Landtag von Sachsen-Anhalt **Drucksache 3/1587**
Dritte Wahlperiode **05.05.1999**

Unterrichtung

Präsident des Landtages von Sachsen-Anhalt

Magdeburg, 5. Mai 1999

Vierter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 1997 bis 31. März 1999

Sehr geehrte Damen und Herren,

mit Schreiben vom 26. April 1999 hat der Landesbeauftragte für den Datenschutz Sachsen-Anhalts gemäß § 22 Abs. 4 Satz 3 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) vom 12. März 1992 (GVBl. LSA S. 152) dem Landtag seinen Vierten Tätigkeitsbericht übermittelt. Er schließt an den Dritten Tätigkeitsbericht an, der als Drucksache 2/3490 vorliegt und im Ausschuß für Inneres und im Ausschuß für Recht und Verfassung beraten wurde.

Die Unterrichtung des Landtages erfolgt gemäß § 54 Abs. 1 Satz 2 der Geschäftsordnung des Landtages von Sachsen-Anhalt (GO.LT).

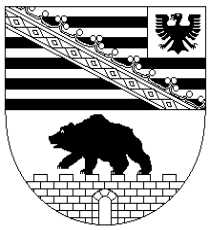
Gemäß § 40 Abs. 1 i. V. m. § 54 Abs. 1 Satz 3 GO.LT überweise ich den Tätigkeitsbericht zur Beratung und zur Berichterstattung an die Ausschüsse für Inneres (federführend) sowie für Recht und Verfassung.

Mit freundlichen Grüßen

Wolfgang Schaefer

(Ausgegeben am 10.05.1999)

Landesbeauftragter
für den Datenschutz
Sachsen-Anhalt



IV. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

**für die Zeit
vom
1. April 1997 bis 31. März 1999**

IV. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Landesbeauftragter für den Datenschutz - Postfach 1947 - 39009 Magdeburg
Tel. (0391) 8 18 03 - 0
Fax (0391) 8 18 03 33

Dienstgebäude: Berliner Chaussee 9 - 39114 Magdeburg

Inhaltsverzeichnis

1.	**Entwicklung des Datenschutzes**	1
2.	**Der Landesbeauftragte**	3
2.1	Tätigkeit im Berichtszeitraum	3
2.2	Zusammenarbeit mit anderen Aufsichts- und Kontrollinstitutionen	5
2.3	Meldungen zum Dateienregister und innerbehördliches Dateienverzeichnis	6
3.	**Archivwesen**	9
	Einsicht in die Personalakte eines verstorbenen Mitarbeiters des MfS	9
4.	**Ausländerangelegenheiten**	10
4.1	Datenübermittlungen im Kostenabrechnungsverfahren	10
4.2	Prüfung von Ausländerbehörden	11
5.	**Ausweis- und Meldewesen**	11
5.1	Melderegisterauskünfte für Verkehrssicherheitsaktion	11
5.2	Melderegisterauskünfte aus Anlaß der Landtagswahl	12
5.3	Automatisiertes Abrufverfahren für Melderegisterdaten	13
6.	**Bau- und Bodenrecht**	14
6.1	Planfeststellungen	14
6.2	Datenübermittlung an Beteiligte im Flurneuordnungsverfahren	16
6.3	Nutzung des Automatisierten Liegenschaftsbuches	17
7.	**Europäischer Datenschutz**	18
7.1	Richtlinie der Europäischen Union	18
7.2	EUROPOL	19
8.	**Entwicklung der automatisierten Datenverarbeitung**	21
8.1	Automatisierte Datenverarbeitung in der Landesverwaltung	21
8.2	Neue Strukturen und Technologien im Landesnetz	24
8.2.1	Elektronische Post	25
8.2.2	Sicherheitskonzept für das ITN-LSA	26
8.2.3	Datenschutz durch Technik - Datenschutzfreundliche Technologien	27
9.	**Finanzwesen**	28
9.1	Änderung der Abgabenordnung	28
9.2	Hundebestandsaufnahme zur Erfassung steuerpflichtiger Hundehalter	29
9.3	Steuergeheimnis und Grunderwerbsteuer	30
9.4	Steuerfahndung überprüfte Fördermittelunterlagen	31
9.5	Kontrolle eines Finanzamtes	33
9.5.1.	Probleme der Zugangskontrolle	33
9.5.2	Probleme bei der Schriftgutvernichtung	34
9.5.3	Versäumnisse bei den Melde- und Dokumentationspflichten	35
9.6	Unzulässige Datenübermittlungen bei den Steuerberaterkammern	36

10.	**Forschung**	37
10.1	Ausgewählte Forschungsprojekte	38
10.2	Epidemiologie und Datenschutz	39
10.3	Schutz medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen	40
11.	**Gesundheitswesen**	40
11.1	Gesetz über den Öffentlichen Gesundheitsdienst und die Berufsausübung im Gesundheitswesen	40
11.2	Chipkarten im Gesundheits- und Sozialwesen	41
11.3	Ärztliche Schweigepflicht	42
12.	**Gewerbe, Handwerk und Wirtschaft**	43
12.1	Novellierung der Handwerksordnung	43
12.2	Bekanntmachung öffentlich bestellter Sachverständiger im Internet	44
12.3	Einsicht des Gewerbeaufsichtsamtes in Stundennachweise	45
12.4	Datenabgleich von Ausbildungsverhältnissen	45
12.5	Korruptionsregister	46
12.6	Industrie- und Handelskammern	47
13.	**Hinweise zum technischen und organisatorischen Datenschutz**	48
13.1	Datumsumstellung 2000	48
13.2	Telefax	49
13.3	Datenübermittlungen im Internet und per E-Mail	50
13.4	Auftragsdatenverarbeitung durch nicht-öffentliche Auftragnehmer	51
13.4.1	Unterrichtung des Landesbeauftragten	51
13.4.2	Aktenvernichtung durch nicht-öffentliche Stellen	52
13.5	Datentransfer zwischen Anwendungsprogrammen unterschiedlicher Sicherheitsdomänen	53
13.6	Computerviren	54
13.7	Paßwortgestaltung	55
13.8	Fehlende Datenträgerkontrolle	57
14.	**Hochschulen**	58
	Lebenslauf bei der Veröffentlichung von Dissertationen	58
15.	**Kommunalverwaltung**	58
15.1	Veröffentlichung eines Redebeitrages aus einer Stadtratssitzung	58
15.2	Personaldaten für Haushaltsberatungen des Gemeinschafts-ausschusses	59
15.3	Kommunales Sachsen-Anhalt Netz (komsaNet)	60
15.4	Personaldatenübermittlung zwischen Stadtverwaltung und Stadtrat	62
15.5	Personaldatenübermittlung an den Gemeinschaftsausschuß	63
15.6	Datenerhebung für Aufgaben des Katastrophenschutzes	64
15.7	Bekanntgabe eines Bestattungstermins	65
16.	**Landtag**	65
	Datenschutz im Petitionsausschuß des Landtages	65
17.	**Landwirtschaft**	68
	Nachweis zweckentsprechender Verwendung von Fördermitteln	68

18.	**Personalwesen**	69
18.1	Personalfragebögen	69
18.2	Ungeschützte Personaldaten bei der Versendung von Lohnsteuerkarten	69
18.3	Personaldaten im sog. Konkurrentenklageverfahren	70
18.4	Datenschutz im Justizministerialblatt	72
18.5	Datenübermittlung aus Personalakten von Polizeibeamten	73
18.6	Formulare und Personenbezug	75
18.7	Anhörung von Beschäftigten vor den Personalkommissionen bei Gauck-Überprüfungsverfahren	75
18.8	Vorlage von ärztlichen Bescheinigungen auf dem Dienstweg	76
19.	**Personalvertretung**	77
19.1	Fragebögen zur Gesundheitsförderung aller Bediensteten	77
19.2	Einsichtnahme in Bewerbungsunterlagen durch den Personalrat	78
20.	**Polizei**	79
20.1	Überprüfung der Kriminalakten	79
20.2	ADV und Datensicherheit in den Polizeidirektionen	79
20.3	Defizite bei der polizeilichen Vorgangsverwaltung	81
20.4	Aufbewahren von Lichtbildern in der Lichtbildvorzeigekartei	82
20.5	Wahllichtbildvorlagen	84
20.6	Videoaufzeichnungen	84
20.6.1	Zur Gefahrenabwehr durch kommunale Stellen	84
20.6.2	Für die Aufgaben der Polizei	85
21.	**Rechtspflege**	86
21.1	Justizmitteilungsgesetz	86
21.2	Strafverfahrensänderungsgesetz	87
21.2.1	Generelle Anmerkungen	87
21.2.2	Anmerkungen zur Öffentlichkeitsfahndung	89
21.3	Einführung des sog. „Großen Lauschangriffs"	90
21.4	Parlamentarische Kontrolle des Einsatzes technischer Mittel in Wohnungen	92
21.5	DNA-Identitätsfeststellungsgesetz	94
21.6	Aufbewahrungsbestimmungen im Bereich der Justiz	96
21.7	Öffentlichkeitsfahndung mit Mängeln	96
21.8	Verdachtsanzeigen nach dem Geldwäschegesetz	97
21.9	Länderübergreifendes staatsanwaltschaftliches Verfahrensregister	98
21.10	Postbedienstete als Hilfsbeamte der Staatsanwaltschaft?	99
21.11	Übermittlung personenbezogener Daten aus Ermittlungsakten	99
21.12	Datenschutz beim Täter-Opfer-Ausgleich	102
21.13	Ein bissiger Hund - und seine Bewältigung durch die Staatsanwaltschaft	103
21.14	Organisatorische und andere Mängel bei einem Amtsgericht	105
21.15	Zusammenarbeit zwischen Justiz und Presse	106
21.16	Erstellung eines Vermögensverzeichnisses im Betreuungsverfahren	107
21.17	Abdrucke aus dem Schuldnerverzeichnis	107
21.18	Datenschutz bei Notaren	108
22.	**Schulen**	109
22.1	Wahlen zum Landeselternrat und Landesschülerrat	109

