von Versicherungsleistungen gegenüber dem Petenten bereits abgelehnt worden war und der UVT diese Angaben nur im Hinblick auf ein mögliches Widerspruchsverfahren auf Vorrat angefordert hat, ohne dass zu diesem Zeitpunkt bereits eine konkrete Erforderlichkeit dafür bestand. Diese Erhebung von Gesundheitsdaten auf Vorrat verstieß gegen § 67 a Abs. 1 Satz 1 SGB X, wonach nur die Erhebung der zur Aufgabenerfüllung erforderlichen Daten zulässig ist, woran es hier fehlte. Auch dies habe ich ggü. dem UVT beanstandet.
Schließlich hatte sich der UVT in diesem Fall auch noch an den Arbeitgeber des Petenten gewandt, um Erkenntnisse über eine möglicherweise schon vor dem Unfall bei der betroffenen Person vorliegenden psychischen Erkrankung zu gewinnen, was eine Leistung des UVT aufgrund einer dann fehlenden Kausalität zwischen Unfall und Gesundheitsschaden ausschließen könnte. In § 192 Abs. 3 SGB VII ist der Arbeitgeber jedoch lediglich zur Auskunft über den Hergang des Unfallgeschehens und zu der Frage verpflichtet, ob der Arbeitnehmer

nach dem Unfallereignis wieder und ggf. in welchem Umfang seiner Beschäftigung nachgehen kann. Keinesfalls können vom Arbeitgeber Angaben über Erkrankungen des Arbeitnehmers erhoben werden, da diese schon aufgrund der sozialdatenschutzrechtlichen Vorschriften, bspw. im Fall der Krankschreibung, den Arbeitgebern überhaupt nicht bekannt gemacht werden dürfen. Darüber hinaus hat der Arbeitgeber auch keinerlei medizinische Sachkenntnis, um Krankheitssymptome oder Ähnliches zu beurteilen. Gegenüber dem UVT habe ich deshalb auch diese ungeeignete und damit nicht zulässige Datenanforderung beanstandet. Parallel hierzu hat der BfD die Datenübermittlung durch die seiner Kontrolle unterliegende Krankenkasse überprüft. Die Krankenkasse hat daraufhin ggü. dem UVT ein Verwertungsverbot hinsichtlich der übermittelten nicht erforderlichen Daten ausgesprochen, worauf dieser in seinen Akten diejenigen Angaben geschwärzt hat, die nicht den Beschränkungen des § 188 Satz 2 SGB VII entsprochen haben. Darüber hinaus habe ich den UVT aufgefordert, durch eine organisatorische Regelung sicherzustellen, dass dessen Mitarbeiter grundsätzlich die Hinweisschreiben mit dem Inhalt des § 188 Satz 4 SGB VII verwenden, was zwischenzeitlich erfolgt ist. Desweiteren hat der UVT das Formular zur Anforderung von Vorerkrankungen dahingehend verändert, dass zwingend die Einschränkungen nach § 188 Satz 2 SGB VII beachtet werden. Ebenfalls umgesetzt wurden einige Verbesserungsvorschläge für die vom UVT verwendeten Einwilligungserklärungen, um dem Betroffenen transparent zu machen, in welche Übermittlung welcher Daten an welche Stellen auf welcher Rechtsgrundlage zu welchem Zweck er einwilligen soll.

11.9 Datenerhebung bei Schülern und Lehrern

Nach den tragischen Ereignissen im Erfurter Gutenberg-Gymnasium am 26. April 2002 stellte sich u. a. die Aufgabe, Opfer psychologisch zu betreuen. Zu diesem Zweck beauftragte die Unfallkasse Thüringen spezielle Psychologen, die mittels einer Befragung durch standardisierte Fragebögen bei Schülern feststellen sollten, welche Belastungsstörungen (Traumatisierungen) jeweils vorlagen und inwieweit hieraus ggf. therapeutische Maßnahmen abzuleiten waren. Die diagnostische Auswertung der Bögen erfolgte dabei durch eine externe wissenschaftliche Einrichtung.
Nachdem Informationen vorlagen, dass eine Anzahl ausgefüllter Bögen verschwunden war, prüfte ich das Vorgehen der Beteiligten bei dem Projekt unter datenschutzrechtlichen Gesichtspunkten, wobei ich

auch einen Kontrollbesuch bei der Unfallkasse Thüringen durchführte. Dabei stellte sich heraus, dass weder mit den Psychologen noch mit der wissenschaftlichen Stelle vertraglich die bei der Befragung und Auswertung einzuhaltenden technischen und organisatorischen Datenschutzmaßnahmen geregelt worden waren, obwohl dazu die Sozialleistungsträger nach § 78 a SGB X verpflichtet sind. Die Unfallkasse Thüringen hätte sich dementsprechend sowohl mit dem Psychologen als auch der wissenschaftlichen Einrichtung über klare Regelungen verständigen und mit Blick auf das hohe Schutzbedürfnis der Daten insbesondere eine lückenlose Dokumentation der Weitergabe der Daten vorgeben müssen.
Im Hinblick auf die Weiterleitung ausgefüllter Bögen an eine wissenschaftliche Einrichtung zur diagnostischen Auswertung hätte die Unfallkasse zu beachten gehabt, dass die Übermittlung der Daten nicht in personenbezogener Form erfolgt. Hierzu fehlte die Erforderlichkeit. Wie auch die Unfallkasse einräumte, hätte es ausgereicht, die einzelnen Bögen mit einer Nummer zu pseudonymisieren, um die einzelnen Ergebnisse im Rücklauf durch die Psychologen den bekannten Personen zuordnen zu können. Dieser Mangel war umso gravierender, als durch den Verlust der ausgefüllten Fragebögen, jede Person, die sie in Besitz erlangte, den Inhalt und die Darlegungen den jeweiligen Schülern aufgrund der Eintragung des Namens (statt einer Ordnungsnummer) eindeutig zuordnen konnte, sodass das informationelle Selbstbestimmungsrecht der betroffenen Schüler in erheblichem Maß beeinträchtigt wurde.
Darüber hinaus war das Verfahren auch im Zusammenhang mit der Einholung des Einverständnisses der Eltern zur Teilnahme ihrer Kinder an dem Projekt datenschutzrechtlich nicht zufriedenstellend. Die verwendeten Fragebögen enthielten unterschiedliche Einwilligungsformulare für die Eltern. Das für die höheren Klassen vorgesehene Einwilligungsformular beinhaltete lediglich die Formulierung, dass sich die Eltern damit einverstanden erklärten, dass ihr Sohn/ihre Tochter im Rahmen des Nachsorgekonzepts zur Frage einer Traumatisierung an einer schriftlichen Befragung teilnimmt. Eine schriftliche Information darüber, auf welcher Rechtsgrundlage diese Befragung erfolgte, dass diese Befragung freiwillig durchgeführt würde und welche Folgen die Verweigerung der Einwilligung hatte, fehlte. Bei den Fragebögen für die jüngeren Klassenstufen wurde ein Elternbrief beigefügt, in dem der Zweck der Erhebung etwas näher erläutert wurde. Aber auch hier fehlten Angaben zur Rechtsgrundlage, Freiwilligkeit der Daten und der Folgen der Verweigerung der Einwilligung. Im

Ergebnis wurden damit die Anforderungen des § 67 b Abs. 2 SGB X nicht eingehalten, da die Eltern unzureichend über das Verfahren, ihre Rechte und Pflichten informiert wurden.
Selbstverständlich war bei der Gesamtbewertung des Vorgangs die besondere Situation am Erfurter Gutenberg-Gymnasium zu berücksichtigen. Der Umgang mit sensiblen personenbezogenen Daten der Betroffenen wies jedoch gravierende Mängel auf, die bei Beachtung der datenschutzrechtlichen Forderungen hätten vermieden werden können. Ich sprach daher eine Beanstandung aus. Die Unfallkasse Thüringen hat umgehend die notwendigen Maßnahmen zur Behebung der festgestellten Unzulänglichkeiten ergriffen und meine datenschutzrechtlichen Forderungen erfüllt.

11.10 Entbindung von der ärztlichen Schweigepflicht wegen des Informationsinteresses des Arbeitgebers

Die Kenntnis über die Arbeitsfähigkeit seiner Arbeitnehmer ist für einen Arbeitgeber von erheblichem Interesse, denn er ist ohne die entsprechenden Informationen in seiner Dispositionsfähigkeit eingeschränkt. Dementsprechend regelt § 5 Abs. 1 Entgeltfortzahlungsgesetz, dass ein Arbeitnehmer dem Arbeitgeber eine Arbeitsunfähigkeit und deren voraussichtliche Dauer unverzüglich mitzuteilen bzw. bei länger als drei Kalendertage dauernder Arbeitsunfähigkeit eine ärztliche Bescheinigung hierzu beizubringen hat. Grundsätzlich ist der Arbeitnehmer nicht verpflichtet, sich zur Art der Erkrankung und deren Ursache zu äußern, ebenso wenig der ihn behandelnde Arzt, es sei denn, er wäre hierzu durch den Arbeitnehmer ermächtigt worden. Allerdings obliegt es ausnahmsweise dem Arbeitnehmer, sich zu äußern, bspw. wenn die Erkrankung Schutzmaßnahmen des Arbeitgebers für andere erfordert.
Sinngemäß gelten genannte Grundsätze auch für den Fall, dass ein Arbeitnehmer aufgrund seiner Krankheit zwar nicht arbeitsunfähig, jedoch in seiner Verwendungsfähigkeit eingeschränkt ist. Der Arbeitgeber hat ein gewichtiges Interesse daran zu wissen, dass eine Einschränkung besteht und wie sie sich konkret auswirkt. Nicht erforderlich ist, dass der Arbeitgeber etwas über die Erkrankung und deren Ursache selbst erfährt. Ist der Arbeitnehmer nicht bereit, seinem Arbeitgeber die von diesem als für seine Dispositionen notwendig erachteten medizinischen Auskünfte zu geben oder seinen behandelnden Arzt von der Schweigepflicht zu entbinden, so wird die Auseinandersetzung nicht selten vor einem Arbeitsgericht fortgesetzt werden.

Verfügt der Arbeitgeber über einen Betriebsarzt, so besteht die Möglichkeit, dass der Arbeitnehmer dort vorstellig wird, um medizinische Fragen im Hinblick auf das Arbeitsverhältnis zu klären. Damit bestände keine Veranlassung, dem Arbeitgeber selbst, d. h. dessen Personalverwaltung, Angaben über die Erkrankung zu machen.
Aber auch Konstellationen wie die zuletzt genannte sind in der Praxis nicht immer völlig komplikationslos, wie sich aus einer Eingabe ergab. Danach wollte ein öffentlicher Arbeitgeber einen Arbeitnehmer an einen anderen Ort versetzen. Der Arbeitnehmer verwies auf gesundheitliche Einschränkungen, die einer Versetzung entgegen ständen. Um die Versetzung dennoch vornehmen zu können, gleichzeitig aber die Bedürfnisse des Arbeitnehmers zu berücksichtigen, bat der Arbeitgeber um Äußerungen zu verschiedenen medizinischen Fragen bzw. Überlassung u. a. von Fachgutachten. Hierzu war der Arbeitnehmer nicht bereit, hatte jedoch angeboten, sich einer betriebsärztlichen Untersuchung zu unterziehen und bei diesem Anlass auch Einsicht in vorliegende Unterlagen zu gewähren. Hierzu kam es jedoch aus von keiner Seite zu vertretenden Gründen nicht. Auch später bestand zwar die Bereitschaft des Arbeitnehmers zur betriebsärztlichen Untersuchung, er bot sie allerdings nicht mehr schriftlich an. Der Arbeitgeber hingegen war nicht bereit, seinen Arbeitnehmer zu einer solchen Untersuchung aufzufordern und wollte unmittelbar in der beschriebenen Art und Weise informiert werden. Als ich mich deswegen an ihn wandte und um Stellungnahme bat, wurde zunächst meine Zuständigkeit in der Angelegenheit in Frage gestellt, nachdem dieses Problem gelöst war, meine Fragen nur unzureichend beantwortet. Ich führte daher schließlich einen Kontrollbesuch bei dem Arbeitgeber durch, bei dem die aufgetretenen Missverständnisse ausgeräumt werden konnten. Gleichzeitig wurde mir erläutert, dass der Arbeitnehmer selbstverständlich jederzeit die Möglichkeit gehabt hätte, von sich aus beim Betriebsarzt vorstellig zu werden, davon allerdings keinen Gebrauch gemacht habe. Letztlich war man jedoch bereit, den Arbeitnehmer ausdrücklich aufzufordern, sich beim Betriebsarzt untersuchen zu lassen bzw. dort die einschlägigen Unterlagen vorzulegen. Damit wurde auf eine unmittelbare Unterrichtung der personalverwaltenden Stelle des Arbeitgebers über medizinische Daten des Mitarbeiters verzichtet.

11.11 Unerklärliche Übermittlung von Sozialdaten

Die Zulässigkeit der Übermittlung von Sozialdaten ergibt sich aus den entsprechenden bereichsspezifischen Übermittlungsregelungen der einzelnen Sozialgesetzbücher, insbesondere aber auch aus den §§ 67 d ff. SGB X. Die Auslegung und Anwendung dieser Normen bereitet in der Praxis nicht selten Schwierigkeiten. Nicht minder kompliziert aber können Fälle sein, in denen zu klären ist, ob überhaupt eine Übermittlung von Sozialdaten durch verantwortliche Stellen im Sinne des § 67 Abs. 9 SGB X stattgefunden hat. Nicht immer lässt sich dabei die gewünschte Klarheit erreichen.

Einer Eingabe zufolge hatte ein Rechtsanwalt in einem Gerichtsverfahren die Beiziehung einer sozialgerichtlichen Akte beantragt. Dabei war seinen Ausführungen zu entnehmen, dass ihm neben dem Aktenzeichen zumindest teilweise auch der Inhalt der Sozialgerichtsakte bekannt war. Darüber hinaus war er offenkundig auch über eine vorliegende Behinderung des Prozessgegners informiert. In der Eingabe wurde der Verdacht geäußert, dass die genannten Informationen über die Krankenkasse des Petenten nach außen gedrungen seien, insbesondere deshalb, weil eine dem Mandanten des Anwalts nahe stehende Person bei dieser Krankenkasse tätig war. Die Stellungnahme, die ich von der Krankenkasse aufgrund meiner Nachfrage zunächst erhielt, führte in der Sache nicht weiter. Danach seien die betreffenden Daten für die Sachbearbeitung in Angelegenheiten des Petenten nicht erforderlich gewesen und lägen dementsprechend nicht vor. Soweit Mitarbeitern anderweitig Einzelheiten zur Erkrankung des Versicherungsnehmers bekannt waren, seien diese nicht an Dritte weitergegeben worden. Der ebenfalls um Erklärung gebetene genannte Rechtsanwalt gab an, zumindest das Aktenzeichen im Rahmen einer Anfrage beim Sozialgericht erhalten zu haben und sich im Übrigen auf allgemein bekannte Tatsachen bezogen zu haben. Die damit vorliegenden Informationen waren für die Klärung des Sachverhalts wenig erhellend. Bei weiteren Recherchen, an denen neben meiner Dienststelle auch u. a. der Petitionsausschuss des Landtags beteiligt war, ergab sich zunächst, dass die vom Anwalt genannte Anfrage beim Sozialgericht von dort nicht bestätigt werden konnte. Darüber hinaus veranlassten mich weitere Präzisierungen des Sachverhalts durch den Petenten, die beteiligte Krankenkasse nochmals um Prüfung zu bitten, ob nicht doch möglicherweise bestimmte Sozialdaten an andere Stellen oder Personen übermittelt worden seien. Die Antwort fiel wiederum negativ aus.

Dennoch bat ich die Krankenkasse zum dritten Mal um eine Überprüfung, nachdem der Petent weitere zusätzliche Informationen gegeben hatte. Nunmehr stellte sich heraus, dass in einer ihrer Geschäftsstellen eine Akte, die auch die fraglichen Sozialdaten des Petenten enthielt, zeitweilig bearbeitet worden war. Dort hatte zu dem betreffenden Zeitpunkt aber auch der Ehepartner des Prozessgegners gearbeitet. Er habe allerdings aufgrund seiner Aufgaben keine Möglichkeit gehabt, auf die Akte zuzugreifen. Damit war der Sachverhalt nach wie vor nicht eindeutig. Ich führte daher zur Klärung weiterer Einzelheiten eine Überprüfung bei der Krankenversicherung durch. Durch die Einsichtnahme in die betreffende Akte bestätigte sich, dass darin auch Unterlagen über das sozialgerichtliche Verfahren einschließlich eines Gutachtens unter Angabe des Aktenzeichens enthalten waren. Auch konnte die Kenntnisnahme durch unzuständige Mitarbeiter nicht mit absoluter Sicherheit ausgeschlossen werden. Im Ergebnis lag damit zumindest ein plausibler Sachverhalt vor, der jedoch nicht verifiziert werden konnte. Die Krankenversicherung überprüfte daraufhin ihre bereits getroffenen technischen und organisatorischen Maßnahmen zum Datenschutz in der Geschäftsstelle, die einen Zugriff durch unzuständige bzw. unbefugte Mitarbeiter in der Geschäftsstelle ausschließen sollten, dabei insbesondere die Postregelung hinsichtlich ihrer Eignung und praktischen Anwendung. Darüber hinaus wurden alle Mitarbeiter nochmals nachdrücklich über die Einhaltung des Sozialgeheimnisses belehrt.

11.12 Abrechnung interkurrenter medizinischer Behandlungen im Maßregelvollzug

Bereits in meinem 4. TB (11.10) hatte ich mich zu datenschutzrechtlichen Fragen bei der Praxis der Abrechnung interkurrenter medizinischer Behandlungen im Maßregelvollzug im Freistaat Thüringen geäußert. Das damals in Thüringen angewandte Verfahren führte dazu, dass sensible Daten über den Gesundheitszustand der Betroffenen an mehreren Stellen doppelt vorgehalten wurden, ohne dass hierfür ein zwingender Grund ersichtlich war. Im Ergebnis wurde dem TLVwA die Bewirtschaftungsbefugnis für die entsprechenden Haushaltsmittel vom TJM übertragen. Seit dieser Zeit erfolgt die Abrechnung interkurrenter Kosten nur noch durch das TLVwA, sodass eine mehrfache Vorhaltung patientenbezogener Daten ausgeschlossen ist. Die von mir seinerzeit beanstandete Thüringer Verwaltungsvorschrift zu Kostenregelungen für Unterbringungen in Maßregelvollzugseinrichtungen des

Freistaats Thüringen wird seit Januar 2002 in Folge des Trägerwechsels der psychiatrischen Landeskrankenhäuser nicht mehr angewandt. Der Maßregelvollzug wird nunmehr durch die neuen Träger auf der Grundlage eines Beleihungsverhältnisses durchgeführt.
Allein die Tatsache, dass gemäß § 33 Abs. 4 Thüringer Gesetz zur Hilfe und Unterbringung psychisch Kranker (ThürPsychKG) das Land die Kosten der Unterbringung beim Maßregelvollzug trägt, ist nicht als normenklare Rechtsgrundlage anzusehen, in welchem Umfang sensible Daten der Untergebrachten personenbezogen zu Abrechnungszwecken verarbeitet werden dürfen. Das TMSFG hat mitgeteilt, die datenschutzrechtliche Ermächtigungsgrundlage im Rahmen einer Novellierung des ThürPsychKG zu schaffen.

11.13 Ein Computerverkauf mit Folgen

Patientendaten zählen nach § 4 Abs. 5 ThürDSG zu den besonders geschützten Daten. Sie unterfallen einem Berufsgeheimnis und der ärztlichen Schweigepflicht nach § 203 des Strafgesetzbuches. Für den Umgang mit Patientendaten in Krankenhäusern legt das Thüringer Krankenhausgesetz (ThürKHG) eine strenge Zweckbindung fest. So hat die Daten verarbeitende Stelle, das Krankenhaus, die angemessenen technischen und organisatorischen Maßnahmen sicherzustellen, dass Patientendaten nur dem befugten Personenkreis bzw. den befugten Stellen im erforderlichen Umfang (§ 27 Abs. 6 ThürKHG) zugänglich gemacht werden können. Dennoch zeigt sich mitunter, dass der Umgang mit Patientendaten deren Sensibilität nicht angemessen ist.
Durch Presseverlautbarungen erhielt ich Kenntnis darüber, dass Patientendaten eines Krankenhauses in unbefugte Hände gelangt sein mussten, was mich zu einem Kontrollbesuch bei der Klinik veranlasste. Es stellte sich heraus, dass nach einer Aussonderungsaktion Computer verkauft worden waren. Beim Verkauf von PCs ist sicherzustellen, dass vor der Übergabe personenbezogene Daten unwiederbringlich gelöscht sind, sodass keine Rekonstruktion der ehemaligen Datenbestände möglich ist (15.8; 1. TB, 15.9). Die Datenschutzordnung des Krankenhauses schrieb auch vor, dass bei interner Aussonderung von Speichereinheiten eine physische Zerstörung vorzunehmen und zu dokumentieren ist. Dies wäre eine geeignete Maßnahme gewesen, um einen angemessenen Datenschutz und Datensicherheit zu gewährleisten. Tatsächlich aber wurde eine solche Datenlöschung nicht vorgenommen. Vielmehr sollte die Unkenntlichmachung der Daten durch

Formatierung und Neuinstallation des Betriebssystems erreicht werden. Dies sind aus meiner Sicht grundsätzlich keine geeigneten Maßnahmen zum Schutz von Patientendaten, da eine Rekonstruktion der Daten nicht ausgeschlossen werden kann. Erschwerend kam hinzu, dass die vorgesehenen, ohnehin nicht hinreichenden, Löschungsmaßnahmen nicht bei allen PCs durchgeführt worden waren.

Angesichts der Sensibilität der betroffenen Daten und deren unzureichender Behandlung in datenschutzrechtlicher Hinsicht sah ich mich veranlasst, eine Beanstandung auszusprechen. Das Krankenhaus hat die sich im Ergebnis meiner Kontrolle geforderten Regelungen, zu denen auch die Überarbeitung der Datenschutzordnung gehörte, getroffen.

11.14 Zweckwidrige Nutzung und Übermittlung von Gutachten

In einer Eingabe wandte sich ein Bürger an den TLfD mit der Bitte um eine datenschutzrechtliche Prüfung, ob die in seiner Führerscheinstelle über ihn geführte Akte den datenschutzrechtlichen Anforderungen entspricht. Hintergrund dafür war ein Fahrerlaubnisentziehungsverfahren, in dem auch Unterlagen aus einem gerichtlichen Betreuungsverfahren genutzt worden waren. Im konkreten Fall hatte die Führerscheinstelle erfahren, dass für die betreffende Person vom Vormundschaftsgericht die Betreuung in Vermögens- und Behördenangelegenheiten angeordnet war. Mit der Begründung der Prüfung einer Entziehung der Fahrerlaubnis hatte man daraufhin die Betreuungsakte vom Amtsgericht angefordert und daraus Kopien von einer Vielzahl von Unterlagen genommen. Hierzu gehörte auch das im Rahmen des Betreuungsverfahrens vom Amtsgericht in Auftrag gegebene Gutachten, welches von der Führerscheinstelle der Begutachtungsstelle für Fahreignung beim TÜV mit der Bitte um Stellungnahme übersandt worden war. Darüber hinaus hatte die Fahrerlaubnisbehörde unter Verwendung von Auszügen aus dem Gutachten und ergänzt mit eigenen Wertungen und Erkenntnissen andere Ämter innerhalb der Kommune über das bestehende Betreuungsverhältnis der betreffenden Person informiert.
Diese Verfahrensweise wurde gemäß § 39 Abs. 1 ThürDSG beanstandet. Begründet wurde dies damit, dass für einen Teil der Unterlagen über das Betreuungsverhältnis keine Erforderlichkeit für eine Aufnahme in die Führerscheinakte bestand. Desweiteren war die Weiter-

leitung von „Erkenntnissen“ über die Betreuung an andere Stellen innerhalb der Kommunalverwaltung unzulässig, da es nicht die Aufgabe eines Ordnungsamtes ist, andere öffentliche Stellen vorsorglich auf Betreuungsverhältnisse hinzuweisen. Dies war im konkreten Fall umso problematischer, als in dem Informationsschreiben neben subjektiven Eindrücken auch tief greifende persönliche Bewertungen über den Betroffenen enthalten waren, die aus einem psychologischen Gutachten stammten, dessen Inhalt gemäß § 4 Abs. 5 ThürDSG als besonders schützenswert gilt. Zum Fahrerlaubnisentzugsverfahren wurde festgestellt, dass hierfür § 3 Abs. 1 StVG zur Anwendung kommt. Danach hat die Fahrerlaubnisbehörde die Fahrerlaubnis zu entziehen, wenn sich der Betroffene als ungeeignet oder nicht befähigt zum Führen von Kraftfahrzeugen erweist. Gemäß § 2 Abs. 7 StVG hat die Fahrerlaubnisbehörde zu ermitteln, ob der Betroffene zum Führen von Fahrzeugen geeignet und befähigt ist. Werden nach § 2 Abs. 8 StVG Tatsachen bekannt, die Bedenken gegen die Eignung oder Befähigung begründen, kann die Fahrerlaubnisbehörde dem Betroffenen die Beibringung eines entsprechenden Gutachtens auferlegen. Im vorliegenden Fall wurde als zulässig eingeschätzt, dass zur Prüfung, ob eine Ungeeignetheit vorliegt, beim Amtsgericht gemäß § 34 FGG Akteneinsicht über das Betreuungsverfahren begehrt worden war. Die Aufnahme von Kopien in die Fahrerlaubnisakte muss sich jedoch auf Sachverhalte oder Anhaltspunkte beschränken, aus denen sich Gründe für die Entziehung der Fahrerlaubnis ableiten lassen. Hierzu enthielt jedoch das betreffende Gutachten keine konkreten Aussagen. Es beinhaltete vielmehr eine Vielzahl besonders sensibler personenbezogener Daten, die sich u. a. neben der Darstellung und des Eindrucks der Wohnung insbesondere auf das Erscheinungsbild und das Verhalten des Betroffenen im Rahmen einer gegen seinen Willen und unter polizeilicher Mitwirkung erfolgten Begutachtung bezogen. Anstatt wie nach § 3 Abs. 1 i. V. m. § 2 Abs. 8 StVG vorgesehen, vom Betroffenen ein Gutachten über die Fähigkeit zur Führung eines Fahrzeugs zu fordern, hatte man einem Gutachter beim TÜV ein in einem völlig anderem Zusammenhang und für einen anderen Zweck erstelltes Gutachten zur Beurteilung übersandt.

Im Ergebnis der Überprüfung der Führerscheinakte wurden deshalb zunächst die für das Entzugsverfahren nicht erforderlichen Unterlagen daraus entfernt. Gleichzeitig wurden in Auswertung des Sachverhaltes Festlegungen dahingehend getroffen, dass künftig bei ähnlich gelagerten Fällen Auszüge bzw. Kopien aus zu anderen Zwecken erstellten Schriftstücken oder Gutachten nur im erforderlichen Umfang zu ferti-

gen sind und nur insoweit diese ausschließlich Informationen umfassen, die nach Überzeugung der Fahrerlaubnisbehörde als Nachweis für die Nichteignung zur Führung eines Fahrzeugs dienen können. Keine Bedenken bestehen auch, wenn sich die Fahrerlaubnisbehörde bei anderen Stellen in allgemeiner, nicht personenbeziehbarer Form fachlichen Rat holen, ob und inwieweit der Entzug einer Fahrerlaubnis möglich oder nötig wäre. Soweit aber von der Fahrerlaubnisbehörde die Nichteignung des Betroffenen nicht zweifelsfrei ohne die weitere Beteiligung Dritter gemäß § 11 Abs. 7 FeV festgestellt werden kann, sind die rechtlichen Möglichkeiten der Prüfung entsprechend § 11 Abs. 1 FeV durch die Anordnung der Beibringung eines ärztlichen Gutachtens auszuschöpfen.
Neben diesen Maßnahmen wurden darüber hinaus die Empfänger des Informationsschreibens über das Betreuungsverhältnis angewiesen, dieses unverzüglich zu vernichten.

11.15 Übermittlung von Sozialdaten an Dritte bei der Gewährung von Sachleistungen nach dem BSHG

Sozialhilfe als einmalige Leistung gemäß § 21 Abs. 1 a BSHG kann als Bar- oder Sachleistung an den Hilfeempfänger erfolgen. Dabei besteht nach der Rechtsprechung auch aus datenschutzrechtlicher Sicht kein Vorrang der Barleistung vor einer Sachleistung. Der Sozialhilfeträger entscheidet nach pflichtgemäßen Ermessen im Einzelfall, welche der beiden Hilfearten gewählt wird. Soll die Hilfe zum Lebensunterhalt im Wege einer durch Dritte zu erbringenden Sachleistung, wie etwa bei der Ausstellung von Warengutscheinen, erfolgen, so ist zu berücksichtigen, dass bereits die Tatsache des Sozialhilfebezugs ein schützenswertes Sozialdatum darstellt. Dies schließt jedoch nicht von vornherein eine Offenbarung von Sozialdaten gegenüber Dritten zum Zweck der Leistungsgewährung aus. Sie ist nach § 69 Abs. 1 Satz 1 Nr. 1 2. Alternative SGB X zulässig, wenn es für die Erfüllung der gesetzlichen Aufgabe der übermittelnden Stelle erforderlich ist. Bei der Prüfung, ob eine solche Datenübermittlung zur Abwicklung von Sachleistungen als erforderlich anzusehen ist, sind die Gesichtspunkte einer effektiven und wirtschaftlichen Erbringung von Sozialleistungen mit dem Recht des Betroffenen auf informationelle Selbstbestimmung in jedem Einzelfall abzuwägen.
Wie ich durch verschiedene Petenten erfahren habe, entspricht die Praxis der Ausgabe von Warengutscheinen durch Sozialhilfeträger nicht immer diesen Anforderungen. So werden bei der Verwendung

von Gutscheinen teilweise standardisiert die Namen und Anschriften der Hilfeempfänger sowie die Sozialleistungsträger eingetragen. Selbstverständlich können die Umstände des Einzelfalls, insbesondere auch das Vorverhalten des Hilfeempfängers, die Offenlegung bestimmter Sozialdaten unumgänglich machen, um den Leistungszweck auch tatsächlich zu erfüllen. So wird bei Hilfeempfängern, die nachgewiesenermaßen die Neigung haben, ihnen überlassene Warengutscheine missbräuchlich zu verwenden, gegen eine Nennung von Identifikatoren wie dem Namen nichts einzuwenden sein. Für die Mehrzahl der Fälle dürfte allerdings davon auszugehen sein, dass die Angaben des Namens und der Anschrift des Betroffenen in einem Warengutschein zur Abrechnung von Sozialhilfesachleistungen mit dem Lieferanten nicht regelmäßig erforderlich sind und insofern eine Pseudonymisierung des Gutscheins bspw. durch das Anbringen des Aktenzeichens des Sozialhilfeträgers oder eines anderen den Fall eindeutig kennzeichnenden Merkmals zur Abrechnung ausreichen. Zur konkreten Umsetzung dieser Einschätzung, die von der Aufsicht der Sozialhilfeträger, dem TLVwA, geteilt wird, wäre es, soweit es die organisatorischen Gegebenheiten vor Ort zulassen, z. B. denkbar, ein dem bei der Ausgabe von Reiseschecks vergleichbares Verfahren anzuwenden. Der Hilfeempfänger würde dabei im Beisein des Mitarbeiters des Sozialamtes auf dem pseudonymisierten Warengutschein eine Unterschrift leisten. Den Erhalt der Ware müsste er dann in der Verkaufsstelle nochmals mit seiner Unterschrift auf dem Warengutschein quittieren. Damit würde dem Händler und der Sozialbehörde eine dem Missbrauch vorbeugende Kontrollmöglichkeit eingeräumt werden, ohne gleichzeitig weitere Sozialdaten zu offenbaren. Soweit eine Anlieferung der Ware vorgesehen ist, bestehen selbstverständlich keine datenschutzrechtlichen Bedenken gegen eine entsprechende Eintragung auf dem Warengutschein. Eine direkte Übermittlung des Warengutscheins vom Sozialhilfeträger an Lieferanten hielte ich nur dann für zulässig, wenn nachweisbar Erkenntnisse vorliegen, dass anderenfalls der Zweck der Hilfeleistung aus den verschiedensten Gründen nicht erreicht wird oder der Hilfesuchende zustimmt.

In diesem Zusammenhang ist beispielhaft ein Fall zu nennen, in dem sich ein Sozialhilfeempfänger beschwerte, dass ein Sozialhilfeträger im Rahmen der Gewährung von Sachleistungen Warengutscheine ausstellte, die den Namen und die Adresse des Sozialhilfeempfängers enthielten. Darüber hinaus ergab sich aus dem Gutschein, dass der Hilfeempfänger berechtigt war, „zu Lasten des unterfertigten Sozialhilfeträgers“ bestimmte Waren einzukaufen. Im Rahmen des Kon-

trollbesuchs beim Sozialhilfeträger war festzustellen, dass im konkreten Fall die Nennung von Namen und Adresse verhältnismäßig war. Zur Verhinderung eines möglichen Missbrauchs des Warengutscheins, wie etwa einer Weiterveräußerung, war die Nennung des Namens auf dem Gutschein nicht zu kritisieren. Auch die Angabe der Adresse war nicht zu kritisieren, da der auf dem Warengutschein genannte Gegenstand aufgrund seiner Größe angeliefert werden sollte. Anders zu bewerten war allerdings die Verwendung des Begriffs „Sozialhilfeträger". Damit wurde deutlich, dass der im Gutschein genannte Kaufgegenstand eine Leistung der Sozialhilfe darstellte, der Käufer mithin Sozialhilfeempfänger war. Zwingende Gründe, die Behördenbezeichnung auf dem Warengutschein zu belassen, waren nicht ersichtlich. Der Sozialhilfeträger erklärte sich daher bereit, mit dem die betreffenden Leerformulare herstellenden Verlag eine Änderung zu vereinbaren. Er bezieht nun Warengutscheinvordrucke, in denen der Begriff „Sozialhilfeträger" durch die neutrale Bezeichnung „Behörde" ersetzt wurde.