22.2	Schulentwicklungsplanung	109
22.3	Antrag auf Schulwechsel	110
23.	**Sozialwesen**	111
23.1	Probleme mit Jugendlichen	111
23.2	Ermäßigungs-/Erlaßanträge zu Kindertagesstätten	112
23.3	Aufweichung des Sozialgeheimnisses	112
23.4	Ein Antrag auf Wohnberechtigung und die Sammelwut einer Behörde	113
23.5	Anforderung von Krankenhausentlassungsberichten	114
23.6	Werbemaßnahmen der Krankenkassen	115
23.7	Übermittlung von Patientendaten zwischen Krankenhaus und gesetzlicher Krankenversicherung	116
23.8	Fehlbelegungsprüfungen in Krankenhäusern	117
23.9	Einsichtnahme in Unterlagen der ehemaligen Krankenversicherung	118
23.10	Entbindung von der ärztlichen Schweigepflicht in der Pflegeversicherung	118
23.11	„Datenabgleich“ zwischen zwei Sozialleistungsträgern	119
24.	**Statistik**	120
24.1	Volks- und Wohnungszählung 2001	120
24.2	Ausländereigenschaft kein Erhebungsmerkmal der Einkommens- und Verbrauchsstichprobe (EVS) 1998	121
24.3	Mikrozensus	122
25.	**Strafvollzug**	123
25.1	Gesetz zur Änderung des Strafvollzugsgesetzes	123
25.2	Entwurf eines Untersuchungshaftvollzugsgesetzes (UVollzG-E)	124
26.	**Verfassungsschutz**	127
27.	**Verkehr**	127
27.1	Neues Mammutregister im Straßenverkehrsrecht	127
27.2	Neues Fahrerlaubnisrecht - die Fahrerlaubnis-Verordnung	129
28.	**Vermessungs- und Katasterwesen**	132
	Datenübermittlung an einen Öffentlich bestellten Vermessungsingenieur	132
29.	**Wahlen**	133
	Ausschluß vom Wahlrecht und die datenschutzrechtlichen Folgen	133
30.	**Waffenrecht**	135
	Übermittlung personenbezogener Informationen aus Stasi-Unterlagen	135
31.	**Wasserrecht**	135
	Auskünfte an Bürgermeister über Gebührenschuldner	135

Anlagen

1	Organigramm der Geschäftsstelle	137
2	Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 - Beratungen zum StVÄG 1996	138
3	Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 - Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke	141
4	Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 - Geplante Verpflichtung von Teledienstean-bietern, Kundendaten an Sicherheitsbehörden zu übermitteln	144
5	Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 - Achtung der Menschenrechte in der Europäischen Union	146
6	Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997 - Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen	147
7	Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20. Oktober 1997 zu den Vorschlägen der Arbeitsgruppe des ASMK - „Verbesserter Datenaustausch bei Sozialleistungen“	149
8	Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 - Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts	153
9	Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 - Informationelle Selbstbestimmung bei Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren	156
10	Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 - Erforderlichkeit datenschutzfreundlicher Technologien	159
11	Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998 - Datenschutz beim digitalen Fernsehen	161

12 Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998 - Datenschutzprobleme der Geldkarte 163

13 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998 - Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten 164

14 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 - Fehlende bereichsspezifische Regelungen bei der Justiz 165

15 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 - Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge 168

16 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 - Weitergabe von Meldedaten an Adressbuchverlage und Parteien 169

17 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 - Entwicklungen im Sicherheitsbereich 170

18 Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998 - Dringlichkeit der Datenschutzmodernisierung 171

19 Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 1999 - Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben 173

20 Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 1999 - Transparente Hard- und Software 175

21 Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 1999 - Zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation 177

22 Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 1999 - Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL ‘98) 179

23 Deutsche Arbeitsgemeinschaft für Epidemiologie (DAE) Arbeitskreis Wissenschaft der Konferenz der Datenschutz-beauftragten des Bundes und der Länder - Epidemiologie und Datenschutz 180

Stichwortverzeichnis

Abkürzungsverzeichnis

A

AAÜG	Anspruchs-Anwartschafts-Überleitungs-Gesetz
ADV	Automatisierte Datenverarbeitung
AFIS	Automatisiertes Fingerabdruckidentifizierungssystem
AG	Aktiengesellschaft
AGE	Automatische Gebührenerhebung
AGIHKG	Gesetz über die Industrie- und Handelskammern in Sachsen-Anhalt
AKB e.V.	Arbeitsgemeinschaft Kammerleitstelle für Bemessungsgrundlagen e.V.
AKG GmbH	Arbeitsgemeinschaft Kammerleitstelle für Bemessungsgrundlagen GmbH
AktO-oG	Aktenordnung für die Gerichte der ordentlichen Gerichtsbarkeit und die Staatsanwaltschaften des Landes Sachsen-Anhalt
ALB	Verfahren Automatisiert geführtes Liegenschaftsbuch
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS - Innere Sicherheit
ArchG-LSA	Landesarchivgesetz
AuslG	Ausländergesetz
a.F.	alte Fassung

B

BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesarbeitsgericht
BArchG	Bundesarchivgesetz
BAT	Bundesangestelltentarifvertrag
BAT-O	Bundesangestelltentarifvertrag-Ost
BauGB	Baugesetzbuch
BauO LSA	Bauordnung des Landes Sachsen-Anhalt
BBiG	Berufsbildungsgesetz
BDSG	Bundesdatenschutzgesetz (neue Fassung)
BDSG 77	Bundesdatenschutzgesetz (alte Fassung)
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl. I	Bundesgesetzblatt, Teil I
BG LSA	Beamtengesetz Sachsen-Anhalt
Bit	Binary Digit (binäres Zeichen - kleinste Informationseinheit in der Datenverarbeitung)
BKA	Bundeskriminalamt
BKAG	Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes (Bundeskriminalamt)
BKK	Betriebskrankenkasse
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BNotO	Bundesnotarordnung
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
Btx	Bildschirmtext

BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz

C

CCITT	Comité Consultatif International Télégraphique et Téléphonique, Internationaler Normungsausschuß für Telekommunikation
CD-ROM	**C**ompact-**D**isk-**R**ead-**O**nly-**M**emory (im Preßverfahren erstellter bzw. einmal beschreibbarer und mehrfach lesbarer, optischer Datenträger im CD-Format)
CGI	Common Gateway Interface; CGI-Skripte dienen dem Anlegen interaktiver WWW-Seiten
CNPV LSA	Corporate Network der Polizei und der Verwaltung des Landes Sachsen-Anhalt

D

DEVO	Datenerfassungsverordnung
DIHT	Deutscher Industrie- und Handelstag e.V.
DNS	Domain Name Service
DONot	Dienstordnung für Notare
DORA	Dialogorientiertes Recherche- und Informationssystem
DÖV	Die öffentliche Verwaltung
Drs.	Drucksache
DSG-LSA	Datenschutzgesetz des Landes Sachsen-Anhalt
DV	Datenverarbeitung
DVO-EBG	Verordnung zur Durchführung des Gesetzes zur Förderung der Erwachsenenbildung im Lande Sachsen-Anhalt

E

EBG	Gesetz zur Förderung der Erwachsenenbildung im Lande Sachsen-Anhalt
ED	Erkennungsdienst
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
E-Mail	Electronic-Mail
EStG	Einkommenssteuergesetz
EU	Europäische Union
EUROCAT	Europäisches Register über große Fehlbildungen
EUROPOL	Europäisches Polizeiamt

F

FeV	Fahrerlaubnis-Verordnung
FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit
FISCUS	**F**öderales **i**ntegriertes **s**tandardisiertes **c**omputergestütztes **S**teuersystem
FRV	Fahrzeugregisterverordnung
FRZ	Finanzrechenzentrum
FTP	File Transfer Protocol
FVG	Finanzverwaltungsgesetz
FZR	Fahrzeugzentralregister

G

GBl.	Gesetzblatt der DDR
GBO	Grundbuchordnung
GDG-LSA	Gesundheitsdienstgesetz Sachsen-Anhalt
GemHVO	Gemeindehaushaltsverordnung
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz für die Bundesrepublik Deutschland
GLKA	Gemeinsames Landeskriminalamt
GO LSA	Gemeindeordnung des Landes Sachsen-Anhalt
GVBl. LSA	Gesetz- und Verordnungsblatt des Landes Sachsen-Anhalt
GVG	Gerichtsverfassungsgesetz
GwG	Geldwäschegesetz
GWZ	Gebäude- und Wohnungszählung