11.16 Datenübermittlung von Sozialdaten gegenüber Dritten

Eine Fragestellung, mit der ich in unterschiedlichen Fallkonstellationen immer wieder konfrontiert werde, ist, inwieweit Sozialbehörden bei ihren Ermittlungen, bspw. zur Feststellung der Hilfsbedürftigkeit einer Person, Sozialdaten Dritten übermitteln dürfen oder Daten bei Dritten zu erheben befugt sind. In Zeiten knapper Kassen gehen Sozialbehörden durchaus auch vor Ort, um zu überprüfen, ob im Einzelfall die gesetzlichen Voraussetzungen für die Bewilligung einer gewünschten Sozialleistung tatsächlich gegeben sind. Dabei berufen sie sich auf allgemeine Verfahrensgrundsätze des Sozialgesetzbuchs, wonach sie den Sachverhalt von Amts wegen ermitteln und Art und Umfang der Ermittlungen bestimmen (§ 20 SGB X) sowie Auskünfte jeder Art einholen sowie Beteiligte anhören, Zeugen und Sachverständige vernehmen können (§ 21 SGB X). Allerdings: Im Sozialgesetzbuch (§ 37 Satz 3 SGB I) ist ausdrücklich geregelt, dass die Regelungen zum Schutz der Sozialdaten diesen Bestimmungen vorgehen. Dementsprechend dürfen Sozialdaten nur erhoben werden, wenn ihre Kenntnis zur Erfüllung einer Aufgabe des Sozialleistungsträgers erforderlich ist (§ 67 a Abs. 1 SGB X). Weiter sind Sozialdaten grundsätzlich beim Betroffenen selbst zu erheben (§ 67 a Abs. 2 Satz 1 SGB X). Ohne seine Mitwirkung dürfen sie bei anderen Personen wie Mitbewohnern, Vermietern, Nachbarn usw. nur unter den Vorausset-

zungen des § 67 a Abs. 2 Satz 2 Nr. 2 SGB X erhoben werden, d. h. insbesondere, wenn die Erhebung beim Betroffenen selbst einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Bei der Interessenabwägung ist auch zu berücksichtigen, dass bei der Befragung anderer Personen regelmäßig Informationen über den Betroffenen preisgegeben werden, die möglicherweise einen schädigenden Einfluss auf seinen Ruf haben.
Um die korrekte Anwendung der genannten Rechtsvorschriften ging es auch in dem nachfolgend skizzierten beispielhaften Fall. Im Rahmen eines Verfahrens zur Gewährung einer Sozialleistung erkundigten sich Mitarbeiter der Behörde in der Nachbarschaft des Antragstellers über dessen Wohnverhältnisse, die die Sozialbehörde in der Sache selbst für relevant hielt. Die Sozialbehörde hielt ihr Vorgehen u. a. auch deshalb für erforderlich, weil ihr Sachverständigengutachten zur Hilfsbedürftigkeit des Betroffenen vorlagen, die zu unterschiedlichen Ergebnissen gelangten. Sie wollte sich daher selbst ein Bild von den Lebensbedingungen des Antragstellers vor Ort machen. Ungeachtet dessen, dass im konkreten Fall die Befragung der Nachbarschaft unter dem Aspekt der Erforderlichkeit datenschutzrechtlichen Bedenken begegnete, da den Mitbewohnern des Hauses nur in begrenzten Umfang Einblick in die tatsächlichen Verhältnisse des Antragstellers möglich sein dürften und damit die Eignung der Maßnahme zumindest zweifelhaft war, stellte sich bei der Frage der Zulässigkeit des Vorgehens unter dem Gesichtspunkt der Erhebung bei anderen Personen (§ 67 Abs. 2 Satz 2 Nr. 2 SGB X) heraus, dass in diesem besonderem Fall die gesetzlichen Voraussetzungen gegeben waren. Die Mitarbeiter der Sozialbehörde hatten, bevor sie sich an die Nachbarschaft wandten, vergeblich versucht, den Betroffenen zu erreichen. Da in der gleichen Angelegenheit eine gerichtliche Entscheidung unmittelbar bevorstand - die zu erhebenden Informationen sollten seitens der Behörde in das Verfahren einfließen - und insoweit ein weiterer Besuch beim Betroffenen zeitlich nicht mehr möglich war, konnte bei ihm selbst keine Datenerhebung mit verhältnismäßigen Aufwand erfolgen.
Die Sozialbehörde versicherte mir, dass es sich hier lediglich um einen Ausnahmefall gehandelt habe, der keinesfalls das übliche Verfahren darstellte. Gleichwohl überprüfte die Behörde anlässlich des Falles ihre Vorgehensweisen und erklärte, dass künftig bei Ermittlungen der Grundsatz der Erhebung beim Betroffenen ausreichend beachtet werden wird.

11.17 Rehabilitierungsbescheid und Datenerhebungen durch die Sozialämter

Nach dem Gesetz über den Ausgleich beruflicher Benachteiligungen für Opfer politischer Verfolgung im Beitrittsgebiet (BerRehaG) haben ehemals politisch Verfolgte unter bestimmten Voraussetzungen Anspruch auf soziale Ausgleichsleistungen. Der gegenüber den Sozialbehörden zu erbringende Nachweis über das Vorliegen der Voraussetzungen zur Gewährung von Leistungen wird u. a. mit der Vorlage einer von der Rehabilitierungsbehörde erstellten Rehabilitierungsbescheinigung (§ 17 BerRehaG) geführt. Die Bescheinigung enthält dabei die erforderlichen Daten, um seitens der Sozialbehörde über den geltend gemachten Anspruch entscheiden zu können.
Irritationen ergaben sich in einem mir bekannt gewordenen Fall, in dem der zuständigen Sozialbehörde an Stelle der üblichen Rehabilitierungsbescheinigung von einem Antragsteller eine Kopie der ersten Seite des eigentlichen Rehabilitierungsbescheides vorgelegt wurde. Da die Behörde dies nicht als ausreichend erachtete, forderte sie zum Zwecke der Antragsbearbeitung den gesamten Rehabilitierungsbescheid an, der eine Reihe sensibler Daten enthielt, die zur Bearbeitung nicht erforderlich waren. Wie sich herausstellte, lag der Grund hierfür darin, dass die Sozialbehörde im Rahmen des Ausgleichsverfahrens nur die Vorlage der Rehabilitierungsbescheinigung oder des vollständigen Bescheides als zulässigen Nachweis anerkannte. Sie hielt daher ihr Vorgehen im konkreten Einzelfall, in dem der Antragsteller (noch) nicht über eine entsprechende Bescheinigung verfügte, für korrekt.
Nach § 17 Abs. 1 BerRehaG haben die Betroffenen auf Antrag einen Anspruch gegenüber der Rehabilitierungsbehörde auf Erteilung einer - im Vergleich zum Rehabilitierungsbescheid verkürzten - Bescheinigung. Der Antragsteller ist damit nicht gezwungen, zum Teil sensible Daten aus dem Rehabilitierungsbescheid gegenüber der Sozialbehörde zu offenbaren. Bisher war aber neben dem Rehabilitierungsbescheid als solchem nur eine zusätzliche „Bescheinigung zur Vorlage beim Versicherungsträger“ erstellt worden. Ich setzte mich deshalb mit dem für den Erlass von Rehabilitierungsbescheiden zuständigen Landesamt für Soziales und Familie in Verbindung, welches zusagte, künftig auf Wunsch eines Antragstellers auch eine gesonderte Rehabilitierungsbescheinigung zu erteilen, die zur Vorlage bei Sozialbehörden bestimmt ist. Gleichzeitig forderte ich die betreffende Sozialbehörde auf, Antragsteller, die über keine Rehabilitierungsbescheinigung verfügen,

darauf hinzuweisen, dass die Rehabilitierungsämter zur Erstellung einer solchen separaten Bescheinigung gesetzlich verpflichtet sind.
Die von mir im konkreten Fall zusätzlich gewünschte Löschung nach § 84 Abs. 2 SGB X der im zwischenzeitlich vorgelegten Rehabilitierungsbescheid enthaltenen, aber für die Bearbeitung nicht erforderlichen, Daten wurde ebenfalls entsprochen.

11.18 Vorlage von Vermögenserklärungen bei der Antragstellung auf Sozialhilfe

Wesentliches Kriterium für die Bewilligung von Sozialleistungen ist die Feststellung der Bedürftigkeit der Antragsteller auf Sozialhilfe. Da die Feststellung von Vermögenswerten jedoch mit der Erhebung der entscheidungsrelevanten personenbezogenen Daten verbunden ist, bedeutet dies stets einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen. Verständlich ist, dass hierbei mitunter zum Inhalt und der Form der Datenerhebung unterschiedliche Auffassungen zwischen den Beteiligten bestehen. Bei entsprechenden Anfragen vertritt hierzu der TLfD folgende Auffassung: Unstrittig ist, dass zur Feststellung der Bedürftigkeit bei Antragstellern auf Sozialhilfe deren Vermögenswerte ermittelt werden müssen. Bei der Erhebung der entscheidungsrelevanten und somit zwingend erforderlichen personenbezogenen Daten ist stets der verfassungsrechtlich gewährleistete Grundsatz der Verhältnismäßigkeit zu beachten. Das bedeutet, dass bei der Aufgabenerfüllung des Sozialamtes stets vom geringst möglichen Eingriff in das Persönlichkeitsrecht der Betroffenen auszugehen ist. Unstrittig ist weiterhin, dass das Sozialamt bei der Prüfung des Anspruchs auf Sozialhilfe berechtigt bzw. auch verpflichtet ist, Nachweise für die Richtigkeit einzelner Angaben vom Antragsteller zu fordern. In erster Linie ist dabei der Antragsteller selbst gefragt, seine Einkommens- und Vermögenssituation darzulegen und hierzu die erforderlichen Nachweise vorzulegen. In welcher Form er dieser Nachweispflicht nachkommt, bleibt zunächst dem Antragsteller überlassen. Nur wenn er diese Nachweise nicht erbringen kann oder im begründeten Einzelfall der Verdacht besteht, dass er z. B. bei einem von ihm benannten Geldinstitut über weitere Konten verfügt, ist die Forderung, dass er dem Sozialamt eine vom Geldinstitut unterzeichnete schriftliche Bestätigung über alle dort unter seinem Namen vorliegenden Geld- bzw. Vermögenswerte vorzulegen hat, gerechtfertigt. Eine generelle Forderung zur Vorlage einer Bankauskunft von Antragstellern, ohne konkrete Anhaltspunkte dafür, dass die vom Hilfe

Suchenden abgegebene Erklärung zu den Vermögensverhältnissen unrichtig ist, stellt nach der Rechtsprechung eine überflüssige Ermittlungstätigkeit dar, die nach § 60 Abs. 1 Nr. 1 SGB I nicht erforderlich und somit unzulässig ist. In diesem Zusammenhang darf nicht unberücksichtigt bleiben, dass bei der Einzelfallentscheidung hinsichtlich der Forderung zur Vorlage einer zusätzlichen Bescheinigung der genannten Geldinstitute, sich diese ohnehin nur auf die vom Antragsteller genannten Einrichtungen beziehen kann, da jede Forderung nach „Negativbescheinigungen“ aller möglichen Geldinstitute oder Versicherungen unangemessen und von den gesetzlichen Möglichkeiten nicht gedeckt wäre. Darüber hinaus dürfte es auch wenig wahrscheinlich sein, dass der Antragsteller eine Bestätigung des Geldinstitutes, dass die vorstehenden Angaben nicht richtig sind, dem Sozialamt vorlegen wird, sodass insoweit berechtigte Zweifel am praktischen Nutzen der Antwortmöglichkeiten bestehen. Ebenso verstößt eine Vorgabe des Sozialamtes, dass sich der Hilfe Suchende gegenüber dem Geldinstitut durch die Vorlage eines einheitlichen Vordrucks des Sozialamtes aufgrund der darin enthaltenen direkten oder indirekten Hinweise als Sozialhilfeantragsteller oder Empfänger offenbaren muss, gegen das Sozialgeheimnis, da hierzu grundsätzlich kein Erfordernis besteht. Statt dessen sind, soweit erforderlich, andere Möglichkeiten der Nachweisführung, wie z. B. Einsichtnahme in Kontoauszüge, Sparbücher usw. zu nutzen. Eine Forderung, sofern eine Bankbestätigung im Einzelfall geboten erscheint, dass auf dieser der Zweck der Vermögenserklärung zu benennen ist, würde gleichfalls gegen das Sozialgeheimnis verstoßen. Ebenso ist die generelle Forderung des Sozialamtes nach einer Einwilligung zur Einholung von Bankauskünften durch das Sozialamt von der Verpflichtung des Hilfeempfängers zur Angabe leistungsabhängiger Tatsachen und von seiner Mitwirkungspflicht nicht gedeckt. Es ist in jedem Fall dem Betroffenen vorrangig Gelegenheit zu geben, Bankauskünfte selbst und ohne dass das Geldinstitut den Verwendungszweck erkennen kann, beizubringen. Nur soweit es im begründeten Einzelfall erforderlich wird, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben. Da Nachfragen bei Dritten durch das Sozialamt aber nur zulässig sind, wenn konkrete Zweifel an der Richtigkeit oder Vollständigkeit der Angaben bestehen, kann in diesem Fall die Zustimmung zur Auskunftserteilung gesondert eingeholt, andernfalls die Leistungserbringung eingestellt werden.

11.19 Datenübermittlung von Sozialdaten auf Überweisungsträgern

Dass es sich bei der Tatsache des Sozialbezugs um ein schützenswertes Sozialdatum handelt, wurde bereits im Zusammenhang mit der Gewährung von Sachleistungen nach dem BSHG (11.15) dargestellt. Der sozialbehördliche Umgang mit Sozialdaten gestaltet sich allerdings nicht nur bei Sachleistungen mitunter schwierig, er kann auch bei der Hilfe zum Lebensunterhalt im Wege der Geldleistung Probleme mit sich bringen. Nach § 35 Abs. 1 SGB I hat jeder Anspruch darauf, dass seine personenbezogenen Daten von Leistungsträgern als Sozialgeheimnis gewahrt und nicht unbefugt übermittelt werden. Trotzdem kam es in der Vergangenheit vor, dass bei Hilfeleistungen in der Form der Geldleistung, die durch Banküberweisungen erbracht wurden, bei einer eindeutigen Deklaration des Überweisungszwecks „Sozialhilfe“ auf dem Überweisungsträger der überweisenden Bank die Tatsache der Sozialhilfegewährung übermittelt wurde, obwohl bereits mit Urteil vom 23. Juni 1994 (DVBl. 1994, S. 1313 f.) das Bundesverwaltungsgericht entschieden hat, dass es nicht zulässig sei, die Zahlung von Sozialhilfe generell ohne Zustimmung des Hilfeempfängers auf Überweisungsträgern mit dem Vermerk „Sozialhilfe“ zu kennzeichnen. Es handelt sich dabei um ein personenbezogenes Datum, welches den wirtschaftlichen Status des Leistungsempfängers kennzeichnet. Ich habe daher 1996 mit einem Rundschreiben an alle für Sozialleistungen zuständigen Leistungsträger im Freistaat Thüringen um eine Überprüfung der praktizierten Verfahrensweise unter Beifügung eines Alternativvorschlags gebeten. Aufgrund einer Eingabe erfuhr ich jedoch von einem Fall, in dem das Sozialamt bei der Leistung von Sozialhilfe als Geldleistung wiederum den Verwendungszweck konkret angegeben hatte. Bei der Prüfung ergab sich allerdings, dass das Sozialamt datenschutzgerecht Überweisungen grundsätzlich nur mit dem Vermerk „laut Bescheid“ kennzeichnete. Die Form der Kennzeichnung war auch bereits von der im Sozialamt genutzten Software vorgegeben, sodass nur in Ausnahmefällen von den Bearbeitern die Sozialhilfeleistung als Zahlungsgrund einzugeben war. Dass die Überweisung im konkreten Fall als Sozialhilfeleistung gekennzeichnet worden war, lag an einer personellen Veränderung. Die Angelegenheit wurde in der Sozialhilfebehörde zum Anlass genommen, nochmals alle dort tätigen Personen über die Vorschriften des Datenschutzes und insbesondere über die im konkreten Fall nicht ausreichend beachtete Rechtslage zu belehren.

12. Statistik

12.1 Umsetzung des Testgesetzes durch das Thüringer Landesamt für Statistik (TLS)

Im Abschnitt 12.1 des 4. TB hatte ich bereits darüber berichtet, dass im Jahr 2001 das Testgesetz für einen rechnergestützten Zensus (Zensusvorbereitungsgesetz, BGBl. I, S. 1882 ff.) beschlossen wurde. Darin war festgelegt, dass die für den Test erforderlichen personenbezogenen Daten ausschließlich von den statistischen Landesämtern und dem statistischen Bundesamt erhoben und verarbeitet werden. Sie unterliegen dabei der statistischen Geheimhaltung und dürfen in keiner Weise der Verwaltung zur Kenntnis gelangen. Die besondere Problematik bei der Umsetzung des Testgesetzes bestand insbesondere darin, mögliche widersprüchliche Informationen bei den Datenabgleichen zu klären, ohne dass dabei die betreffenden Verwaltungsstellen Rückinformationen erhalten. Aufgrund der Bedeutung des Verfahrens wurde dies vom TLfD zum Anlass genommen, die Einhaltung des Datenschutzes und der Datensicherheit bei der Umsetzung des Zensusvorbereitungsgesetzes im TLS zu prüfen. Verletzungen datenschutzrechtlicher Bestimmungen wurden dabei nicht festgestellt.

12.2 Datenschutzrechtliche Bewertung von Studienverlaufsstatistiken

Im Ergebnis des Volkszählungsurteils wurde bei der Novellierung des Hochschulgesetzes 1990 ausdrücklich auf eine Studienverlaufsstatistik verzichtet, um den verfassungs- und datenschutzrechtlichen Bedenken Rechnung zu tragen. Wie entsprechende Bestrebungen zeigen, wurden die Informationsverluste, die durch den Verzicht auf die Verlaufsstatistik eingetreten sind, nicht wie vorgesehen durch andere statistische Erhebungen kompensiert. Aufgrund dessen beschäftigten sich die DSB des Bundes und der Länder erneut mit der Frage der Wiederaufnahme einer Studienverlaufsstatistik auf Bundesebene.
Selbstverständlich ist man sich dabei bewusst, dass Informationsdefizite hinsichtlich des Studienverhaltens, der Abbrüche oder des Wechsels von Studieneinrichtungen oder Fachrichtungen entsprechende Auswirkungen auf die Planungen und Finanzierungen an den Universitäten und Hochschulen haben. Insoweit ist das wachsende Informationsbedürfnis der für diesen Bereich zuständigen Stellen insbesondere auch unter dem Aspekt begrenzter materieller und finanzieller Res-

sourcen nachvollziehbar. Unter Abwägung mit dem Recht auf informationelle Selbstbestimmung erscheint es dennoch nicht gerechtfertigt, für diesen Zweck eine zentrale Studentendatei, wenn auch ggf. in pseudonymisierter Form zu schaffen. Es wurde deshalb der Vorschlag unterbreitet, zunächst alle anderen Möglichkeiten der Informationsgewinnung auszuschöpfen, insbesondere in dem z. B. anonyme studienbegleitende Befragungen bei den Studenten durchzuführen.

12.3 Normenklarheit bei der Durchführung von Verkehrserhebungen

Im Rahmen seiner Beratungsfunktion wurde dem TLfD auch eine von einer Kommune bereits beschlossene Verkehrserhebung zur datenschutzrechtlichen Beurteilung übergeben. Dabei musste festgestellt werden, dass die zur Durchführung beschlossene Satzung die Forderungen des Bundesverfassungsgerichts nach normenklaren Regelungen für Eingriffsbefugnisse in das informationelle Selbstbestimmungsrecht nicht im vollen Umfang erfüllte. Dies betraf neben eindeutigen Aussagen zu den Verantwortlichkeiten insbesondere auch die Festlegungen zum Datenumfang und der Speicherdauer. Darüber hinaus enthielt sie widersprüchliche Aussagen über die vermeintliche Anonymität der Befragung. Im konkreten Fall war vorgesehen, die Datenerhebung „in Zusammenarbeit mit einer wissenschaftlichen Einrichtung“ durchzuführen. Weiter gehende Festlegungen zu den näheren Aufgaben und Verantwortlichkeiten hierzu enthielt die Satzung nicht. Als Erhebungseinheit und Auskunftsstellen wurden in der Satzung „Haushalte“ und als deren Datenbasis das Einwohnermelderegister genannt, obwohl dieses Merkmal dort nicht gespeichert wird. Gleichzeitig fehlte eine Erläuterung zum Haushaltsbegriff. Desweiteren gehörte zu den Erhebungsmerkmalen die „telefonische Erreichbarkeit“. Da im allgemeinen Sprachgebrauch unter dieser Angabe die Telefonnummer für Rückfragen verstanden wird, hätte dies beim Adressaten des Fragebogens zu Irritationen führen können, ob er seine Telefonnummer (was der „versprochenen“ Anonymität der Befragung widersprochen hätte) oder lediglich das Vorhandensein eines Telefonanschlusses/Mobiltelefones eintragen sollte. Darüber hinaus war es trotz „anonymer Auskunftserteilung“ vorgesehen, zunächst von den Auskunftspersonen als Hilfsmerkmale den Familiennamen, Anschriften und das Jahr der Geburt bis zum Abschluss der gesamten Erhebung (z. B. für Eingangskontrollen, Rückfragen, Erinnerungen u. ä.) zu speichern. Weiterhin sollte die Erhebung in einer Kombination von

schriftlichen und telefonischen Interviews bei konkret ausgewählten Haushalten durchgeführt werden, obwohl nicht nur die weitere Verarbeitung, sondern auch die Auskunftserteilung laut Satzung ausdrücklich anonym erfolgen sollte.
Im Ergebnis der Stellungnahme des TLfD wurde die Satzung überarbeitet und dem datenschutzrechtlichen Anliegen entsprochen.

13. Bildung, Wissenschaft, Forschung

13.1 Änderungen im Thüringer Schulgesetz

Im Berichtszeitraum beteiligte sich der TLfD auch an den Beratungen zur Änderung des Thüringer Schulgesetzes (ThürSchulG). Dabei wurde meine bereits in der Vergangenheit vorgebrachte Anregung (4. TB, 13.6) bezüglich der Aufnahme einer Vorschrift zur Nutzung des Internets durch Schulen dahingehend aufgegriffen, dass künftig Veröffentlichungen personenbezogener Daten nur noch mit Einwilligung der Betroffenen erlaubt sind. Desweiteren wurde die Ermächtigungsklausel für den Erlass von Rechtsverordnungen um eine Vorschrift ergänzt, die die Verarbeitung personenbezogener Schülerdaten auf privaten Datenverarbeitungsgeräten der Lehrer näher regelt. Schließlich wurden auf meine Empfehlungen hin auch alle datenschutzrechtlichen Regelungen des ThürSchulG an die im novellierten ThürDSG gebräuchlichen Termini angepasst.
Eine Änderung erfuhr das Schulgesetz auch hinsichtlich der Informationspflicht der Schulen gegenüber Eltern erwachsener Schüler. Hintergrund dafür waren die schrecklichen Ereignisse im Erfurter Gutenberg-Gymnasium am 26. April 2002. Es stellte sich deshalb die Frage, ob auch die Eltern bzw. Erziehungsberechtigten erwachsener Schüler über bestimmte Probleme, Vorkommnisse und wichtige Maßnahmen in der Schule unterrichtet werden können oder müssen. Als Nachtrag zu o. g. Änderungsentwurf wurde deshalb eine Ergänzung des § 31 ThürSchulG für eine Informationspflicht der Eltern volljähriger Schüler über „sonstige wesentliche, den Schüler betreffende Vorgänge“ vorgelegt, zu der ich um eine Stellungnahme gebeten wurde. Hierzu hatte ich bereits im Vorfeld die Auffassung des TKM geteilt, wonach dann durch Gesetz festzulegen ist, dass in den Fällen einer Versetzung in eine Parallelklasse der gleichen Schule, dem zeitlich begrenzten Ausschluss vom Unterricht sowie der Zuweisung an eine andere Schule auch eine Informationspflicht der Schule gegenüber Eltern volljähriger Schüler bis zur Vollendung des 21. Lebensjahres besteht, sofern

der volljährige Schüler dem nicht generell oder im Einzelfall widersprochen hat, wobei die Eltern über einen Widerspruch des Schülers von der Schule zu informieren sind.
Ich machte dabei deutlich, dass die Information von Eltern über schulische Angelegenheiten einerseits einen Eingriff in das Recht auf informationelle Selbstbestimmung von volljährigen Schülern darstellt, dem auf der anderen Seite aber das Recht der Eltern auf Pflege und Erziehung der Kinder gemäß Art. 6 Abs. 2 Satz 1 GG und Art. 21 der Verfassung des Freistaats Thüringen gegenüber steht. Eine Einschränkung des Rechts auf informationelle Selbstbestimmung volljähriger Schüler halte ich insoweit für vertretbar, als das Zusammenwirken von Eltern und Schule im Rahmen des Erziehungs- und Bildungsauftrags dem Wohl des Kindes dient. Nach meiner Auffassung endet dies nicht automatisch bei Beendigung der Pflicht der elterlichen Sorge mit dem Eintritt der Volljährigkeit gemäß § 1626 Abs. 1 Satz 1 BGB. Durch die dem volljährigen Schüler eingeräumte Möglichkeit, der Datenübermittlung an die Eltern zu widersprechen, wird auch dem Recht des Schülers auf informationelle Selbstbestimmung in angemessener Weise Rechnung getragen. Insgesamt ist die Aufnahme einer Regelung zur Informationspflicht der Schule an Eltern volljähriger Schüler unter dem Aspekt der schulischen Fürsorgepflicht im Interesse des Schülers gerechtfertigt.
In diesem Zusammenhang wurden auch die Möglichkeiten der Beteiligung von Schulen vor der Erteilung waffenrechtlicher Genehmigungen an Schüler erörtert. Seit den tragischen Ereignissen am Gutenberg-Gymnasium beschäftigen sich nicht nur die zuständigen Stellen, sondern insbesondere auch der Landtag damit, im Einklang mit den gesetzlichen Regelungen weitere Möglichkeiten für eine „Qualifizierung“ der Eignungsprüfung zu erschließen, um dadurch „Fehlentscheidungen“ bei der Erteilung einer waffenrechtlichen Erlaubnis auszuschließen. Von einer Seminargruppe am Gutenberg-Gymnasium wurden Vorschläge für eine Anhörungspflicht der Schulen im Erlaubnisverfahren erarbeitet und im Rahmen einer öffentlichen Anhörung im Landtag öffentlich bekannt gemacht.
In meiner Stellungnahme habe ich ausgeführt, dass man sich selbstverständlich dem Grundanliegen einer „Qualifizierung“ der Eignungsprüfung nicht verschließt soweit hierzu die vorhandenen gesetzlichen Möglichkeiten ausgeschöpft oder neue geschaffen werden. Nach der derzeitigen Rechtslage sind jedoch die Schulen nicht befugt, Auskünfte zum Verhalten der Schüler ohne deren Einwilligung an die Waffenerlaubnisbehörde zu übermitteln. Ungeachtet dessen müssen bei der

Datenerhebung die Grundsätze der Verhältnismäßigkeit und Gleichbehandlung beachtet werden, da nur ein geringer Teil der jungen Antragsteller bis zum Alter von 25 Jahren noch eine Schule besuchen. Darüber hinaus wurde bisher noch nicht dargelegt, welche konkreten Konsequenzen sich für den Antragsteller aus seiner Nichteinwilligung ergeben. Solange nach den derzeitigen Aussagen die Verwaltungsentscheidung auch ohne Kenntnis der Angaben der Schule über das Verhalten des Antragstellers getroffen und somit die Verwaltungsaufgaben erfüllt werden können, stellt sich die Frage der Erforderlichkeit einer zusätzlichen Datenerhebung.
Da nach § 19 Abs. 3 ThürDSG dem Betroffenen vor der Abgabe seiner Einwilligung auch ein Informationsrecht über mögliche (negative) Konsequenzen bei der Verweigerung seiner Einwilligung zusteht, sind hierzu ebenso wie zu den konkreten Fragestellungen an die Schulen bzw. den Umfang der Datenübermittlungen von den Schulen für alle Beteiligten transparente und einheitlich Festlegungen zu treffen.

Zwischenzeitlich wurde von einer Stadtverwaltung bereits der Entwurf einer Einwilligungserklärung erarbeitet, nach dem die Schulen, die der Antragsteller in den letzten 5 Jahren besucht hat, künftig der Waffenerlaubnisbehörde auf der Grundlage des Schülerbogens Besonderheiten im Verhalten, Ordnungsmaßnahmen und besondere Vorkommnisse mitteilen sollen. Diese sehr allgemeinen Fragestellungen können aber zu einer Vielzahl von Informationen führen (z. B. mangelhafte Ordnung, unentschuldigtes Fehlen u. a.), deren Kenntnis für die Waffenerlaubnisbehörde nicht erforderlich ist, soweit sie keine Verweigerung der Erteilung einer waffenrechtlichen Erlaubnis begründen. Es bedarf deshalb zumindest weiterer Präzisierungen des Auskunftsersuchens (z. B. für Hinweise für ein unbeherrschtes aggressives oder gewalttätiges Verhalten), um unzulässige Datenübermittlungen auszuschließen. Hierzu hat auch das TKM seine Bedenken dahingehend geäußert, dass gemäß § 136 Abs. 3 Thüringer Schulordnung Eintragungen von Ordnungsmaßnahmen spätestens zwei Jahre nach dem Vorfall zu löschen sind und das so genanntes „Erinnerungswissen“ einzelner Lehrer sicher nicht hinreichend sein kann, um eine fehlerfreie Persönlichkeitscharakterisierung ehemaliger Schüler vornehmen zu können. Darüber hinaus erscheint es zweifelhaft, ob die Mitteilung von Tatsachen über volljährige ehemalige Schüler bis zu ihrem 25. Lebensjahr zur Feststellung der Voraussetzung im Zusammenhang mit der Erteilung einer waffenrechtlichen Erlaubnis mit dem

Bildungs- und Erziehungsauftrag der Schule, wie im Thüringer Schulgesetz festgelegt, vereinbar ist.
Wie mir zwischenzeitlich auf Anfrage vom TIM mitgeteilt wurde, wird aus den vorgenannten Gründen eine Regelanfrage bei Schulen nicht weiterverfolgt. Ungeachtet dessen wurde jedoch in diesem Zusammenhang darauf hingewiesen, dass von den Waffenbehörden bei Vorliegen von Gründen, die für eine Annahme der Unzuverlässigkeit sprechen, nach § 5 WaffG Einzelermittlungen in eigener Verantwortung durchzuführen sind.

13.2 Aushang von Geburtsdaten im Lehrerzimmer

In einer Eingabe fragte ein Lehrer an, ob die Schulleitung im Lehrerzimmer den Namen und das Geburtsdatum der dort beschäftigten Lehrer zur allgemeinen Ansicht aushängen darf. Ich teilte mit, dass diese Verfahrensweise, insbesondere ohne Einwilligung der betroffenen Lehrer gemäß § 57 Abs. 4 Nr. 3 Thüringer Schulgesetz nicht zulässig ist. Danach ist eine Übermittlung personenbezogener Daten an Dritte nur zulässig, soweit eine rechtswirksame Einwilligung des Betroffenen vorliegt. Lehrer, die ihre Einwilligung nicht erteilen, dürfen daher auf einer solchen Liste nicht erscheinen. Die Veröffentlichung des Geburtsjahres halte ich in diesem Rahmen darüber hinaus für grundsätzlich unzulässig, da es für die Aufgabenerfüllung der Schule nicht erforderlich ist.

13.3 Inhalt der ärztlichen Bescheinigung zur Aufnahme in einer Kindertagesstätte

Nach § 15 Abs. 1 KitaG ist bei der Aufnahme eines Kindes in einer Kindertageseinrichtung durch den Erziehungsberechtigten eine ärztliche oder amtsärztliche Bescheinigung über die gesundheitliche Eignung des Kindes zum Besuch der Einrichtung vorzulegen. Darüber hinaus ist laut Gesetz dem Erziehungsberechtigten die Vervollständigung der empfohlenen Impfungen anzuraten.
Im Rahmen der Unterstützung der kommunalen Gebietskörperschaften hatte hierzu die Aufsichtsbehörde einen Vordruck zur „Ärztlichen Bescheinigung zur Aufnahme in einer Kindertageseinrichtung“ erarbeitet und den für die Kindertagesstätten zuständigen kommunalen Gebietskörperschaften zur weiteren Verwendung übergeben. Zum Inhalt des Formulars gehörte auch eine Eintragung des Impfstatus bzw. konkrete Angaben über die durchgeführten Impfungen ein-

schließlich der überstandenen impfprävalenten Krankheiten. Dies war für eine Elternvertretung Anlass, sich an den TLfD zu wenden, mit der Bitte um eine datenschutzrechtliche Prüfung. Als problematisch wurde dabei die Eintragungspflicht durch den Arzt bzw. Auskunftspflicht der Eltern über Impfdaten im Rahmen der vom Gesetzgeber geforderten Vorlage einer ärztlichen Bescheinigung über die gesundheitliche Eignung des Kindes zum Besuch einer Kindertageseinrichtung angesehen. Da eine Erforderlichkeit für die Erhebung von Impfdaten zwar nicht grundsätzlich in Abrede gestellt wird, eine gesetzliche Auskunftspflicht hierüber jedoch nicht besteht, entsprach der Vordruck nicht den datenschutzrechtlichen Anforderungen ohne einen Hinweis auf die Freiwilligkeit der Auskunftserteilung durch die Eltern. In Zusammenarbeit mit der zuständigen Aufsichtsbehörde wurde deshalb das Formular überarbeitet. Danach ist nunmehr im oberen Abschnitt des Vordrucks vom Arzt durch Unterschrift zu bestätigen, dass gegen den Besuch der Kindertagesstätte keine Bedenken bestehen. Ergänzend können dann im unteren optisch abgetrennten Teil mit Einverständnis der Sorgeberechtigten noch Eintragungen über die erfolgten Impfungen oder überstandene impfprävalente Krankheiten vorgenommen werden. Damit bleibt es den Sorgeberechtigten überlassen, ob sie diese Angaben machen.

13.4 Datenabgleich zwischen den Ämtern für Ausbildungsförderung und dem Bundesamt für Finanzen

Ein Auszubildender hat nach Maßgabe des Bundesausbildungsförderungsgesetzes (BAföG) einen Anspruch auf individuelle Ausbildungsförderung, wenn ihm anderweitig die erforderlichen Mittel für seinen Lebensunterhalt nicht zur Verfügung stehen. Der Umfang der Ausbildungsförderung richtet sich u. a. auch nach dem Einkommen und dem Vermögen des Auszubildenden. Hierüber hat der Antragsteller in einem speziellen Antragsbogen Auskunft zu erteilen, auf dessen Grundlage die BAföG-Ämter über die Höhe der monatlichen Förderung entscheiden.
Um zu überprüfen, ob Angaben von Auszubildenden, die Leistungen nach dem BAföG erhalten, zu ihrem Vermögen zutreffend sind, erfolgt seit einiger Zeit sowohl in Thüringen als auch in allen anderen Bundesländern ein 100%iger Abgleich durch die Ämter für Ausbildungsförderung beim Bundesamt für Finanzen (BfF) im automatisierten Verfahren hinsichtlich einer Mitteilung über den jeweiligen Frei-

stellungsauftrag als auch die tatsächliche Freistellungssumme der Zinserträge für jeden BAföG-Empfänger. Um mich näher über die konkrete Verfahrensweise zu informieren, erfolgte eine datenschutzrechtliche Kontrolle bei einem BAföG-Amt. Wie sich herausstellte übermitteln die BAföG-Ämter zunächst personenbezogene Daten aller BAföG-Empfänger (Nachname, Vorname, Geburtsdatum, Postleitzahl) zur Identifizierung an das BfF. Von dort erhalten die BAföG-Ämter dann Informationen darüber, wie viele Freistellungsaufträge mit welchem Betrag gestellt wurden und wie hoch die Freistellungssumme tatsächlich war. Ergibt sich aus diesem Abgleich für einzelne BAföG-Empfänger, dass die auf dem Antragsbogen gemachten Angaben zum Vermögen nicht den Tatsachen entsprechen, werden die Betroffenen angeschrieben und zu einer Stellungnahme unter Beifügung entsprechender Nachweise aufgefordert. Das BAföG-Amt stellt auf dieser Grundlage nachträglich den Vermögenswert zum Stichtag der Antragstellung fest und ermittelt damit das anzurechnende Vermögen des Auszubildenden nach §§ 26 ff BAföG. Anschließend ergeht an den Betroffenen ein Bescheid über die geforderte Rückzahlungssumme zu der bereits erhaltenen Ausbildungsförderung. Auf die Durchführung von Ordnungswidrigkeitsverfahren nach § 58 BAföG hat das von mir geprüfte BAföG-Amt bislang verzichtet.
Da mir keine Rechtsgrundlage bekannt ist, die einen regelmäßigen und umfassenden Datenabgleich zwischen den BAföG-Ämtern und dem BfF erlaubt, wandte ich mich in dieser Angelegenheit an das TMWFK als zuständige oberste Aufsichtsbehörde für BAföG-Angelegenheiten. In seiner Anwort teilte mir das Ministerium mit, dass der Abgleich auf § 45 d Abs. 3 Einkommensteuergesetz (EStG) gestützt wird, der dem BfF ausdrücklich zum Zwecke der Überprüfung von Einkommen und Vermögen die Berechtigung einräume, einen automatisierten Datenabgleich vorzunehmen und dessen Ergebnis den Sozialleistungsträgern mitzuteilen. Die genannte Rechtsvorschrift erlaubt es dem BfF die in Abs. 1 genannten Daten an die Sozialleistungsträger zu übermitteln, soweit dies zur Überprüfung des bei der Sozialleistung zu berücksichtigenden Einkommens oder Vermögens erforderlich ist oder der Betroffene zustimmt. Insoweit wird mit dieser gesetzlichen Bestimmung eine Durchbrechung des Steuergeheimnisses normiert. Allerdings bestehen aus meiner Sicht nach wie vor erhebliche Zweifel an der Zulässigkeit des durchgeführten, 100%igen Abgleichs, da bei der vorstehenden Betrachtung völlig außer Acht gelassen wird, dass zunächst die BAföG-Ämter ihrerseits für den Abgleich aller BAföG-Empfänger die genannten Sozialdaten

an das BfF übermitteln müssen, damit das Verfahren überhaupt durchzuführen ist. Die Übermittlung von Sozialdaten ist aber gemäß § 67 d Abs. 1 SGB X nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt. Eine solche Rechtsnorm zur Aufhebung des Sozialgeheimnisses ist aber nicht vorhanden. Eine Ausnahme bildet die Tatsache, wenn einem BAföG-Amt Anhaltspunkte oder Hinweise dafür vorliegen, dass ein BAföG-Empfänger bei seiner Antragstellung, sei es vorsätzlich oder fahrlässig, falsche Angaben gemacht hat. Hier besteht für das BAföG-Amt nach § 67 a Abs. 2 Nr. 2 b (bb) SGB X die Möglichkeit für diesen konkreten Verdachtsfall, den durch den betroffenen BAföG-Empfänger erfolgten Freistellungsauftrag und die Freistellungssumme beim BfF zu erheben. Die von mir vertretene Rechtsauffassung, wonach für die umfassenden Datenübermittlungen der BAföG-Ämter an das BfF keine gesetzliche Erlaubnisnorm vorhanden ist, wird von allen anderen Landesdatenschutzbeauftragten geteilt.
Ich habe das TMWFK über diese Rechtsauffassung informiert und dieses bereits mehrfach zu einer Überprüfung der von den BAföG-Ämtern praktizierten Verfahrensweise aufgefordert. Nach Mitteilung des TMWFK wurde für das Jahr 2002 noch kein Datenabgleich durchgeführt.
Nachdem der BfD sich an die beteiligten Bundesministerien gewandt hatte und diese über die Rechtsposition der DSB des Bundes und der Länder informierte, wurde ihm zwischenzeitlich aus dem BMBF zugesagt, dass für den Datenabgleich eine klarstellende Regelung im BAföG geschaffen werden soll.