H

HAMISSA	**H**aushalts-**A**ufstellung, -**M**anagement- und **I**nformations-**S**ystem **S**achsen-**A**nhalt
HandwO	Gesetz zur Ordnung des Handwerks (Handwerksordnung)
HGB	Handelsgesetzbuch
HK	Handwerkskammer
HTML	HyperText Markup Language; Definitionssprache für WWW-Dokumente
HTTP	HyperText Transport Protocol; Protokoll zur Kommunikation zwischen WWW-Client und WWW-Server

I

IABV	Integriertes Automatisiertes Besteuerungsverfahren
IHK	Industrie- und Handelskammer
IHK-G	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern
IHK-GfI	IHK Gesellschaft für Informationsverarbeitung mbH Dortmund
IMA-IT	Interministerieller Arbeitskreis IT
INPOL	Informationssystem der Polizei auf Bundesebene
IRG	Gesetz über die internationale Rechtshilfe in Strafsachen
IT	Informationstechnik
ITN-LSA	Informationstechnisches Netz Sachsen-Anhalt
IuK	Informations- und Kommunikationstechnik

J

JAPrO	Ausbildungs- und Prüfungsordnung für Juristen
JBeitrO	Justizbeitreibungsordnung
JuMiG	Justizmitteilungsgesetz

K

KAG-LSA	Kommunalabgabengesetz des Landes Sachsen-Anhalt
KAI	Kriminalaktenindex
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KGHB-LSA	Gesetz über die Kammern für Heilberufe Sachsen-Anhalt
KiBeG	Gesetz zur Förderung und Betreuung von Kindern
KNSA	Kommunalnachrichten Sachsen-Anhalt
komsaNet	Kommunales Sachsen-Anhalt Netz
KpS	Kriminalpolizeiliche personenbezogene Sammlungen

KunstUrhG	Kunsturheberrechtsgesetz

L

LAN	Lokal Area Network
LKA	Landeskriminalamt
LKO LSA	Landkreisordnung des Landes Sachsen-Anhalt
LRZ	Landesrechenzentrum (in Halle)
LSA	Land Sachsen-Anhalt
LVerf	Verfassung des Landes Sachsen-Anhalt
LWG	Landeswahlgesetz

M

MAN	Metropolitan Area Network
MBl. LSA	Ministerialblatt des Landes Sachsen-Anhalt
MdE	Minderung der Erwerbsfähigkeit
MDK	Medizinischer Dienst der gesetzlichen Krankenversicherung
MDR	Mitteldeutscher Rundfunk
MeldDÜVO LSA	Meldedatenübermittlungsverordnung des Landes Sachsen-Anhalt
MfS	Ministerium für Staatssicherheit
MG LSA	Meldegesetz des Landes Sachsen-Anhalt
MHS	Message Handling System
MiStra	Anordnung über die Mitteilungen in Strafsachen
MiZi	Anordnung über die Mitteilungen in Zivilsachen
MO	**M**agnetic-**O**ptical (optischer Datenträger auf der Basis magnetischer Beschichtung), als - WORM-MO (nur einmal beschreibbar, mehrfach lesbar) und als - ROD-MO (**R**ewritable **O**ptical **D**isc, mehrfach wiederbeschreib- und lesbar)
MRRG	Melderechtsrahmengesetz
MTA	Message Transfer Agent

N

NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NotVO	Verordnung über die Tätigkeit von Notaren in eigener Praxis
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NUB-Richtl.	neue Untersuchungs- und Behandlungsmethoden
n.F.	neue Fassung

O

ÖbVermIng	Öffentlich bestellter Vermessungsingenieur
OECD	Internationale Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität
OVG	Oberverwaltungsgericht
Owi	Ordnungswidrigkeit
OWiG	Ordnungswidrigkeitengesetz

P

PC	Personal Computer
PersVG LSA	Landespersonalvertretungsgesetz Sachsen-Anhalt
PET	Privacy enhancing technology

PKH	Prozeßkostenhilfe
PKZ	Personenkennziffer
POLAS	Polizeiliche Auskunftssysteme
POLIS	**Pol**izeiliches **I**nformations**s**ystem Sachsen-Anhalt
PRAS	Planungs-, Realisierungs- und Abrechnungssystem
ProdGewStatG	Gesetz über die Statistik im Produzierenden Gewerbe
PVS	Personalverwaltungssystem

R

RettDG-LSA	Rettungsdienstgesetz des Landes Sachsen-Anhalt
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
RiVASt	Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten
RuStAG	Reichs- und Staatsangehörigkeitsgesetz

S

Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung
SchuVVO	Verordnung über das Schuldnerverzeichnis
SchwbG	Schwerbehindertengesetz
SGB	Sozialgesetzbuch
SGB X	Sozialgesetzbuch - Verwaltungsverfahren (10. Buch)
SGSA	Städte- und Gemeindebund Sachsen-Anhalt
SLA	Statistisches Landesamt
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SPUDOK	Spurendokumentation
SSL	Secure Socket Layer
StARegG	Gesetz zur Regelung von Fragen der Staatsangehörigkeit
StatG-LSA	Landesstatistikgesetz Sachsen-Anhalt
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StUG	Stasi-Unterlagen-Gesetz
StVÄG 1996	Entwurf eines Strafverfahrensänderungsgesetzes 1996
StVG	Straßenverkehrsgesetz
StVollzG	Strafvollzugsgesetz
StVZO	Straßenverkehrszulassungsordnung

T

TCP/IP	Transmission Control Protocol/Internet Protocol
TPA	Technisches Polizeiamt
TÜV	Technischer Überwachungs-Verein

U

UIG	Umweltinformationsgesetz
UNIFA	**Uni**x im **F**inanz**a**mt
UVollzG	Gesetz über den Vollzug der Untersuchungshaft

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
VermG	Vermögensgesetz
VermKatG	Vermessungs- und Katastergesetz des Landes Sachsen-Anhalt
VO	Verordnung
VONot	Verordnung über die Tätigkeit von Notaren in eigener Praxis

VRZ	Verbindungsstelle zum Finanzrechenzentrum
VV	Verwaltungsvorschrift
VwGO	Verwaltungsgerichtsordnung
VwKostG LSA	Verwaltungskostengesetz des Landes Sachsen-Anhalt
VwVfG	Verwaltungsverfahrensgesetz
VZR	Verkehrszentralregister

W

WAN	Wide Area Network
WoStatG	Wohnungsstatistikgesetz
WORM	Write Once Read Many (einmal beschreibbarer und mehrfach lesbarer, optischer Datenträger)
WWW	World Wide Web

X

X.25	Protokoll für Datenpaketvermittlung
X.400	Empfehlungen der Serie X.400 des CCITT (1984) für ein MHS

Z

ZER	Zentrales Einwohnermelderegister (DDR)
ZEVIS	Zentrales Verkehrsinformationssystem
ZFER	Zentrales Fahrerlaubnisregister
ZFR	Zentrales Fahrzeugregister
ZPO	Zivilprozeßordnung
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

1. Entwicklung des Datenschutzes

Die Entwicklung des Datenschutzes, richtiger der Schutz des Grundrechtes auf informationelle Selbstbestimmung und seine Sicherung mit Hilfe technischer und organisatorischer Maßnahmen, verlangt nach schnellerem und intensiverem Schutz für die betroffenen Bürger. Der Übergang zur Informationsgesellschaft, den wir alle teils mit Staunen, teils mit großem Unbehagen beobachten und vollziehen, bringt auch für dieses Gebiet ganz neue Herausforderungen. So ist es nicht verwunderlich, daß in einer 1998 von allen Datenschutzbeauftragten des Bundes und der Länder veranlaßten Repräsentativbefragung mehr als 55 % der Befragten angegeben haben, der Datenschutz sei für sie eine ganz wichtige Größe, und nahezu zwei Drittel der Befragten haben sich dafür ausgesprochen, daß der Datenschutz künftig mehr Bedeutung bekommen muß. Ebenso aufschlußreich war aber auch, daß keine 20 % der Befragten genau sagen konnten, wie man dieses künftig erreichen soll und welchen Weg sie persönlich für die Durchsetzung ihres persönlichen Schutzes einschlagen würden.

Auch die hohe Politik und die Fachwelt haben diesen wichtigen Bereich im täglichen Leben einer demokratischen Gesellschaft erneut ins Blickfeld genommen. So wird in einer weltweit beachteten Erklärung der G 7-Staaten im Jahre 1998 der Datenschutz ebenso erwähnt wie in der Koalitionsvereinbarung der neuen Bundesregierung vom Oktober 1998. Der angesehene Deutsche Juristentag sprach sich auf seiner Tagung im September 1998 in seinen Beschlüssen dafür aus, die Datenschutzrechte der Bürger zu stärken, ihre Information und die Aufklärung über ihre Wahlmöglichkeiten auszuweiten und in einem zu modernisierenden Datenschutzrecht die Grundsätze der Datenvermeidung, den Schutz durch Technik und die Zweckbindung der Daten in den Mittelpunkt zu stellen. Ob dies so geschehen wird und dann auch noch rechtzeitig, darf bezweifelt werden.

Schon lange beklagen wir, daß die rechtlichen Absicherungen zum Schutz der Bürger nur halbherzig erfolgen und weit hinter den technischen Entwicklungen herlaufen. Seit Oktober 1998 ist die Bundesrepublik säumig bei der Umsetzung der Europäischen Datenschutzrichtlinie, und in der bundesdeutschen Gesetzgebung wird der Schutz des Bürgers gegenüber staatlichen Eingriffen eher verwässert und zurückgedrängt, wie sich bei den neu geschaffenen Abhörmöglichkeiten im privaten Wohnungsbereich und bei der Aufweichung des Sozialgeheimnisses für bereichsübergreifende Leistungsabgleiche gezeigt hat.