13.5 Datenschutzrechtliche Fragen bei der Archivierung und Nutzung von Archivgut mit personenbezogenen Daten

Bei Kontrollen und durch entsprechende Anfragen habe ich in der Vergangenheit des Öfteren festgestellt, dass teilweise noch Unsicherheiten darüber bestehen, ob und wann Unterlagen vor ihrer Vernichtung dem zuständigem Archiv zur Übernahme anzubieten sind. Bis zur Novellierung des Thüringer Datenschutzgesetzes im Jahr 2001 waren alle öffentlichen Stellen gemäß § 16 Abs. 3 ThürDSG verpflichtet, alle bei ihnen vorhandenen Daten, gleichgültig ob sie zulässigerweise erhoben und gespeichert waren oder nicht, vor ihrer Löschung dem zuständigen Archiv zur Übernahme anzubieten. Mit der

Verabschiedung des neuen Thüringer Datenschutzgesetzes am 28. September 2001 gilt gemäß § 16 ThürDSG, dass alle personenbezogenen Daten von den öffentlichen Stellen zu löschen sind, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Vor ihrer Löschung sind aber nur die Daten, die zulässigerweise erhoben waren und deren Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist, dem zuständigen Archiv zur Übernahme anzubieten. Das Nähere wird durch Rechtsvorschriften über öffentliche Archive geregelt. Hierzu heißt es in § 11 Thüringer Archivgesetz (ThürArchivG): „Die in § 3 Abs. 1 und § 4 Abs. 1 genannten öffentlichen Stellen sind verpflichtet, alle Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind und deren Aufbewahrungsfristen abgelaufen sind, auszusondern und dem zuständigen Archiv zur Übernahme anzubieten, sofern bundesrechtlich nicht anders bestimmt ist... Anzubieten sind auch Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder über den Datenschutz unterworfen sind. Unberührt bleiben gesetzliche Vorschriften über die Löschung oder Vernichtung unzulässig erhobener oder verarbeiteter Daten oder Unterlagen.“ Entsprechend dieser Vorschrift sind die Behörden zur Anbietung verpflichtet, sofern keine spezialgesetzlichen Bestimmungen etwas anderes regeln. Hierzu hat der Gesetzgeber in der amtlichen Begründung ausgeführt: „Die Regelungen [Anbietungspflicht] gelten auch für Daten und sonstige personenbezogene Unterlagen, die besonderen Rechtsvorschriften über Geheimhaltung oder über den Datenschutz unterliegen, gesperrt und vernichtet bzw. gelöscht werden könnten oder gar müssten.“ Insoweit ist klargestellt, dass mit Ausnahme unzulässig erhobener Daten zunächst alle bei öffentlichen Stellen vorgehaltenen Unterlagen durch das zuständige Archiv im Benehmen mit der anbietenden Stelle gemäß § 12 ThürArchivG vor ihrer Vernichtung auf eine Archivwürdigkeit zu prüfen sind, um Unterlagen, die aufgrund ihres rechtlichen, politischen, wirtschaftlichen, sozialen und kulturellen Wertes als Quellen für die Erforschung und das Verständnis für Geschichte und Gegenwart dienen oder die zur Rechtswahrung sowie aufgrund von Rechtsvorschriften dauerhaft aufzubewahren sind, zu erhalten. Selbstverständlich können und sollten dabei die öffentlichen Stellen zur Verwaltungsvereinfachung mit dem jeweiligen Archiv soweit möglich auch Vereinbarungen für ein normiertes Bewertungsverfahren nach § 13 ThürArchivG insbesondere auch hinsichtlich gleichförmiger oder wiederkehrender Unterlagen treffen.

Entsprechend den Vorgaben im Thüringer Archivgesetz (§ 15 und § 17 ThürArchivG) darf ein Zugang zu unzulässig erhobenen Daten durch das Archiv nur dann gewährt werden, wenn die Benutzung der Rehabilitation des Betroffenen, der Wiedergutmachung dient oder im Ergebnis einer Einzelschutzfristenverkürzung die Nutzung zur Durchführung eines wissenschaftlichen Forschungsvorhabens erlaubt wird. Ansonsten gilt für die Nutzung personenbezogenen Archivguts eine Schutzfrist bis 10 Jahre nach dem Tod der betreffenden Person oder soweit das Todesjahr nicht feststellbar ist, bis 90 Jahre nach dessen Geburt. Bei besonders schützenswerten Unterlagen kann diese Schutzfrist auf 30 Jahre nach dem Tod bzw. 120 Jahre nach der Geburt verlängert werden. Schutzfristenverkürzungen sind unter den in § 17 Abs. 5 ThürArchivG genannten Voraussetzungen im Einzelfall möglich und müssen für den Bereich des Staatsarchivs von der obersten Archivbehörde genehmigt werden. In anderen Archiven ist dieses Verfahren nicht geregelt, sodass hierzu eine entsprechende Festlegung in der jeweiligen Archivsatzung getroffen werden sollte. Da die Schutzfristen gemäß § 17 Abs. 4 ThürArchivG auch für die Benutzung durch öffentliche Stellen gelten, bedarf es zur Verkürzung der Schutzfristen im Einzelfall nach Abs. 5 ThürArchivG seitens des Antragstellers einer entsprechenden Begründung für das (überwiegende) öffentliche Interesse für eine Schutzfristenverkürzung. Lediglich für die Stelle, bei denen das Archivgut entstanden ist oder die es abgegeben hat, sind die Schutzfristen unbeachtlich, soweit das Archivgut nicht aufgrund besonderer Vorschriften hätte ansonsten gesperrt, gelöscht oder vernichtet werden müssen.

Letztgenannte Problematik ist bspw. insbesondere auch bei der Nutzung archivierter Meldeunterlagen zu beachten. Gemäß § 43 Abs. 2 ThürMeldeG waren die Meldebehörden verpflichtet, in den Melderegistern alle Daten, die über die in § 3 ThürMeldeG genannten hinausgehen, innerhalb eines Jahres nach Inkrafttreten des Meldegesetzes vom 23. März 1994 zu löschen. Soweit jedoch die alten Meldekarteien vor der Löschung vom jeweiligen zuständigen Archiv bereits als Archivgut übernommen worden waren, enthalten sie noch diese Informationen (Daten), die nicht nur nach heutigem Recht nicht erhoben werden dürfen sondern teilweise auch als unzulässig erhoben betrachtet werden müssen. Da es sich in dem Fall aber um Archivgut handelt, gilt für deren Benutzung nicht das Melderecht sondern Archivrecht, d. h. die jeweilige Archivsatzung, die gemäß § 4 Abs. 1 ThürArchivG den Grundsätzen des Thüringer Archivgesetzes entsprechen muss. Danach sind bei der Benutzung von Archivunterlagen auch durch

öffentliche Stellen die Schutzfristen zu beachten. Schutzfristenverkürzungen sind danach nur im Einzelfall auf Antrag und für Verwaltungsaufgaben nur hinsichtlich der zulässigerweise erhobenen Daten möglich. Insoweit ist ein jederzeitiger Zugang auf Daten alter Meldeunterlagen auch für die Meldebehörden nur erlaubt, wenn es sich um Daten handelt, die nach heutigem Recht von den Meldebehörden erhoben bzw. verarbeitet und genutzt werden dürfen. Eine Kenntnisnahme oder Nutzung weiterer Meldedaten ist auch für Meldebehörden nur im Rahmen einer Schutzfristenverkürzung unter Nachweis eines öffentlichen Interesses an der Kenntnis dieser Daten im Einzelfall zulässig.

14. Wirtschaft, Verkehr, Wohnungswesen, Umwelt

14.1 Erstellung von Luftbildaufnahmen zur Gebührenberechnung

Wie den Eingaben von Bürgern zu entnehmen war, fertigen einige Zweckverbände Luftbildaufnahmen von ihrem jeweiligen Verbandsgebiet an. Die dabei gewonnenen Erkenntnisse würden nach Angaben eines Petenten bei der Berechnung von Abwassergebühren genutzt, ohne dass er hierüber zuvor unterrichtet worden sei.
Um einen Überblick darüber zu erhalten, zur Erfüllung welcher Aufgaben Luftbildaufnahmen verarbeitet werden und inwieweit die dabei gewonnenen Erkenntnisse in den Erlass von Beitragsbescheiden eingehen, wurde bei einem Abwasserzweckverband eine Kontrolle durchgeführt.
Wie sich herausstellte, werden die von einer privaten Firma durch Überfliegen des bebauten Verbandsgebietes erstellten Aufnahmen, die aufgrund der groben Auflösung Details von Grundstücken oder Gebäuden nicht erkennen lassen, in ein geographisches Informationssystem zur Darstellung, Bearbeitung und Auswertung von digitalen Landkarten eingebunden. Hierbei kann auf einem Computerbildschirm ein bestimmter Bildausschnitt ausgesucht werden, über den sich dann maßstabgerecht die entsprechende automatisierte Liegenschaftskarte einblenden lässt. Somit lassen sich sofort Abweichungen zwischen der Realität und der Liegenschaftskarte erkennen. Die Luftbildaufnahmen werden ausschließlich zu Planungszwecken verwendet, z. B. beim Verlegen von Leitungstrassen oder zur Feststellung der tatsächlichen Rechtsverhältnisse von Grundstücken. Diese Abwei-

chungen sollen nach Angaben des Zweckverbands aufgrund einer bestehenden Vereinbarung zwischen dem TIM und den Katasterämtern sukzessive zu einer Aktualisierung der Liegenschaftskarten führen.
Da als alleiniger Maßstab des Heranziehungsbescheids die im amtlichen automatisierten Liegenschaftsbuch sowie im Bebauungsplan enthaltenen Angaben genutzt werden, die Luftbildaufnahmen nicht unmittelbar personenbezogene Daten erkennen lassen und die Verarbeitung der Aufnahmen auch nicht personenbezogen erfolgt, stehen aus datenschutzrechtlicher Sicht schutzwürdige Belange der insoweit betroffenen Grundstückseigentümer der Verfahrensweise des Zweckverbandes nicht entgegen. Die Eigentümer von erfassten Grundstücken müssen nicht über diesen Vorgang unterrichtet werden. Nach § 4 Thüringer Verordnung über die Einrichtung und Führung des Landesluftbildarchivs kann jeder, der ein berechtigtes Interesse hat, Auszüge und Auskünfte aus diesem Archiv erhalten, soweit öffentliche Belange oder Rechte Dritter dem nicht entgegenstehen und die Gewähr für eine sachgerechte Verwendung gegeben ist.

14.2 Datenaustausch zwischen einem Zweckverband und Stadtwerken

Ein Zweckverband bat um Beurteilung, ob die Einrichtung eines Datennetzes zwischen dem Zweckverband und den Stadtwerken zur beiderseitigen Nutzung von Kundendaten wie Eigentümer- und Grundstücksangaben datenschutzrechtlich zulässig sei.
Vom Standpunkt des Zweckverbandes, einer öffentlichen Stelle im Sinne des § 2 Abs. 1 ThürDSG, werden mit der Datenvernetzung personenbezogene Daten bei den Stadtwerken und damit ohne eine Mitwirkung der Betroffenen erhoben. Dies ist nach § 19 Abs. 2 Satz 1 ThürDSG (Grundsatz der Direkterhebung) unzulässig, da die Ausnahmetatbestände des § 19 Abs. 1 ThürDSG nicht vorliegen. Der Zweckverband könnte die erforderlichen personenbezogenen Daten direkt bei den Betroffenen oder z. B. den hierfür vorgesehenen Liegenschaftskatastern erheben. Bei den Stadtwerken handelt es sich um eine öffentliche Stelle im Sinne des § 2 Abs. 2 ThürDSG, für die die Zulässigkeit der Datenübermittlung auf Grund ihrer Teilnahme am Wettbewerb nach § 28 BDSG zu beurteilen ist. Da es sich um Kundendaten handelt, die nur im Rahmen der Zweckbestimmungen des Vertragsverhältnisses genutzt werden dürfen, ist eine derartige Datenvernetzung auch aus Sicht der Stadtwerke datenschutzrechtlich unzu-

lässig. Eine Verarbeitung der Kundendaten ist dann nicht zu beanstanden, wenn die Betroffenen gemäß § 4 ThürDSG schriftlich hierin eingewilligt haben.

14.3 Einführung eines Kunden-Beziehungsmanagementsystems (CRM) in einem Verbund von Versorgungsunternehmen

Ein Verbund einzelner Versorgungsunternehmen beabsichtigte die gemeinsame Verarbeitung und Nutzung aller bei seinen Tochterunternehmen anfallenden Kundendaten an einer zentralen Stelle. Eine solche CRM-Lösung biete die Möglichkeit der Kostenreduzierung und einer gezielten Bewerbung der Kunden.
Bei den Tochterunternehmen handelt es sich um öffentliche Stellen im Sinne des § 2 Abs. 2 ThürDSG, für die der Sachverhalt aufgrund ihrer Teilnahme am Wettbewerb nach § 28 BDSG zu beurteilen ist. Da sie als Einzelunternehmen jeweils eigene Verträge mit ihren Kunden abgeschlossen haben, ist eine Zusammenführung aller Kundendaten in einer zentralen Datei und die damit gegebenen Zugriffsmöglichkeiten durch die beteiligten Unternehmen aus datenschutzrechtlicher Sicht ohne schriftliche Einwilligung der Betroffenen gemäß § 4 a Abs. 1 BDSG als unzulässig anzusehen. Eine Datenübermittlung für Zwecke der Werbung sowie der Markt- und Meinungsforschung ist lediglich für die in § 28 Abs. 3 Nr. 3 BDSG aufgeführten Daten möglich, wobei der Betroffene dem widersprechen kann und über sein Widerspruchsrecht spätestens „bei der Ansprache zum Zweck der Werbung“ zu unterrichten ist.

14.4 Kataster zu Standorten von Mobilfunksendeanlagen

Unter dem Eindruck zunehmender Verunsicherung hinsichtlich der gesundheitlichen Auswirkungen des Mobilfunks und dem damit auftretenden öffentlichem Informationsbedürfnis wurde auch die Frage an den TLfD herangetragen, ob und inwieweit von den Kommunen Übersichten zu Standorten von Mobilfunksendeanlagen geführt und diesbezügliche Auskünfte an Dritte, insbesondere besorgten Bürgern, erteilt werden dürfen.
Hierzu ist zunächst festzustellen, dass bei der Führung eines flächendeckenden Mobilfunkstandortkatasters die entsprechenden Grundstücke einzelnen natürlichen Personen (Grundstückseigentümern) zuge-

ordnet werden können und damit im Sinne des ThürDSG personenbezogene Daten verarbeitet und genutzt werden.
Gemäß § 4 Abs. 1 ThürDSG ist eine Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn dies eine Rechtsvorschrift erlaubt oder anordnet oder soweit der Betroffene darin eingewilligt hat. Rechtsgrundlage für die Datenverarbeitung von Mobilfunkstandortdaten ist auf kommunaler Ebene die 26. Bundesimmissionsschutzverordnung (BImSchVO). Danach besteht für alle Betreiber von Hochfrequenzanlagen sowie bestimmten Niederfrequenzanlagen eine Anzeigepflicht gemäß § 7 der 26. BImSchVO gegenüber den dafür zuständigen Behörden, zu denen in Thüringen die Umweltämter der Landkreise und kreisfreien Städte bestimmt wurden. Da die Angaben über Standorte von Mobilfunkantennen im Sinne des Umweltinformationsgesetzes (UIG) umweltrelevante Daten sind, hat nach § 4 Abs. 1 UIG grundsätzlich jedermann bei der für den Umweltschutz zuständigen Behörde einen Anspruch auf freien Zugang zu diesen Informationen. Ein Ausschluss oder eine Beschränkung dieses Anspruchs besteht insbesondere zum Schutz privater Belange und zwar dann, wenn bei der Auskunftserteilung personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden (§ 8 Abs. 1 Nr. 1 UIG). Zur Prüfung möglicher schutzwürdiger Interessen sind die Betroffenen gemäß § 8 Abs. 2 UIG vor der Entscheidung über die Offenbarung zu hören.
Eine Erforderlichkeit zur dauernden Vorhaltung und Aktualisierung der vorgenannten Daten und eine Rechtsgrundlage zur Führung eines Katasters über Mobilfunkantennen gibt es derzeit für kreisangehörige Städte und Gemeinden nicht. Insoweit können dort lediglich Einzelinformationen über Mobilfunkstandorte, die im Rahmen von Verwaltungsverfahren (z. B. bei Baugenehmigungsverfahren) erhoben werden oder Übersichten bei konkreten Planaufgaben vorliegen. Da die Daten aber bei Stellen anfallen, die keine Aufgaben des Umweltschutzes wahrnehmen, sind hier die Vorschriften des UIG bei möglichen Auskunftsersuchen durch Dritte nicht einschlägig. In diesem Fall gelten, soweit spezialgesetzlich geregelt, die jeweiligen Übermittlungsvorschriften (z. B. § 69 ThürBO oder §§ 29, 30 ThürVwVfG), ansonsten die allgemeinen Normen des ThürDSG. Danach kommen i. d. R. bei Auskunftsersuchen von Dritten für Daten, die von den Gemeinden und kreisangehörigen Städten für kommunale Aufgaben (z. B. konkrete Planungsvorhaben) von der Regulierungsbehörde oder dem jeweiligen Umweltamt zuvor abgerufen bzw. angefordert wurden, die Bestimmungen der §§ 21 bis 23 ThürDSG zur Anwendung.

Ein Auskunftsanspruch durch Dritte besteht hierbei nicht. Gemäß § 22 Abs. 1 Nr. 2 ThürDSG dürfen Daten an nicht öffentliche Stellen innerhalb des Geltungsbereichs der EG nur dann übermittelt werden, wenn diese ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft dargelegt haben und der Betroffene keine schutzwürdigen Interessen an dem Ausschluss der Übermittlung hat. Aufgrund dieser Vorschrift bestehen keine datenschutzrechtlichen Bedenken gegen eine Übermittlung konkreter Standortdaten, wenn diese ohnehin öffentlich zugänglich, d. h. wenn z. B. die Sendemasten deutlich sichtbar sind. Eine Namensnennung der Grundstückseigentümer sollte aber dabei in jedem Fall unterbleiben. Wurde demgegenüber eine Sendeanlage verdeckt angebracht, ist neben dem berechtigten Interesse für die Auskunft insbesondere das schutzwürdige Interesse des Betroffenen am Ausschluss einer Übermittlung zu prüfen.
Eine Veröffentlichung von personenbezogenen Daten im Internet ist mangels einer gesetzlichen Ermächtigung nur dann zulässig, wenn gemäß § 23 Abs. 2 Nr. 1 ThürDSG zweifelsfrei hierfür die Einwilligung der Betroffenen vorliegt.
Nur dann wenn die Auskünfte hinreichend anonymisiert sind, indem z. B. die Standortdaten nicht personen- bzw. grundstücksbbezogen sondern straßen- und wohnquartiersweise aggregiert zur Verfügung gestellt werden, bestehen aus datenschutzrechtlicher Sicht dagegen keine Bedenken (siehe auch Entschließung zur 64. Konferenz der DSB des Bundes und der Länder, Anlage 7).

14.5 Übermittlung von Fahrzeug- und Halterdaten nach Straßenverkehrsgesetz (StVG)

Gegenstand einer Beschwerde war die Übermittlung von Fahrzeug- und Halterdaten. Dem lag folgender Sachverhalt zu Grunde: Nach einem Verkehrsunfall war es zwischen den Fahrzeugführern lediglich zu einem Austausch der Kfz-Kennzeichen gekommen. Während dem Unfallgegner bereits am nächsten Tag die Fahrzeug- und Halterdaten des Beschwerdeführers bekannt waren, sei diesem von der Kfz-Zulassungsstelle eine telefonische Auskunft über den Unfallgegner verweigert worden.
Eine Überprüfung der Dokumentation in der Zulassungsstelle ergab, dass zur fraglichen Zeit keine Auskünfte zu den Fahrzeugakten des Beschwerdeführers erteilt wurden, wobei jedoch auch die Möglichkeit der Auskunftserteilung durch Polizeidienststellen gegeben ist. Aus datenschutzrechtlicher Sicht war die Verfahrensweise der Zulassungs-

stelle, bei telefonischen Anfragen keine Fahrzeug- und Halterdaten zu übermitteln, auf Grund der eingeschränkten Möglichkeiten zur Identitätsfeststellung des Anrufenden nicht zu beanstanden. Die Behörde hat Halteranfragen gem. § 39 Abs. 1 StVG dahingehend zu überprüfen, ob die gesetzlichen Voraussetzungen einer Auskunft gegeben sind. Hierzu gehört die zweifelsfreie Identifizierung des Anfragenden sowie die Darlegung dass „er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt (einfache Registerauskunft).“

14.6 Erhebung von Mieterdaten durch Vermieter

Im Vorfeld des Abschlusses von Mietverträgen werden den potentiellen Mietern insbesondere von großen Wohnungsunternehmen zunehmend sog. Selbstauskunftsbögen übergeben. Dabei werden auf freiwilliger Basis mitunter auch Daten erhoben, deren Erforderlichkeit und Zweck für die Betroffenen nicht nachvollziehbar sind. So wurde der TLfD von einem Interessenten für eine Mietwohnung zum Umfang und Inhalt einer Selbstauskunft eines Wohnungsunternehmens, in der u. a. Auskünfte zum Geburtsdatum, zum Familienstand, über eine mögliche Schwangerschaft oder zum Vorliegen einer Schwerbehinderung um eine Stellungnahme gebeten. Da die dabei geäußerten Zweifel an der Erforderlichkeit für die Erhebung auch von mir geteilt wurden, habe ich zunächst das Wohnungsunternehmen um eine entsprechende Begründung gebeten. In der Stellungnahme des Wohnungseigentümers wurde ausgeführt, dass z. B. das Geburtsdatum notwendig sei, um auf Besonderheiten bei Personen im höheren Lebensalter eingehen zu können, eine Kenntnis des Familienstandes notwendig sei, um das Interesse an der Anmietung einer Wohnung bei getrennt lebender Personen vertraulich zu behandeln oder bei belegungsgebundenem Wohnraum die Besonderheiten gegenüber dem Wohnungsamt beachten zu können. Desweiteren wurde ausgeführt, dass man aus sozialen Gründen schwangere Frauen bevorzugt versorgen wolle und die Schwerbehinderung dahingehend von Interesse sei, um behinderten- oder rollstuhlgerechte Wohnungen bzw. leer stehende Erdgeschosswohnungen vorrangig anbieten zu können. Diese Argumente waren jedoch nicht überzeugend, da sowohl Form und Inhalt des Fragebogens den Eindruck vermittelten, dass die Kenntnis aller Angaben für eine Vertragsanbahnung zwingend notwendig seien und somit für

das Wohnungsunternehmen die Voraussetzung für eine - von ihr bezeichnete - „Antragsbearbeitung“ wären.
Für den Interessenten muss erkennbar sein, welche Daten für die Anbahnung eines möglichen Vertragsverhältnisses vom Wohnungsunternehmen als unabdingbar angesehen werden, wie gegenwärtige Erreichbarkeit, Anzahl der mitziehenden Personen und Angaben zur gesuchten Wohnung, wie Wohngebiet, Wohnlage, Ausstattung einschl. Sonderwünsche (z. B. behindertengerecht) und maximale Miethöhe. Die so genannte Selbstauskunft zur Prüfung der Bonität der Mieter über Einkommensverhältnisse, Bürgschaften, Bankverbindungen u. a. ist ohne ein konkretes Wohnungsangebot aus datenschutzrechtlicher Sicht als eine unzulässige Datenvorratshaltung zu bewerten. Im Ergebnis meiner Intervention wurde deshalb der Fragebogen für Mietinteressen vom Wohnungsunternehmen nochmals vollständig überarbeitet. Unter ausdrücklichem Hinweis auf die Freiwilligkeit der Angaben werden künftig nur noch Daten erhoben werden, die für eine gezielte Auswahl von Wohnungsangeboten durch das Wohnungsunternehmen notwendig sind.

In einem anderen Fall hatten alle Mieter eines kommunalen Wohnungsunternehmens einen Ausdruck über ihre im automatisiert geführten Mieterverzeichnis des Unternehmens gespeicherten Daten mit der Bitte um Prüfung und Aktualisierung erhalten. Hierbei stellten die Mieter fest, dass im Mieterverzeichnis neben den Daten zur gemieteten Wohnung auch Angaben zum Geburtsdatum, zur Staatsangehörigkeit und Nationalität, zum Berufsstand und zum Haushaltseinkommen der Mieter erhoben werden sollten. Hinweise darüber, ob und inwieweit eine Auskunftspflicht der Mieter aufgrund des Mietvertrages besteht bzw., dass es sich lediglich um eine freiwillige Auskunft handelt und für welche Zwecke die Daten verwandt werden sollten, enthielt das Anschreiben an die Mieter nicht. In seiner Stellungnahme erklärte das Wohnungsunternehmen zunächst, dass die Erhebung personenbezogener Daten der Vertragspartner (Mieter und ggf. Angehöriger) Grundlage eines jeden Mietvertrages sei. Desweiteren würde nach ihrer Auffassung der Zweck der Anfrage - die Überprüfung und Aktualisierung der Daten - eindeutig aus dem Anschreiben hervorgehen und somit den Mietern die Möglichkeit bieten, unrichtige Angaben berichtigen zu lassen. Gründe dafür, für welche Aufgabe die Kenntnis obiger Daten der Mieter notwendig sind, wurden aber nicht dargelegt. Stattdessen wurde nur versichert, dass eine Auswertung, ob

einzelne Mieter geantwortet hätten, zu keinem Zeitpunkt stattgefunden habe.
Hierzu wurde meinerseits Folgendes festgestellt. Adressaten des Rundschreibens waren nur Personen, mit denen bereits Mietverträge bestehen, so dass sich z. B. Fragen zu den Einkommensverhältnissen bzw. zur Prüfung der Bonität erübrigen. Die Rechte und Pflichten der Mieter auch hinsichtlich der Erteilung von Auskünften ergeben sich ausschließlich aus dem Mietvertrag. Der Mieter hat den Vermieter lediglich über Sachverhalte zu informieren, die sich im Zusammenhang mit der vertragsgerechten Nutzung der Wohnung (wie z. B. zur Veränderung der Zahl der Bewohner) oder aufgrund von Verfahrensänderungen zur Zahlung des Mietzins (Kontodaten für Einzugsermächtigungen) ergeben. Eine Erforderlichkeit für die Erhebung und Kenntnis aktueller Mieter- und Bewohnerdaten über deren Staatsangehörigkeit, Nationalität, Geburtsdatum, Berufsstand, Nettoeinkommen wie auch über Telefon- und E-Mail-Anschlüsse durch den Vermieter sind in keiner Weise begründet und insoweit nicht nachvollziehbar. In diesem Zusammenhang ist darüber hinaus zu berücksichtigen, dass es sich bei den erhobenen Angaben teilweise auch um „besondere Arten personenbezogener Daten“ gemäß § 3 Abs. 9 BDSG gehandelt hat, die als äußerst schützenswert gelten und deshalb den besonderen restriktiven Regelungen des § 28 Abs. 6 BDSG unterfallen. Den Forderungen des Gesetzgebers folgend, sind bei der Prüfung der Erforderlichkeit für die Verarbeitung dieser Daten besonders strenge Maßstäbe anzulegen. Dass hierzu bereits Zweifel beim Wohnungsunternehmen bestanden, wurde auch dadurch deutlich, dass eine Auswertung, ob die entsprechenden Rückantworten vollständig eingegangen sind, zu keinem Zeitpunkt stattfand. Aus der Berechtigung bei hinreichender Konkretisierung der Vertragsanbahnung vor Abschluss des Mietvertrages vom Bewerber einer Wohnung bestimmte Daten insbesondere zur Prüfung der Bonität erheben zu können, lässt sich nicht generell und zwingend ein Recht oder eine Auskunftspflicht zur weiteren Aktualisierung dieser Daten ableiten. Wesentlicher Maßstab für die Speicherung und Aktualisierung dieser Daten ist stets die Frage der Erforderlichkeit für die weitere Aufgabenerfüllung. So ist z. B. die Tatsache eines vollzogenen Arbeitsplatzwechsels oder Veränderungen der Einkommenssituation für ein Mietverhältnis unerheblich solange der Mieter seinen vertraglichen Pflichten nachkommt. Im Hinblick auf die Argumentation, dass das Wohnungsunternehmen die Daten auf freiwilliger Grundlage erhoben habe, wurde darauf hingewiesen, dass eine Einwilligung zur Verarbeitung und Nutzung personenbezogener

Daten gemäß § 4 a BDSG nur dann rechtswirksam ist, wenn sie auf der freien Willensentscheidung der Betroffenen beruht. Voraussetzung dafür ist, dass der Einwilligende die Bedeutung und Tragweite seiner Entscheidung zu überblicken vermag. Hierzu hat der Gesetzgeber entsprechende Regelungen in § 4 a BDSG aufgenommen (Hinweispflichten), die im konkreten Fall nicht beachtet worden waren.
Aus den vorgenannten Gründen wurde die vom Wohnungsunternehmen durchgeführte unzulässige Datenerhebung und -verarbeitung gemäß § 39 Abs. 1 ThürDSG beanstandet und die Stelle aufgefordert, die rechtswidrig erhobenen Daten zu löschen und die Betroffenen zumindest in allgemeiner Form darüber zu informieren. Diesen Forderungen wurde seitens des Wohnungsunternehmens unverzüglich entsprochen.

14.7 Die Erreichbarkeit von Mitgliedern des Katastrophenschutzes zur Bekämpfung von Tierseuchen

Ein Recht auf Schutz ihrer privaten Daten haben selbstverständlich auch Mitglieder des Katastrophenschutzes. Ich wurde daher von einem Landkreis gebeten, zu prüfen, inwieweit eine Datenerhebung des TMSFG, über die Erreichbarkeit von Mitgliedern des Katastrophenschutzes zur Bekämpfung von Tierseuchen, rechtmäßig ist. Dabei sollte nicht nur die aus der Sicht der Fragesteller unproblematische dienstliche, sondern auch die private Erreichbarkeit, also die Privatanschrift und die private Telefonnummer der Mitglieder an das TMSFG übermittelt werden. In Ermangelung einer spezialgesetzlichen Rechtsgrundlage war deshalb zu klären, ob nach der Regelung des § 19 Abs. 1 ThürDSG die Erhebung der Erreichbarkeitsdaten der Mitglieder der kreislichen Tierseuchenkrisenstäbe, des Landratsamtes bzw. Oberbürgermeisteramtes sowie der Bürgermeister der Gemeinden zulässig, d. h. zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich war. Im Ergebnis wurde festgestellt, dass das in Krisenfällen zuständige TMSFG in der Lage sein muss, die möglichen Ressourcen betroffener Landkreise der Seuchenbekämpfung zu erkennen, einzuschätzen und ggf. einzusetzen. Hierzu gehören der Einsatz der kreislichen Tierseuchenkrisenstäbe ebenso wie die Gemeinden, denen nach § 3 Thüringer Tierseuchengesetz (ThürTierSG) auf Anforderung der zuständigen Behörde verschiedene ordnungsbehördliche Aufgaben obliegen, wie auch die Erreichbarkeit der Landratsverwaltung. Da eine Tierseuche gewöhnlich nicht nur während der Dienstzeit einer Behör-

de oder sonstigen Einrichtung ausbricht, ist es erforderlich, die Ansprechbarkeit der Mitglieder der Tierseuchenkrisenzentren, der Gemeinden und auch Kreisverwaltungen insbesondere auch außerhalb der Dienstzeiten sicherzustellen, um ohne Zeitverlust die erforderlichen Maßnahmen koordinieren zu können. Voraussetzung dafür ist allerdings, dass der betroffene Personenkreis aufgrund seiner Aufgabenstellung dienst- bzw. arbeitsrechtlich dazu verpflichtet ist, in Notfällen auch außerhalb der gewöhnlichen Dienst- und Arbeitszeiten erreichbar zu sein. Die Datenerhebung zur Erreichbarkeit der betroffenen Personen begegnete aus datenschutzrechtlicher Sicht im Ergebnis keinen Bedenken.

15. Technischer und organisatorischer Datenschutz

15.1 Entwicklung der IuK

15.1.1 Grundsätzliche Tendenzen

Nach Angaben des Onliner Atlas 2003[1] verfügt nunmehr die Hälfte der Deutschen über einen Internetzugang. Die Zahl der Internetnutzer stieg damit auf über 32 Millionen Bundesbürger im Alter über 14 Jahre. Allein in der Altersgruppe zwischen 50 und 69 Jahren sind seit 2002 1,8 Millionen neue Internetnutzer zu verzeichnen. Auch das noch deutlich ausgeprägte Gefälle der Internetnutzung zwischen West und Ost verschwindet zusehends. So nutzen 47 % der Bevölkerung der neuen Länder das Internet. Hiermit verbunden ist eine verstärkte Erwartungshaltung seitens der Bürger, auch das Internet für die elektronische Kommunikation mit den Behörden zu nutzen, um bspw. Zeit raubende Behördenbesuche vor Ort einzusparen. Das Internet wird somit für die öffentliche Verwaltung im Rahmen von eGovernment zwangsläufig an Bedeutung zunehmen. Für den Freistaat Thüringen wurde bereits im Jahre 2001 ein vom TIM vorgelegtes Konzept zum eGovernment bestätigt. Insbesondere der Aufbau eines gemeinsamen Internet-Portals für die Landes- und die Kommunalverwaltung als auch die elektronische Vorgangsverwaltung wird als ein Schwerpunkt bei der Konzeptumsetzung angesehen. In dem zugehörigen Technologiekonzept sind auch sicherheitstechnische Aspekte enthalten. Empfehlungen des TLfD insbesondere zum Einsatz von möglicherweise schadensstiftenden Softwareelementen wie ActiveX-Controls,

[1] www.nonliner-atlas.de; www.tns-emnid.com

VBScripts und Java Applets aber auch zu den aus datenschutzrechtlicher Sicht bedenklichen Cookies wurden hier berücksichtigt. In der Präambel zur Argumentation der eGovernment-Suite des Landes Thüringen wird als wesentliches Merkmal und Kriterium für die Umsetzung von eGovernment in Thüringen eine flexible IT-Plattform gefordert, die insbesondere den Forderungen nach Datensicherheit und Verfügbarkeit gerecht wird. Die Umsetzung dieser Forderungen wird von mir datenschutzrechtlich begleitet (15.4).