Immer schwieriger wird es, Bürgerinnen und Bürger vor Gefahren und Mißbräuchen beim Umgang mit der modernen Informations- und Kommunikationstechnik zu schützen. Dabei verwischen sich die gerade im deutschen Recht noch vorhandenen Unterschiede bei der Qualität des Schutzes im privaten (nicht-öffentlichen Lebensbereich) und dem im Grundsatz besser geschützten öffentlichen Bereich. Im privaten Bereich geht das Interesse der Anbieter eher dahin, dem Kunden möglichst schnell und ohne großen Aufwand etwas zu verkaufen. Da ist die Beschränkung bei der Sammlung personenbezogener Kundendaten und ihre Sicherung bei der Kommunikation eher hinderlich.

Die öffentlichen Stellen sind bemüht, ihr schlechtes Image als Dienstleistungsanbieter mit Hilfe der modernen Technik zu verbessern und gleichzeitig mit Hilfe der modernen elektronischen Datenverarbeitungsmöglichkeiten Aufgabenbewältigung und Personaleinsatz zu rationalisieren. Auch dabei ist der Datenschutz wegen der Zweckgebundenheit der Daten oft hinderlich. Und in der ungetrübten Euphorie beim Einsatz neuer Kommunikationswege (Internet/Intranet) werden die Schwachstellen bei der Datensicherheit mangels ausreichender Aus- und Fortbildung im öffentlichen Bereich nicht erkannt.

Ein bei der Rationalisierung in öffentlichen Stellen auch in Sachsen-Anhalt oft zu hörender Begriff ist "Outsourcing". Die Auslagerung bestimmter öffentlicher Aufgaben auf eine andere (öffentliche oder nicht-öffentliche) Stelle zur selbständigen Aufgabenerledigung ist für die Bürger besonders gefährlich, wenn die neue Stelle nicht mehr in der Form der Auftragsdatenverarbeitung tätig wird, sondern ihr die Verarbeitung der personenbezogenen Daten eigenverantwortlich übertragen wird. Dabei ist nicht die zulässige Übertragung öffentlicher Aufgaben auf private Dienstleister das Problem. Problematisch ist die unzureichende Absicherung des Datenschutzes durch vertragliche und technische Grenzen.

Mehr als bisher können bei einer so gewandelten rechtlichen und technischen Arbeitsweise die Kontrollen des Landesbeauftragten bei den öffentlichen Stellen nur noch punktuell Grenzen setzen. Schwerpunkte müssen deshalb künftig in der Beratung des Bürgers zur wachsamen Selbsthilfe einerseits und zur Anwendung sicherer Datenverarbeitungskonzepte bei den öffentlichen Stellen andererseits gesehen werden. Der Einsatz von Internet und E-Mail kann auch öffentlichen Stellen bei der Arbeitsbewältigung gute Dienste leisten. Dies setzt aber rechtlich wie tatsächlich einen gut durchdachten und sicher erlernten Umgang mit dieser Technik voraus. Daran fehlt es noch sehr.

2. Der Landesbeauftragte

Der Landesbeauftragte und seine Mitarbeiter können am Ende dieses Berichtszeitraumes auf eine Tätigkeit von fast 8 Jahren zurückblicken, davon 7 Jahre als eigenständige Behörde. Damit war der Auf- und Umbau der vielen öffentlichen Stellen in und außerhalb der Landesverwaltung von Beginn an datenschutzrechtlich begleitet. Die langjährige Tätigkeit hat für die Mitarbeiterinnen und Mitarbeiter des Landesbeauftragten zu umfangreichen Erfahrungen und Detailkenntnissen geführt. Aus der Aufbauarbeit wurde in einen neuen Abschnitt der konstanten und routinierten Erledigung der Aufgaben übergeleitet. Bewährt hat sich dabei die Teamarbeit zwischen den rechtlich und technisch ausgeprägten Arbeitsbereichen.

Im Frühjahr 1998 kam es erstmals seit längerem auch wieder zu einem personellen Wechsel im Bereich des höheren Dienstes. Ein Referatsleiter wechselte zunächst ins Ministerium der Justiz und später ins Ministerium des Innern, und der Landesbeauftragte konnte als Nachfolgerin eine versierte Referatsleiterin aus dem Ministerium des Innern gewinnen.

Die globale Entwicklung der Datenverarbeitung zwingt auch zur Neubesinnung bei den Arbeitsschwerpunkten, deshalb wurde im Referat 1 ein neuer Querschnittsbereich "Europa" eingerichtet. Die derzeitige Aufgabengliederung ergibt sich aus dem als **Anlage 1** ausgedruckten Organigramm der Behörde.

2.1 Tätigkeit im Berichtszeitraum

Der Landesbeauftragte hat sich in diesem Bericht wieder bemüht, aus der Vielzahl der angefallenen Arbeitsvorgänge in den folgenden Ziffern einen repräsentativen Querschnitt darzustellen. Der im letzten Tätigkeitsbericht (S. 4) festgestellte ständige Anstieg der Geschäftseingänge in den Jahren 1995 und 1996 hat sich erfreulicherweise im Berichtszeitraum nicht fortgesetzt, sondern sich - insbesondere nach dem Rückgang der Gesetzesnovellierungen auf Bundes- und später auch auf Landesebene - auf einem etwas niedrigerem Niveau stabilisiert. 1997 gab es fast 3.200 schriftliche Eingänge, im Jahre 1998 fast 3.000. 1997 sind dazu 733 und 1998 570 schriftliche Stellungnahmen erarbeitet worden.

Gleich geblieben ist die Zahl der fernmündlichen Anfragen durch öffentliche und private Stellen; sie liegt bei ca. 700 pro Jahr.

Konstant geblieben ist auch die Anzahl der persönlichen Anfragen und Vorsprachen in der Behörde des Landesbeauftragten (ca. 30 bis 35 im Jahr). Leicht erhöht hat sich demgegenüber die Zahl der Bürgereingaben (ca. 180 pro Jahr). Die Erhöhung liegt, offenbar einem Zug der Zeit folgend, mehr in den fernmündlich vorgetragenen Anliegen. Leicht gefallen ist demgegenüber die Erfolgsquote der Eingaben; die Überprüfung ergab nur noch in etwa jedem 4. Fall datenschutzrechtliche Fehler beim Umgang mit den personenbezogenen Daten durch die öffentlichen Stellen.

Die formellen Beanstandungen nach § 24 DSG-LSA sind auch im Berichtszeitraum im einstelligen Bereich geblieben, in etwa 30 weiteren Fällen hat der Landesbeauftragte von einer Beanstandung abgesehen. Beide Beobachtungen dürften ihren Grund in der zunehmend verbesserten Aus- und Fortbildung in den öffentlichen Stellen des Landes haben.

Auffällig war in diesem Berichtszeitraum die Häufung von Mängeln und Fehlern im Geschäftsbereich des Ministeriums der Justiz, ohne daß es dort besondere Kontrollen gegeben hat. Dies war im Laufe des letzten Jahres Anlaß für zwei eingehende Besprechungen mit der Staatssekretärin. Akzeptanzprobleme der datenschutzrechtlichen Kontrolle und Nervositäten zeigten sich dabei insbesondere im nachgeordneten Bereich bei einzelnen Staatsanwaltschaften.

Weiter stark angestiegen sind der Bedarf an Besprechungen und die Bitten um Beratungen der Probleme vor Ort. Dabei lagen die Problembereiche gut verteilt je zur Hälfte im materiell-rechtlichen und im technisch-organisatorischen Bereich. Diffiziler Punkt ist die Datensicherheit bei den überall im Lande aufbrechenden Wünschen nach Vernetzung und Teilhabe an einer behörden- und auch landesübergreifenden Datenkommunikation. Einzelheiten dazu finden sich im folgenden Bericht unter den Ziffern 8 und 13.

Schwerpunkte der unabhängigen Anlaßkontrollen waren im Berichtszeitraum die neuen Kontrollen bei den kriminalaktenführenden Behörden der Polizei, die fortgesetzten Querschnittskontrollen bei den Ausländer- und Meldebehörden

und bei personalaktenführenden Stellen im Lande. Eine erste Kontrolle gab es im Bereich der Finanzämter des Landes und der OFD. Neue Kontrollen sind im weitgefächerten Bereich des Gesundheitswesens vorgesehen.

Die gleichbleibend hohe Arbeitsbelastung hat die Mitarbeiterinnen und Mitarbeiter nicht davon abgehalten, an Aus- und Fortbildungsveranstaltungen im öffentlichen und im privaten Bereich teilzunehmen und selbst auch als Dozenten aufzutreten.

Fortgeführt und intensiviert wurde auch die Zusammenarbeit mit den Medien. Die Auswertung ihrer Berichte und ihre gezielten Anfragen anhand aktueller Probleme der Bürger sind eine wichtige Größe im direkten Umsetzen datenschutzrechtlicher Anliegen.

2.2 Zusammenarbeit mit anderen Aufsichts- und Kontrollinstitutionen

Nahtlos kann hier an die positiven Erfahrungen aus dem III. Tätigkeitsbericht (S. 5 ff) angeknüpft werden. Unverändert gut ist die Zusammenarbeit mit dem Landtag sowohl im Verwaltungs- als auch im parlamentarischen Bereich. Wünsche zu Beratungen und Informationen einzelner Fraktionen nach der Landtagswahl 1998 hat der Landesbeauftragte gerne aufgegriffen. Dank schulden der Landesbeauftragte und seine Mitarbeiter auch dem langjährigen Landtagspräsidenten der Ersten und Zweiten Legislaturperiode, Dr. Keitel, für sein stets großes Interesse an der Arbeit dieser Behörde, seiner Akzeptanz ihrer unabhängigen Sacharbeit und seiner konsequenten Unterstützung bei administrativen Maßnahmen.

Einvernehmlich und vertrauensvoll ist auch die Zusammenarbeit mit dem neuen Landtagspräsidenten. Zwischen Herrn Schaefer und der Arbeit des Landesbeauftragten gab es bereits in der Vergangenheit aus seiner parlamentarischen Tätigkeit als Vorsitzender des Finanzausschusses und aus seiner späteren Tätigkeit als Finanzminister der Landesregierung viele positive Berührungspunkte.

Aus der guten und sachorientierten Zusammenarbeit mit den obersten Landesbehörden ist insbesondere die intensive und konstruktive Zusammenarbeit mit

dem bei der Exekutive für den Datenschutz verantwortlichen Ministerium des Innern hervorzuheben. Wie bereits in der Vergangenheit haben auch im letzten Berichtszeitraum rechtzeitige Abstimmungen und das Ringen um praxisbezogene datenschutzrechtliche Lösungen seitens der Exekutive die Arbeit des Landesbeauftragten erleichtert. Das schließt sachliche Differenzen in der Bewertung nicht aus. Die Anpassung des Gesetzes zum Schutz personenbezogener Daten der Bürger an die seit Oktober 1998 geltende EG-Datenschutzrichtlinie und eine Überarbeitung des SOG LSA sind die nächsten wichtigen Aufgaben im datenschutzrechtlichen Bereich.

Erfolgreich und gut ist auch die dem Landesbeauftragten gesetzlich obliegende Zusammenarbeit mit den datenschutzrechtlichen Kontrollinstitutionen im nationalen und internationalen Bereich. Gerade die vielfältigen Zuständigkeiten auf Bundes- und Länderebene machen die enge Abstimmung in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die Detailarbeit in ihren Arbeitskreisen für einen effektiven Datenschutz auch im Lande Sachsen-Anhalt unentbehrlich.

Das gilt immer mehr auch für die länderübergreifende Zusammenarbeit der für die Beachtung und Einhaltung des Datenschutzes eingesetzten unabhängigen Kontrollinstanzen in Europa und in den außereuropäischen Ländern. Deutlich wird dies z.B. dann, wenn künftig Behörden der europäischen Nachbarländer auch direkt auf automatisierte personenbezogene Datensammlungen in Behörden der Bundesrepublik zugreifen können (vgl. Ziff. 27).

Der Landesbeauftragte hat deshalb auch im Berichtszeitraum an einer europäischen und einer internationalen Datenschutzkonferenz teilgenommen.

Seit Oktober 1998 ist ihm zusätzlich seitens des Bundes die Aufgabe des zweiten unabhängigen deutschen Vertreters in der Gemeinsamen Kontrollinstanz für EUROPOL übertragen worden.

2.3 Meldungen zum Dateienregister und innerbehördliches Dateienverzeichnis

Das Register der automatisiert geführten Dateien, das seit nunmehr 7 Jahren beim Landesbeauftragten geführt wird, beinhaltet mittlerweile über **2300 Meldungen**. Dabei kann festgestellt werden, daß in den vergangenen beiden Jahren die Anzahl der (gesetzlich vorgeschriebenen) Meldungen im Vergleich zu

den Vorjahren erheblich zugenommen hat **(Abb. 1)**. Als Folge der Kritik im III. Tätigkeitsbericht (S. 10 f) sind vor allem im Bereich der Kommunalverwaltung viele Verwaltungsgemeinschaften ihrer Meldepflicht nachgekommen **(Abb. 2)**.

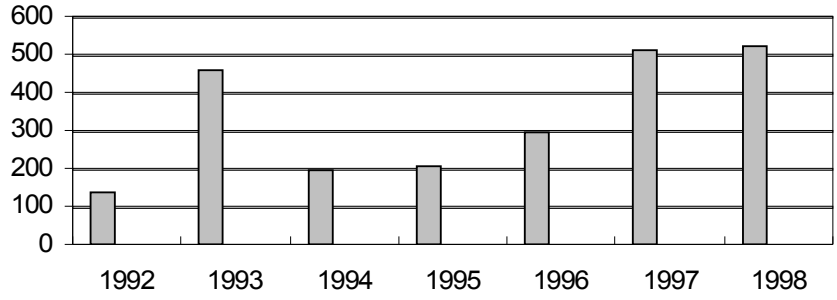


Abb. 1: Anzahl der Meldungen zum Dateienregister in den Jahren 1992 - 1998

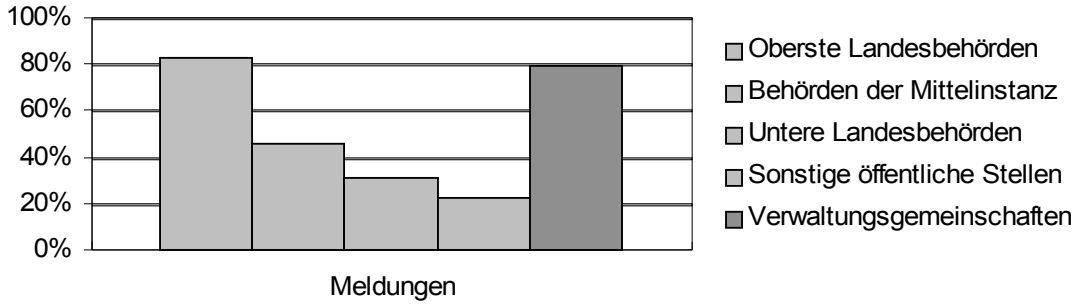


Abb. 2: Meldeverhalten der öffentlichen Stellen

Leider hat sich mit der gewachsenen Quantität die inhaltliche Qualität der Meldungen nicht verbessert. Obwohl der Landesbeauftragte in allen seinen Tätigkeitsberichten (vgl. Tätigkeitsberichte I., S. 22; II., S. 12; III., S. 10 f) auf die Mängel hingewiesen hat, bestehen nach wie vor erhebliche Defizite. Die häufigsten Kritikpunkte sind immer noch:

- ungenaue Angabe der Art der gespeicherten Daten,
- falsche Rechtsgrundlage für die Verarbeitung der Daten und
- fehlende Löschungsfristen.

Des öfteren erreichten den Landesbeauftragten Dateimeldungen, die außer der Dateibezeichnung, dem Zweck und dem betroffenen Personenkreis keine weiteren Angaben enthielten. Einige Behörden schickten seitenweise Programmbeschreibungen und Dokumentationen, die den Aufbau der einzelnen Datensätze des Programms beschrieben, ob mit oder ohne Personenbezug. Und es gab öffentliche Stellen, die sogenannte "Fehlmeldungen" schickten, d. h. eigentlich,

daß in der jeweiligen Behörde keine personenbezogenen Daten automatisiert verarbeitet werden. Auf Nachfrage des Landesbeauftragten stellte sich dies jedoch jedesmal als falsch heraus.

Bei der Vielzahl der Dateimeldungen aus den Verwaltungsgemeinschaften, Stadt- und Gemeindeverwaltungen fiel auf, daß oft nur eine einzige automatisierte Datei, nämlich die Einwohnermeldedatei zum Dateienregister gemeldet wurde. Der Landesbeauftragte regt deshalb an, in diesen öffentlichen Stellen noch einmal zu prüfen, ob nicht auch z. B. Personaldaten der Beschäftigten, Daten Zahlungspflichtiger bzw. -empfänger, Daten von Grundstückseigentümern und andere personenbezogene Daten automatisiert verarbeitet werden.

Die Möglichkeit der kostenlosen Einsichtnahme in das Dateienregister wurde von den Bürgerinnen und Bürgern auch in den vergangenen 2 Jahren nicht wahrgenommen (vgl. schon III. Tätigkeitsbericht, S. 8). Obwohl das Dateienregister ebenso für die Durchführung von Kontrollen bei den öffentlichen Stellen des Landes genutzt wird, wurde es nach dem Willen des Gesetzgebers vorrangig zur Information für die Bürgerinnen und Bürger eingerichtet.

Der Landesbeauftragte sieht sich deshalb in seiner Auffassung bestätigt, bei der bevorstehenden Novellierung des DSG-LSA entsprechend der von ihm unterbreiteten Vorschläge diese Bestimmungen zu ändern (vgl. III. Tätigkeitsbericht, S. 9).

Davon unberührt bleibt die gesetzliche Verpflichtung jeder öffentlichen Stelle gem. § 14 Abs. 2 Satz 2 DSG-LSA, ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen sowie ein innerbehördliches Dateienverzeichnis zu führen.

Diese Regelung bildet eine grundsätzliche Voraussetzung zur Durchsetzung der Ordnungsmäßigkeit der automatisierten Datenverarbeitung innerhalb der öffentlichen Stelle. Sicherheit in diesem Bereich verlangt Ordnung und Übersicht. Nur so ist es in einer öffentlichen Stelle möglich, z. B. im Falle einer Unregelmäßigkeit bei der Verarbeitung, einer eventuellen Manipulation, eines Diebstahls oder Brandes festzustellen, welche Geräte und Datenbestände betroffen sind und wie groß der entstandene Schaden ist.