Bei den eingesetzten IT-Geräten ist weltweit insgesamt eine Zunahme an mobiler Rechnertechnik, wie der Einsatz von Laptop und PDA, gegenüber herkömmlichen Desktop-PC zu verzeichnen. Mittlerweile beträgt der Anteil an mobilen PCs am Gesamt-PC-Markt über 33 %, wobei die Tendenz steigend ist.[2] Der Umsatz mit mobilen Datendiensten wird allein in Westeuropa im Jahr 2003 16,5 Milliarden US-Dollar erreichen, was ein Wachstum von über 30 % im Vergleich zum Vorjahr bedeutet.[3] In Folge der technischen Entwicklung verschmelzen Mobiltelefon und PDA miteinander und bieten somit neue Anwendungsmöglichkeiten. Mit den so genannten „Tablet-PCs“ wird zeitnah eine neue Generation von mobilen Geräten auf den Markt kommen, die eine uneingeschränkte Mobilität mit den technischen Möglichkeiten eines PCs verbinden. Hiermit dürften sich wiederum neue Anwendungen im mobilen Bereich ergeben, die weit über die bisherigen klassischen Lösungen hinaus gehen. Das Spektrum der hierfür eingesetzten Technologien, reicht vom Festnetz-Internet-Anschluss über drahtlose LAN-Anbindung bis zum Mobilfunk. Insbesondere drahtlose Kommunikationsmethoden für Sprache und Daten verbreiten sich zunehmend und verdrängen verkabelte Systeme. Neue Dienste wie bspw. Voice over IP (Internet-Telefonie) stehen vor dem breiten Einsatz. Bereits Realität sind WLANs (drahtlose lokale Netzwerke, 15.16) zum schnellen und breitbandigen Datenaustausch. So genannte Bluetooth-Verbindungen werden zur Vernetzung von Geräten des persönlichen Nahbereichs eingesetzt. Auch in anderen Einsatzgebieten wird zunehmend Datenaustausch per Funk durchgeführt. Dazu gehören kontaktlose Chipkartensysteme, die bspw. im öffentlichen Personennahverkehr eingesetzt werden, um dort schnell, sicher und bargeldlos zu bezahlen oder den sicheren Zugang zum Arbeitsplatz zu ermöglichen. Auch öffentliche Stellen versuchen mit mobilen Anwendungen Abläufe und Prozesse zu vereinfachen und zu beschleunigen sowie

[2] c’t 2003, Heft 13, Seite 20
[3] www.gartner.com (Funkschau 18/2003, Seite 6)

neue Dienstleistungen anzubieten. So sind z. B. in der Landesverwaltung besonders für die Nutzung mobiler IT-Geräte externe Zugriffe über das CN auf das interne Behördennetz eingerichtet worden (15.7). Diese Techniken bergen naturgemäß aber auch neue Gefahren im Hinblick auf die Absicherung der Zugangskontrolle und die Sicherheit der zu verarbeitenden Daten, insbesondere bei der Datenübertragung. Mit dem Einsatz von aktuellen Sicherheitsprotokollen kann und wird diesen Gefahren begegnet. Die Remote-Zugänge sollen auch für Telearbeit genutzt werden. Eine Umfrage des TLfD zum Stand der Telearbeit in der Landesverwaltung ergab, dass schon einige Behörden diese Arbeitsform in geringem Umfang nutzen. Weitere Stellen beabsichtigen Telearbeit einzuführen (15.6). Über die datenschutzrechtlichen und sicherheitstechnischen Aspekte, die bei der Einrichtung von Telearbeitsplätzen zu beachten sind, habe ich schon im 3. TB (15.13) berichtet. Anhand dieser Orientierungshilfe sollte von allen Behörden die Einführung und der Betrieb von Telearbeit aus datenschutzrechtlicher Sicht vollzogen werden.

Die neue Lizenzpolitik von Microsoft hat in der öffentlichen Verwaltung zur Suche nach Alternativen, so die Hinwendung zu Open-Source-Produkten geführt (4. TB, 15.15). Das Bundesministerium des Inneren hat deshalb ein Kooperationsabkommen zur Förderung von frei zugänglicher Software in der Verwaltung abgeschlossen. Mehr als 500 Behörden aus Bund, Ländern und Gemeinden sind bzw. beabsichtigen diesen Rahmenvertrag beizutreten[4]. Das Betriebssystem Linux ist das bekannteste Beispiel für so genannte Open Source-Software. Open Source (Offene Quelle) bedeutet, dass der Kern des Programms frei und kostenlos verfügbar ist. Im IMA-IT wurde im Hinblick auf einen Einsatz solcher Software in der Landesverwaltung dazu festgestellt, dass im Betriebssystembereich ein Einsatz solcher Produkte am ehesten realisierbar ist. Im Kommunikations- und Office-Bereich, so wurde eingeschätzt, ist ein Wechsel auf andere Produkte nur langfristig möglich. So bedarf es z. B. im E-Mail-Bereich noch der Verfügbarkeit von Schnittstellen zwischen den unterschiedlichsten Office-Produkten. Weiterhin ist zu beachten, dass mit einer Umorientierung auch ein nicht unerheblicher Qualifizierungbedarf für die Systemadministratoren und die Nutzer verbunden ist. Ein eventueller Ablöseprozess wird somit als ein längerfristiges Verfahren eingeschätzt. Zunächst hat Vorrang die Betriebsfestigkeit und ständige Verfügbar-

[4] dpa-Nachricht Montag, 23. Juni 2003, dpa-Basisdienst

keit der umfänglichen Internet-, Intranet- und Mail-Verbünde. Zur Zeit wird in der Landesverwaltung vorwiegend noch das Betriebssystem Windows-NT eingesetzt. Mit dem im März 2003 gefassten Beschluss des IMA-IT zur Einführung eines landesweiten Verzeichnisdienstes auf der Basis von Windows 2000/2003 ist die Ablösung von Windows-NT vorgezeichnet. Aus datenschutzrechtlicher Sicht ist der Einsatz von Windows 2000/2003 überwiegend positiv einzuschätzen. Denn diese Betriebssysteme verfügen über weitaus mehr Sicherheitsfunktionen als die Vorgängerversion.
Der Einsatz eines landesweiten Verzeichnisdienstes birgt aber auch datenschutzrechtliche und sicherheitstechnische Risiken (15.3).
Der Trend zur Ablösung der bisher papierenen Schriftgutverwaltung durch eine elektronische Verwaltung der Dokumente (Dokumenten Management System DMS) hat sich verstärkt. Mit einem DMS wird eine Erhöhung der Leistungsfähigkeit der Verwaltung einhergehend mit einer Kostenreduzierung angestrebt. Desweiteren sind solche Systeme aber auch eine Voraussetzung für eGovernment. Der IMA-IT hat sich deshalb die Aufgabe gestellt, ein zukunftsorientiertes einheitliches Vorgangsverwaltungssystem zu empfehlen. Dazu wurden entsprechende Evaluierungen durchgeführt. Im Ergebnis dieser wurde ein einheitliches Produkt als Basis für eine elektronische Vorgangsbearbeitung der Thüringer eGovernment Suite festgelegt. Derzeit erfolgt ein stufenweiser Einsatz im TIM. Das DMS stellt neben der elektronischen Vorgangs- und Dokumentenverwaltung weitere Werkzeuge zur Registratur, zum Umgang mit Aktenplänen und elektronischen Akten, zur Volltextrecherche, zur Verwaltung von Adressen und Postbüchern zur Verfügung. Mit einem solchen System werden i. d. R. auch personenbezogene Daten verarbeitet. Es kann sich hierbei um inhaltliche Daten des jeweiligen Sachvorgangs selbst, z. B. Angaben über Bürger, als auch um Daten der betreffenden Sachbearbeiter, die aus systemverwaltungstechnischen Gründen vorgehalten werden müssen, handeln. Ohne hinreichende organisatorische und technische Maßnahmen besteht beim Einsatz solcher Systeme die Gefahr, dass die hier vorgehaltenen Daten auch missbräuchlich entgegen den datenschutzrechtlichen Grundsätzen der Zweckbindung und Erforderlichkeit genutzt werden können. Insbesondere kann hiermit auch das Verhalten und die Leistung der Beschäftigten überwacht werden, ein Tatbestand der nach § 74 Abs. 2 Nr. 11 ThürPersVG der vollen Mitbestimmung des Personalrats unterliegt. Unerlässlich sind somit aus datenschutzrechtlicher Sicht gemäß § 9 Abs. 2 ThürDSG auf der Grundlage eines Sicherheitskonzeptes die technischen und organisatorischen Maßnah-

men festzulegen, um die Vertraulichkeit, Authentizität, Integrität und die Verfügbarkeit der Daten, die Revisionsfähigkeit ihrer Verarbeitung sowie die Transparenz des Verfahrens zu gewährleisten. In die sicherheitstechnische Betrachtung ist dazu die gesamte Arbeitskette einzubeziehen, angefangen mit einer eventuellen Erfassung der Dokumente (Scannen) über eine erforderliche Wiedergabe bis zu ihrer physischen Löschung gemäß den jeweiligen Vorschriften.

15.1.2 Aktuelle Sicherheitsaspekte

Viren und Würmer (2. TB, 15.11; 4. TB, 15.5) stellen mit ihrer rasanten Wachstums- und enormen Verbreitungsrate gegenwärtig den größten Risikofaktor für die Sicherheit der IuK dar. Aufgrund der Vernetzung und damit auch dezentralen Verteilung von Computersystemen ergibt sich eine immense Angriffsfläche für Virenattacken. In einer aktuellen Studie zur IT-Sicherheit im Unternehmen[5] bezeichnen rund die Hälfte der Unternehmen Viren und Würmer als hohe oder sehr hohe Gefahr.

Gewöhnlich sind Virenscanner auf den Servern und Desktop-PCs der Landesverwaltung installiert. Potenzielle Schadensbringer sind aber auch Laptops und PDAs. Immer mehr Mitarbeiter benutzen zusätzlich diese mobile Rechentechnik. Große Aufmerksamkeit ist deshalb seitens der IT-Verantwortlichen im Land im Hinblick auf die Sicherheit des internen Netzes zu legen. Beim Anschluss dieser mobilen Geräte an das interne Netz dürfen die eingesetzten Virenabwehrmaßnahmen sowie installierte Firewalls nicht umgangen werden. Um die angestrebte Sicherheit auch zu erreichen, müssen Virenscanner und die Sicherheitssoftware der Firewalls laufend aktualisiert werden. Jedoch alle Angriffe können hiermit nicht abgewehrt werden. So werden bspw. neue Angriffsmuster oder Attacken von einer Firewall i. d. R. nicht oder zu spät erkannt. Hier kann der Einsatz eines Intrusion-Detection-Systeme (IDS) Abhilfe schaffen. Diese Sicherheitssoftware analysiert den gesamten Datenverkehr und informiert bei Gefahr den Administrator. IDS stellen somit neben Firewalls und spezieller Erkenntnissoftware zur Überprüfung des Datenstroms auf bösartige Codes eine weitere Säule für eine durchgängige Sicherheit dar. Unter Beachtung des Grundsatzes der Erforderlichkeit ist auch der Einsatz von IDS in den Netzwerken des Landes zu prüfen mit dem Ziel, die

[5] www.ernst-young.de (Funkschau 18/2003, Seite 7)

Sicherheit der IT-Systeme und der hier vorgehaltenen Daten zu gewährleisten.
Auch die Hard- und Softwarehersteller selbst können noch mehr zur IT-Sicherheit beitragen, in dem sie in höherem Maße moderne Sicherheitsfunktionen in ihre Produkte etablieren und die Benutzer hierüber umfassend informieren. Letztere benötigen aber auch unabhängige Aussagen darüber, inwieweit diese Produkte die vorgegebenen Sicherheitsfunktionen erfüllen. Die DSB des Bundes und der Länder forderten deshalb die Hersteller von IuK auf, Software so zu entwickeln und herzustellen, dass Benutzer und unabhängige Dritte sich jederzeit von der Wirksamkeit der Sicherheitsvorkehrungen überzeugen können (4. TB, 15.15). Die zunehmende Evaluierung und Zertifizierung von IuK-Produkten durch unabhängige Instanzen stellt ebenso wie die Definition von Sicherheitsanforderungen (Schutzprofile) seitens der Anwender vor der Produktentwicklung einen richtungsweisenden Beitrag für eine vertrauenswürdige IT dar (15.11).

Ein wichtiges Ziel der Datensicherheit ist unverändert weiterhin eine unversehrte Datenübertragung insbesondere über öffentliche Netze zu ermöglichen. Innerhalb des CN wird ein sicherer Datentransfer zunehmend durch den Aufbau von Virtual Private Networks (VPNs) realisiert. Wobei auf entsprechende Anforderungen in Form einer Punkt-zu-Punkt-Verbindung zwischen zwei Rechnern eine geschützte virtuelle Verbindung aufgebaut wird. Mit dem hierzu eingesetzten Sicherheitsprotokoll (IPSec) wird die Vertraulichkeit, und die Integrität der Daten sowie die Authentizität dieser als auch der Kommunikationspartner abgesichert. Auch die Integration mobiler Nutzer (z. B. Laptop- oder PDA-Anwender) sowie künftig auch Handynutzer können hier einbezogen werden. In den Behördennetzen selbst steht der Einsatz von VPNs noch am Anfang.
Im 4. TB (15.8) berichtete ich ausführlich über den in der Landesverwaltung mit ausgewählten Ressorts durchgeführten Testbetrieb zu einem durchgängigen Einsatz (Ende-zu-Ende-Sicherheit) von Verschlüsselung und elektronischer Signatur. Obwohl der Testbetrieb 2001 erfolgreich abgeschlossen wurde, gibt es innerhalb der Landesverwaltung immer noch keinen nennenswerten Einsatz dieser Schlüsseltechnologien für einen sicheren E-Mail-Verkehr. Auch eine wesentliche Voraussetzung für ein sicheres eGovernment fehlt damit. Insofern wird nicht nur aus datenschutzrechtlicher Sicht ein forcierter Einsatz der Verschlüsselung und elektronischen Signatur in der Landesverwaltung im breiten Umfang nachdrücklich gefordert.

Auch der AK Technik der DSB des Bundes und der Länder hat mit einer Orientierungshilfe „Kryptographische Verfahren“ nochmals die grundlegende Bedeutung dieser Technologien für eine sichere automatisierte Datenverarbeitung und elektronische Kommunikation nachdrücklich unterstrichen (15.14).

In vielen öffentlichen Stellen des Landes hat die Vernetzung einen solchen Stand erreicht, dass alt hergebrachte Sicherheitskonzepte auf den Prüfstand gehören. Dabei ist zu klären, inwieweit die ergriffenen Sicherheitsmaßnahmen unter Berücksichtigung des Standes der eingesetzten Technik den gesetzlichen Anforderungen gemäß § 9 ThürDSG (noch) entsprechen. Insbesondere Web-Services und die zunehmend einrichtungsübergreifende Datenverarbeitung und Kommunikation bedingen erhöhte Anforderungen an die IT-Sicherheit. Bei der Planung der notwendigen Sicherheit stellt sich für jede öffentliche Stelle des Landes die Frage, ob es die entsprechenden Lösungen selbst erarbeitet oder hierfür externe Dienstleistungen in Anspruch nimmt. Insbesondere kleinere Stellen sind hierdurch in der Lage, über die Planung der Sicherheit hinaus, die entsprechenden Sicherheitsfunktionen schnell zu implementieren und jeweils in kürzester Zeit neuen Bedingungen anzupassen.
IT-Sicherheit darf keine Nebensache sein. Das zentrale Element jeglicher Sicherheit ist nach wie vor der Mensch als Nutzer der IT. Leider zeigt sich in der Praxis auch, dass Sicherheit nicht selten unterschätzt wird. Sie muss deshalb in der Leitungsebene verankert sein und mit im Mittelpunkt der eingesetzten und neuer IT-Anwendungen stehen. Ein hohes Sicherheitsniveau kann nur dauerhaft erzielt werden, wenn die IT-Sicherheit durch alle Benutzer aktiv unterstützt wird. Dies ist keine geringe Herausforderung, denn Sicherheitsmaßnahmen werden manchmal als Arbeitsbehinderung gesehen und vernünftige Risikoannahmen als realitätsfern abgetan. Es kommt also zunehmend darauf an, die Sensibilität der Benutzer für IT-Sicherheit zu erhöhen und wo notwendig entsprechende Verhaltensänderungen zu bewirken. Dazu ist es wichtig, dass sie über den Sinn und das Ziel der Sicherheitsmaßnahmen informiert sind, um sich mit diesen auch zu identifizieren. Anderseits dürfen sie nicht mit all zu komplexen Vorgängen zur Einhaltung von Sicherheitsvorschriften überfordert werden. Ein richtiger Ansatz hierzu ist der Einsatz von Single Sign On Verfahren, dass heißt jeder Benutzer authentifiziert sich für alle Dienste nur noch anhand eines Passwortes. Der zukünftige Einsatz von z. B. Windows

2000/2003 in der Landesverwaltung bietet hierzu die entsprechenden Voraussetzungen.

15.2 Technische und organisatorische Kontrolltätigkeit

Öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen des Thüringer Datenschutzgesetzes zu gewährleisten. Mit der Novellierung des ThürDSG am 10. Oktober 2001 sind die Zielstellungen Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten sowie die Revisionsfähigkeit und Transparenz der Verfahren ausdrücklich im Gesetz verankert worden (4. TB, 15.11).
Bei den im Berichtszeitraum durchgeführten Kontrollen und Informationsgesprächen ergaben sich mitunter Mängel, deren Beseitigung durch entsprechende Forderungen abzuhelfen war.

- Schon mehrmals wies ich in den vorhergehenden Tätigkeitsberichten auf die Notwendigkeit der Vorhaltung eines IT-Sicherheitskonzeptes bei der Verarbeitung von personenbezogenen Daten hin. Gemäß den Regelungen des neuen ThürDSG sind nunmehr die öffentlichen Stellen verpflichtet, die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage eines Sicherheitskonzepts festzulegen (§ 9 Abs. 2 ThürDSG). Unter Berücksichtigung sich verändernder Rahmenbedingungen und der Entwicklung der Technik ist die Wirksamkeit der festgelegten Maßnahmen regelmäßig zu überprüfen. Die sich daraus ergebenen notwendigen Anpassungen sind zeitnah umzusetzen. Es wurde festgestellt, dass dieser gesetzlichen Vorgabe nicht immer nachgekommen wird.
- Ein IT-Sicherheitskonzept bedarf einer regelmäßigen Überarbeitung hinsichtlich der tatsächlich umgesetzten technisch-organisatorischen Maßnahmen und der Anpassung an den jeweiligen Stand der Technik. Ein zur Einführung eines Verfahrens erstelltes IT-Konzept kann nicht in den Folgejahren ohne besondere Anpassungen und Ergänzungen als IT-Sicherheitskonzept deklariert werden.
- Passwortregeln sind in regelmäßigen Abständen dem Stand der Technik anzupassen, weil sie der Authentisierung des Benutzers für eine rechtmäßige Zugangs- und Zugriffsverwaltung des Systems dienen und somit die Vertraulichkeit und Integrität der Daten absichern. Passwörter mit einer Mindest-Länge von 5 Zeichen oder

wie sogar vorgefunden von nur 3 Zeichen bieten keine ausreichende Sicherheit.
Ermöglicht die eingesetzte Betriebs- und Anwendungssoftware keine zeitliche Einschränkung der Gültigkeitsdauer des Passwortes und eine Festlegung einer Mindest-Zeichenlänge, muss mittels organisatorischer Regelungen oder dem Einsatz zusätzlicher Sicherheitssoftware die Zugangskontrolle gewährleistet werden.

- Aus Gründen der Nachvollziehbarkeit der Datenverarbeitung angelegte Protokolldateien, anhand deren Daten z. B. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit), müssen zumindest stichprobenweise ausgewertet werden. Zur Auswertung, Aufbewahrung und Löschung der protokollierten Daten sind schriftliche Regelungen erforderlich.
- Für den Umgang mit Sicherungskopien von Daten sind ebenfalls technische und organisatorische Maßnahmen zu ergreifen, insbesondere um die Vertraulichkeit und Verfügbarkeit der Daten und die Revisionsfähigkeit und Transparenz ihrer Verarbeitung zu gewährleisten.
- Auch personenbezogene Daten, die nur für Testzwecke vorgehalten werden, unterliegen dem ThürDSG und sind, wenn der Zweck ihrer Speicherung entfällt, zu löschen.
- Bei der Absicherung von Serverräumen sollten auch Maßnahmen zur Installation von Brand- bzw. Bewegungsmeldern/Alarmanlagen in die Erwägungen einbezogen werden. Zur Erhöhung der IT-Sicherheit sind gleichfalls bauliche Veränderungen zu prüfen.
- Ebenso sind für den Betrieb von Telekommunikationsanlagen technische und organisatorische Maßnahmen notwendig (1. TB, 15.7). Für die Gebührenabrechnung (Erfassung der Verbindungsdaten) bedarf es der Beteiligung des Personalrats.
- Auch für die Videoüberwachung gilt gemäß § 9 ThürDSG, dass öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, technische und organisatorische Maßnahmen zu treffen haben, um die Ausführungen dieses Gesetzes zu gewährleisten.
  So bedarf es neben Festlegungen, wer wann was beobachtet, aufzeichnet, auswertet und löscht auch Regelungen zur Übernahme der Informationen auf andere Speichermedien, bspw. für die Weitergabe an die Strafverfolgungsbehörden und zur Entsorgung nicht mehr benötigter Datenträger.

Öffentliche Stellen, die am Wettbewerb teilnehmen und für die somit das BDSG gilt (§ 26 ThürDSG), haben gemäß § 6 b Abs. 2 BDSG durch geeignete Maßnahmen den Umstand der Beobachtung und die verantwortliche Stelle erkennbar zu machen. Dies geschieht zweckmäßigerweise durch das Anbringen von deutlich sichtbaren Hinweisschildern.

- Das Verfahrensverzeichnis gemäß § 10 ThürDSG ist aktuell zu führen.
- Um die gesetzlich vorgegebene Transparenz der Datenverarbeitung zu gewährleisten, ist eine aktuelle Dokumentation zum jeweiligen Verfahren, die insbesondere neben der Darstellung der verschiedenen Arten der Datenübermittlungen auch die hierbei ablaufenden Kommunikationsbeziehungen zwischen dem Auftraggeber, Auftragnehmer und dem Unterauftragsnehmer umfassen, notwendig.

  Insbesondere bei Verfahren, an denen mehrere öffentliche Stellen beteiligt sind, muss aus datenschutzrechtlicher Sicht die Transparenz für das Verfahren nicht nur bei der öffentlichen Stelle, dem die Administration obliegt, sondern auch bei allen anderen Stellen, gewährleistet sein.
- Im Rahmen der Auftragsdatenverarbeitung sind gemäß § 8 ThürDSG technische und organisatorische Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen. Der Auftraggeber hat sich von der Einhaltung der Maßnahmen zu überzeugen. Dies gilt bspw. für die Beauftragung privater Unternehmen durch öffentliche Stellen zur Akten- und Schriftgutentsorgung, als auch für Wartung oder Fernwartung automatisierter Datenverarbeitungsanlagen, soweit ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Die schriftlich festzulegenden Maßnahmen dienen insbesondere der gemäß § 9 Abs. 2 Ziffer 6 ThürDSG geforderten Transparenz des Verfahrens für den Auftraggeber.
- Eine datenschutzgerechte Entsorgung von Papierdokumenten, welche personenbezogene Daten enthalten, erfordert ein DIN-gerechtes Schreddern (1. TB, 15.14.5). Es reicht nicht aus, diese von Hand zu zerreißen und in Papierkörbe einzuwerfen, um sie dann vom Reinigungspersonal (auch wenn diese nach dem Verpflichtungsgesetz verpflichtet sind) dem Hausmeister zur weiteren Zerkleinerung zuzuführen. Die Möglichkeit einer unbefugten Kenntnisnahme personenbezogener Daten kann dabei nicht ausgeschlossen werden.

- Beim Verkauf von IT-Geräten ist durch eine datenschutzgerechte Löschung der Datenspeicher, z. B. Festplatten, sicherzustellen, dass schutzwürdige Daten nicht mehr physisch zur Verfügung stehen (15.8).

15.3 Aufbau eines landesweiten Verzeichnisdienstes

Zunehmende Rechnervernetzung und verteilte Verarbeitung von Daten erfordern eine effektive Verwaltung der Benutzer, Netze, Rechner und dezentraler peripherer Geräte. Die Organisation solcher Informationen ist eine wichtige Aufgabe, damit für die Systemverwalter die Vielzahl der anfallenden und benötigten Daten zentral zur Verfügung stehen. Das bisherige Vorhalten und Pflegen einer Vielzahl von einzelnen Verzeichnissen kann somit entfallen. Damit wird vor allem eine mehrfache Speicherung von Daten an verschiedenen Orten und eine oft daraus folgende Inkonsistenz dieser Daten verhindert. Diese Aufgaben übernehmen so genannte Verzeichnisdienste (4. TB, 15.13). Moderne Betriebssysteme stellen hierzu die entsprechenden Mechanismen bereit.
Im März 2003 fasste der IMA-IT einen Grundsatzbeschluss zur Einführung eines landesweiten Verzeichnisdienstes auf der Basis des Active Directory (AD) von Windows 2000/2003. Eine hierzu vom TLRZ erarbeitete Konzeption sowie ein Betriebskonzept wurde inzwischen vom IMA-IT bestätigt. Das TLRZ erhielt den Auftrag, alle in diesem Zusammenhang zentral zu erfüllenden Aufgaben wahrzunehmen. Der zentrale Verzeichnisdienst wird ressortübergreifend für alle Dienststellen der Landesverwaltung eingerichtet. Aus datenschutzrechtlicher Sicht ist ein solcher Dienst bedeutsam, da hier eine Vielzahl an personenbezogenen Daten gespeichert und verwaltet werden. Demzufolge sind auch datenschutzrechtliche Fragen und sicherheitstechnische Aspekte zu beachten. Im Mittelpunkt steht dabei, dass die schutzwürdigen Belange hier verzeichneter Personen nicht beeinträchtigt werden.
Um mögliche datenschutzrechtliche und sicherheitstechnische Risiken, die mit dem Betrieb eines solchen Dienstes verbunden sein können, zu erkennen und zu bewerten, bedarf es zunächst einiger grundsätzlicher Informationen zu seiner Funktion und zum systemtechnischen Umfeld.
Mit der Einführung des zentralen Verzeichnisdienstes ist auf absehbare Zeit eine Ablösung des zumeist in der Landesverwaltung eingesetzten Betriebssystems Windows NT-Server verbunden. Mit dem künfti-

gen Einsatz von Windows 2000/2003 stehen zusätzliche Sicherheitsfunktionen zur Verfügung, die hier involviert sind. Hervorzuheben sind das Dateisystem EFS (Encryption File System), mit dem die Benutzer Dateien oder komplette Verzeichnisse verschlüsseln können. Mit dem Protokoll IPSec (Internet Protocol Security) wird eine gesicherte Ende-zu-Ende-Datenübertragung ermöglicht. Die Authentifizierung der Benutzer erfolgt mit dem Sicherheitsprotokoll Kerberos über nur einen Anmeldevorgang für alle Ressourcen. Sowohl Server und Client müssen sich (gegenseitig) authentifizieren. Desweiteren wird ein Zertifikationsdienst angeboten, mit der eine Infrastruktur für öffentliche Schlüssel (2. TB, 15.7; 4. TB, 15.8) verwaltet werden kann und somit u. a. den Einsatz der elektronischen Signatur ermöglicht.
Eine wesentliche Neuerung unter Windows 2000/2003 stellt auch das schon erwähnte AD dar, ein Verzeichnisdienst zur Speicherung programm- und systemübergreifender Informationen. Hiermit können bspw. für Benutzer die Namen, E-Mail-Adressen, Telefonnummern, ihre Berechtigungen und Einbindung in die Organisationsstruktur unter Wahrung der Datenkonsistenz zentral verwaltet werden. Die physische Speicherung der Daten des AD erfolgt auf einen oder mehreren Servern, die als Domänen-Controller bezeichnet werden. Eine Domäne ist ein logischer Zusammenschluss von Rechnern, welche hierarchisch strukturiert zusammenarbeiten, eine gemeinsame Benutzerverwaltung und eine einheitliche Sicherheitsrichtlinie nutzen sowie eine zentrale Authentifizierung der Benutzer ermöglichen. Der Ort, an dem die Informationen des AD abgelegt werden, stellt das Verzeichnis dar. Jede Domäne besitzt ihr eigenes Verzeichnis. Es entspricht einer Datenbank, in der die Objekte eingetragen und abgerufen werden. Mit Hilfe von Schemata werden Regeln und Definitionen für die zu speichernden Objekte festgelegt. Ein Schema besteht aus den Objekttypen Klassen (z. B. Benutzer) und Attribute (z. B. Telefonnummer des Benutzers). Hier wird definiert, welche Objekte eingetragen werden können und wie diese aufgebaut sind sowie welche Inhalte erfasst werden können.
Die Informationen werden zur Sicherheit gegen einen möglichen Verlust der Verfügbarkeit i. d. R. auf mehreren Domänen-Controllern gespeichert. Änderungen auf einem beliebigen Domänen-Controller werden an die anderen Domänen-Controller weitergegeben (repliziert), sodass alle über den gleichen aktualisierten Informationsstand verfügen. AD verfügt auch über Dienste, um die gesuchten Informationen aus dem Verzeichnis bereitzustellen. Hierzu benutzt es Standardtechniken des Internet. Die Schnittstelle für den Abruf von Daten aus

dem AD bildet das Lightweight Directory Access Protocol (LDAP). Es handelt sich hierbei um ein zentrales Zugriffsprotokoll, das viele E-Mail-Programme, Web-Browser sowie Serversysteme nutzen, um mit dem AD zu kommunizieren. Zur Verbesserung der Performance beim Suchen eines Objektes verfügt das AD über einen speziellen Indexdienst, den Global Catalog (GC). Dieser durchsucht fortlaufend das gesamte Verzeichnis auf bestimmte Informationen, wobei er häufig gesuchte Informationen eines Objektes (z. B. die Telefonnummern von Benutzern) in einer speziellen Datenbank speichert. Damit wird das AD von solchen Suchanfragen entlastet. Der GC besitzt auch Informationen darüber, in welcher Domäne die gesuchte Information, bspw. die E-Mail-Adresse eines Benutzern, registriert ist. So kann der GC die Suchanfrage gezielt an den bestimmten Domänen-Controller richten, ohne jede Domäne einzeln durchsuchen zu müssen. Dies ist ein wesentlicher Vorteil, wenn das AD mehrere Domänen umfasst.
Das vom IMA-IT bestätigte Konzept zur Einführung des AD sowie das zugehörige Betriebskonzept sehen für die Dienststellen der Landesverwaltung eine gemeinsame stellenübergreifende AD-Gesamtstruktur vor. Jedes Ressort erhält eine eigene Domäne, die gemäß den ressortspezifischen Kriterien weiter untergliedert werden kann. Die Domäne stellt dabei eine Sicherheitsgrenze der Administration dar. Generell obliegt die Administration der jeweiligen Domäne oder ihrer Untergliederungen den lokalen Administratoren des jeweiligen Ressorts. Für die Administration der AD-Gesamtstruktur wird vom TLRZ eine übergeordnete separate Domäne (Root-Domäne) eingerichtet und betrieben. Die Administratoren dieser zentralen Domäne gehören zur Gruppe der Organisations-Administratoren und besitzen damit standardmäßig privilegierte Rechte für den Zugriff auf alle Domänen.
Bisher liegt noch kein IT-Sicherheitskonzept für die Einführung und den Betrieb des AD vor. Gemäß § 9 Abs. 2 ThürDSG sind die technischen und organisatorischen Maßnahmen auf der Grundlage eines Sicherheitskonzepts zu ermitteln. Für ein solches zentrales Vorhaben, das eine nicht unerhebliche datenschutzrechtliche Relevanz aufweist, ist ein solches Konzept auch für eine zukunftssichere Systemgestaltung von Bedeutung. In der Konzeption zur Einführung des AD wird zwar auf ein zu erstellendes Sicherheitskonzept hingewiesen und Sicherheitsziele aufgezeigt, eine Umsetzung dieser Ziele durch konkrete technische und organisatorische Maßnahmen steht jedoch aus.
Der gemäß IMA-IT-Beschluss vorgesehene Lösungsansatz, dass jedes Ressort selbständig seine Domäne administrieren kann, entspricht

einer wesentlichen datenschutzrechtlichen Forderung. Ebenso die im o. g. Beschluss enthaltene Bestimmung, dass die Organisations-Administratoren im TLRZ keine Befugnis haben, die Ressort-Domänen und deren Untergliederungen zu administrieren. Dies wird nur dann durchgeführt, wenn dem TLRZ explizit der Auftrag vom Domänen-Betreiber dazu erteilt wird.
Von zentraler Bedeutung und aus sicherheitstechnischer Sicht nicht unproblematisch ist in diesem Zusammenhang die Rolle der schon erwähnten Organisations-Administratoren. Sie besitzen automatisch die Berechtigung, sich in allen Domänen anzumelden, um hier administrative Arbeiten durchzuführen. Hiermit sind standardmäßig zwar keine unmittelbaren Rechte für einen Zugriff auf die in den Domänen lokal vorgehaltenen Daten verbunden. Die Organisations-Administratoren können sich aber aufgrund ihrer privilegierten Stellung solche Rechte zuordnen. Um einen solchen möglichen Zugriff zu verhindern sind somit technische und organisatorische Vorkehrungen zu treffen. Entsprechende Vorgaben sind in dem Sicherheitskonzept verbindlich festzulegen. Hier sind u. a. auch weitere Festlegungen für die Arbeit der „allmächtigen" Organisations-Administratoren zu treffen, wie bspw. die Ausführung sicherheitsrelevanter Aufgaben nach dem „Mehr-Augen-Prinzip", Vorgaben zur Protokollierung dieser Aktivitäten sowie zur Auswertung und Löschung der Protokolldateien.
Zu beachten ist auch, wenn dem TLRZ explizit der Auftrag zur Administration seitens des Domänen-Betreibers erteilt wird, liegt eine Auftragsdatenverarbeitung gemäß § 8 ThürDSG vor. Dies bedeutet u. a., dass der Auftrag schriftlich zu erteilen ist und die technischen und organisatorischen Maßnahmen zum Schutz der in der Domäne vorgehaltenen Daten festzulegen sind.
Von datenschutzrechtlicher Relevanz sind auch der Umfang und die Art der personenbezogenen Daten, die in die Verzeichnisse AD und GC aufgenommen werden. Hierzu liegen mir bisher noch keine Angaben vor. Nach § 2 und § 34 ThürDSG ist die jeweils öffentliche (Daten verarbeitende) Stelle für die Verarbeitung und Nutzung ihrer Daten verantwortlich. Nur gemäß den laut § 20 ThürDSG zu beachtenden Grundsätzen der Erforderlichkeit und der Zweckbindung können personenbezogene Daten von ihr in die jeweiligen Verzeichnisse eingestellt werden. Dies bedeutet, dass personenbezogene Daten von Mitarbeitern in Abhängigkeit ihrer dienstlichen Aufgaben differenziert zu veröffentlichen sind. Aus datenschutzrechtlicher Sicht kommen hierfür gemäß obiger Grundsätze folgende Informationsebenen in Betracht: Innerhalb der öffentlichen Stelle, ressortweit, landesweit

(CN), bundesweit (TESTA-Deutschland), europaweit (TESTA-Europa) sowie im Internet (z. B. zur Wahrnehmung von eGovernment-Aufgaben). Die Prüfung auf Erforderlichkeit und die hiermit verbundene Entscheidung auf bzw. bis zu welcher Ebene die Daten veröffentlicht werden, muss die betreffende Stelle unter Einbindung der Mitarbeiter vornehmen. Das einzusetzende technische System muss eine solche abgestufte Veröffentlichung personenbezogener Daten der Mitarbeiter ermöglichen.