Zum anderen dient das innerbehördliche Dateienverzeichnis zur Sicherstellung der Auskunftsverpflichtung gegenüber den Bürgerinnen und Bürgern gem. § 15 Abs. 1 DSG-LSA. Auf diesen weiteren Aspekt hatte der Landesbeauftragte bereits in seinem III. Tätigkeitsbericht (S. 8 f) hingewiesen.

3. Archivwesen

Einsicht in die Personalakte eines verstorbenen Mitarbeiters des MfS

Ein Landkreis übersandte dem Landesbeauftragten den Antrag eines Bürgers auf Einsicht in die archivierte Personalakte eines verstorbenen MfS-Mitarbeiters mit der Bitte, "eine Prüfung nach dem Datenschutzgesetz vorzunehmen".

Der Landkreis wurde darauf hingewiesen, daß das DSG-LSA nur auf natürliche und lebende Personen Anwendung findet (vgl. § 2 Abs. 1 DSG-LSA), der Landesgesetzgeber aber mit dem Landesarchivgesetz (ArchG-LSA) im Jahre 1995 eine spezialgesetzliche Rechtsgrundlage geschaffen hat, die den Umgang mit Archivgut im Landesbereich regelt.

Nach § 10 Abs. 3 Satz 3 ArchG-LSA darf öffentliches Archivgut, das sich nach seiner Zweckbestimmung auf natürliche Personen bezieht, erst 30 Jahre nach dem Tode der Betroffenen durch Dritte genutzt werden. Zwar sieht das ArchG-LSA die Möglichkeit einer Verkürzung der Schutzfrist vor, diese bedarf jedoch einer gesonderten Prüfung durch den Landkreis. Allein der Hinweis des Antragstellers, es handele sich um einen Mitarbeiter des MfS (IM), läßt nicht darauf schließen, daß die Voraussetzungen des § 10 Abs. 4 Ziff. 3 ArchG-LSA erfüllt sind.

Bei dieser Gelegenheit wurde durch den Landesbeauftragten auch festgestellt, daß der im Kreisarchiv verwendete Benutzerantrag auf Rechtsgrundlagen verweist, die durch § 15 ArchG-LSA aufgehoben wurden.

Der Vollständigkeit halber sei angefügt, daß die Möglichkeiten zur Einsichtnahme in Vorgänge, die bei der sog. "Gauck-Behörde" aufbewahrt werden, in den Bestimmungen des Stasi-Unterlagen-Gesetzes geregelt sind.

4. Ausländerangelegenheiten

4.1 Datenübermittlungen im Kostenabrechnungsverfahren

Gegenüber den Regierungspräsidien des Landes machten gleich mehrere Landkreise ihre datenschutzrechtlichen Bedenken geltend, als sie aufgefordert wurden, ihren Erstattungsanträgen im Kostenabrechnungsverfahren detaillierte personenbezogene Datenaufstellungen aller betroffenen Ausländer beizufügen. Das Ministerium des Innern hatte dafür anfangs kein Verständnis und wollte deshalb vom Landesbeauftragten wissen, wie er den Sachverhalt beurteile.

Nach Auffassung des Landesbeauftragten ist die - gewissermaßen automatische - Übermittlung personenbezogener Daten der von der Kostenerstattung betroffenen Ausländer nicht zulässig. § 11 Abs. 1 i.V. mit § 10 Abs. 1 und 3 Satz 1 DSG-LSA läßt die Übermittlung personenbezogener Daten nur zu, soweit sie zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben **erforderlich** ist. Nach den - die Verwaltung bindenden - Verwaltungsvorschriften zum Gesetz zum Schutz personenbezogener Daten der Bürger (VV-DSG-LSA) ist bei der Beurteilung der Erforderlichkeit ein strenger Maßstab anzulegen und das Übermittlungsersuchen auf das zum Erreichen des angegebenen Zieles erforderliche Minimum zu beschränken (vgl. 9.1 VV-DSG-LSA). Nur so läßt sich im Ergebnis die vom Bundesverfassungsgericht zugunsten der Bürger geforderte Übersichtlichkeit und enge Zweckbindung bei der personenbezogenen Datenverarbeitung gewährleisten. Mit diesen datenschutzrechtlichen Vorgaben wäre die Übermittlung der personenbezogenen Daten **sämtlicher** Kostenerstattungsfälle aus den Landkreisen an das jeweilige Regierungspräsidium nicht zu vereinbaren.

Die personenbezogene Rechnungsprüfung obliegt zunächst den Rechnungsprüfungsämtern. Die in § 10 Abs. 3 Satz 1 DSG-LSA vorgesehene Ausnahmeregelung läßt personenbezogene Datenübermittlung zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen nur zur **konkreten Einzelfallprüfung** im Rahmen der Fachaufsicht zu. Darüber hinaus bleibt die Möglichkeit der Geschäftsprüfung.

Das sah das Ministerium ein und änderte das Verfahren.

4.2 Prüfung von Ausländerbehörden

Der Landesbeauftragte hat im Berichtszeitraum die Prüfung von Ausländerbehörden fortgesetzt (vgl. III. Tätigkeitsbericht, S. 14 f). Die dort getroffenen generellen Feststellungen haben sich auch bei den weiteren Kontrollen bestätigt.

Außerdem hat der Landesbeauftragte festgestellt, daß die Ausländerdateien A und B von den Ausländerbehörden überwiegend automatisiert geführt werden. Dazu wird meistens das Programm "AUSO" eingesetzt. Diese Software läßt den Zugriff jedes Sachbearbeiters der Ausländerstelle auf alle personenbezogenen Daten sämtlicher gespeicherter Ausländer zu.

Das hält der Landesbeauftragte jedenfalls bei größeren Behörden nicht für datenschutzgerecht.

Datenschutzrechtlich erforderlich und damit ausreichend dürfte sein, daß jeder Sachbearbeiter (bzw. die Vertreter) auf die personenbezogenen Daten seines Zuständigkeitsbereiches zugreifen kann.

Das Ministerium des Innern des Landes hat es unter Hinweis auf § 6 Abs. 1 Satz 2 DSG-LSA wegen des seiner Ansicht nach unangemessen großen Aufwands abgelehnt, den Ausländerbehörden des Landes eine Änderung dieses Verfahrens nahezulegen.

Die Kontrollen werden fortgesetzt.

5. Ausweis- und Meldewesen

5.1 Melderegisterauskünfte für Verkehrssicherheitsaktion

Der Deutsche Verkehrssicherheitsrat e.V. plante gemeinsam mit dem Ministerium des Innern eine Verkehrssicherheitsaktion zur Verhütung von Alkoholunfällen. Junge Leute zwischen 16 und 24 Jahren sollten direkt angeschrieben und zur Eigen- und Mitverantwortung animiert werden. Die Meldedatenübermittlungen an den Deutschen Verkehrssicherheitsrat e.V. waren als Gruppenauskunft gem. § 33 Abs. 3 MG LSA zu beurteilen. Das geforderte "öffentliche Interesse" konnte angenommen werden, weil die Verkehrssicherheitsaktion zur Verhütung

von Alkoholunfällen in Anbetracht der hohen Unfallzahlen unter Alkoholeinfluß eine sinnvolle Präventivmaßnahme ist. Auswahl und Übermittlung der in Frage kommenden Meldedaten waren durch das Meldegesetz des Landes Sachsen-Anhalt gedeckt.

Der Landesbeauftragte hat jedoch angeregt, dem Deutschen Verkehrssicherheitsrat e.V. lediglich Adreßaufkleber mit der Maßgabe zur Verfügung zu stellen, sie ohne Anfertigung einer Kopie zu verwenden. Unverbrauchte Adreßaufkleber seien zu vernichten. Außerdem sollte gem. § 35 Abs. 1 MG LSA auf die Zweckbindung und bei deren Nichtbeachtung auf die Strafbarkeit hingewiesen werden. Damit lassen sich z.B. unerwünschte Werbemaßnahmen von vornherein rechtlich verhindern.

5.2 Melderegisterauskünfte aus Anlaß der Landtagswahl

Vor der Landtagswahl 1998 haben viele wahlberechtigte Bürger Post mit Wahlwerbung erhalten. Dies hat zu unzähligen, zum Teil empörten Anfragen beim Landesbeauftragten hinsichtlich der Zulässigkeit von Meldedatenübermittlungen geführt.

Nach § 34 Abs. 1 MG LSA **darf** die Meldebehörde Parteien, Wählergruppen und Einzelbewerbern ab 6 Monaten vor dem Wahltermin Auszüge aus dem Melderegister erteilen, damit diese z.B. Einladungen zu Werbeveranstaltungen, Werbebriefe und Kandidatenvorstellungen versenden können. Der Melderegisterauszug umfaßt folgende gespeicherte Daten:
Vor- und Familienname, Doktorgrad und Anschrift von Wahlberechtigten.