15.4 E-Government in der Thüringer Landesverwaltung

E-Government ist heute ein Begriff, den man nicht mehr erklären muss. Im 4. TB im Punkt 5.1.6 gab ich bereits einen Ausblick auf die Entwicklungen in Bund und Land. Bereits damals signalisierten die DSB des Bundes und der Länder ausdrücklich ihre Bereitschaft, solche Entwicklungsprozesse konstruktiv datenschutzrechtlich zu begleiten.
Die hierfür im Jahr 2001 eingerichtete Arbeitsgruppe „Electronic Government“ unter Federführung des LfD Niedersachsen, an der sich auch meine Behörde aktiv beteiligte, erarbeitete zum Thema „Datenschutzgerechtes eGovernment“ eine Broschüre.
Aus datenschutzrechtlicher Sicht werden hier ausgehend von den Erscheinungsformen und Modellen sowie den grundsätzlichen Anforderungen und Herausforderungen für eGovernment Handlungsempfehlungen zur Gewährleistung von Datenschutz und Datensicherheit aufgezeigt. Darüber hinaus werden technisch organisatorische Werkzeuge dargestellt und Beispiellösungen aus der Praxis aufgeführt.
Die eGovernment-Broschüre ist im Internet veröffentlicht unter der Adresse www.datenschutz.de.

Im Freistaat Thüringen wurde unter der Leitung des TIM eine Arbeitsgruppe „Electronic Government“ gebildet, um die Bestrebungen zur Verwaltungsmodernisierung auf allen Ebenen der Verwaltung auf der Basis einer einheitlichen Technologie zu unterstützen und zu koordinieren.
Für eGovernment-Projekte, die beispielhaft nachfolgend erwähnt werden, ist aus datenschutzrechtlicher Sicht die Sicherheit ein wichtiger Faktor für deren Erfolg und Akzeptanz.
Die Projekte „Einsatz von IP-Sec-Boxen“ und „Einführung Digitale Signatur“ (4. TB, 15.8) bilden dabei aus datenschutzrechtlicher Sicht die entscheidende Grundlage zur Gestaltung eines datenschutzgerech-

ten eGovernment in Thüringen, weil dadurch die gemäß § 9 Abs. 2 ThürDSG geforderte Vertraulichkeit und Integrität der Daten sowie deren Authentizität gewährleistet werden kann.

Ein weiteres Projekt in der Thüringer Landesverwaltung ist die Realisierung gesicherter Wählzugänge in das CN, z. B. für Telearbeitsplätze, mobile Arbeitsplätze sowie Wartungsarbeiten der IT. Aus datenschutzrechtlicher Sicht spielen auch hier sicherheitstechnische Aspekte eine wichtige Rolle (15.7).

Gemäß § 9 Abs. 2 Ziff. 3 ThürDSG haben öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, technische und organisatorische Maßnahmen zu treffen, die gewährleisten, dass personenbezogene Daten zeitgerecht zur Verfügung stehen oder ordnungsgemäß verarbeitet werden können (Verfügbarkeit). Das Projekt „7x 24 Stunden Verfügbarkeit Internet/Intranet“ bildet dementsprechend für weitere Projekte eine entscheidende Voraussetzung. Die Verfügbarkeit wurde insbesondere im Zusammenhang mit dem Mail-Konzept der Thüringer Landesverwaltung und mit dem Aufbau eines einheitlichen Verzeichnisdienstes (15.3) diskutiert.
Eine wichtige technische Maßnahme zur Gewährleistung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten stellt der Virenschutz im CN dar (4. TB, 15.5). Die Praxis hat gezeigt, dass mit dem Projekt „Einsatz Virus-Wall im Mailverbund“ wesentlich zur Sicherheit beigetragen wurde, aber derzeit eine vollständige Verfügbarkeit noch nicht gewährleistet werden kann. Im Jahr 2003 kam es, aufgrund des erheblichen Virenaufkommens und der damit auftretenden Massenmails, zu Einschränkungen der Verfügbarkeit der Mail-Kopfstelle. Ziel ist es nach Aussagen des TLRZ, künftig derartige Ausfälle zu vermeiden, indem alle wichtigen IT-Prozesse kontinuierlich überwacht werden.

Die zentralen Maßnahmen zur Gewährleistung der Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität gemäß ThürDSG tragen aus meiner Sicht wesentlich dazu bei, geplante eGovernment-Fachprojekte datenschutzgerecht zu gestalten.
Hierzu gehören bspw. das Personalinformationssystem (6.1) und die Telearbeit (15.6).

Bei den eGovernment-Anwendungen, die eine internetbasierte Kommunikation mit dem Bürger ermöglichen, ist die öffentliche Stelle

gemäß § 2 TDG Diensteanbieter und hat somit nach § 4 Abs. 2 Nr. 3 TDDSG durch technische und organisatorische Vorkehrungen sicherzustellen, dass Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können.

15.5 Protokollierungen auf Webserver und Firewall des Landes

Der zentrale Internet-Server und die zentrale Firewall werden im Auftrag der Landesverwaltung vom TLRZ betrieben. Auf dem Webserver werden die Internet-Präsentationen (Web-Sites) der Ressorts, deren nachgeordneter Bereiche sowie weiterer öffentlicher Stellen des Landes vorgehalten. Die zentrale Firewall ist eine aus Hardware- und Softwarekomponenten aufgebaute Kontrollinstanz, die das Corporate Network (CN) der Landesverwaltung gegenüber dem öffentlichen Netz absichert. Aus sicherheitstechnischen Gründen erfolgen normalerweise alle netzübergreifenden Aktivitäten vom öffentlichen Netz in das CN als auch umgekehrt vom CN in das öffentliche Netz nur über diesen eingerichteten Schutzwall. Sowohl auf dem Webserver als auch auf der Firewall werden Protokollierungen durchgeführt. In einer Kontrolle vor Ort wurden diese auf ihre datenschutzrechtliche Zulässigkeit geprüft.

Zahlreiche Eigner der auf dem Web-Server eingestellten Web-Sites wünschen eine statistische Auswertung der auf ihre Seiten vorgenommenen Zugriffe. Dabei geht es nicht darum, den einzelnen Nutzer zu identifizieren, sondern um nicht personenbezogene Aussagen bspw. über die Anzahl der zugegriffenen Benutzer, welche Web-Sites wie oft aufgerufen und nach welchen Begriffen gesucht wurde sowie einer gewissen geographischen Zuordnung der Benutzer. Für Eigner, die solche Auswertungen wünschen, wurde vom TLRZ eine entsprechende Protokollierung in der Betriebssoftware des Web-Servers aktiviert. Die protokollierten Daten werden monatlich ausgewertet und danach gelöscht.
U. a. wird die IP-Adresse des zugreifenden Clients protokolliert. Unbestritten sind statische IP-Adressen personenbezogene Daten, da diese einen direkten und andauernden Bezug zu den Benutzern enthalten und ohne weiteres Rückschlüsse auf diesen zulassen. Mit Hilfe Dritter ist es darüber hinaus in vielen Fällen möglich, auch Benutzer mit nicht statischen IP-Adressen zu identifizieren. Insofern müssen auch dynamische IP-Adressen als personenbezogene Daten behandelt

werden, da sie durch Zusammenführung mit dahinter stehenden Zuordnungstabellen den Rückschluss auf bestimmbare Personen zulassen. Damit sind die aufgezeichneten Daten nicht mehr anonym und könnten zum Erstellen von Profilen über das Nutzungsverhalten der Benutzer herangezogen werden.
Da es sich bei inhaltlichen Internet-Angeboten gemäß § 2 Teledienstegesetz (TDG) um einen Teledienst handelt, gilt bei der Nutzung solcher Dienste für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten das Teledienstedatenschutzgesetz (TDDSG). Nach § 3 Abs. 1 TDDSG dürfen personenbezogene Daten vom Diensteanbieter nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat. Desweiteren darf gemäß § 6 Abs. 4 TDDSG der Anbieter Nutzungsdaten, wie die IP-Adressen der Benutzer, über das Ende des Nutzungsvorgangs hinaus nur verarbeiten und nutzen, soweit sie für Zwecke der Abrechnung erforderlich sind.
Da die Internet-Angebote auf dem zentralen Web-Server des Landes den Benutzern kostenlos für jedermann öffentlich zur Verfügung stehen, ist eine Abrechnung dieser Leistung gegenüber den Benutzern nicht erforderlich. Eine Einwilligung der Benutzer für eine Speicherung liegt nicht vor, da seitens der Web-Eigner eine solche nicht eingeholt wird. Auch die allgemeinen Vorschriften zur Datensicherheit nach § 9 ThürDSG sind für eine Protokollierung der IP-Adresse nicht anwendbar. Zudem hat es keine Vorkommnisse gegeben, die aus Sicherheitsgründen eine solche Protokollierung erforderlich erscheinen lassen. Somit ist die Speicherung von IP-Adressen über die Nutzungsdauer hinaus rechtlich nicht zulässig.
Das TLRZ wurde deshalb aufgefordert eine Vorhaltung der vollen IP-Adresse zu unterbinden und angeraten zu prüfen, inwieweit die statistischen Auswertungen auch mit einer um die letzten drei Stellen verkürzten IP-Adresse, die eine Personenbeziehbarkeit nicht mehr zulässt, ermöglicht wird oder sofort mit dem Nutzungsende die für die Sitzung erfassten Daten statistisch auszuwerten und damit auf die Speicherung der IP-Adresse grundsätzlich zu verzichten.
Vom TLRZ wurde zunächst ausgeführt, dass für die von einigen Web-Anbietern geforderten Auswertungen seitens der hierfür eingesetzten Software, die volle IP-Adresse benötigt wird. Durch programmtechnische Änderungen wurde jedoch ermöglicht, ohne Speicherung der letzten drei Stellen der IP-Adresse die geforderten statistischen Auswertungen zu erstellen. Damit wird den rechtlichen Anforderungen Genüge getan.

Auf der zentralen Firewall des Landes werden unabhängig davon, inwieweit die öffentlichen Stellen selbst eigene Firewalls vorhalten, Zugriffe der Mitarbeiter in das Internet protokolliert. Die durchgeführte datenschutzrechtliche Kontrolle diente dem Ziel, festzustellen, inwieweit diese Protokollierung erforderlich und rechtlich zulässig ist. In der „Dienstregelung zur Nutzung des Internetzugangs der Landesverwaltung“ ist festgelegt, dass die Internetanschlüsse ausschließlich zur dienstlichen Nutzung dienen. Protokollierungen werden für die Dienste HTTP, FTP und SMTP vorgenommen und in Abhängigkeit der hierbei anfallenden Datenmenge bis zu sechs Monaten aufbewahrt. U. a. wird die Adresse der aufgerufenen Web-Sites festgehalten. Die protokollierten Daten sind personenbeziehbar, da auch die jeweilige IP-Adresse der Benutzerclients erhoben wird. Obwohl viele der öffentlichen Stellen eigene Firewalls betreiben und beim Übergang in das CN hier zumeist die interne IP-Adresse des Client durch eine externe Adresse der öffentlichen Stelle ersetzt wird, kann durch Rückverfolgung über entsprechende Zuordnungstabellen der lokale Client bestimmt werden. Im Nutzungshandbuch -Intranet/Internet der Thüringer Landesverwaltung für die Administratoren- ist unter Punkt 1.2.4 Protokollierungen dargelegt, dass eine Protokollierung sicherheitsrelevanter Ereignisse an den zentralen Sicherheitssystemen im CN als eine grundlegende Maßnahme unumgänglich ist, um Hinweise auf eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkennen zu lassen. Insofern war die Erforderlichkeit und Angemessenheit der Protokollierung auch im Hinblick auf festgestellte Sicherheitsverletzungen zu prüfen.
Beim Bereitstellen eines Internet-Zugangs für die ausschließlich dienstliche Nutzung handelt es sich nicht um einen Teledienst im Sinne des Teledienstegesetzes. Zulässigkeit und Umfang der Protokollierung richten sich nach den Vorschriften, die auf die Verarbeitung von Daten im jeweiligen Beschäftigungsverhältnis Anwendung finden, z. B. nach dem Thüringer Datenschutzgesetz. Nach § 19 ThürDSG ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Eine pauschale, flächendeckende, vorbeugende Protokollierung der Internetzugriffe ist aus datenschutzrechtlicher Sicht bedenklich als hiermit die Möglichkeit für eine unzulässige Verhaltens- und Leistungskontrolle gegeben ist. Der Dienstherr hat zwar grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Nutzen des Internets der Beschäftigten dienstlicher Natur ist, eine automatisierte Vollkontrolle wird jedoch nur bei konkretem Missbrauchsver-

dacht im Einzelfall für zulässig angesehen. Meiner Empfehlung, die Internetzugriffe in anonymer Form zu protokollieren, um den Dienstherrn zumindest noch eine grundsätzliche Kontrolle auf Missbrauch zu ermöglichen, wurde vom TLRZ abschlägig beschieden, da die eingesetzte Software eine solche Protokollierungsart nicht ermöglicht. Nach Aussagen des TLRZ liegen auch keine Erkenntnisse und Feststellungen zu sicherheitstechnischen Verstößen vor, die zumindest für einen begrenzten Zeitraum eine Protokollierung rechtfertigen könnten. Somit ist eine Erforderlichkeit für die derzeit ohne Anlass durchgeführte personenbeziehbare automatisierte Vollprotokollierung aller Internetzugriffe der Mitarbeiter des Landes nicht gegeben. Das TIM als verantwortliches Ressort für den Betrieb der Firewall wurde deshalb um Stellungnahme gebeten und aufgefordert, soweit aus seiner Sicht keine weiteren Erkenntnisse vorliegen, die eine solche Erforderlichkeit begründen, das TLRZ anzuweisen die Protokollierung einzustellen.

15.6 Telearbeit

15.6.1 Telearbeit in der Thüringer Landesverwaltung

Eine eGovernment-Maßnahme in der Thüringer Landesverwaltung (15.4) ist das Projekt Telearbeit. Ziel des Projektes ist es, die technischen und organisatorischen Voraussetzungen zur sicheren Telearbeit für alle Dienststellen der Landes- und Kommunalverwaltungen zu schaffen. Projektkomplexe sind dabei

- die Einrichtung von Testarbeitsplätzen im TIM,
- das Sicherheitskonzept für Telearbeitsplätze,
- die Erarbeitung einer Muster-Dienstvereinbarung,
- die Erarbeitung typischer Tele-Arbeitsanwendungen und
- die Ausstattungsvorgaben für Tele-Arbeitsplätze.

Schon im 3. TB (15.13) zeigte ich datenschutzrechtliche und sicherheitstechnische Aspekte auf, die bei der Einführung und der Nutzung von Telearbeit zu beachten sind.
Gemäß § 40 Abs. 5 Satz 1 ThürDSG beobachtet der Landesbeauftragte für den Datenschutz die Entwicklung und Nutzung der Informations- und Kommunikationstechnik, insbesondere der automatisierten Datenverarbeitung und ihre Auswirkungen auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen. Um mir eine aktuelle Übersicht zum Einsatz der Telearbeit in der Landesverwal-

tung zu verschaffen, wurden im Februar 2003 alle obersten Landesbehörden, der TLT und der TRH um Mitteilung gebeten, inwieweit in ihrem Zuständigkeitsbereich (einschließlich nachgeordneter Dienststellen) Telearbeit bereits eingesetzt oder getestet wird bzw. ob und wann eine solche geplant ist.
Zum Zeitpunkt der Umfrage, waren - abgesehen von den Hochschulen - 35 Telearbeitsplätze zumeist noch in der Testphase in der Landesverwaltung im Einsatz.
Die Mehrzahl der Telearbeitsplätze waren zum Zeitpunkt der Umfrage stand-alone-PCs oder hatten Zugriff auf lokale Netzwerke, die nicht an das CN der Landesverwaltung angeschlossen sind.
Entsprechend vorliegender Auskünfte sind weitere Telearbeitsplätze vorgesehen.
Insbesondere im Bereich des TMLNU sollen schrittweise ca. 370 Forstreviere an das Landesdatennetz angeschlossen werden. Dieser Prozess wird nach Angaben des TMLNU voraussichtlich mehrere Jahre in Anspruch nehmen und ist eng mit dem TLRZ abgestimmt.
Eine Muster-Dienstvereinbarung zur Einrichtung von Telearbeitsplätzen, in der auch die Anregungen und Hinweise des TLfD Berücksichtigung fanden, ist vom TIM als IMA-IT Geschäftsstelle an alle Ministerien übersandt worden.
Darüber hinaus sind für die Festlegung konkreter ressortspezifischer Regelungen und insbesondere in den Hinweisen für die Benutzer auch die im 3. TB dargelegten datenschutzrechtlichen Hinweise zum Einsatz von Telearbeit einzubeziehen, deren Umsetzung im Rahmen der Kontrolltätigkeit auch kontrolliert wird.

15.6.2 Einrichtung eines Telearbeitsplatzes

Im Geschäftsbereich des TIM wurden im Rahmen eines Pilotprojektes zwei Telearbeitsplätze eingerichtet. Bei der Einführung des Projektes wurde ich bereits in der Konzeptionsphase beteiligt. So wurden entsprechende Muster einer Rahmendienstvereinbarung, einer Nebenabrede zum Arbeitsvertrag sowie ein Merkblatt für den Telearbeiter mit Informationen zum Datenschutz und zur Datensicherheit zur datenschutzrechtlichen Bewertung übergeben. Die Anregungen und Hinweise wurden bei der Überarbeitung der o. g. Unterlagen berücksichtigt. Im Rahmen einer vom TIM durchgeführten Zwischenevaluierung für das Pilotprojekt Telearbeit wurde die Umsetzung der in den Unterlagen vorgesehenen Maßnahmen zum Datenschutz und zur Datensicherheit kontrolliert. Schon im 3. TB (15.13) informierte ich über

datenschutzrechtliche Aspekte, die bei der Einrichtung von Telearbeitsplätzen zu beachten sind. U. a. sind hier grundlegende technische und organisatorische Maßnahmen aufgezeigt. Im Rahmenkonzept des TIM ist festgelegt, dass Telearbeitsplätze nicht für eine Verarbeitung personenbezogener Daten mit einem hohen Schutzbedarf (Schutzklasse 2, 1. TB, 15.3) eingesetzt werden dürfen. Es handelt sich hierbei um Daten, deren Verarbeitung eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts insofern erwarten lässt, als der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann. Darüber hinaus wurde vom TIM im Rahmen der durchgeführten Zwischenevaluierung mitgeteilt, dass Telearbeitsplätze nur für Aufgaben eingerichtet werden, bei denen keine personenbezogenen Daten verarbeitet werden. Insofern ist es zu begrüßen, dass das TIM unabhängig davon bei den zu treffenden Maßnahmen die Sicherheitsziele des § 9 Abs. 2 ThürDSG zugrunde legt.

Die Datenverarbeitung an dem kontrollierten Telearbeitsplatz findet unmittelbar auf einem Server im TIM statt. Am Arbeitsplatz befinden sich ein Laptop mit Modem für einen DSL-Anschluss sowie Drucker und Fax. Über den Anschluss erfolgt die Einwahl in das CN und hier die Durchleitung in das lokale Netz des TIM. Dazu wird vom Laptop bis in das CN ein virtuelles privates Netz aufgebaut. Der Remote-Zugang in das CN ist unter 15.7 beschrieben. Vom CN bis zum lokalen Netz des TIM wird eine Hardwareverschlüsselung anhand von Kryptoboxen vorgenommen. Im Laptop selbst ist ein Programm zur Verschlüsselung der Festplatte eingesetzt. Desweiteren ist ein Virenerkennungssystem auf dem Laptop installiert, das durch entsprechende Abgleiche automatisch aktualisiert wird. Dienstlich notwendige Zugriffe in das Internet erfolgen nur über das Netz des TIM. Wartung und Reparatur der eingesetzten Technik erfolgen arbeitsteilig durch das TIM und das TLRZ. Der Telearbeiter wird durch ein mehrstufiges Identifizierungs- und Authentifizierungsverfahren verifiziert. Gemäß dem derzeitigen Kenntnisstand entsprechen die ergriffenen Sicherheitsmaßnahmen dem Stand der Technik und präsentieren ein über den normalen Grundschutz hinausgehendes Sicherheitsniveau. Bezüglich der Verfügbarkeit gibt es keine nennenswerten Probleme. Dem TIM wurde im Rahmen der Zwischenevaluierung empfohlen, die konkreten ergriffenen Sicherheitsmaßnahmen für den Telearbeitsplatz, für die Telekommunikationsverbindung und für die Anbindung an die Infrastruktur des TIM in einem Sicherheitskonzept zusammengefasst

darzulegen. Der technische Verfahrensablauf sollte nachvollziehbar aufgezeigt werden. Desweiteren bedarf es für die Administration der am Telearbeitsplatz eingesetzten IT klarer Vorgaben für die Einrichtung der befugten Benutzer/Administratoren, ihre Rechte, die Richtlinien ihrer Konten sowie die einzustellenden Protokollierungsereignisse und deren Auswertung. Auch wurde dem TIM aus praktischen und organisatorischen Gründen empfohlen soweit möglich, einheitlich für alle Telearbeitsplätze und für die Datenübertragung das gleiche Sicherheitsniveau vorzuhalten.
Zwischenzeitlich teilte mir das TIM mit, dass an der Umsetzung meiner Anregungen gearbeitet wird.

15.7 Kontrolle Remote-Zugang in das CN (Landesnetz)

Gemäß dem eGovernment-Konzept des Freistaates Thüringen werden Remote-Zugänge für Telearbeitsplätze und mobile Arbeitsplätze sowie Wartungsarbeiten der computergestützten Anlagen und Geräte benötigt und sind für das analoge Fernsprechnetz, ISDN, Mobilfunk und Internet/T-DSL einzurichten. Im Auftrag des TIM wurde vom TLRZ ein solcher Zugang eingerichtet und desweiteren technisch betreut.
Mit dem Remote-Zugang können sich lokal entfernte und berechtigte Benutzer (Remote-Client) in das Corporate Network (CN) der Landesverwaltung einwählen und hierüber Zugang in das jeweilige lokale Netz der Behörde erhalten. Die Remote-Benutzer können auf diesem Weg vollständig in das lokale Netzwerk (LAN) integriert werden und gemäß ihrer Zugriffsrechte i. d. R. so arbeiten, wie sie es von einem direkt angeschlossenen IT-Arbeitsplatz am Netzwerk gewohnt sind. Damit soll für ausgewählte Mitarbeiter und externe Nutzer eine größere Mobilität und Flexibilität beim Zugriff auf die zentralen IT-Systeme erreicht werden. Bei den Nutzungsarten des Remote-Zugangs sind spezifische Unterschiede erkennbar. Während z. B. bei Telearbeit i. d. R. der Zugriff immer von derselben Stelle erfolgt (z. B. gleiche Telefonnummer), erfolgt der Zugriff auf Dienstreisen i. d. R. von wechselnden Standorten. Dabei werden je nach dem erforderlichen Informations- bzw. Kommunikationsbedarf einzelne Dienste (z. B. E-Mail) bis hin zum umfassenden Zugriff auf zentrale Datenbestände benötigt.
Aus datenschutzrechtlicher Sicht sind ohne vorbeugende Sicherheitsmaßnahmen bei entfernten Zugriffen auf zentrale Systeme und Daten sowohl der Remote-Client, die erreichbaren IT-Systeme im CN und in

den lokalen Netzen, als auch in diesen vorgehaltene und die zu übertragenen Daten gefährdet. Insofern spielen sicherheitstechnische Aspekte bei Remote-Zugriffen eine wichtige Rolle. So sind insbesondere gemäß § 9 Abs. 2 ThürDSG die Integrität, die Vertraulichkeit und die Authentizität der übermittelten Daten zu sichern. Weiterhin spielen Revisionsfähigkeit und Transparenz des Verfahrens eine wesentliche Rolle.
Inwieweit diese Sicherheitsziele bisher umgesetzt sind, wurde von mir im Rahmen einer datenschutzrechtlichen Kontrolle geprüft.
Im Mittelpunkt dieser Kontrolle standen die eingesetzte IT-Struktur und Applikationen, insbesondere die implementierten technischen und organisatorischen Maßnahmen, um die gemäß § 9 Abs. 2 ThürDSG vorgegebenen Sicherheitsziele zu gewährleisten.

Für den Remote-Zugang in das CN wurde eine VPN (Virtual Private Network) - Einwahllösung vom TLRZ installiert. Das VPN wird zwischen dem externen Client und einer rechentechnisch mit erheblicher Intelligenz ausgestatteten zentralen Schnittstelle (VPN-Gateway) im CN aufgebaut. Ein VPN ermöglicht die Vorteile öffentlicher Informationsstrukturen (z. B. Internet) mit der Vertraulichkeit und Informationssicherheit eines Privaten Netzwerkes zu kombinieren. Im herkömmlichen Internet-Protokoll der Netzwerkebene sind zwar bereits einfache Verfahren zur Erkennung von Fehlern bei der Datenübertragung vorhanden. Sie dienen aber lediglich dazu, Fehler zu erkennen, die durch unzuverlässige Übertragungsmedien auftreten können. Sie enthalten keine Mechanismen, um die Authentizität, die Integrität sowie die Vertraulichkeit abzusichern. Bei einem VPN wird hierzu als Sicherheitsarchitektur das erweiterte Internetprotokoll IPSec genutzt. Die grundlegende Idee von IPSec besteht darin, jedes einzelne IP-Paket unterwegs vor Verfälschung zu schützen (Authentizität und Integrität) und verschlüsselt zu übertragen (Vertraulichkeit). Das verwendete Sicherheitsprotokoll setzt hierzu kryptographische Verfahren zur Verschlüsselung der Daten und zur Erzeugung signierter Daten-Prüfsummen ein, anhand letzterer sowohl die Integrität als auch die Authentizität der Daten und ihrer Quelle nachgewiesen wird. Auch ein Anti-Replay-Schutz ist involviert, der ein wiederholtes Einspielen des gleichen Datenpaketes erkennt und somit eine diesbezügliche Datenmanipulation verhindert. Weiterhin wird das IP-Paket mit einem neuen Vorsatz versehen (getunnelt), der als feste Zieladresse die des VPN-Gateway enthält. Somit wird sichergestellt, dass der Client gezielt nur mit dem VPN-Gateway eine Verbindung aufbauen kann.

Auf dem Remote-Client selbst werden i. d. R. Sicherheitsapplikationen installiert, wie eine Personal-Firewall, Virenscanner und ein Dateiverschlüsselungssystem.
Die Sicherheitsapplikationen und das Subnetzwerk für den Remote-Zugang in das CN wird mit dem so genannten Policy Manager verwaltet und gesteuert. Der Administrator ist hiermit in der Lage, die Sicherheitsapplikationen mittels Fernzugriff automatisch zu konfigurieren und zu aktualisieren. Es ist somit möglich, jedes diesbezügliche IT-Gerät auch sicherheitstechnisch anhand spezieller Richtlinien-, Konfigurations- und Installationsdateien zu verwalten. Über die Policy Manager-Konsole empfängt der Administrator auch Alarme und Warnungen, wenn Sicherheitsrichtlinien bedroht werden oder Einbruchsversuche stattgefunden haben.
Für die personenbezogene Anmeldung des Remote-Nutzers kommen alternativ zwei Authentifizierungsverfahren zur Auswahl. Beide Verfahren basieren auf dem Prinzip Wissen (PIN) und Besitz (Chipkarte). Das eine Authentifizierungssystem arbeitet mit einem achtstelligen Einmalpasswort. Das zweite Authentifizierungssystem arbeitet mit Zertifikaten, die von der TESTA-CA (Certification Authority) gemäß dem Signaturgesetz für eine fortgeschrittene Signatur (4. TB, 15.8) ausgestellt werden.

Im Ergebnis der Kontrolle kam ich aufgrund der für das Verfahren Remote-Zugang eingesetzten Sicherheitsmechanismen zu der Einschätzung, dass aus datenschutzrechtlicher Sicht gemäß dem derzeitigen Kenntnisstand keine grundsätzlichen Bedenken gegen die eingesetzte VPN-Lösung bestehen. Entscheidend für die Wirksamkeit der Sicherheitsmerkmale ist jedoch eine sorgfältige Konfiguration und qualifizierte Wartung des Systems. Beachtet werden muss, dass die VPN-Lösung nur eine verschlüsselte Übertragung zwischen dem Remote-Client und dem VPN-Gateway ermöglicht. Damit ist zumindest der wichtige Schutz für eine Übertragung im Bereich der öffentlichen Netze bis in das CN gewährleistet. Eine Ende zu Ende Verschlüsselung ist damit allerdings nicht gegeben. Für eine Übertragung sensibler Daten ist somit eine zusätzliche Verschlüsselung erforderlich, um eine durchgängige Vertraulichkeit zwischen Remote-Client und Endsystem zu gewährleisten.
In den Empfehlungen beim Einsatz des Verfahrens wies ich auch auf die gemäß § 9 Abs. 2 Nr. 6 ThürDSG geforderte Transparenz für das Verfahren Remote-Zugang hin. Hierzu fehlte eine aktuelle Dokumentation der Verfahrensbeschreibung, in welcher auch die Sicherheits-

merkmale und eventuelle Schwachstellen dieses Verfahrens dargelegt sind. Desweiteren sollte das TLRZ für eine sichere Handhabung des Systems auch Schulungen für zukünftige Endbenutzer anbieten. Unter Abwägung sicherheitstechnischer Aspekte waren auch die Art und der Umfang der notwendigen Protokollierungen festzulegen und einzurichten. Die Auswertung der Protokolldaten ist zu regeln. Über die eingerichteten Protokollierungen und Auswertungen sind die Endnutzer zu informieren.
Die Verantwortung für einen ordnungsgemäßen Betrieb des Remote-Client liegt bei der jeweiligen Behörde. Um diese Verantwortung umfassend wahrnehmen zu können, muss diese über die auf dem Client im Rahmen der VPN-Nutzung erfolgten Eingriffe seitens der VPN-Administration (TLRZ) informiert sein. Das TLRZ muss hierzu schriftlich hinreichend und abschließend den genauen Funktionsumfang seiner administrativen Tätigkeit auf dem Client aufzeigen. Der Behörde obliegt die Entscheidung, inwieweit sie diese Eingriffe, im Hinblick auf ihre Konfiguration und Sicherheit der Daten, tolerieren kann. Soweit auf dem Remote-Client personenbezogene Daten vorgehalten werden, sind diese zur Wahrung der Vertraulichkeit verschlüsselt zu speichern. In der Stellungnahme zum Kontrollbericht wurde die Umsetzung meiner o. g. Forderungen und Empfehlungen seitens des TIM zugesichert.

15.8 Löschung und Vernichtung von Daten und Datenträgern

Aufgrund von Anfragen möchte ich nochmals auf die datenschutzgerechte Löschung von Daten und Datenträgern eingehen. Schon im 1. TB (15.9) habe ich hierzu grundlegende Ausführungen gemacht.
Grundsätzlich ist bei der Verarbeitung von personenbezogenen Daten gemäß § 9 ThürDSG zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit). Personenbezogene Daten sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist (§ 16 Abs. 1 ThürDSG). Gemäß § 16 Abs. 4 ThürDSG unterbleibt eine Löschung nur, wenn Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden, eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder einer Löschung ge-

setzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.
Beauftragen öffentliche Stellen andere Personen oder Stellen mit der Löschung personenbezogener Daten (z. B. Entsorgung von Datenträgern/Aktenvernichtung) sind die Bestimmungen des § 8 ThürDSG zu beachten. Der Auftrag zur Datenträgervernichtung ist jeweils vom Auftraggeber schriftlich zu erteilen.
Soweit der Umgang mit den personenbezogenen Daten besonderen Geheimhaltungsbestimmungen unterliegt (z. B. Arztgeheimnis) ist zu gewährleisten, dass eine Kenntnisnahme dieser Daten durch den Auftragnehmer unmöglich wird (z. B. durch Beaufsichtigung der Vernichtung).

Gemäß § 3 Abs. 3 Nr. 6 ThürDSG ist unter „Löschen“ das endgültige Unkenntlichmachen gespeicherter personenbezogener Daten zu verstehen. Zum Unkenntlichmachen gespeicherter personenbezogener Daten auf magnetischen Datenträgern reichen die in den Betriebssystemen enthaltenen Löschkommandos nicht aus, da diese nur den Verweis, wo sich die Daten auf der Festplatte befinden, löschen. Mittels spezieller Software, sogenannter Datenrettungsprogramme, kann i. d. R. auf diese physisch noch vorhandenen Daten zugegriffen werden, da der Speicherbereich dieser Daten i. d. R. frühestens erst wieder beschrieben wird, wenn keine freie Speicherkapazität mehr zur Verfügung steht. Um Daten physisch auf elektronischen Datenträgern zu löschen, müssen diese mehrfach mit gleichverteilten Zufallszahlen überschrieben werden. Mit zunehmender Anzahl solcher Schreibvorgänge erhöht sich die Wahrscheinlichkeit, dass die Daten nicht mehr rekonstruiert werden können. Hierzu auf dem Markt angebotene Software sollte vor Einsatz auf ihre diesbezügliche Eignung geprüft werden.
Insbesondere bei der Aussonderung von IT-Geräten wozu u. a. auch moderne Drucker und Kopierer zählen, ist darauf zu achten, dass die gespeicherten Daten so gelöscht werden, dass eine Rekonstruktion mit hoher Wahrscheinlichkeit ausgeschlossen werden kann. Aber auch bei der Umsetzung bspw. von PCs in ein anderes Sachgebiet sind notwendige Löschmaßnahmen zu prüfen. Elektronische Datenträger die zur Aussonderung gedacht sind und sensible Daten enthalten, sollten vorzugsweise durch Schreddern oder Verbrennen/Einschmelzen physisch vernichtet werden. Letzteres ist naturgemäß z. Z. die unumstrittenste Methode zum endgültigen Unkenntlichmachen gespeicherter personenbezogener Daten.

In einem rechtmäßigen Löschvorgang sind alle Datenträger, auch Datensicherungskopien, einzubeziehen, auf denen die betreffenden Daten vorgehalten werden.

Die zu treffenden Maßnahmen zur Löschung von personenbezogenen Daten sind im Sicherheitskonzept der öffentlichen Stelle mit entsprechenden Verantwortlichkeiten festzulegen. Die Wirksamkeit der Maßnahmen ist gemäß § 9 Abs. 2 ThürDSG unter Berücksichtigung sich verändernder Rahmenbedingungen und der Entwicklung der Technik regelmäßig zu überprüfen und zeitnah umzusetzen.

15.9 Sicherheitsaspekte beim Online-Banking von Gerichtsvollziehern

Der Einsatz von EDV bei Gerichtsvollziehern wird durch die Verwaltungsvorschrift des TJM „Unterstützung der Geschäftstätigkeit des Gerichtsvollziehers durch Einsatz von EDV-Systemen“ vom 23. April 1999 bestimmt (3. TB, 10.14). Unter 5.2 dieser Vorschrift ist festgelegt, dass eingesetzte EDV-Systeme grundsätzlich nicht mit einem anderen EDV-System oder Kommunikationsnetzen verbunden werden dürfen. Das für Justiz zuständige Ministerium kann jedoch generell oder für den Einzelfall Ausnahmen zulassen. Damit sollte nach Aussage des TJM die Möglichkeit eröffnet werden, neue Techniken und Verfahrensweisen zu erproben, wie bspw. EDV-Systeme zusätzlich zur Abwicklung des Zahlungsverkehrs einzusetzen. Zwischenzeitlich teilte mir das TJM mit, dass ein Gerichtsvollzieher beantragt hat, ihm zu gestatten, seine Geschäftskonten über Online-Banking per BTX abzuwickeln. Die erforderliche Software hierzu wurde von dem Kreditinstitut erworben. Für den Einsatz von BTX benötigt der Kunde für den Zugriff über T-Online auf sein Konto als Passwort eine PIN (Persönliche Identifikationsnummer) und für jede Transaktion eine TAN (Transaktions-Nummer). Dazu muss der Benutzer sicherstellen PIN und TAN so aufzubewahren, dass Unbefugte nicht darauf zugreifen können. Grundsätzlich ist hierzu anzumerken, dass eine Nutzung des Online-Banking nur dann keinen datenschutzrechtlichen Bedenken begegnet, wenn durch entsprechende technische und organisatorische Maßnahmen eine hinreichende Datensicherheit gewährleistet ist. In der Regel ist Online-Banking an die Nutzung von öffentlichen Netzen gebunden und damit den hiermit verbundenen netzspezifischen Gefährdungen ausgesetzt. Inwieweit diese Risiken auf ein hinnehmbares Maß reduziert werden können, hängt entscheidend von den sicher-

heitsspezifischen Merkmalen der hierfür eingesetzten Online-Banking-Software und der Umsetzung hiermit verbundener Sicherheitsvorkehrungen seitens des Anwenders ab. Ich teilte dem TJM mit, dass in der öffentlichen Diskussion das Verfahren BTX mit PIN und TAN als nicht sehr sicher eingestuft wird und derzeit durch den HBCI-Standard (Home Banking Computer Interface) der Deutschen Kreditwirtschaft abgelöst wird. Dieser Standard enthält kryptographische Elemente zur Gewährleistung der Vertraulichkeit und zur Überprüfung der Integrität der Daten sowie der Authentizität der beteiligten Kommunikationspartner. Unabhängig davon besteht ohne zusätzliche Sicherheitsvorkehrungen immer die Gefahr, dass bei einem Anschluss eines PCs, auf dem sensible Daten verarbeitet werden, an öffentliche Netze auf die hier gespeicherten Daten durch Unbefugte zugegriffen werden kann. Das TJM teilte mir daraufhin mit, dass es die Erprobung des Online-Banking-Verfahrens mit der Maßgabe, dass die elektronische Datenübermittlung nicht über den Dienst-PC sondern über einen zweiten PC erfolgen kann, gestattet. Aufgrund der ergriffenen technischen und organisatorischen Maßnahmen, die u. a. einen Zugriff auf das Internet sowie eine Speicherung von PIN und TAN in dem Homebanking-Programm ausschließen und unter dem Aspekt, dass zukünftig eine Umstellung auf HBCI erfolgen soll, wird den sicherheitstechnischen Bedenken Rechnung getragen. Das TJM wurde gebeten, zu gegebener Zeit über das Ergebnis der Erprobung zu informieren.

Inzwischen teilte mir das TJM mit, dass der Gerichtsvollzieher das von ihm erprobte Online-Banking auf den HBCI-Standard umgestellt und einen positiven Erfahrungsbericht übermittelt hat. Desweiteren sei über das Thüringer Oberlandesgericht auch der Wunsch herangetragen worden, dass Online-Banking-Verfahren allgemein für die Gerichtsvollzieher des hiesigen Geschäftsbereiches zuzulassen. Hierzu wurde mir ein Entwurf von Ergänzungen für die o. g. Verwaltungsvorschrift für den Einsatz von EDV-Technik im Gerichtsvollzieherbüro zugesandt, in der u. a. die sicherheitstechnischen Maßgaben zum Online-Banking aufgeführt sind. Im Hinblick auf eine höchstmögliche Sicherheit wird nur die Nutzung des Standards HBCI unter Verwendung von Chipkarte und Lesegerät gestattet.

In meiner Stellungnahme wies ich u. a. darauf hin, dass Virenscanner und Personalfirewalls verbindlich einzusetzen sind. Die einzusetzenden Produkte sollten möglichst zentral vorgegeben und für ihre Einrichtung auf dem PC klare Vorgaben zur Installation/Konfiguration als auch zum Updaten dieser Sicherheitsapplikationen erlassen werden.

Da die Installation und Konfiguration solcher Systeme gemäß den technischen Kenntnissen und Fähigkeiten der Nutzer problematisch sein kann, sollten alle Nutzer entsprechend unterrichtet bzw. geschult werden. Meine Hinweise wurden berücksichtigt und vom TJM in die ergänzende Regelung zur o. g. Verwaltungsvorschrift aufgenommen und damit die Teilnahme am Online-Banking-Verfahren zugelassen. Gemäß dem derzeitigen Erkenntnisstand stellen die vorgegebenen technischen und organisatorischen Maßnahmen geeignete Sicherheitsvorkehrungen dar, um den mit Online-Banking verbundenen Gefahren vorzubeugen. Das Thüringer Oberlandesgericht wurde vom TJM gebeten, bis 30. Juni 2004 einen diesbezüglichen Erfahrungsbericht zu erarbeiten, auf dessen Grundlage die noch vorläufigen Regelungen zum Online-Banking in der o. g. Verwaltungsvorschrift unter Berücksichtigung möglicher Änderungen aufgenommen werden.

Da diese Thematik bundesweite Bedeutung hat und zu erwarten ist, dass künftig auch andere Verwaltungsbereiche solche Verfahren nutzen werden, befasst sich eine Arbeitsgruppe des AK Technik der DSB mit der Erarbeitung einer Orientierungshilfe für den Einsatz von IT bei Gerichtsvollziehern. Ziel ist, einheitliche Standards für ein sicheres Online-Homebanking zu formulieren. Zu gegebener Zeit werde ich über diese Orientierungshilfe und weitere Erfahrungen berichten.

15.10 Datenschutzrechtliche Risiken bei der Aktualisierung von Software

Jede bei einem IT-Verfahren zum Einsatz kommende Betriebs- und Anwendungssoftware erfordert im Laufe ihres Lebenszyklus eine Überarbeitung seitens der Hersteller, um neuen gesetzlichen oder technischen Anforderungen Genüge zu leisten. Die geänderten Versionen werden dem Anwender auf einem Datenträger (Diskette, CD, DVD) oder über das Internet zur Installation auf den hier vorgehaltenen IT-Systemen zur Verfügung gestellt. Dazu ließen sich bisher die Nutzer beim Hersteller der Software registrieren und erhielten die neuesten Versionen auf entsprechenden Datenträgern automatisch durch die Post zugeschickt. Dieser Vorgang einschließlich der Installation der neuen Softwareversion durch den Anwender wird als Update bezeichnet. Im Zuge der wachsenden technischen Möglichkeiten auf dem Gebiet der Informations- und Kommunikationstechnologie werden zunehmend seitens der Hersteller solche Updates über das Internet den Anwendern zur Verfügung gestellt. Der Anwender lädt

das entsprechende Update-Produkt von dem Webserver des Herstellers auf seinen PC herunter (Download), und verteilt dieses Produkt, wenn erforderlich, auf die verschiedenen IT-Geräte, um die entsprechenden Installationen der neuen Software vorzunehmen. Diese Verfahrenstechnologie erfolgt oft schon seitens des Anwenders in automatisierten Schritten, ist zumeist kostengünstiger und weist auch hinsichtlich der Verfügbarkeit und Aktualität wesentliche Vorteile auf, die auch von den Anwendern geschätzt werden. Beide Verfahrenstechnologien zeichnen sich dadurch aus, dass das Update-Verfahren unter der Kontrolle des Anwenders/Administrators erfolgt. Er ist der Herr des Verfahrens, welches erst durch seine Aktivitäten ausgelöst wird.
In letzter Zeit wird zunehmend von weltweit agierenden Softwareherstellern angeboten, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf den Rechner des Anwender zu laden und diese gleichzeitig automatisch zu installieren. Die auf den ersten Blick für den Anwender bequeme und anscheinend komfortable Verfahrenstechnologie birgt jedoch nicht unerhebliche Datenschutzrisiken in sich. Ein solcher Update-Vorgang wird ausschließlich durch den Software-Hersteller gesteuert, der hierbei auf den Rechner des Anwenders zugreift. Dabei werden zunehmend - oftmals vom Anwender unbemerkt oder zumindest nicht transparent - Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt. Darüber hinaus bewirken solche Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann i. d. R. ohne die erforderlichen Tests und Freigabeverfahren genutzt werden. Leider ist hierbei nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Insbesondere das unbemerkte Update wird dann nicht immer als Fehlerursache erkannt. Die derzeit angebotenen Verfahren zum automatischen Software-Update entsprechen nicht den Anforderungen des deutschen Datenschutzrechts. Deshalb wenden sich die DSB des Bundes und der Länder in einer Entschließung zum automatischen Software-Update vom 7. August 2003 entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen (Anlage 19). Nicht nur für die geschäftliche Datenverarbeitung auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit Risiken für den Schutz der Privatsphäre verbunden. Wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nut-

zerinnen und Nutzer gefährdet wird, wird den Erfordernissen des Datenschutzes nicht ausreichend Rechnung getragen. Die DSB fordern u. a. die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen. Diese Verfahren sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher erfolgt. Eine Übermittlung personenbezogener Daten an die Hersteller ist nur dann erlaubt, wenn ihr Verwendungszweck vollständig bekannt ist und der Anwender in die Verarbeitung ausdrücklich eingewilligt hat.

Der TLfD wies in diesem Zusammenhang die öffentlichen Stellen des Freistaates darauf hin, dass Änderungen an der Softwareausstattung und Konfiguration nur in Abstimmung bzw. mit Kenntnis der Systembetreuung vorzunehmen sind. Ansonsten wird gegen die gesetzlich vorgegebenen Sicherheitsziele verstoßen. Gemäß § 9 Abs. 2 ThürDSG haben die öffentlichen Stellen unter anderem zu gewährleisten, dass

- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
- die Verfahrensweise bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

Updates dürfen deshalb nur im Rahmen eines auch aus datenschutzrechtlicher Sicht geregelten Verfahrens eingespielt werden. Basis für eine solche Regelung ist, dass die Anwender zunächst darüber informiert sind, welche Daten im Rahmen des Updates übermittelt und ggf. gespeichert werden und in welchem Umfang Rückschlüsse auf die Hard- und Softwareausstattung sowie die Konfiguration eines IT-Systems und auf einzelne anonyme oder konkrete Benutzer möglich ist. Bei den o. g. automatisierten Online-Updates besitzen die Software-Hersteller i. d. R. eine unbeobachtete Eingriffsmöglichkeit auf die IT-Systeme, da der Administrator des Systems die Updates weder zuvor prüfen noch freigeben kann. Insofern ist für IT-Systeme, die personenbezogene Daten verarbeiten, der Einsatz solcher automatischer Updates nicht zulässig. Sie sind zumindest mit Zugriffen auf IT-Systemen verbunden, die eine Änderung an automatisierten Verfahren oder der auf ihnen basierenden Betriebssysteme ermöglichen. Ein solcher Zugriff ist aber nur durch ausdrücklich hierzu berechtigte Personen zulässig. Es handelt sich hierbei um eine Wartung oder

Fernwartung automatisierter Datenverarbeitungsanlagen und soweit ein Zugriff auf personenbezogene Daten hierbei nicht sicher ausgeschlossen werden kann, liegt eine Auftragsdatenverarbeitung gemäß § 8 ThürDSG vor. Danach ist der Auftrag schriftlich zu erteilen, wobei auch die technischen und organisatorischen Maßnahmen festzulegen sind, von deren Einhaltung sich der Auftraggeber zu überzeugen hat.

15.11 Vertrauenswürdige Informationstechnik

Auf ihrer 65. Konferenz am 27./28. März 2003 in Dresden forderten die DSB des Bundes und der Länder in einer Entschließung eine vertrauenswürdige Informationstechnik (Anlage 10). Insbesondere kann dieses Vertrauen durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Um dieses Ziel zu erreichen, sollten die Anwender ihre Sicherheitsanforderungen präzise definieren sowie Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Dazu wollen die DSB des Bundes und der Länder den Herstellern und Anwendern von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen. So werden vorab schon zwei Schutzprofile angeboten, mit denen die Anwender ihre datenschutzspezifischen Anforderungen für IT-Produkte im Gesundheitswesen, eGovernment, Tele- und Mediendienste sowie E-Commerce spezifizieren können.
Der o. g. Entschließung der DSB liegen folgende Gegebenheiten zu Grunde:
Für den Anwender wird es immer schwieriger, die für seine IT eingesetzten Hard- und Softwareprodukte sicherheitstechnisch zu bewerten. Die Komponenten moderner informationstechnischer Systeme sind mittlerweile so komplex, dass eine Beurteilung, inwieweit die eingesetzten IT-Produkte tatsächlich die anwenderspezifischen Sicherheitsvorgaben erfüllen, umfangreiche Spezialkenntnisse erfordert.
Erfahrung und Praxis zeigen, dass absolute Sicherheit i. d. R. nicht erreichbar ist. Demzufolge ist es wichtig festzustellen, welches Maß an Sicherheit ein IT-Produkt realisiert. Für die Prüfung und Bewertung (Evaluation) der Sicherheit von IT-Systemen wurden deshalb zunächst nationale und in letzter Zeit internationale Kriterienkataloge entwickelt. Die ältesten Kriterien zur Bewertung von IT-Systemen sind die TCSEC (Trusted Computer System Evaluation Criteria), die 1980 in den USA entwickelt worden. Seit 1991 stehen die europäi-

schen ITSEC (Information Technology Security Evaluation Criteria) als harmonisierte Kriterien der Länder Deutschland, Großbritannien, Frankreich und Niederlande zur Verfügung. Beide Kriterien bildeten die Ausgangsbasis für die seit 1999 in der Version 2.1 vorliegenden CC (Common Criteria), gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik.
Mit diesen steht jetzt ein international anerkanntes Bewertungsschema zur Verfügung, um die Sicherheit verschiedener IT-Systeme oder Komponenten, die eine vergleichbare Funktionalität besitzen, anhand eines einheitlichen Maßstabes zu bewerten. Gleichzeitig dienen diese Kriterien den IT-Herstellern als Leitlinien zur Entwicklung und Konstruktion sicherer IT-Systeme. Eine Evaluierung der hergestellten Produkte erfolgt durch unabhängige Stellen, in Deutschland z. B. durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein, die entsprechende Zertifikate ausstellen. Mit dem Zertifikat werden bestimmte Sicherheitseigenschaften beglaubigt. In einem Zertifizierungsbericht werden die Sicherheitseigenschaften des Evaluierungsgegenstandes relativ zu den aufgeführten Bedrohungen beschrieben, die Wirksamkeit der eingesetzten Sicherheitsmechanismen bewertet und mit der Vergabe einer Evaluierungsstufe der Grad des Vertrauens in die Korrektheit der Funktionalität des Produkts bescheinigt. Außerdem werden hier detailliert die konkreten Einsatzbedingungen aufgezeigt, unter denen die festgestellten Sicherheitseigenschaften wirksam sind. Weiterhin werden neben Angaben zur Installation des Produktes auch erkannte Schwachstellen sowie mögliche Gegenmaßnahmen dargelegt. Im Ergebnis erhalten Anwender weltweit verlässliche Aussagen über die Sicherheitsleistung von IT-Systemen bzw. deren Komponenten.

Die CC bieten die Möglichkeit, die Sicherheitsanforderungen eines Produktes unabhängig von dessen Einsatzumgebung in so genannten Protection Profiles (Schutzprofile) zu beschreiben. Diese Schutzprofile werden nicht vom Hersteller eines Produktes, sondern von dem Anwender definiert und erstellt. Sie sind somit benutzer- und nicht produktorientiert. Damit haben Anwender die Möglichkeit, ihren Sicherheitsbedarf mit Hilfe von Schutzprofilen in Form von maßgeschneiderten IT-Sicherheitskonzepten darzulegen und zu definieren. So können bspw. bestimmte Interessenverbände ihre Vorstellungen im Hinblick auf die Sicherheit bestimmter IT-Produktgruppen (wie Firewalls, Chipkarten) in Form von Schutzprofilen ausdrücken.

Die Anforderungen zur Funktionalität und zur Vertrauenswürdigkeit, die in den Schutzprofilen für den Evaluierungsgegenstand spezifiziert werden, werden aus einem in den CC enthaltenen Katalog entnommen. Aus datenschutzrechtlicher Sicht ist hierbei von besonderem Interesse, dass in diesem Katalog erstmalig auch Anforderungen zum Schutz der Privatsphäre, wie Anonymität und Unbeobachtbarkeit, aufgeführt sind. Mit den CC können somit auch datenschutzspezifische Anforderungen an IT-Produkte beschrieben werden.

Im Auftrag des AK Technik der DSB des Bundes und der Länder beschäftigte sich eine Arbeitsgruppe mit dem Ziel, eine Basis für das Erstellen von Schutzprofilen zu erarbeiten. Aktive Unterstützung leistete hierbei das BSI. Im Auftrag des BfD erarbeitete auf Grundlage dieser Ergebnisse das Deutsche Forschungszentrum für Künstliche Intelligenz die in der o. g. Entschließung genannten zwei Schutzprofile „Benutzerbestimmbare Informationsflusssicherheit (BISS)“ für Single-User und Multi-User. Die Profile sind vom BSI zertifiziert. Sie haben aus der Sicht der Anwender die Aufgabe, alle Informationsflüsse innerhalb eines IT-Systems aber auch den Versand oder Empfang von E-Mails transparent zu kontrollieren. Dies wird durch eine regelbasierte und systemübergreifende Informationsflusssteuerung erreicht, womit desweiteren die Anwender zum Teil auch von Pflichten zur Einhaltung von Sicherheitsauflagen entlastet werden. Es geht bspw. um den Schutz von Daten, die einen Sicherheitsbedarf in Bezug auf die Aspekte Vertraulichkeit, Integrität und/oder Authentizität unterliegen. Diese Sicherheitsleistung ist eine sinnvolle Ergänzung zu herkömmlichen Sicherheitskomponenten wie etwa Zugriffsschutz, Übertragungsschutz, Netzabsicherung etc. Entsprechend dem Schutzbedarf der Daten können unterschiedliche Kombinationen von Sicherheitsmechanismen eingesetzt werden. Dazu wird für jeden Informationsfluss mittels Regeln die erforderliche Sicherheit bestimmt. So wird bspw. die Integrität der Daten durch elektronische Signatur, ihre Vertraulichkeit durch Verschlüsselung und die Authentizität durch elektronische Zertifikate gewährleistet. Gegenüber herkömmlichen Sicherheitsstrategien wird mit BISS eine durchgängige Sicherheit über alle beteiligten Systeme hinweg erzielt. So ist eine integrierte Realisierung sowohl für Betriebssysteme, Datenbanksysteme, E-Mail-Clients und -Server möglich.

15.12 Datenschutzaspekte beim Trusting Computing Platform Alliance (TCPA)

Trusted Computing Platform Alliance (TCPA) ist eine Alliance international führender Unternehmen der Computerindustrie mit dem Ziel, einen Standard für eine Hardware-Sicherheitsplattform zu entwickeln. Gründungsmitglieder der TCPA sind Firmen wie Compaq/Hewlett Packard, IBM, Intel und Microsoft. Mittlerweile umfasst TCPA weltweit rund 200 Firmen.
Geplant ist in die Rechner - später eventuell in die Prozessoren - ein Hardware-Sicherheitsmodul, das so genannte TPM (Trusted Platform Modul) zu integrieren. Dieser TPM kann z. B. eingesetzt werden, um Benutzer zu identifizieren, Verschlüsselungen zu erzeugen und Zertifikate zu nutzen und zu verifizieren. Zusätzlich kann es durch Überwachung des Bootvorgangs auf Anfrage einen vertrauenswürdigen Zustand des Rechners attestieren und Manipulationen an der Rechnerkonfiguration oder am Betriebssystem ausschließen[1]. Von der neuen Technologie erhoffen sich Anbieter urheberrechtlich geschützter digitaler Inhalte eine deutliche Verbesserung der Durchsetzbarkeit ihrer Nutzungs- und Verwertungsrechte, z. B. indem eine illegale Nutzung und Verbreitung geschützter Inhalte hiermit verhindert wird.
Microsoft bspw. unterstützt diese Zielstellung mit dem „Palladium"-Konzept, mittlerweile als „NGSCB" (Next Generation Secure Computing Base) bezeichnet, welches auf TCPA aufsetzt und zusätzliche Sicherheitsfeatures bereitstellt.

Auch aus datenschutzrechtlicher Sicht besteht Verständnis für die berechtigten Forderungen der Softwarehersteller, kostenpflichtige Software nur gegen Entgeltleistung zu nutzen. Allerdings bedarf es darüber hinaus Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen.
Die DSB des Bundes und der Länder betrachten deshalb die Pläne zur Entwicklung zentraler Kontrollmechanismen und Infrastrukturen auf der Basis der Spezifikationen der Industrie-Alliance „TCPA" mit einer gewissen Skepsis.
Anwender müssen sich beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit einer solchen externen Instanz verlassen können. Es ist z. B. untragbar, wenn

[1] Bundestags-Drucksache 15/795 vom 07.04.2003

- Nutzer die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,
- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,
- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann,
- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden können.

Die DSB des Bundes und der Länder haben deshalb im März 2003 bei der 65. DSB-Konferenz in der Entschließung „TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden“ Hersteller von Informations- und Kommunikationstechnik aufgefordert, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,
- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und
- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden (Anlage 11).

15.13 Orientierungshilfe „Datenschutz bei Windows XP“

Die Betriebssysteme Windows XP Home Edition (für Privatanwender) und Windows XP Professionell (für Unternehmen) sind seit Oktober 2001 als Nachfolgerversionen von Windows 2000, 95, 98 und ME auf dem Markt.

Öffentliche Stellen, die die Wahl zwischen dem Einsatz der Windows XP Home Edition oder Windows XP Professionell haben, sollten

Windows XP Professionell den Vorrang einräumen, weil hier neue Sicherheitsmechanismen wie bspw.:

- die Verschlüsselung von Dateien und Ordner auch für mehrere Benutzer,
- Analysefunktionen für Angriffe, Firewallfunkionen,
- und die automatische Konfiguration sicherheitsrelevanter Einstellungen

bereitgestellt werden.
In einer Orientierungshilfe „Datenschutz bei Windows XP Professionell" erläutert der AK Technik der DSB des Bundes und der Länder wesentliche Sicherheitsaspekte des Betriebssystems und gibt Hinweise wie bestimmte sicherheitsrelevante Einstellungen vorgenommen werden können.
Ausgehend von der Betrachtung, was neu bei Windows XP ist und welche Vor- und Nachteile dieses Betriebssystem aufweist, geht die Orientierungshilfe neben allgemeinen Installationshinweisen auf die Sicherheit im Netzwerk ein. Auch interne Sicherheitsmechanismen und der Einsatz von Smart-Cards, deren Unterstützung direkt im Betriebssystem integriert ist, der Windows-Dateischutz, welcher das Überschreiben von geschützten Systemdateien verhindert oder das Verschlüsseln von Dateien und Ordnern mit EFS (Encrypting File System), um Daten auf der Festplatte vor unbefugtem Zugriff zu schützen, werden dargelegt.
Am Schluss der Orientierungshilfe werden Sicherheitsempfehlungen gegeben, einschließlich Verweise auf Webseiten, wo die Sicherheit eines Systems getestet werden kann.
Die Orientierungshilfe steht im Internet beim Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern als Vorsitzender des AK Technik unter www.lfd.m-v.de zur Verfügung.

15.14 Zum Einsatz kryptographischer Verfahren

Mit dem Einsatz kryptographischer Verfahren können wesentliche datenschutzrechtliche Forderungen zum Schutz elektronisch gespeicherter oder zu übermittelnder personenbezogener Daten angemessen realisiert werden. Sie sind besonders geeignet, um eine unberechtigte Kenntnisnahme von Daten zu verhindern sowie Manipulationen und Übertragungsfehler nachzuweisen. Desweiteren kann der Nachweis der Urheberschaft der Daten beweissicher gestaltet werden. Dies ist insbesondere erforderlich für moderne Kommunikationsverfahren, bei denen die Daten/Informationen/Dokumente über öffentliche Netze

versandt werden. Hier können die Daten während der Übertragung von Unberechtigten gelesen (Verlust der Vertraulichkeit) und verändert (Verlust der Integrität) werden. Weiterhin kann mit falschen Absenderangaben gearbeitet werden, sodass der Ursprung (Authentizität) der Nachricht nicht gesichert ist und somit auch die Urheberschaft geleugnet werden kann. Durch den Einsatz kryptographischer Verfahren ergeben sich Maßnahmen zur Sicherung der Vertraulichkeit, Integrität und Verbindlichkeit der zu verarbeitenden Daten. Zur Lösung dieser Sicherheitsfragen gibt es zwei grundlegende Mechanismen, die Verschlüsselung und die elektronische Signatur. Mit ersterer wird eine unbefugte Kenntnisnahme der Daten verhindert, mit letzterer wird eine Kontrolle der Integrität sowie die Authentizität der Daten als auch des Urhebers abgesichert. Authentizität und Integrität stellen die Voraussetzungen zur (Rechts-)Verbindlichkeit dar. Diese Rechtsverbindlichkeit wird zum einen ermöglicht durch das am 1. August 2001 in Kraft getretene „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr“, welches die Forderung der EU einer Gleichstellung elektronischer Signaturen mit handschriftlicher Unterschrift berücksichtigt. Die technische Grundlage hierfür bildet das seit dem 22. Mai 2001 in Kraft getretene „Gesetz über Rahmenbedingungen für elektronische Signaturen“ (Signaturgesetz). Sofern ein Dokument mit einer im Signaturgesetz definierten und als qualifiziert bezeichneten elektronischen Signatur versehen ist, wird nach dem neuen § 126a BGB die Möglichkeit des Ersetzens der Schriftform durch die elektronische Form vorgesehen. Damit sind die rechtlichen Rahmenbedingungen vorhanden, um einen sicheren elektronischen Rechts- und Geschäftsverkehr abzuwickeln. Der Einsatz von kryptographischen Verfahren beschränkt sich aber nicht auf die bisher dargelegten Tätigkeitsfelder. Kryptographische Verfahren werden auch für eine sichere Identifikation und Authentifizierung von Benutzer und IT-Systemen eingesetzt. In den vorangegangenen Tätigkeitsberichten wurde schon mehrfach ausführlich über die Arbeitsweise, den Einsatz und den Funktionsumfang von kryptographischen Verfahren als auch über die aktuellen rechtlichen Grundlagen dazu berichtet (2. TB, 15.7, 15.8; 3. TB, 15.9; 4. TB, 15.7, 15.8). Jetzt liegt eine Orientierungshilfe zum Einsatz kryptographischer Verfahren vor, die von einer Arbeitsgruppe des Arbeitskreises für technische und organisatorische Fragen des Datenschutzes der Konferenz der DSB des Bundes und der Länder erarbeitet wurde. Sie gibt insbesondere Hilfestellung für die Frage, welche kryptographischen Methoden, Verfahren und Produkten in unterschiedli-

chen Szenarien der Informationsverarbeitung und Kommunikation unter den Aspekten der Wirksamkeit und der Wirtschaftlichkeit der Vorzug zu geben ist. Sie richtet sich auch an die DSB in Bund und Ländern, um sie bei ihrer Beratungstätigkeit zu unterstützen. Ausgehend von den Schutzzielen des Datenschutzes, werden die technischen Grundlagen der Kryptographie, die Grundszenarien für den Einsatz kryptographischer Verfahren sowie allgemeine Lösungsansätze zur technischen Realisierung aufgezeigt. Desweiteren werden anhand von ausgewählten Infrastrukturen und ausgesuchten Anwendungsfällen für die hier auftretenden Sicherheitsprobleme Lösungswege beschrieben. Die Orientierungshilfe ist über die Internetadresse des TLfD www.datenschutz.thueringen.de unter „Veröffentlichungen“ abrufbar.

15.15 Datensicherheit beim Anschluss externer Speicher an der USB-Schnittstelle von IT-Geräten

Seit einiger Zeit werden Personalcomputer mit Buchsen für den Universal Serial Bus (USB) ausgestattet, die dem einfachen Anschluss verschiedener Hardwarekomponenten wie Disketten-, DVD- oder CD-ROM-Laufwerke, transportable Festspeicher-Medien oder Netzwerk-Hardware dienen.
Über USB anschließbare Speichermedien stellen ein erhebliches Sicherheitsrisiko dar. Der unkontrollierte Einsatz von USB-Schnittstellen kann die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten bedrohen. Da moderne Betriebssysteme die neu angeschlossenen Geräte i. d. R. ohne zusätzliche Softwareinstallation sofort erkennen und einbinden, besteht die Gefahr, diese Schnittstellen auch für nicht freigegebene dienstliche oder private Technik zu nutzen.
Die im Handel erhältlichen USB-Sticks in der Größe eines Schlüsselanhängers, die über nicht flüchtige Speicher in verschiedensten Größenordnungen (z. B. 32 MB, 516 MB oder 2 GB) verfügen, werden vom Betriebssystem wie Festplatten angesprochen. Sie ermöglichen neben dem Speichern von Daten, den Zugriff auf mitgebrachte private Daten sowie das Ausführen auch von unerlaubten, nicht freigegebenen Betriebssystemen und Anwendungsprogrammen, mit denen auch Sicherheitsmechanismen unterlaufen werden können.

Den genannten Risiken bei der Nutzung von USB-Peripherie stehen aber auch Vorteile für die Datensicherheit gegenüber. So ist es bspw.

sinnvoll, besonders vertrauliche Datenbestände auf Memory-Sticks oder USB-Festplatten zu speichern.
Sollte auf ihnen vertrauenswürdige Daten abgespeichert werden, so sind derzeit der Einsatz von Verschlüsselungssoftware oder auch USB-Sticks mit biometrischen Identifikationssystemen incl. Hardwareverschlüsselung geeignete Mittel, um nur Befugten den Zugriff auf die Daten zu gewährleisten (Vertraulichkeit).

Da USB-Controller in den PCs kaum noch abgeschaltet werden können, ohne die Funktionalität wesentlich einzuschränken, kann der Zugriffsschutz folglich nur über die Konfiguration des USB-Protokollstacks oder über allgemeine Zugriffsmechanismen des Betriebssystems realisiert werden. Darüber hinaus muss das Booten von USB-Geräten im BIOS abgeschaltet werden, wie dies schon von fest eingebauten Laufwerken her bekannt ist.
Mit den Bordwerkzeugen von Windows kann der Zugriff auf USB-Geräte nicht auf einfache Weise verhindert werden. Jedoch kann mit moderatem zusätzlichen Aufwand die Installation nicht zugelassener Gerätetypen erkannt und blockiert werden. Entsprechende Skripte oder kommerzielle Produkte sind hierfür erforderlich.
Auch unter Linux ist es mit geringem bis moderatem Aufwand möglich, den Zugriff auf ausdrücklich benannte Geräteklassen oder -typen zu beschränken. Die dazu nötigen Schritte lassen sich zumeist aus der Dokumentation zum USB-Subsystem ableiten. Wer auf welche Geräte zugreifen darf, kann über die Zugriffsrechte auf die entsprechenden Gerätedateien festgelegt werden.

Der Arbeitskreis technische und organisatorische Datenschutzfragen der DSB des Bundes und der Länder hat in der Orientierungshilfe „Datensicherheit bei USB-Geräten diesbezügliche Lösungsansätze hinsichtlich der Betriebssysteme Windows und Linux aufgezeigt“ (im Internet unter www.lfd.m-v.de abrufbar).

15.16 Sicherheitsaspekte drahtloser Netze (WLANs)

WLANs (Wireless Local Array Networks) -drahtlose lokale Netze- ermöglichen eine Rechner-Kommunikation per Funk, ohne lästige Kabel und unabhängig von einem festen Standort. Sie sind sowohl für den Einsatz im Freien als auch in Gebäuden geeignet und zeichnen sich insgesamt durch eine hohe Flexibilität aus. Auch öffentliche Stellen des Freistaates Thüringen erwägen einen Einsatz dieser Technik,

die weltweit einen rapiden Zuwachs aufweist. Mit dem Einsatz von WLANs, die Funksignale als Transportmedium und nicht wie konventionelle LANs als Signalträger ein geschirmtes Kabel benutzen, sind allerdings auch höhere Risiken für die Sicherheit der übertragenen Daten verbunden. Die Absicherung von Funknetzen ist wesentlich schwieriger als die von drahtgebundenen Netzwerken. Der Übertragungsweg ist grundsätzlich nicht gegen unbefugtes Mithören geschützt. Auch eine benutzerbezogene Zugangskontrolle ist problematisch.

Funktionsweise von WLANs

Mit einer Funknetzkarte (WLAN-Karte) ausgerüstete mobile IT-Geräte aber auch Desktop-PCs werden drahtlos an ein bestehendes verkabeltes lokales Netzwerk (LAN) angebunden oder bilden die Basis eines neuen Netzes. Mit dem Versenden spezieller Datenpakete ermitteln die drahtlosen IT-Geräte automatisch, ob innerhalb ihrer Reichweite sich ein anderer drahtloser Rechner oder ein Access-Point (Basisstation/zentraler Funkknoten) befindet, in dem dieser den Empfang der Pakete bestätigt. So genannte IEEE (Institut of Electrical and Electronic Engeneers)-Standards sichern dabei eine einheitliche Technologie sowie die Kompatibilität der Geräte untereinander.

WLANs können sowohl zentral als auch dezentral ausgerichtet sein. Zentralisierte WLANs bestehen aus einem Access-Point, über den der komplette Datenverkehr läuft und mit dem die drahtlose Kommunikation der Computer untereinander verwaltet sowie die Zugriffe kontrolliert und gesteuert werden können. Über einen Access-Point kann auch das Funknetz mit einem verkabelten Netzwerk verbunden werden. Der Access-Point als zentraler Koordinator und die ihm untergeordneten in das Netzwerk eingebundenen weiteren Sende- und Empfangsstationen bilden eine Einheit, die man Zelle nennt. Die WLAN-Kommunikation findet innerhalb der Funkzellen statt. Der Radius einer Funkzelle hängt von der Sendeleistung der Geräte sowie von den Umgebungsbedingungen (wie Wände, örtliche Lage) ab, wobei ein Gerät einen Radius von 50 bis 300 Metern abdeckt. Durch eine Überlappung von mehreren Funkzellen ist ein reibungsloser Übergang mit einem mobilen Endgerät von Zelle zu Zelle möglich (Roaming-Verfahren). Durch die Roaming-Möglichkeiten der WLAN-Technik eröffnen sich auch viel sagende Perspektiven für öffentliche Angebote. So wird diese Technik auch zunehmend an stark frequentierten Orten, so genannten Hotspots wie Flughäfen, Bahnhöfen, Hotels, im Bereich größerer Städte oder bei Informationsveranstaltungen einge-

setzt. Nutzer mit mobilen IT-Endgeräten (z. B. Laptops, PDAs und Mobiltelefone) können sich hier ad-hoc über einen Access-Point drahtlos ins Internet einwählen, auf ihr eigenes LAN zugreifen oder E-Mail-Dienste nutzen. Mit mehreren Access-Points lassen sich zudem größere Netze aufbauen. Die Funkverbindung bleibt dabei nicht nur auf das lokale Netzwerk beschränkt. So lassen sich über ein entsprechendes Antennensystem auch Reichweiten von mehreren Kilometern überbrücken.
Dezentrale WLANs (ad-hoc-Modus) besitzen keine Basisstation, die den Zugriff kontrolliert. Hier kann jede Station im Netzwerk grundsätzlich mit jeder anderen Station im Netzwerk direkt Daten austauschen.
Basistechnologien für Funk-LAN sind bspw. neben WLAN nach dem Standard IEEE 802.x auch die Bluetooth-Technik. Beide Technologien basieren auf verschiedenen Grundlagen. Obwohl für unterschiedliche Einsatzzwecke vorgesehen, sind sie kombinierbar und können sich ergänzen. Der Anwendungsbereich von Bluetooth beschränkt sich dabei vorwiegend auf die kabellose Anbindung von peripheren Geräten, z. B. für eine Funk-Verbindung von Tastatur, Maus, Drucker und Scanner mit dem Computer oder zur Kommunikation eines Handys mit der Freisprecheinrichtung. Bluetooth-Sender reichen lediglich 10 Meter weit.
Das IEEE-Protokoll 802.11b stellt derzeit die verbreitetste WLAN-Gruppe dar, mit dem ein Datendurchsatz bis zu 11 MBit/s (netto bis zu 5 MBit/s) erzielt wird. Derzeit stehen schon Standards (IEEE 802.11a/g) bis zu 52 MBit/s Technologie zum Einsatz an.