Die Meldebehörden können das ihnen eingeräumte Ermessen aber auch dahin auslegen, daß sie im Interesse der Bürger eine Datenübermittlung an die Parteien generell verweigern. Dies haben einzelne Gemeinden auch getan. Diese Rechtsauffassung haben das Verwaltungsgericht Dessau (Beschluß vom 04.03.1998, Az: B2K 104/97) und das Oberverwaltungsgericht Magdeburg ausdrücklich bestätigt. Eine Differenzierung zwischen einzelnen Parteien ist den Behörden jedoch versagt, denn jede durch den Landeswahlleiter zur Wahl zugelassene Partei oder Gruppierung hat einen Anspruch auf Gleichbehandlung.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, daß die Rechte der Bürgerinnen und Bürger verbessert werden. Dazu haben sie in ihrer Entschließung vom 05./06.10.1998 vorgeschlagen, Melderegisterauskünfte an Parteien und Adreßbuchverlage nur bei vorheriger **Einwilligung** der Bürger vorzunehmen **(Anlage 16).**

Ob der Landesgesetzgeber diesem Ratschlag folgt, bleibt abzuwarten. Bis dahin bleibt den Bürgern nichts anderes übrig, als selber tätig zu werden. Jeder hat das Recht, seinerseits gegenüber der Meldebehörde einer solchen Übermittlung seiner Daten zu widersprechen. Darauf muß jeder Einwohner sowohl bei der Anmeldung als auch mindestens einmal jährlich durch öffentliche Bekanntmachung (z.B. in der Tageszeitung oder im örtlichen Schaukasten) hingewiesen werden. Der Widerspruch muß **nicht** begründet werden und wird gebührenfrei bearbeitet.

5.3 Automatisiertes Abrufverfahren für Melderegisterdaten

Eine kommunale Gebietskörperschaft hat die Frage aufgeworfen, ob die Einrichtung eines automatisierten Abrufverfahrens von Daten aus dem Melderegister für Zwecke des Sozialamtes und des Ordnungsamtes zulässig ist. Hierzu hat der Landesbeauftragte in Übereinstimmung mit dem für Melderecht zuständigen Ministerium des Innern folgende Auffassung vertreten:

Bereichsspezifische Grundlage ist das Meldegesetz des Landes Sachsen-Anhalt, das den Verwaltungsgemeinschaften und Gemeinden die Aufgaben der Meldebehörde zugewiesen hat (§ 2 MG LSA).

Das Gesetz sieht in § 32 eine Rechtsgrundlage für eine regelmäßige Datenübermittlung, d.h. die Bekanntgabe der gespeicherten Daten **an einen Dritten,** durch Rechtsverordnung vor. Eine derartige Verordnung ist die MeldDÜVO-LSA, die den dort im einzelnen aufgeführten öffentlichen Stellen ein automatisiertes Abrufverfahren gestattet (§ 1 MeldDÜVO-LSA).

Für eine dienstliche Verwendung personenbezogener Einwohnerdaten **innerhalb** der Meldebehörde hat der Gesetzgeber in § 29 Abs. 5 MG LSA ein erleichtertes Verfahren zur Weitergabe vorgesehen. Das bedeutet aber nicht, daß dort

jeder Bedienstete oder jedes Amt in der Behörde auf alle in § 22 **Abs. 1** MG LSA genannten Daten ohne weiteres Zugriff erhalten kann. Vielmehr muß die Zugriffsberechtigung im automatisierten Verfahren für die Aufgabenwahrnehmung im Regelfall zwingend erforderlich sein. Dazu gehört u.a., daß die jeweilige Amtsleitung einen Katalog der benötigten aufgabenorientierten Daten erarbeitet und die Freischaltung des gewünschten Datenbestandes bei der Verwaltung des Melderegisters beantragt. Dies hat in schriftlicher Form zu geschehen, damit der Umfang von den zuständigen Stellen - ggf. auch vom Landesbeauftragten für den Datenschutz - geprüft werden kann. Dadurch, daß die Verwaltung des Melderegisters beim automatisierten Abrufverfahren auf die Einzelfallprüfung verzichtet, wird auch die Zweckbindung der Daten nicht außer Kraft gesetzt, sondern lediglich durch die Freigabe einem praktischen Bedürfnis für wiederkehrende Fälle angepaßt. Mit Ausnahme der in § 33 Abs. 1 MG LSA aufgeführten sog. einfachen Meldedaten muß deshalb beim Empfänger für die übrigen erhaltenen Daten ein Zwecknachweis vorhanden sein.

Sind in einem begründeten Einzelfall weitere als die für das automatisierte Abrufverfahren freigeschalteten Daten notwendig, muß deren Weitergabe für diesen Fall bei der Verwaltung des Melderegisters angefordert werden.

Als zusätzliche Sicherung für das automatisierte Abrufverfahren ist es unabdingbar, die Online-Zugriffe mit allen Daten zu protokollieren. Hinsichtlich der Protokollierungshäufigkeit gibt es einen gewissen Spielraum (vgl. z.B. die Regelung in § 2 Abs. 3 Satz 2 MeldDÜVO-LSA).

6. Bau- und Bodenrecht

6.1 Planfeststellungen

Aufgrund verschiedener Einzelfälle - auch in anderen Bundesländern - hat der Landesbeauftragte den betroffenen Ministerien des Landes Anregungen und Hinweise zur Einhaltung des Datenschutzes in Planfeststellungsverfahren gegeben.

Zur **öffentlichen Bekanntmachung** des Planfeststellungsbeschlusses wies er auf zwei Beschlüsse des Bundesverfassungsgerichts hin, in denen die Veröffentlichung von personenbezogenen Daten, die ein Einwendungsführer der Planfeststellungsbehörde preisgibt, für verfassungswidrig erklärt worden war. Das Gericht war dabei zu Gunsten der Betroffenen davon ausgegangen, daß keine Gründe ersichtlich sind, warum eine ordnungsgemäße Begründung des Planfeststellungsbeschlusses notwendigerweise neben den sachbezogenen Erwägungen zur Beurteilung und Gewichtung der geltend gemachten Einwendungen auch die personenbezogenen Daten des Einwenders enthalten muß.

Bezüglich der **öffentlichen Auslegung** von Planunterlagen hat der Landesbeauftragte deutlich gemacht, daß auch die Veröffentlichung der Grunderwerbsverzeichnisse **mit Namen und Anschriften** der Grundstückseigentümer im Rahmen der Auslegung gem. § 73 Abs. 3 VwVfG LSA einen unzulässigen Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Grundstückseigentümer darstellt. Das gilt ebenso für die Veröffentlichung der Namen und Anschriften der Grundstückseigentümer im Planfeststellungsbeschluß.

Dagegen hält der Landesbeauftragte die Übermittlung der personenbezogenen Daten der Einwendungsführer an den Träger des Vorhabens grundsätzlich für datenschutzrechtlich erforderlich. Dabei ist zu berücksichtigen, daß sich der Einwender mit der form- und fristgerechten Erhebung einer Einwendung förmlich am Verwaltungsverfahren beteiligt und damit die Rechtsstellung eines Beteiligten im Sinne des § 13 VwVfG LSA erhält, der gegenüber dem Projektträger aus dem Kreis der Anonymität heraustritt.
Etwas anderes gilt nur, wenn der Einwender erkennbar gar keinen Beteiligtenstatus anstrebt, indem er nicht die Verletzung eigener Rechte geltend macht, sondern für allgemeine Belange, z.B. die des Naturschutzes, eintritt.

Die beteiligten Ministerien des Landes taten sich mit einer Reaktion auf die Anregungen des Landesbeauftragten schwer. Auch nachdem das Ministerium des Innern einen "gemeinschaftlichen Beitrag" vorgeschlagen hatte, ließ die Antwort noch lange auf sich warten und konnte den Landesbeauftragten nicht ganz zufriedenstellen.

Zur Verteidigung der Veröffentlichung von Grunderwerbsverzeichnissen mit Namen und Anschriften der Grundstückseigentümer im Rahmen der Auslegung von Planunterlagen berief man sich auf die "Planfeststellungsrichtlinien 1994", die erst im Interesse einer bundeseinheitlichen Vorgehensweise geändert werden müßten. Das ist schon deshalb wenig überzeugend, weil die Richtlinien die Planfeststellungsbehörden natürlich nicht davon befreien, die **gesetzlichen** Vorgaben zum Datenschutz zu beachten.

Im übrigen weiß der Landesbeauftragte von einem Regierungspräsidium, daß dort die auszulegenden Planunterlagen bereits seit Dezember 1997 keine Eigentümerangaben mehr enthalten. Dieser Vorgehensweise entspricht die Verwaltungspraxis in den meisten anderen Bundesländern.

Unabhängig davon hat der Landesbeauftragte beim Bundesbeauftragten für den Datenschutz angeregt, auf eine bundesweite Änderung der Planfeststellungsrichtlinien hinzuwirken.

6.2 Datenübermittlung an Beteiligte im Flurneuordnungsverfahren

Ein Grundstückseigentümer beschwerte sich beim Landesbeauftragten über ein Amt für Landwirtschaft und Flurneuordnung, weil es unaufgefordert einer benachbarten Familie mitgeteilt hatte, der Petent habe einen Verhandlungstermin zur Neuregelung der Eigentumsverhältnisse wegen seines Urlaubs abgesagt.

Ein anderer Nachbar hatte zuvor einen Antrag auf Zusammenführung von Boden- und Gebäudeeigentum gestellt. In diesem Zusammenhang sollte ein Teil des dem Petenten gehörenden Grundstückes, an dem sich noch weitere Eigenheime befanden und der als Grundstückszuwegung dient, öffentlich werden.