Risiken beim Einsatz von WLANs
Hauptangriffspunkt bei WLANs sind - technisch bedingt - die Funkwellen, mit denen die Daten übertragen werden. Sie sind quasi von jedermann zu empfangen, der über einen mobilen PC mit Funknetzkarte verfügt und sich im Einzugsbereich einer Funkzelle des Netzwerks befindet. Selbst bei einer Installation innerhalb eines Gebäudes, sind diese Funksignale auch noch in der weiteren Umgebung zu empfangen. Soweit der Datenverkehr nicht verschlüsselt erfolgt, kann er somit leicht ausgeforscht und mitgeschnitten werden.
Desweiteren ist potenziell die Gefahr gegeben, über WLANs unter Ausnutzen von Sicherheitslücken in angeschlossene lokal verkabelte Netzwerke einzudringen.
Von Bedeutung für eine sicherheitstechnische Einschätzung können auch die nachfolgenden Aspekte sein. Gegenüber verkabelten PC-

Netzen ist in einem WLAN eine Eingrenzung der teilnehmenden mobilen Clients von vornherein kaum möglich. Jeder der sich im Empfängerbereich befindet, ist ein potenzieller Teilnehmer. Auch ohne bewusste Absicht lassen sich ungeschützte WLANs aufspüren, indem unvermutet eine Verbindung hergestellt wird. Zumeist sind die Clients auch der unmittelbaren Kontrolle der Systemadministration entzogen. Ein nicht geringes Risiko stellen mögliche Datei-Freigaben dar, die vom Benutzer über das Betriebssystem des Client erfolgen können. Dabei besteht die Gefahr, dass auch weitere WLAN-Teilnehmer auf die hier gespeicherten Daten zugreifen können. Auch die Verfügbarkeit des WLAN kann durch Stören der Funksignale beeinträchtigt werden.
Unzulängliche Sicherungsmaßnahmen beim Einsatz von drahtlosen Computernetzwerken wurden in der öffentlichen Berichterstattung schon wiederholt kritisiert. So wurden vielerorts keine der seitens der Hersteller implementierten Sicherheitsmaßnahmen aktiviert, um zumindest einen minimalen Schutz des WLAN und der Daten zu gewährleisten.
Neben Hackern nutzen Sicherheitslücken auch andere Angreifer, so genannte Wardriver, die mit Notebook oder Pocket-PC sowie einer Dachantenne durch besiedelte Gebiete fahren und offene Netzwerke orten, um über diese kostenlos ins Internet zu gelangen.

Vorhandene Sicherheitsmechanismen und Schwachstellen
Das Standardprotokoll für WLAN (802.11x) beinhaltet Mechanismen zur Datensicherheit. Diese sind allerdings i. d. R. nicht standardmäßig eingeschaltet, sondern müssen vom Benutzer einzeln aktiviert werden. Die Mechanismen zielen darauf ab, einen kontrollierten Zugang in das WLAN zu ermöglichen sowie die Vertraulichkeit und die Integrität der Datenkommunikation zu wahren. Die derzeit standardmäßig vorhandenen Sicherheitsmechanismen weisen allerdings Schwachstellen auf, sodass sie für eine Verarbeitung sensibler Daten keinen ausreichenden Schutz bieten.
Im Einzelnen stehen folgende Sicherheitsmechanismen zur Verfügung:
- Definition einer eindeutigen Gruppenidentität über den Netzwerknamen SSID,
- Client-Identifikation über MAC-Adresse,
- Einsatz des Protokolls WEP.

Eine mögliche Zugangskontrolle basiert auf dem WLAN-Netzwerknamen SSID (Service Set Identifier), der im Standard 802.11

spezifiziert ist. Dieser dient zur Unterscheidung mehrerer WLANs und kann vom Betreiber gewählt werden. Er wird vom Access-Point in regelmäßigen Intervallen gesendet, sodass jeder Client mit der Einstellung SSID „any“ sich hier anmelden kann. Um einen kontrollierten Zugang zu ermöglichen, muss das Aussenden der SSID am Access-Point unterdrückt werden. Damit soll der Zugang nur den Clients ermöglicht werden, die über die SSID verfügen.

Eine weitere Kontrolle des Zugangs erfolgt anhand der WLAN-Karte des zugreifenden Clients. Jede Funkkarte besitzt eine eindeutige, so genannte MAC-Adresse (Media Access Control), die auch in der Zugangsliste (Access Control List) im dazugehörigen Access-Point eingetragen werden muss, soweit ein mit dieser Karte ausgestatteter Client Zugriff erhalten soll. Beim Aufbau der Verbindung eines Client zum Access-Point wird zur Kontrolle die Adresse der WLAN-Karte mit dem auf dem Access-Point in der Liste gespeicherten zugangsberechtigten MAC-Adressen abgeglichen. Clients mit einer WLAN-Karte, deren MAC-Adresse nicht in der ACL eingetragen ist, werden abgewiesen.
Beide o. g. Kontrollmechanismen weisen insofern Schwachstellen auf, als sie zur Identifizierung Merkmale verwenden, die nicht ausschließlich dem Einflussbereich des jeweiligen Nutzers unterliegen. So ist die SSID eine Gruppenkennung. Die Gefahr einer Weitergabe über den Nutzerkreis hinaus ist somit nicht unwahrscheinlich. Aber auch bei der unverschlüsselten Übertragung der SSID vom Client zum Access-Point kann diese abgefangen werden.
Eine sichere Identifikation zugangsberechtigter Clients ist auch anhand der MAC-Adresse nicht möglich. Auch die MAC-Adressen der aktiven Client werden wie die SSID unverschlüsselt übertragen, können abgehört und zur Manipulation der eigenen MAC-Adresse missbraucht werden. Desweiteren kann nicht ausgeschlossen werden, dass ein Nutzer seine zugangsberechtigte Funkkarte einem nicht Zugangsberechtigten zur Verfügung stellt.
Eine weitaus sichere Zugangskontrolle wird durch eine persönliche Authentifizierung der Nutzer erzielt. Dies wird über die Einbindung eines Authentifizierungsserver (wie RADIUS oder Kerberos) ermöglicht. Im Standard IEEE 802.1x ist hierfür das vom Funk unabhängige Transportprotokoll EAPoL (Extensible Authentication Protocol over LAN) definiert. Erst wenn der Access-Point den Nutzer des Funkclients verifiziert hat, kann dieser mit dem Access-Point Daten austauschen und erhält Zugriff auf das dahinter liegende Netzwerk.

Um eine sichere Datenübertragung zwischen Client und Access-Point zu ermöglichen, ist im Standard IEEE 802.11 das WEP-Protokoll (Wired Equivalent Privacy) als Option definiert. Dieses Protokoll soll die Vertraulichkeit und die Integrität der Daten bei der Datenübertragung sowie die Authentifizierung der eingesetzten Clients absichern. Das WEP-Protokoll verwendet als Verschlüsselungsalgorithmus das Verfahren RC4. RC4 ist eine Stromchiffrierung mit variabler Schlüssellänge, die 1987 für RSA Data Security Inc. entwickelt wurde. Der Algorithmus ist bekannt, obwohl er nicht offiziell veröffentlicht wurde.
Die zu übertragenden Daten werden mit einem Schlüssel und einem zusätzlichen so genannten Initialisierungsvektor mit dem RC4-Algorithmus verschlüsselt. Für die Länge des Schlüssels stehen 40 Bit oder 104 Bit zur Verfügung. Der Initialisierungsvektor umfasst eine Länge von 24 Bit. So ergeben sich Schlüssellängen insgesamt von 64 Bit bzw. 128 Bit. Der Schlüssel ist auf allen zugelassenen Clients und Access-Points eingetragen und wird somit gemeinsam im WLAN genutzt. Jedes zu übertragende Datenpaket besitzt einen eigenen Initialisierungsvektor, der vor dem verschlüsselten Datenpaket unverschlüsselt übertragen wird. Auf der Empfängerseite werden mit dem gemeinsamen Schlüssel und dem unverschlüsselten Initialisierungsvektor die Daten dekryptiert, d. h. sie liegen wieder im Klartext vor.
Vor der Verschlüsselung des Datenpaketes wird über den Klartext eine Prüfsumme erzeugt, die an das Datenpaket angehangen und in die Verschlüsselung einbezogen wird. Anhand dieser Prüfsumme wird beim Empfänger die Integrität (Unversehrtheit) der übertragenen Daten geprüft. Fehlerhafte Datenpakete werden verworfen.
Für die Authentifizierung des Benutzerclients setzt WEP das so genannte Challenge-Response-Verfahren ein. Dazu wird am Access-Point eine Zufallszahl in der Länge von 128 Byte generiert und unverschlüsselt an den Client gesendet (Challenge). Hier wird die Zufallszahl mit dem gemeinsamen Schlüssel chiffriert und an den Access-Point zurückgesandt (Response), wo die Antwort entschlüsselt und mit der zuvor erzeugten Zufallszahl verglichen wird. Stimmen beide überein, wird von einer erfolgreichen Authentifizierung des Clients ausgegangen.
Auch das WEP-Protokoll weist Schwachstellen auf. So kann bspw. bei einem Verlust des Client der gemeinsame Schlüssel ausgelesen und kopiert werden. Die Speicherung des Schlüssels erfolgt je nach Hersteller auf der Funkkarte oder auf dem Client, oftmals nicht besonders abgesichert. So wird bspw. der Schlüssel auf dem Client in

der Windows Registry oder unter dem Betriebssystem Linux in einer Textdatei vorgehalten, teilweise sogar im Klartext. Wenn der WEP-Schlüssel eines WLANs offenbart ist, sind davon alle Nutzer des WLAN betroffen. In diesem Fall muss auf allen Clients und den Access-Point der Schlüssel neu eingetragen werden. Soweit kein automatisiertes Schlüsselmanagement hierzu vorgehalten wird, muss der Schlüsselwechsel manuell durchgeführt werden, was sehr mühsam ist. Ein weiterer Angriffspunkt stellt der nur 24-Bit lange Initialisierungsvektor dar. Nach Ablauf der 24 Bit-Kombinationen beginnen sich die Initialisierungsvektoren zu wiederholen. Durch Aufzeichnen der Datenströme können diese Wiederholungen ermittelt werden und über Abgleiche der Datenpakete der verwendete Schlüssel aufgedeckt werden. Entsprechende Tools hierzu werden über das Internet angeboten. Insofern bietet die WEP-Verschlüsselung nur einen begrenzten Schutz, insbesondere wenn sensible Daten übertragen werden. Auch das Authentisierungsprotokoll und die Prüfsumme weisen Schwachstellen für Angreifer auf.

Derzeit gibt es verschiedene Ansätze, um die Sicherheitslücken (gleicher Schlüssel für alle Stationen, kurzer Initialisierungsvektor) im WEP-Protokoll zu schließen. Dies erfordert Verfahren, die eine Rekonstruktion der sicherheitsrelevanten Parameter aus dem Funkverkehr durch eine starke Verschlüsselung und einem dynamischen Wechsel der Schlüssel verhindern. Der hierzu von der IEEE entwickelte WLAN-Standard wird voraussichtlich im Frühjahr 2004 verabschiedet. Wesentliche Teile dieses Standards werden schon derzeit als eine Sicherheitslösung unter dem Begriff WPA (Wireless Protocol Access) auf dem Markt angeboten. Hier handelt jeder Client bei der Anmeldung am Access-Point einen individuellen Schlüssel aus und der Initialisierungsvektor ist jetzt 48 statt 24 Bit lang. Desweiteren erfolgt nach Ablauf einer bestimmten Frist eine automatische Neuaushandlung des Schlüssels.

Datenschutzrechtliche Empfehlungen

Aus datenschutzrechtlicher Sicht ist zunächst zu prüfen, ob ein WLAN erforderlich ist. Wenn dies zutrifft, ist für die Einführung und den Betrieb des WLAN eine Sicherheitsrichtlinie notwendig. In dieser sind ausgehend von einer Bedrohungs- und Risikoanalyse die technischen und organisatorischen Sicherheitsmaßnahmen für dieses Netz und darüber hinaus sich hiermit noch ergebende weitere Maßnahmen zum Schutz des internen Netzes der Behörde oder des Unternehmens

aufzuführen. In der Sicherheitsrichtlinie müssen alle mobilen Zugänge zum verkabelten Netz berücksichtigt werden. Dabei ist zu beachten, dass diese spezifische Sicherheitsrichtlinie im Einklang mit dem gemäß § 9 Abs. 2 ThürDSG vorzuhaltenden generellen IT-Sicherheitskonzept der Behörde steht, wo sie auch thematisch eingebunden werden sollte.
Grundsätzlich sind alle Sicherheitsmaßnahmen des IEEE 802.11x-Protokolls zu aktivieren.
Für die WEP-Verschlüsselung ist die maximal mögliche Schlüssellänge von 128 Byte einzustellen. Sofern keine temporären Schlüssel zum Einsatz kommen, sind die Schlüssel des Öfteren zu wechseln. Für eine Verarbeitung schutzwürdiger Daten sollte allerdings aufgrund der o. g. Schwachstellen des WEP-Protokolls anstatt oder zusätzlich zu diesem ein stärkeres Sicherheitsprotokoll eingesetzt werden. Hier bietet sich z. B. IPSec an, dass nach dem derzeitigen Erkenntnisstand eine sichere Übertragung der Daten ermöglicht. Da hier auch im Gegensatz zum WEP-Protokoll nicht nur die Daten sondern auch die Protokollköpfe mit den Verbindungsdaten (Quell- und Zieladressen) in die Verschlüsselung einbezogen werden können, kann hiermit auch eine unbefugte Analyse der Kommunikationsverbindungen unterbunden werden.
Der Einsatz eines WLAN in einer Behörde erfordert i. d. R. eine personenbeziehbare Identifikation und Authentisierung der Benutzer. Dies kann z. B. durch den Einsatz eines RADIUS-Servers realisiert werden, auf dem alle zugangsberechtigten Nutzer mit ihren verschlüsselten Kennungen sowie ihre erforderlichen Zugriffsrechte eingetragen sind. Jeder Client/Nutzer sollte in die sicherheitstechnische Überwachung einbezogen werden, wobei bspw. das Einloggen in das Netz und alle sicherheitskritischen Aktivitäten zu protokollieren und auszuwerten sind. Zur Feststellung von Sicherheitsverletzungen leisten auch spezielle Erkennungssysteme (Intrusion Detection Systeme) einen wesentlichen Beitrag.
Die Schnittstelle zwischen dem WLAN und dem LAN ist mittels einer Firewall vor Angreifern abzusichern. Inzwischen werden auch Lösungen angeboten, die auf jeden Netzelement eine Firewall-Funktionalität realisieren, egal auf welchem Gerät sich der Nutzer in das Netz einloggt. Diese auch als UPN (User Personality Network) bezeichneten Systeme stellen eine elegante Lösung dar, um illegale Zugangsversuche zum Netz oder zu Subnetzen zu blockieren.
Ein aktuelles Sicherheitsthema auch bei drahtlosen Netzanbindungen ist die Virengefahr. Proportional zur permanenten Zunahme der mobilen Endgeräte gewinnt der Virenschutz im WLAN zunehmend an

Bedeutung. Ein Virenschutz sollte daher bei jeder Datenübertragung, insbesondere bei E-Mails aktiv sein.
Ein sicherer WLAN-Betrieb erfordert eine umfassende Planung sowie eine angemessene Dokumentation und korrekte Installation der technischen Verfahrensabläufe. Die Verantwortlichen für die Einrichtung und den Betrieb eines WLAN müssen über umfangreiche Kenntnisse dieser Technologie verfügen. Nicht unterschätzt werden sollte der Zeitaufwand zur Planung und zum Aufbauen eines WLAN. Alle Stationen und Komponenten eines Funk-LANs müssen vor Inbetriebnahme stufenweise getestet werden, um die Verbindung zwischen Access-Points und Clients sowie die Netzperformance, Roaming, Ausfallverhalten und Übertragungssicherheit zu prüfen.

Anlage 1

Entschließung
der 63. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 7./8. März 2002 in Mainz

Biometrische Merkmale in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solcher Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.

2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z. B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.

3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.

4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen

der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.

5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

Positionspapier zu Technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen

1 Ausgangslage

Mit dem Terrorismusbekämpfungsgesetz wurden in § 4 Passgesetz und § 1 Personalausweisgesetz nahezu gleichlautende Regelungen folgenden Inhalts aufgenommen:

- Pässe und Personalausweise dürfen neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von
  - Fingern,
  - Händen oder
  - Gesicht

  des Inhabers enthalten.

- Alle biometrischen Merkmale und die Angaben über die Person dürfen auf den Ausweispapieren verschlüsselt gespeichert werden. Durch ein Bundesgesetz ist Folgendes zu regeln:
  - Arten der biometrischen Merkmale,
  - Einzelheiten der Einbringung von Merkmalen und Angaben in verschlüsselter Form,
  - Art der Speicherung und
  - Art ihrer sonstigen Verarbeitung und Nutzung.

- Die biometrischen Merkmale dürfen nur verwendet werden, um die Echtheit des Dokumentes und die Identität des Inhabers zu prüfen.

- Eine bundesweite Datei darf nicht eingerichtet werden.

Um beurteilen zu können, ob diese Maßnahmen geeignet und angemessen sind, müssen die verschiedenen biometrischen Verfahren aus Datenschutzsicht bewertet werden. Im Folgenden werden verschiedene Verfahren beschrieben und die Risiken aufgezeigt, die im Zusammenhang mit einem flächendeckenden Einsatz biometrischer Merkmale in Ausweisdokumenten zu erkennen sind.

2 Technische Möglichkeiten

2.1 Nutzung vorhandener biometrischer Merkmale

Bevor neue Merkmale in Ausweisen gespeichert werden, sollte geklärt werden, ob die vorhandenen nicht bereits ausreichen, um die Identität des Ausweisinhabers zu prüfen. Auf die Erhebung neuer personenbezogener Daten muss dann verzichtet werden. Könnten Verfahren eingesetzt werden, die bereits vorhandene biometrische Merkmale nutzen, wäre eine geringere Eingriffstiefe in das Recht auf informationelle Selbstbestimmung als bei der Verwendung eines völlig neuen Merkmals ausreichend.

Lichtbild
Mit dem Foto des Inhabers enthalten deutsche Ausweisdokumente bereits biometrische Daten. Mit heute vorhandener Technik ist es grundsätzlich möglich, das Foto auf dem Personalausweis automatisch mit dem Gesicht der Person zu vergleichen, die den Ausweis vorlegt.

Möglicherweise können die zurzeit verwendeten Passbilder die Qualitätsanforderungen an eine automatisierte Verarbeitung nicht in vollem Umfang erfüllen. Bisher gibt es allerdings keine verlässlichen Aussagen über die Bildqualität, die für biometrische Verfahren erforderlich ist. Ebenso wenig ist bisher geklärt, wie sich biometrische Merkmale im Laufe der Zeit ändern. Möglicherweise müsste die Gültigkeitsdauer von Personalausweisen wesentlich verkürzt werden, damit die Verifikation anhand des Passbildes im Ausweis über die gesamte Gültigkeitsdauer sichergestellt werden kann.

Unterschrift
Die Unterschrift des Inhabers ist ein weiteres biometrisches Merkmal, das schon jetzt auf jedem deutschen Ausweisdokument vorhanden ist. Ein automatischer Vergleich der vorhandenen mit einer bei der Kontrolle geleisteten Unterschrift wäre jedoch wenig sinnvoll, weil die zur Erkennung erforderlichen dynamischen Daten der Unterschrift (Druckverlauf, Schreibpausen) im Ausweis nicht gespeichert sind.

2.2 Biometrische Vermessung des Gesichtes

Sollen biometrische Daten des Gesichtes neu erhoben und in den Ausweispapieren maschinenlesbar beispielsweise als Barcode oder elektronischer Datensatz gespeichert werden, sind hohe Qualitätsanforderungen an die Erfassungs- und Kontrollsysteme zu stellen, um eine ausreichende Wiedererkennungsrate sicherzustellen. Für gute Ergebnisse sind gleichmäßig ausgeleuchtete Frontalaufnahmen von Gesichtern erforderlich. In der Praxis werden diese Anforderungen nur mit hohem Aufwand realisierbar sein.

2.3 Papillarmuster der Finger

Werden nur die Merkmale eines bestimmten Fingers genutzt, entstehen Probleme, wenn dieser bei der Erfassung oder bei Vergleichen verletzt oder anderweitig stark beansprucht ist (z. B. bei Bauarbeitern). Die Erfassung von Daten mehrerer Finger und alternative Vergleiche bei Kontrollen sind sehr aufwändig. Außerdem zeigen Tests, dass ein signifikanter (statistisch aber noch nicht abschließend verifizierter) Prozentsatz von Papillarmustern aus physiologischen Gründen nicht nutzbar ist (siehe Punkt 3.2).

2.4 Handgeometrie und Handlinien

Bei der Vermessung der Handgeometrie handelt es sich um ein System, das in den USA bereits im Einsatz ist. Über die Erkennungsqualität gibt es keine verlässlichen Angaben. Über die Möglichkeiten der Nutzung der Handlinien gibt es ebenfalls keine gesicherten Erkenntnisse. Die Problematik der Verletzungen oder sonstigen Einschränkungen der Nutzung einer Hand und der sich daraus ergebenden Notwendigkeit der Alternativdaten ist vergleichbar mit der bei der Papillarmusterverwendung. Unklar ist zurzeit auch die Wiedererkennungs-

qualität bei Handveränderungen durch Arbeits- und Alterungsprozesse.

2.5 Iris- und Retinastruktur

Die gesetzliche Formulierung "Gesicht" lässt eine Erfassung detaillierter Merkmale der Augen nicht zu. Ungeachtet dessen ist festzustellen, dass diese Verfahren bisher noch nicht im größeren Stil eingesetzt worden sind. Sie sind sowohl technisch als auch organisatorisch sehr aufwändig. Bisher ist eine genaue Kopfpositionierung erforderlich, sodass fraglich ist, ob sie durch "Ungeübte" in den Erfassungsstellen und an den Kontrollstellen praktiziert werden können. Sofern das Gesicht, die Iris oder die Retina durch ein Infrarot- oder Lasersystem abgetastet wird, ist damit zu rechnen, dass derartige Systeme auf eine signifikante Ablehnung durch die Betroffenen stoßen.

2.6 Weitere biometrische Merkmale

Aus technischer Sicht ist nicht auszuschließen, dass zur Prüfung der Identität Betroffener auch andere biometrische Merkmale verwendet werden könnten (z. B. Stimme, Bewegungsmuster). Diese Merkmale werden hier jedoch nicht weiter betrachtet, weil laut Pass- und Personalausweisgesetz neben dem Lichtbild und der Unterschrift nur biometrische Merkmale von Fingern, Händen oder dem Gesicht des Inhabers verwendet werden dürfen (siehe 1).

3 Allgemeine technische Randbedingungen

3.1 Vorgaben aus der bestehenden Rechtslage

Aus dem rechtlichen Rahmen ergeben sich für die zu schaffenden Regelungen aus technischer Sicht, unabhängig von der Art der genutzten biometrischen Merkmale, folgende Vorgaben:

- Die Kontrollsysteme bestehen aus vier Komponenten, die untrennbar und unbeeinflussbar miteinander verknüpft sein müssen:
  - Leseeinheit für die aktuellen biometrischen Merkmale,
  - Leseeinheit für die Ausweispapiere,
  - Entschlüsselungs- und Vergleichseinheit und
  - Einheit zur Freigabe bzw. Sperrung der Passage.

- Um Manipulationen ausschließen zu können, müssen die biometrischen Systeme bei der Kontrolle stand-alone arbeiten.
- Die enthaltenen Softwarekomponenten sollten zertifiziert (z. B. nach Common Criteria oder ITSEC) und signiert sein. Das gilt auch für Hardwarekomponenten, soweit mit ihnen Entschlüsselungen vorgenommen werden.
- Eine Speicherung von personenbezogenen Daten auf den Datenträgern der Kontrollsysteme über den Abschluss des Kontrollvorgangs hinaus ist nicht zulässig.
- Die Zahl der Personen, die Kontrollen trotz falscher Identität passieren können, muss möglichst gering sein (vgl. FAR unter 3.2).
- Eine regelmäßige Falsch-Rückweisung durch Unzulänglichkeiten bei den gespeicherten Daten muss vor der Ausgabe der Ausweise und Pässe schon durch die örtlichen Ausweisbehörden ausgeschlossen werden. Bevor die ausgebende Stelle den Ausweis aushändigt, muss sie ihn daher mit einem entsprechenden Referenz-Kontrollsystem prüfen.
- Die Verschlüsselung kann wahlweise bei der örtlichen Behörde oder in der Bundesdruckerei erfolgen.
- Der Verschlüsselungsalgorithmus muss wissenschaftlich anerkannt sein und dem Stand der Technik entsprechend als sicher gelten (mindestens für einen Zeitraum der Gültigkeit der Ausweise).
- Der Schlüssel darf Unbefugten nicht bekannt werden.
- Wird auf eine Verschlüsselung der Daten verzichtet, müssen die gespeicherten Werte auf andere Weise gegen Missbrauch gesichert werden.

3.2 Stand der wissenschaftlichen Erkenntnisse zu biometrischen Verfahren

- Bisher gibt es keine wissenschaftlich gesicherten Erkenntnisse zu biometrischen Verfahren bei großen Anwendergruppen. Es können lediglich Erfahrungen mit kleineren Systemen (z. B. die automatisierte Kontrolle der Einwanderungsbehörde auf amerikanischen Flughäfen [Handgeometrie] oder auf den Flughäfen Schiphol und Frankfurt [Irisscan]) herangezogen werden.
- Die Leistungsfähigkeit biometrischer Systeme wird durch ihre Zurückweisungsrate berechtigter Personen (FRR False Rejection Rate) und ihre Überwindungssicherheit gegenüber unberechtigten Personen (FAR False Acception Rate) beschrieben. Beide Raten stehen in einem engen Zusammenhang. Je größer die Überwin-

dungssicherheit ist, um so mehr berechtigte Personen werden abgewiesen. Die Ermittlung der FAR und der FRR und der Beziehung zueinander ist sehr aufwändig. Für große Anwendergruppen gibt es deshalb bisher keine herstellerneutralen Untersuchungen.

- Biometrische Systeme sind bislang hinsichtlich der FRR und der FAR nicht ausreichend überprüft, um flächendeckend eingesetzt zu werden. Das betrifft auch Fragen der Manipulationssicherheit des Gesamtsystems. Von besonderer Bedeutung ist die Verbindung zwischen Rechner und Sensor, da bei unzureichender Sicherung biometrische Merkmale durch Einspielen (Replay) entsprechender Datensätze vorgetäuscht werden können.
- Auch die Lebenderkennung ist bisher wenig ausgereift. Es ist deshalb nicht auszuschließen, dass biometrische Systeme durch die Präsentation nachgebildeter Merkmale (Silikonabdruck eines Fingerabdrucks, Foto eines Gesichtes usw.) überwunden werden können.
- Zur FER (False Enrollment Rate), die den Anteil der Personen nennt, bei denen das jeweilige biometrische Merkmal nicht geeignet ist oder nicht zur Verfügung steht, gibt es bisher keine gesicherten wissenschaftlichen Erkenntnisse. Eine FER von 1% bedeutet beispielsweise bei bundesweiten Ausweisdokumenten, dass mehr als 500.000 Personen bei Kontrollen immer mit Fehlermeldungen rechnen müssen, da sie durch das System nicht erkannt werden. In jedem Fall muss ein Rückfallsystem für die Nutzer vorhanden sein, die eine sehr schlechte Merkmalsausprägung besitzen oder überhaupt nicht erfasst werden können.

4 Einheitliches Personenkennzeichen

Mit neu erfassten biometrischen Merkmalen bzw. mit den daraus generierten Datensätzen lässt sich eine Vielzahl unterschiedlicher Dateien erschließen und verknüpfen. Deshalb muss ausgeschlossen werden, dass die zusätzlichen biometrischen Merkmale der Ausweise sowohl für weitere staatliche Zwecke (z. B. Strafverfolgung) als auch im privatrechtlichen Bereich (z. B. für Vertragsabschlüsse) verwendet werden. Ein derartiges Merkmal käme sehr schnell einem einheitlichen Personenkennzeichen gleich, das gemäß dem Volkszählungsurteil des Bundesverfassungsgerichts unzulässig ist (BVerfGE 65,1, -53-).

In Bereichen, in denen Biometrie für andere als die in § 4 Passgesetz und § 1 Personalausweisgesetz genannten Zwecke zum Einsatz

kommt (z. B. Zugangskontrolle), wäre eine Verknüpfung der verschiedenen Daten technisch möglich. Dies könnte zum einen durch Verwendung der im Ausweis gespeicherten Daten als Referenzmaterial für solche Zwecke erfolgen. Zum anderen könnten gespeicherte biometrische Daten mit denen abgeglichen werden, die zum Zwecke der Ausweiserstellung verwendet werden. Dies wäre, auch wenn es keine durchgängig verwendeten Standards für die Codierung biometrischer Daten gibt, verfahrensübergreifend prinzipiell durchführbar.

5 Speicherung biometrischer Daten

Zur Vermeidung der unbefugten Nutzung von Ausweisdokumenten ist nur eine biometrische Verifikation erforderlich, d. h. der Abgleich der biometrischen Merkmale einer konkreten Person mit den auf einem Ausweis gespeicherten Daten. Eine Speicherung außerhalb des Ausweises ist dafür nicht erforderlich. Das Ziel der Erkennung von "Doppelidentitäten" durch Abgleich biometrischer Daten einer unbekannten Person mit denjenigen anderer Personen (Identifikation) setzt die Speicherung personenbezogener Daten in zentralen Referenzdateien voraus. Aus Sicht des Datenschutzes ist eine solche Datensammlung insbesondere im Hinblick auf die Bildung eines einheitlichen Personenkennzeichens und die unvermeidlichen Missbrauchsmöglichkeiten jedoch abzulehnen.

Für die Ausweise selbst besteht die Möglichkeit, die Referenzdaten als Rohdaten oder als biometrischen Datensatz zu speichern. Während Rohdaten ggf. auch grafisch gespeichert werden können (z. B. das Bild eines Fingerabdrucks), muss für elektronische Biometriedaten (“Template”, “Vektor”) der Ausweis mit einem maschinenlesbaren Datenträger (Barcode, Speicherchip etc.) versehen werden. Um einen Missbrauch dieser Daten zu verhindern, kommt insbesondere eine verschlüsselte Speicherung in Betracht. Während dies gegen einen alltäglichen Zugriff schützen mag, kann bei der Vielzahl von Geräten, in denen der Entschlüsselungsschlüssel vorhanden sein muss (bei Polizei und Grenzkontrollbehörden), jedoch kaum davon ausgegangen werden, dass die verschlüsselt gespeicherten Daten auf Dauer vor interessierten Dritten verborgen bleiben (siehe 3.1).

6 Überschießende Daten

Einige biometrische Merkmale lassen neben der Nutzung zur Identifizierung auch völlig andere Auswertungen zu. So kann möglicherweise auf bestimmte gesundheitliche Zustände oder Dispositionen, auf Faktoren wie Stress, Betrunkenheit oder Müdigkeit geschlossen werden. Bekannt ist dies von Bildern des Gesichts, der Hand und des Augenhintergrunds, von verhaltensbasierten biometrischen Merkmalen (Sprache, Unterschrift) sowie in besonderer Weise von genetischen Daten.

In der Regel sind nur aus den biometrischen Rohdaten solche Zusatzinformationen ableitbar, nicht aber aus den daraus gewonnenen Templates. Aus diesem Grund dürfen insbesondere die Rohdaten selbst nicht zentral gespeichert werden. Außerdem sind im Verarbeitungsprozess einer biometrischen Kontrolle die Rohdaten möglichst früh zu löschen, um die Gefahr einer Zweckentfremdung zu verringern.

7 Eignung für die Überwachung

Die Speicherung biometrischer Merkmale außerhalb des Ausweises birgt neue Gefahren für das Grundrecht auf informationelle Selbstbestimmung. Gelingt es, biometrische Daten im Alltag zu erfassen und diese mit einer zentralen Datenbank abzugleichen, können weitgehende Bewegungsprofile der Betroffenen erstellt werden. Im Gegensatz zu einer Erfassung eines biometrischen Merkmals unter Mitwirkung des Betroffenen handelt es sich hierbei um nicht-kooperative Vorgänge, die dem Betroffenen womöglich nicht einmal bewusst sind. Dafür sind Merkmale geeignet, die kontaktlos und über eine gewisse Distanz erfasst werden können. Dies trifft zur Zeit vor allem auf die Gesichtserkennung zu, die bei geeignetem Blickwinkel mittels gewöhnlicher Kameras erfolgen kann. Da es datenschutzrechtlich geboten ist, sensitive Daten nur in Kenntnis der Betroffenen zu erheben, sind nichtkooperative passive Systeme abzulehnen.

Demgegenüber ist die flächendeckende Erfassung des Fingerabdrucks oder der Handgeometrie ohne Wissen und Mitwirkung des Betroffenen nicht oder nur unter sehr großem Aufwand möglich. Zwar können Fingerabdrücke auch heimlich von berührten Gegenständen abgenommen werden. Dies eignet sich jedoch - wegen des hierfür erforder-

lichen Aufwands - nur zur Behandlung von Einzelfällen und ist daher mit einer Überwachung nicht vergleichbar.

8 Ergebnis

Im Ergebnis zeigt sich, dass keines der weiteren biometrischen Merkmale unproblematisch ist. Vor der Entscheidung, ob ein bestimmtes biometrisches Merkmal in Ausweise aufgenommen werden soll, müssen die verschiedenen Risiken daher sorgfältig gegeneinander abgewogen werden.

Vor der gesetzlichen Einführung neuer biometrischer Merkmale ist eine Evaluation durch einen Großversuch geboten. Dabei wären Ausweise mit zusätzlichen Sicherheitsmerkmalen (z. B. Hologramm) ohne biometrische Merkmale zu erproben und zu bewerten und mit Ausweisen zu vergleichen, die ebenso ausgestaltet sind, jedoch biometrische Merkmale enthalten. Zu prüfen wäre auch, wie hoch das Risiko für Bürgerinnen und Bürger wäre, wegen Gerätedefekten bei hard- oder softwaregestützter Erkennung der Merkmale bzw. wegen statistisch zu erwartenden Falscherkennungen bei der Ausweiskontrolle trotz eines echten eigenen Ausweises aufgehalten und intensiver überprüft zu werden, als sonst notwendig.

Anlage 2

Entschließung
der 63. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 7./8. März 2002 in Mainz

Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

Mit der rasch wachsenden Nutzung des Internet kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz "Für eine freie Telekommunikation in einer freien Gesellschaft") darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 1.1.2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z. B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.

In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im

Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

Anlage 3

Entschließung
der 63. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 7./8. März 2002 in Mainz

Datenschutzgerechte Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet.

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen, und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

Arbeitskreis Medien[1]

Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner

[1] Die Orientierungshilfe wurde unter Beteiligung des AK Personalwesen erstellt. Sie richtet sich in erster Linie an öffentliche Stellen des Bundes und der Länder. Die hier dargestellten Grundsätze können auch auf den nichtöffentlichen Bereich übertragen werden.

bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. E-Mail und andere Internetdienste sind geeignet, das Verhalten und die Leistung der Beschäftigten zu überwachen. Die Orientierungshilfe stellt die bei der Nutzung dieser Dienste geltenden datenschutzrechtlichen Anforderungen dar.

I. Allgemeines

a. Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit). Hierzu bietet es sich an, datenschutzfreundliche Verfahren einzusetzen. Ebenso ist die Kontrolle der Nutzung dieser Dienste durch den Arbeitgeber[2] so zu gestalten, dass sie zunächst ohne, zumindest aber mit so wenigen personenbezogenen Daten wie möglich durchgeführt wird. Dabei sind präventive Maßnahmen gegen unbefugte Nutzung nachträglichen Kontrollen vorzuziehen.

b. Die Bediensteten sind mit den technischen Möglichkeiten vertraut zu machen, wie die eingesetzten Verfahren datenschutzgerecht angewendet werden können. Um Art und Umfang der Verarbeitung ihrer personenbezogenen Daten nachvollziehen zu können, sind die Bediensteten umfassend darüber zu informieren (Grundsatz der Transparenz).

c. Es sind geeignete Maßnahmen zu treffen, um die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Insbesondere sollte jeder internetfähige PC mit leicht bedienbarer, auch bei den Kommunikationspartnern vorhandener Verschlüsselungssoftware ausgestattet sein, um zu verhindern, dass aus Bequemlichkeit personenbezogene oder andere sensible Daten unverschlüsselt übertragen werden.

[2] Zur Vereinfachung bezeichnet ”Arbeitgeber” sowohl den Arbeitgeber als auch den öffentlich-rechtlichen Dienstherren.

d. Automatisierte zentrale und wegen einer Verschlüsselung auch lokale Virenchecks sind notwendig. Um aktive Inhalte zu überprüfen, empfiehlt sich der Einsatz von lokaler Sandbox-Software.

II. Dienstliche Nutzung

a. Gestattet der Arbeitgeber die Nutzung von E-Mail und Internet ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- (TK-) bzw. Teledienstegesetzes (vgl. § 1 Abs. 1 Nr. 1 Teledienstedatenschutzgesetz, TDDSG); die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den einschlägigen Vorschriften des Beamtenrechts bzw. des BDSG (für Tarifbedienstete des Bundes) oder den Landesdatenschutzgesetzen (für Tarifbedienstete der Länder).

b. Der Arbeitgeber hat grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen bzw. E-Mail-Versenden der Beschäftigten dienstlicher Natur ist. Eine automatisierte Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten hingegen nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. Es wird empfohlen über die Nutzung von E-Mail und Internet eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der die Fragen der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig geregelt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

c. Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen (z. B. Psychologen, Ärzte, Sozialarbeiter und -pädagogen), muss entsprechend der Rechtsprechung des Bundesarbeitgerichtes zu Verbindungsdaten über dienstliche Telefonate eine Kenntnisnahme des Arbeitgebers vom Inhalt der Nachrichten und den Verbindungsdaten, die einen Rückschluss auf die betroffenen Personen zulassen, ausgeschlossen werden.

d. Der Arbeitgeber darf die Nutzungs- und Verbindungsdaten der Personalvertretung nur insoweit kontrollieren, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist. Soweit allerdings nur unerhebliche Kosten bei der Nutzung von Internet und E-Mail anfallen - was überwiegend der Fall sein wird -, ist eine Auswertung dieser Daten unzulässig.

e. Soweit die grundlegenden Datenschutzprinzipien eingehalten werden, kann die Dienstvereinbarung Regelungen enthalten, die im Einzelfall hinter den unter a. genannten Vorschriften zurückbleiben. Weder das BDSG noch die Landesdatenschutzgesetze bzw. die beamtenrechtlichen Vorschriften schließen dies von vornherein aus. Nur wenn eine gesetzliche Regelung unabdingbar ist, kommt eine Abweichung zuungunsten der Beschäftigten nicht in Betracht.

f. Im Regelfall sollte darauf verzichtet werden, die Verarbeitung von Protokolldaten auf die Einwilligung der Beschäftigten zu stützen, da sie aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber nicht immer freiwillig entscheiden können. Nur ausnahmsweise ist auch die Einwilligung der Beschäftigten in eine Verarbeitung der Protokolldaten über die unter a. genannten Vorschriften hinaus möglich. Die Beschäftigten können z. B. die Verwertung ihrer Protokolldaten verlangen, um den Verdacht einer unbefugten Internetnutzung auszuräumen.

g. Soweit die Nutzung von E-Mail und Internet zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren protokolliert wird, dürfen diese Daten nach dem BDSG, den Landesdatenschutzgesetzen und dem Beamtenrecht des Bundes und der Länder auch nur zu diesen Zwecken genutzt werden, nicht aber zur Verhaltens- und Leistungskontrolle der Beschäftigten.

h. Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. Beispielsweise könnte der Vorgesetzte verfügen, dass ihm jede ein- oder ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist.

i. Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, die gefährlichen oder verdächtigen ausführbaren Code enthalten (also insbesondere html-Seiten als Mail-body, Dateien mit den Erweiterungen *.exe, *.bat, *.com oder gepackte Dateien wie *.zip, *.arj, *.lha).

III. Private Nutzung

1. Allgemeines

a. Wenn ein Arbeitgeber den Beschäftigten die private Nutzung von Internet oder E-Mail erlaubt, ist er ihnen gegenüber TK- bzw. Teledienste-Anbieter.

b. Vom Arbeitgeber beauftragte Zugangsanbieter (Access Provider) sind zwar diesem gegenüber TK- bzw. Teledienste-Anbieter, gegenüber den privat nutzenden Beschäftigten sind die Provider aber lediglich Auftragnehmer des dann als Anbieter zu qualifizierenden Arbeitgebers.

c. Der Arbeitgeber ist den Beschäftigten gegenüber zur Einhaltung des Telekommunikationsgeheimnisses verpflichtet. Daher gelten die gleichen Bedingungen wie beim privaten Telefonieren.

d. Es gelten die Regelungen der Telekommunikations-Datenschutzverordnung, des Teledienstedatenschutzgesetzes bzw. des Mediendienste-Staatsvertrages.

e. Der Arbeitgeber ist nicht verpflichtet, den Beschäftigten die private Nutzung des Internet zu erlauben. Entschließt er sich jedoch dazu, muss es ihm grundsätzlich möglich sein, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen (z. B. eine angemessene Art der Kontrolle durchzuführen). Beschäftigte, die diese Voraussetzungen nicht erfüllen wollen, können ihre Einwilligung ohne jeden dienstlichen Nachteil verweigern.

f. Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle, ob diese Bedingungen eingehalten werden, müssen - am sinnvollsten durch Dienstver-

einbarung oder -anweisung - unter Beteiligung des Personalrats eindeutig geregelt werden.

g. Eine Protokollierung darf ohne Einwilligung erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs der Verfahren oder zu Abrechnungszwecken erforderlich ist.

2. Besonderheiten bei E-Mail

a. Private E-Mails sind wie private schriftliche Post zu behandeln. So sind eingehende private, aber fälschlich als Dienstpost behandelte E-Mails den betreffenden Mitarbeitern unverzüglich nach Bekanntwerden ihres privaten Charakters zur alleinigen Kenntnis zu geben.

b. Der Arbeitgeber sollte vor dem Hintergrund des von ihm zu wahrenden Telekommunikationsgeheimnisses entweder für die Beschäftigten separate E-Mail-Adressen zur privaten Nutzung einrichten oder - falls privates Surfen erlaubt ist - sie auf die Nutzung eines (kostenlosen) Web-Mail-Dienstes verweisen.

c. Wie bei der dienstlichen Nutzung (s. II.i.) dürfen aus Gründen der Datensicherheit eingegangene private E-Mails oder deren Anhänge unterdrückt werden, wenn sie ein Format aufweisen, das ausführbaren Code enthalten kann. Die Verfahrensweise ist den Beschäftigten zuvor bekannt zu geben. Generell sind die Beschäftigten darüber zu unterrichten, wenn an sie gerichtete oder von ihnen abgesendete E-Mail ganz oder teilweise unterdrückt werden oder virenverseucht sind. Eine Untersuchung von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist nur unter Einbeziehung der betreffenden Beschäftigten zulässig.

d. Eine darüber hinaus gehende inhaltliche Kontrolle ist nicht zulässig.

Anlage 4

Entschließung
der 63. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 7./8. März 2002 in Mainz

Neues Abrufverfahren bei den Kreditinstituten

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. “know your customer principle”). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

Anlage 5

63. Konferenz der Datenschutzbeauftragten des
Bundes und der Länder
am 7./8. März 2002 in Mainz

Konferenzpapier zur Rasterfahndung

Die 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich intensiv mit den datenschutzrechtlichen Problemen der Rasterfahndung zur Aufdeckung terroristischer "Schläfer" befasst. Wegen der unterschiedlichen Rechtslage in den einzelnen Bundesländern konnte keine einheitliche Bewertung getroffen werden.

Allerdings ist festzustellen, dass hinsichtlich der rechtlichen Voraussetzungen der Maßnahme, aber auch bei der Durchführung im einzelnen die gesetzlichen Vorgaben nicht überall eingehalten wurden. Zum weiteren Verfahren betont die Konferenz folgende Forderungen:

Bei allen polizeilichen Maßnahmen, insbesondere auch bei den weiteren Datenerhebungen zur Abklärung von "Trefferfällen", ist der Verhältnismäßigkeitsgrundsatz in besonderer Weise zu wahren.

Die erhobenen Daten unterliegen einer strengen Zweckbindung und dürfen nur für die unmittelbar der Fahndungsmaßnahme dienenden Zwecken verwendet werden.

Die in die Rasterfahndung einbezogenen Daten müssen unverzüglich gelöscht werden, wenn das Ziel der Maßnahme, nämlich Personen zu ermitteln, auf welche die vorgegebenen Merkmale zutreffen, erreicht ist, da die legitimierenden Gründe für den Grundrechtseingriff insoweit entfallen sind. Auch die "Trefferfälle" sind zu löschen, wenn die weiteren Ermittlungen ergeben, dass von den Betroffenen keine Gefahr ausgeht. Es darf nicht zu einer Vorratsspeicherung zu Personen kommen, die zufälligerweise in die Maßnahme geraten sind.

Die Konferenz bekräftigt ihre Forderung, die laufende Rasterfahndung einer ergebnisoffenen Erfolgskontrolle zu unterziehen. Sie wendet sich energisch gegen Bestrebungen, die in den Polizeigesetzen der Länder enthaltenen Eingriffsschwellen für die Durchführung von Rasterfahndungen herabzusetzen.

Anlage 6

Entschließung
der 64. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 24./25. Oktober 2002 in Trier

Datenschutzgerechte Vergütung für digitale Privatkopien im neuen Urheberrecht

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber - wie es der Bundesrat fordert - jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

Anlage 7

Entschließung
der 64. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 24./25. Oktober 2002 in Trier

Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zur Zeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, sodass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

Anlage 8

Entschließung
der 64. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 24./25. Oktober 2002 in Trier

Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen "Justiz und Inneres" entsprechende Maßnahmen- allerdings unter weitgehendem Ausschluss der Öffentlichkeit - diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung

des WorldWideWeb), wie sie jetzt erwogen wird, ist ebensowenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

Anlage 9

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2003 in Dresden

Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.

Sie sehen dabei folgende essentielle Punkte:

- Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes

  - Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.

- Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.

- Die Freiwilligkeit der Einwilligung muss gewährleistet sein.

- Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in" statt „opt out").

- Technischer Datenschutz

  Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

- Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

  Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.

  Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetz-

lichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

- Förderung von datenschutzgerechter Technik

  Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.

  Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

  Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

- Anonyme Internetnutzung

  Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von e-mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt ge-

währleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

- Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

  Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:

  Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

  Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

  Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten

so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen - wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung - für geboten.

Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts - und zwar nicht nur im Bereich der Telefonüberwachung - als grundrechtssicherndes Verfahrenselement ergreifen muss.

- Stärkung des Schutzes von Gesundheitsdaten

  Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten und zwar auch für deren Verwendung im Einzelfall.

Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z. B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

- Datenschutz und Gentechnik

  Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen - dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

  Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen

Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

- Datenschutz im Steuerrecht

  Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

  Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und -speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

  Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

- Arbeitnehmerdatenschutz

  Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

  - die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,

  - die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,

  - die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

  - die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

  Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

  Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

- Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

  Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

  Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Da-

tenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

- Stellung des Bundesdatenschutzbeauftragten

  Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

- Verbesserung der Informationsrechte

  Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

Anlage 10

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2003 in Dresden

Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und eGovernment werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.
So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im eGovernment detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der “Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)” entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese

Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen. [1]
In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt. [2]
Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und -Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

[1] Die Schutzprofile mit dem Titel „BISS - Benutzerbestimmbare Informationsflusskontrolle“ haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.
[2] Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

Anlage 11

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2003 in Dresden

TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz "Trusted Computing Platform Alliance" (**TCPA**).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt gewordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen

Prüf- und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,

- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,

- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,

- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,

- der Zugang zum Internet und E-mail-Verkehr durch Softwarerestriktionen behindert würde,

- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,

- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und

- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und

- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

Anlage 12

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2003 in Dresden

Elektronische Signatur im Finanzbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3.000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur“ der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur“ gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28.1.2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte „qualifizierte elektronische Signatur mit Einschränkungen„ eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

- Die „qualifizierte elektronische Signatur mit Einschränkungen“ bietet im Gegensatz zur „qualifizierten elektronischen Signatur“ und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung“ keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen“ hat geringeren Beweiswert als die eigenhändige Unterschrift.

- Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen“ vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen. Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.

- Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.

- Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.
Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005“ als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,

- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,

- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,

- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und ggf. Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ staatlich zu fördern,

- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,

- e-Government- und e-Commerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,

- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,

- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

Anlage 13

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2003 in Dresden

Transparenz bei der Telefonüberwachung

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, das die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9.802 Anordnungen, waren es im Jahr 2001 bereits 19.896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Absatz 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

Anlage 14

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2003 in Dresden

Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G 10 Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

Anlage 15

Entschließung
der 65. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 27./28. März 2003 in Dresden

Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.

So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u. a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauens-

beziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,

- das Prinzip der Stichprobe zugrunde legen,

- eine strikte Einhaltung der Zweckbindung gewährleisten und

- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1. Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z. B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2. Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der - von den Betroffenen nicht beeinflussbar - Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

   Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grds. selbst zu entscheiden,
   - ob sie überhaupt verwendet wird,
   - welche Daten darauf gespeichert werden oder über sie abgerufen werden können,
   - welche Daten zu löschen sind und wann das zu geschehen hat,
   - ob sie im Einzelfall vorgelegt wird und
   - welche Daten im Einzelfall ausgelesen werden sollen.

   Sicherzustellen ist weiterhin

   - ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,
   - die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und
   - die Strafbarkeit des Datenmissbrauchs.

   Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26.10.2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“ vom 3. Mai 2002, wonach "der Patient Herr seiner Daten“ sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3. Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski“, „raucht“, „trinkt zwei Biere pro Tag“), diese überwachen und so zur „Gesundheitspolizei“ werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4. Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

Anlage 16

Entschließungen zwischen den Konferenzen 2003

Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation

(Umlaufentschließung/28. April 2003)

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz v. 28.3.2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z. B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss - wie bisher - die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z. B. PINs und PUKs - Personal Unblocking Keys -), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12.3.2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z. B. der Erwerb eines „vertragslosen“ Handys, das mit einer entsprechenden - im Prepaid-Verfahren mit Guthaben aufladbaren - SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs

der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose routinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z. B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunikation zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

Anlage 17

Entschließungen zwischen den Konferenzen 2003

Neuordnung der Rundfunkfinanzierung
(Umlaufentschließung/30. April 2003)

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

- Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind . Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.

- Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst - wie bei den amtlichen Statistiken erfolgreich praktiziert - nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.

- Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die GEZ künftig auch online zugreifen.

- Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten - wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern - zu erheben, ausdrücklich erlaubt werden.

- Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.

Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

Anlage 18

Entschließungen zwischen den Konferenzen 2003

Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

(Umlaufentschließung/16. Juli 2003)

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81 g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (sogen. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr - wie vom geltenden Recht gefordert - in jedem Fall eine Straftat von erheblicher Bedeutung oder - wie jüngst vom Bundestag beschlossen - eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,

- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nicht-codierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise

einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, sodass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z. B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, sodass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

Anlage 19

Entschließungen zwischen den Konferenzen 2003

Automatisches Software-Update
(Umlaufentschließung/07. August 2003)

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei - oftmals vom Nutzer unbemerkt oder zumindest nicht transparent - Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne das dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.

- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.

- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das - unbemerkte - Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind, und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nut-

zern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss. Personenbezogen Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

Anlage 20

Entschließung
der 66. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 25./26. September 2003 in Leipzig

Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai diesen Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten "Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen" vorgelegt. Darin hat es festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 % erhöht (1996: 2149; 2001: 3868) hat,

- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2.494 um das Sechsfache auf 15.741 gestiegen ist,

- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3.730 auf 9.122 fast verdreifacht hat,

- in 21 % der Anordnungen zwischen 1.000 und 5.000 Gespräche, in 8 % der Anordnungen mehr als 5.000 Gespräche abgehört worden sind,

- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf ca. 14 % angestiegen ist,

- die Beschlüsse in ca. ¾ aller Fälle das gesetzliche Maximum von 3 Monaten umfassen, ¾ aller Maßnahmen tatsächlich aber nur bis zu 2 Monaten andauern,

- lediglich 24 % der Beschlüsse substanziell begründet werden,

- es nur in 17 % der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,

- 73 % der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann - entgegen häufig gegebener Deutung - nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100 b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z. B. Beweisverwertungsverbote).

- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.

- Der Umfang des - seit Einführung der Vorschrift regelmäßig erweiterten - Straftatenkataloges des § 100 a StPO muss reduziert werden.

- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Geprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.

- Zur Sicherung der Zweckbindung nach § 100 b Abs. 5 StPO und 477 Abs. 2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.

- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.

- Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

Anlage 21

Entschließung
der 66. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
am 25./26. September 2003 in Leipzig

Gesundheitsmodernisierungsgesetz

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte unterliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.
Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.
Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.
- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z. B. mit data-warehouse-systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahingehend

erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist, und dass
- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.

Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

Anlage 22

Entschließungen zwischen den Konferenzen 2003/2004

Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

(Umlaufentschließung/21. November 2003)

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz beschlossen. Dieser Entwurf sieht jetzt zwar - entsprechend der Forderung der Datenschutzbeauftragten - die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht

ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu machen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

Anlage 23

Vorschlag zur Ausgestaltung von vertraglichen Vereinbarungen im Rahmen der Auftragsdatenverarbeitung nach § 8 Thüringer Datenschutzgesetz (ThürDSG)

In Verträgen zur Auftragsdatenverarbeitung zwischen öffentlichen Stellen und öffentlichen und nicht öffentlichen Stellen sind die Regelungen des § 8 ThürDSG in der jeweiligen Vereinbarung umzusetzen. Die Hinweise des Thüringer Innenministeriums zum Thüringer Datenschutzgesetz - ThürDSG - vom 29. Oktober 1991 (GVBl. S. 516) in der Fassung der Bekanntmachung vom 10. Oktober 2001 (GVBl. S. 276) (www.datenschutz.thueringen.de) zu § 8 ThürDSG geben wichtige Erläuterungen und Hinweise, was bei den Verträgen von Seiten des Auftraggebers zu beachten ist.

Auftragsdatenverarbeitung liegt beispielsweise vor, wenn sich öffentliche Stellen zur Erledigung ihrer Aufgaben Rechenzentren oder externer Stellen für die Wartung oder Fernwartung bedienen, aber auch bei externer Datenerhebung, Datenerfassung auf Datenträgern, Mikroverfilmung von Unterlagen, Vernichtung von Schriftgut und anderen Datenträgern oder Archivierung durch andere öffentliche Stellen oder Private.

Zunächst ist vom Auftraggeber zu prüfen, ob eine Datenverarbeitung im Auftrag grundsätzlich und in welchem konkreten Umfang erforderlich ist, etwa weil die Arbeiten durch eigene Kräfte oder mangels technischer Ausrüstung nicht ausgeführt werden können bzw. der Aufwand erheblich größer wäre beim Auftraggeber.

Soweit spezialgesetzliche Regelungen für die Daten, die im Auftrag verarbeitet oder genutzt werden sollen, Anwendung finden, ist zunächst zu prüfen, ob eine Auftragsdatenverarbeitung überhaupt und unter welchen Maßgaben zulässig ist. Spezialgesetzliche Regelungen bei der Vertragsgestaltung (z. B. bei Sozialdaten und Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, Meldedaten nach dem Thüringer Meldegesetz) sind dabei zu berücksichtigen.

Eine Beauftragung nicht öffentlicher Stellen/Unternehmen soll nur erfolgen, wenn und solange dies zur Aufrechterhaltung eines geordneten Dienstbetriebs unerlässlich ist. Langfristig ist anzustreben, dass hoheitliche Aufgaben - wozu auch das Verarbeiten zwangsweise von den Betroffenen erhobener Daten zählt - durch die Daten verarbeiten-

den Stellen selbst oder durch andere öffentliche Stellen, die der Aufsicht des Landes Thüringen unterliegen, wahrgenommen werden.

Nachfolgend werden in Form eines Mustervertrags die für die Verarbeitung oder Nutzung personenbezogener Daten im Auftrag gemäß § 8 ThürDSG erforderlichen datenschutzrechtlichen Vertragsbestandteile abgedruckt, die inhaltlich aufgabenbezogen anzupassen sind.

Vereinbarung

zwischen

.....

- Auftraggeber -

und

.....

- Auftragnehmer -

§ 1 Gegenstand der Vereinbarung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

(2) Der Auftrag umfasst folgende Arbeiten:

.....
(Definition der Datenverarbeitung),

Beispiele:
- *Vernichtung von dienstlichem Schriftgut mit personenbezogenen Daten*
- *Durchführung von Schreibarbeiten durch ein privates Schreibbüro*
- *Wartung und Fernwartung von IT-Technik, sofern der Zugang zu personenbezogenen Daten nicht ausgeschlossen ist*
- *Bewachungdienstleistung, die die Verarbeitung personenbezogener Daten umfasst*
- *Übernahme von Rechnerleistungen durch ein Rechenzentrum*

§ 2 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung und -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind abzustimmen.

(3) Der Auftraggeber erteilt Weisungen über Art, Umfang und Verfahren der Datenverarbeitung. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Genehmigung des Auftraggebers nicht erstellt.

(2) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen zumindest logisch getrennt verarbeitet werden.

(3) Der Auftragnehmer hat jederzeit vom Auftraggeber veranlasste Kontrollen zu ermöglichen.

(4) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden. Dem Auftraggeber ist der Vollzug schriftlich anzuzeigen.

(5) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verar-

beitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen.

(6) Die Einschaltung von Unterauftragnehmern ist ausgeschlossen.

oder

(6) Die Beauftragung von Unterauftragnehmern ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftragnehmer hat in diesem Falle vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen.

oder

(6) Folgende Teile des Vereinbarungsgegenstandes

.....

werden durch

.....
als Unterauftragnehmer erbracht.
Der Auftragnehmer hat vertraglich sicherzustellen, dass die in dieser Vereinbarung enthaltenen Regelungen auch gegenüber dem Unterauftragnehmer gelten und kontrolliert die Einhaltung dieser Pflichten regelmäßig.

(7) Der Auftragnehmer bestätigt, dass er die nach den für ihn geltenden Vorschriften erforderlichen Maßnahmen, z. B. Meldungen zum Register bei der Aufsichtsbehörde für den Datenschutz vorgenommen hat. Die Ergebnisse der zuletzt vorgenommenen Überprüfung durch die Aufsichtsbehörde gemäß § 38 Abs. 2 BDSG werden dem Auftraggeber zugänglich gemacht.

(8) Entscheidungen zur Änderung der Organisation und Durchführung der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

(9) Der Auftragnehmer beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung. Er gewährleistet die gesetzlich vorgeschriebenen und vertraglich vereinbarten Datensicherheitsmaßnahmen.

(10) Soweit der Auftragnehmer der Ansicht ist, dass eine Weisung des Auftraggebers gegen das ThürDSG oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Dies gilt auch, soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, bei Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

§ 4 Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß § 6 ThürDSG zu wahren.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind und eingehalten werden. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

§ 5 Datensicherungsmaßnahmen (vgl. Erläuterungen im Anhang)

Folgende technische und organisatorische Maßnahmen nach § 9 ThürDSG werden auf der Grundlage eines Sicherheitskonzepts verbindlich festgelegt:

a) zur Gewährleistung der Vertraulichkeit
Maßnahmen, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können

b) zur Gewährleistung der Integrität
Maßnahmen, damit personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben

c) zur Gewährleistung der Verfügbarkeit
Maßnahmen, damit personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können

d) zur Gewährleistung der Authentizität
Maßnahmen, damit personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können

e) zur Gewährleistung der Revisionssicherheit
Maßnahmen, damit festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat

f) zur Gewährleistung der Transparenz
Maßnahmen, damit die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können

Die Wirksamkeit der technischen und organisatorischen Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und der Entwicklung der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen. Wesentliche Änderungen sind schriftlich zu vereinbaren.

§ 6 Vertragsdauer

(1) Der Vertrag beginnt am ..... und endet am ...../mit Auftragserledigung.

oder

(1) Der Vertrag wird auf unbestimmte Zeit geschlossen. Er ist mit unter Einhaltung einer Frist von ..... Monaten zum Quartals-/Jahresende kündbar.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein Verstoß des Auftragnehmers gegen die Bestimmungen des ThürDSG oder dieses Vertrages vorliegt, insbesondere wenn der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers verweigert.

§ 7 Vergütung

....

§ 8 Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem ThürDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

§ 9 Vertragsstrafe

Bei Verstoß gegen die Vereinbarungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... vereinbart.

§ 10 Nichterfüllung der Leistung

....

§ 11 Sonstiges

(1) Der Auftragnehmer übereignet dem Auftraggeber zur Sicherung alle Datenträger, auf denen sich Dateien befinden, die Daten des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen.

(2) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(4) Die Einrede des Zurückbehaltungsrechts nach § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

§ 12 Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im übrigen nicht.

Ort, Datum

.....	.....
Auftraggeber	Auftragnehmer

Anhang zu Anlage 23

Erläuterungen zu § 5 Datensicherungsmaßnahmen

Die Vorgaben sind in § 8 ThürDSG enthalten. Er bestimmt, welche Prüfungen der Auftraggeber vor der Auftragsvergabe durchzuführen hat.

Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. In dem Vertrag müssen die technischen und organisatorischen Maßnahmen festgelegt werden, die bei der Datenverarbeitung umzusetzen sind. Von der Einhaltung der Vorgaben/deren Umsetzung hat sich der Auftraggeber zu überzeugen.

Besitzt der Auftragnehmer ein Datensicherheitskonzept, muss der Auftraggeber prüfen, ob es seinen Anforderungen entspricht. Reichen diese Festlegungen nicht aus, sind ergänzende Maßnahmen zu vereinbaren. Das Datensicherheitskonzept ggf. mit Ergänzungen kann dann zum Vertragsbestandteil gemacht werden. Die in diesem Sicherheitskonzept genannten Maßnahmen müssen dann nicht mehr im Vertragstext wiederholt werden.

Besitzt der Auftragnehmer kein Datensicherheitskonzept, müssen die konkreten Maßnahmen im Vertrag vereinbart werden. Hierzu bietet das Grundschutzhandbuch des BSI für bestimmte technische Konstellationen einen Katalog an Sicherheitsmaßnahmen. Je nach Sensibilität der Daten sind zusätzliche Maßnahmen erforderlich.
Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

- Sichere Identifizierung und Authentifizierung der Nutzer: Die Anmeldung am System oder Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.
- Rechteverwaltung/Zuordnungen/Verantwortlichkeiten: Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.
- Abschottung von internen Netzen: Es müssen Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechner-

netze soweit möglich zu verhindern. Da meist keine absolute Sicherheit zu erreichen ist, müssen derartige Versuche erkannt werden. Technische Komponenten, die u. a. in Betracht kommen, sind Firewalls oder Intrusion Detection Systeme.
- Sichere Datenübertragung: Gewährleistung der Vertraulichkeit und der Integrität der Daten bspw. mittels Verschlüsselung und elektronischer Signatur.
- Beweissicherung: Protokollierung der Aktivitäten von Benutzer und Administrator.

In § 5 des Vertrags sollten die konkreten Maßnahmen übernommen werden. Dabei handelt es sich bei den folgenden Ausführungen nicht um einen abschließenden Katalog:

a) zur Gewährleistung der Vertraulichkeit
Maßnahmen, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können sind u. a. Zutritts-, Zugangs- und Zugriffskontrolle, nachvollziehbare Rechteverwaltung/Berechtigungskonzept, Datenverschlüsselung.
Am Beispiel der Vernichtung von Unterlagen mit personenbezogenen Daten:
- Einwurf der Unterlagen in besonders gesicherte Behältnisse, die nicht unbefugt entfernt werden können und die eine Entnahme der Unterlagen verhindern
- auch während des Transports müssen die Unterlagen so gesichert sein, dass Unbefugte sich keinen Zugang verschaffen können
- die Unterlagen müssen möglichst so dem Aktenvernichter zugeführt werden, dass keine Unbefugten zugreifen können
- ist eine Kenntnisnahme von personenbezogenen Daten durch Mitarbeiter der beauftragten Firma nicht gänzlich auszuschließen, sind diese auf das Datengeheimnis und nach dem Verpflichtungsgesetz zu verpflichten.

b) zur Gewährleistung der Integrität
Maßnahmen, damit personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben sind u. a. Prüfsummenverfahren/Hashverfahren, elektronische Signatur, Einsatz von elektronischen Speichermedien mit Fehlererkennung und -korrektur.

c) zur Gewährleistung der Verfügbarkeit
Maßnahmen, damit personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können sind u. a. Datensicherung, Notfallkonzept, unterbrechungsfreie Stromversor-

gung/Notstromversorgung, redundante Hardwarekomponenten/RAID-Technologie, Alarmanlagen (Brand-/Wassermelder), Virenschutz.

d) zur Gewährleistung der Authentizität
Maßnahmen, damit personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können sind u. a. elektronische Signatur oder bei Schriftgut konventionelle Dokumentation der Herkunft.

e) zur Gewährleistung der Revisionssicherheit
Maßnahmen, damit festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat sind u. a. Protokollierung von An- und Abmeldevorgängen, der Zugriffe auf Dateien und Datenfelder, beim Einfügen/Ändern/Löschen von Daten, von Aktivitäten der System- und Datenbankverwalter.
Am Beispiel der Aktenvernichtung:

- Übergabeprotokoll bei Entgegennahme des zu vernichtenden Materials
- Bestätigung der ordnungsgemäßen Vernichtung

f) zur Gewährleistung der Transparenz
Maßnahmen, damit die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können sind u. a. Dokumentation der Verarbeitungs-, Hilfs- und Sicherheitsprogramme, der Rechteverwaltung, der Schnittstellen Betriebssystem/Anwendungsprogramme.

Anlage 24

Entwurf des Steuervergünstigungsabbaugesetzes lässt sorgfältige Abwägung zwischen Steuergerechtigkeit und informationellem Selbstbestimmungsrecht vermissen

(Gemeinsame Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder vom 13. Dezember 2002)

Gesetzesgerechte Steuererhebung und grundrechtlicher Persönlichkeitsschutz stehen in einer Wechselbeziehung, die sorgfältiger Abwägung bedarf. Im Gegensatz zu Bereichen Sozialleistungen und Rentenversicherungen, wo es gelungen ist, eine Balance zwischen der wirksamen Erfüllung der staatlichen Aufgaben und dem individuellen Persönlichkeitsrecht des Einzelnen, das sich auch in dem Grundrecht auf informationelle Selbstbestimmung manifestiert, zu finden, lässt der Entwurf des Steuervergünstigungsabbaugesetzes diese Abwägung vermissen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die gesetzgebenden Stellen auf, bei den geplanten Maßnahmen zur Sicherung der Steuergerechtigkeit eine datenschutzkonforme Abwägung zwischen diesen Verfassungsprinzipien vorzunehmen und die Datenschutzrechte der Bürger angemessen zu berücksichtigen. Im einzelnen machen sie auf folgendes aufmerksam:

- Die Aufhebung des § 30 a AO führt zu einem Wegfall des Bankgeheimnisses und damit zu einer deutlichen Störung des Vertrauensverhältnisses zwischen Banken und Kunden. Dass künftig auch verdachtunabhängige Prüfungen in Banken angeordnet werden können, schafft den „gläsernen Bankkunden“ und erweckt den Anschein, als sei jeder Steuerpflichtige ein potentieller Steuerverkürzer. Das datenschutzrechtliche Prinzip, dass Daten grundsätzlich beim Betroffenen zu erheben sind (§ 93 a AO), wird außer Kraft gesetzt.

- Der Vertrauensverlust in der Bevölkerung wird durch die automatische Meldepflicht verschärft, die die Banken und andere Finanzdienstleister künftig gegenüber dem Bundesamt für Finanzen (BfF) haben.

- Nach § 23 a EStG-E haben die Kreditinstitute Kontrollmitteilungen an das BfF über private Veräußerungsgeschäfte insbesondere bei Wertpapieren, aber auch bei anderen Wirtschaftsgütern, z. B. Antiquitäten mit Namen, Anschaffungs- und Veräußerungsbeträgen sowie Anzahl zu senden.

- Gemäß § 45 d EStG-E sollen die Banken alle Kapitalerträge, bei denen ein Abzug von Steuern vorgesehen ist, mit Namen, Beträgen und Freistellungssummen dem BfF anzeigen.

- Da die umfangreichen Datenübermittlungen unter einem einheitlichen Identifikationsmerkmal (§ 139 a AO-E) beim BfF zusammengeführt werden sollen, entsteht die Sorge, dass für alle Staatsbürger ein einheitliches Personenkennzeichen ins Auge gefasst wird. Dies widerspricht dem Urteil des Bundesverfassungsgerichts zur Volkszählung vom 15. Dezember 1983, wonach die Erschließung von Datenverbunden durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal nicht zulässig ist.

- Die Zusammenführung der Daten beim Bundesamt der Finanzen schafft eine bundesweite Datensammlung über alle Differenzgewinne und Kapitalerträge sowie sonstige Veräußerungsgewinne und verstärkt die Entwicklung des BfF zum zentralen Datenpool. Es besteht erfahrungsgemäß die Gefahr, dass auch andere Behörden auf solche riesigen Datenbestände zugreifen wollen.

- Die geplante Ausweitung der Befugnis zu Kontrollmitteilungen durch die Neufassung des § 194 Abs. 3 AO verstößt gegen das verfassungsrechtliche Übermaßverbot. Unabhängig von einer zulässigen Verwertung von Zufallsfunden müssen Kontrollmitteilungen über alle steuerpflichtigen Staatsbürger daran gebunden werden, dass tatsächliche Anhaltspunkte für den Verdacht einer Steuerverkürzung bereits entstanden sind. Die gegenwärtig geplante verdachtunabhängige Befugnis zu Kontrollmitteilungen ist unverhältnismäßig.

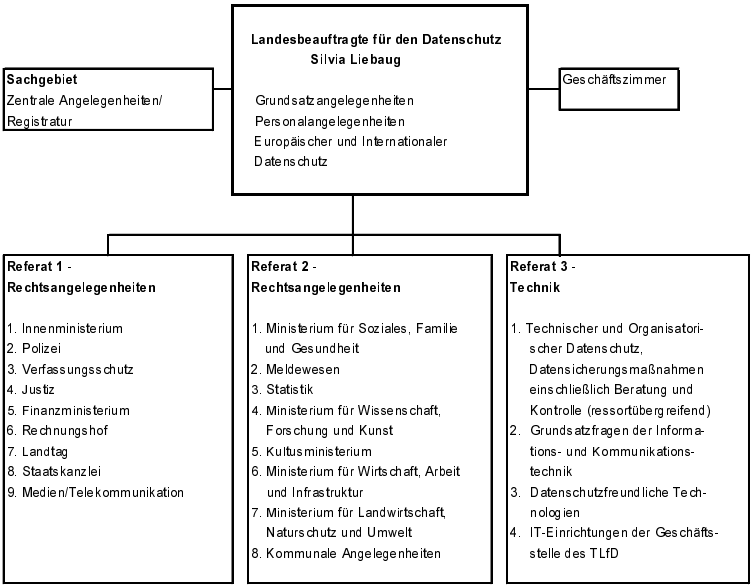
  In diesem Zusammenhang müsste es gesetzlich ausgeschlossen werden, dass kopierte Unterlagen der Betriebe i. S. des § 147 Abs. 6 AO in den Finanzämtern für die massenhafte Herstellung von Kontrollmitteilungen verwendet werden. Da die bisherige Ein-

schränkung des § 194 Abs. 3 AO aufgegeben wird, stehen gesetzlich keine Hindernisse gegen eine solche Auswertung der betrieblichen EDV im Wege. Dies wäre ebenfalls ein Verstoß gegen das verfassungsrechtliche Prinzip der Verhältnismäßigkeit.

Die Konferenz der Datenschutzbeauftragten von Bund und Ländern weist in diesem Zusammenhang darauf hin, dass eine Abgeltungssteuer wie in anderen europäischen Staaten (etwa Österreich und Schweiz) zu vergleichbarem Steueraufkommen führen wird, ohne dass die Banken zu umfassenden Anzeigepflichten über alle Steuerpflichtigen gezwungen werden. Die neuen Überlegungen der Bundesregierung gehen offenbar in diese Richtung und würden damit die Voraussetzungen schaffen, dass Kontrollmitteilungen entfielen, das Bankgeheimnis gewährt bliebe und es bei Betriebsprüfungen weiterhin ausschließlich um die zulässige Verwertung von Zufallskunden ginge.

Anlage 25

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
Internet: www.datenschutz.thueringen.de

Sachregister