Nach dem hier anzuwendenden § 111 des Flurbereinigungsgesetzes können Ladungen und andere Mitteilungen an Beteiligte in jeder Form bekanntgegeben werden. Von daher war die Mitteilung an die benachbarte Familie vom Grundsatz her zulässig.

Da das Flurbereinigungsgesetz aber nur den Inhalt von **Ladungen** und nicht den von **Mitteilungen** regelt, wäre hier ergänzend § 12 Abs. 1 Nr. 1 DSG-LSA zu beachten gewesen. Dieser läßt die Übermittlung personenbezogener Daten an nichtöffentliche Stellen nur zu, wenn die Datenübermittlung zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben **erforderlich** ist. Deshalb wäre jedes einzelne mitzuteilende Datum abzuwägen

gewesen. Die Abwägung hätte zu dem Ergebnis führen müssen, daß Sinn der Mitteilung nur der Hinweis war, daß die Verhandlung zu dem beabsichtigten Termin nicht zustande kommt. Allenfalls wäre datenschutzrechtlich noch die Angabe einer kurzen Begründung (z.B. "durch den Petenten abgesagt") ohne weitere Einzelheiten vertretbar gewesen. Nicht zulässig aber war der Hinweis auf den Urlaub des Petenten.

Der Landesbeauftragte hat dieses Fehlverhalten ohne förmliche Beanstandung gerügt und möchte auch die anderen Ämter für Landwirtschaft und Flurneuordnung auf die datenschutzrechtliche Sensibilität des Themas hinweisen.

6.3 Nutzung des Automatisierten Liegenschaftsbuches

Nach § 11 des Vermessungs- und Katastergesetzes des Landes Sachsen-Anhalt (VermKatG LSA) ist durch die Vermessungs- und Katasterbehörden das Liegenschaftskataster, bestehend aus Liegenschaftsbuch und Liegenschaftskarte, als amtliches Verzeichnis der Grundstücke im Sinne von § 2 Abs. 2 Grundbuchordnung zu führen. Dies geschieht automatisiert und wird als "Automatisiert geführtes Liegenschaftsbuch" (ALB) bezeichnet. Darin enthalten sind neben Angaben über die Lage und andere Eigenschaften der einzelnen Flurstücke auch Angaben zu deren Eigentümern. Gemeinden und Landkreise erhalten auf Antrag für alle Liegenschaften ihres Gebietes Auszüge aus dem ALB und können, im Rahmen des eigenen Wirkungskreises, neben den Eigentümern auch solchen Personen Einblick gewähren, die nach § 13 Abs. 1 VermKatG LSA ein berechtigtes Interesse darlegen.

Allerdings hatte der Landesbeauftragte erfahren, daß eine Kommune in ihren Ämtern allzu sorglos mit den ALB-Daten umging. So erhielten z.B. das Bauordnungs-, das Ordnungs- und das Grünflächenamt sowie die Koordinierungsstelle Straßenreinigung auch die jeweiligen Eigentümerangaben mitgeteilt. Deren ungeprüfte Übernahme aus dem Kataster aber kann unangenehme rechtliche Folgen haben.

So sieht zwar § 11 Abs. 3 VermKatG LSA die Wahrung der Übereinstimmung zwischen Liegenschaftskataster und Grundbuch vor, in der Praxis können jedoch zwischen der Änderung der Eigentümerverhältnisse bei einem Grundstück

durch Änderung des Grundbuches und deren Berücksichtigung im Liegenschaftskataster mehrere Monate, zuweilen sogar Jahre vergehen.

Demgemäß können dem Liegenschaftskataster zwar Eigentumsangaben entnommen werden, diese bergen jedoch die Gefahr, daß sie nicht (mehr) richtig sind.

Der Landesbeauftragte wies darauf hin, daß die Verarbeitung falscher Daten unzulässig ist und die Kommune sich nach § 18 DSG-LSA der Gefahr von Schadenersatzansprüchen Betroffener aussetzt, ohne daß es auf ein Verschulden ankommt.

Soll der Eigentümer eines Grundstückes verbindlich ermittelt werden, z.B. um ihn zum Adressaten eines Verwaltungsaktes zu machen, bedarf es, wenn nicht die Eigentümereigenschaft durch den Betroffenen selbst mitgeteilt worden ist, der Einsichtnahme in das betreffende Grundbuch. Dies allein gibt rechtsverbindlich Auskunft über den Eigentümer.

7. Europäischer Datenschutz

7.1 Richtlinie der Europäischen Union

Seit dem I. Tätigkeitsbericht (S. 40) informiert der Landesbeauftragte fortlaufend über wichtige datenschutzrechtliche Entwicklungen in der EU (II. Tätigkeitsbericht S. 30; III. Tätigkeitsbericht S. 22 ff).

Dazu gehört die bereits im Oktober 1995 vom Ministerrat beschlossene EG-Datenschutzrichtlinie, die den Weg für ein einheitliches Datenschutzrecht in der Europäischen Union freimachen soll. Es zeichnete sich leider ab, daß die (damalige) Bundesregierung keine Neigung verspüren würde, im BDSG rechtzeitig die gesetzliche Anpassung über das unbedingt notwendige Maß hinaus vorzunehmen und damit eine positive Leitfunktion für das bundesdeutsche Recht zu übernehmen.

Seit dem 24. Oktober 1998 ist die dreijährige Umsetzungsfrist verstrichen. Bis heute ist es zu keinerlei Novellierungen der Datenschutzgesetze im Bund und im Land Sachsen-Anhalt gekommen. Die Landesregierung hat - und dafür sprechen Gründe einer einheitlichen Rechtsanwendung - erklärt, sie wolle den seit

langem fälligen Gesetzentwurf des Bundes abwarten, den die neue Bundesregierung noch für diesen Sommer angekündigt hat. Vorschläge für gesetzliche Neuregelungen haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 23./24. Oktober 1997 vorgelegt **(Anlage 8)** und danach mehrfach bekräftigt **(Anlage 18 und Anlage 19)**.

Schon jetzt finden aber einzelne Regelungen der Richtlinie gemäß der ständigen Rechtsprechung des Europäischen Gerichtshofes unmittelbare Anwendung. Voraussetzung für die sog. Direktwirkung ist, daß die Bestimmung dem einzelnen ein hinreichend bestimmtes und unbedingtes Recht im Verhältnis gegenüber dem Staat gewährt.

Da dürfte es für die Bürger des Landes von Interesse sein, daß z.B. die Art. 10 und 11 der Richtlinie den Betroffenen (erweiterte) Informationsrechte einräumen, Art. 14 der Richtlinie den Widerspruch gegen bestimmte Datenverarbeitungsformen zuläßt und Art. 8 der Richtlinie ein grundsätzliches Verarbeitungsverbot für besonders sensible Daten (z.B. über Gesundheit, Religion, ethnische Herkunft) enthält, was dazu führt, daß die Erlaubnistatbestände des BDSG zum Teil schon nicht mehr angewendet werden dürfen.

7.2 EUROPOL

EUROPOL hat - entgegen den weit verbreiteten Erwartungen - bisher seine Tätigkeit noch nicht aufgenommen. Allerdings sind auf deutscher Seite die nicht unerheblichen gesetzlichen Hürden für die Arbeitsaufnahme abgebaut worden. So hat der Deutsche Bundestag mit dem EUROPOL-Gesetz vom 16. Dezember 1997 dem Übereinkommen der Europäischen Union über die Errichtung eines Europäischen Polizeiamtes zugestimmt. Dem sind bis zum September 1998 alle übrigen Mitgliedsländer gefolgt. Damit ist das EUROPOL-Übereinkommen vom 26. Juli 1995 unionsweit am 01. Oktober 1998 in Kraft getreten.

Daß EUROPOL dennoch bisher seine Tätigkeit nicht aufgenommen hat, liegt an den in Art. 45 Abs. 4 des Europäischen Übereinkommens vorgesehenen Rechtsakten. Erst wenn diese in Kraft getreten sind, darf die Arbeitsaufnahme erfolgen. Drei dieser Rechtsakte sind noch nicht ratifiziert. Es sind dies das auch in Deutschland umstrittene Immunitätenprotokoll über die Immunität für

die Mitarbeiter von EUROPOL, die bilateralen Vereinbarungen zwischen den Mitgliedsländern zu den Verbindungsbeamten von EUROPOL und - als schwieriger letzter Punkt - die Ratifizierung der Geschäftsordnung der Gemeinsamen Kontrollinstanz nach Art. 24 des Übereinkommens.

Im Anschluß an die kritischen Ausführungen des Landesbeauftragten im III. Tätigkeitsbericht (S. 23 ff) kann zu den rechtlichen Problembereichen berichtet werden, daß die seinerzeit geäußerten Bedenken zu den grundlegenden Vorschriften über den Inhalt der Durchführungsbestimmungen zu den Analysedateien weitgehend ausgeräumt sind. Unbefriedigend geregelt bleibt - wie zwischenzeitlich auch in der juristischen Fachliteratur beklagt - der vom Landesbeauftragten seit langem monierte unzulängliche Rechtsschutz für betroffene Bürger.

Klarstellungen und leichte Verbesserungen zugunsten der Länder gegenüber dem ursprünglichen Entwurf finden sich nunmehr im deutschen EUROPOL-Gesetz. Zwar ist erwartungsgemäß darin festgelegt worden, daß das Bundeskriminalamt im Rahmen des EUROPOL-Übereinkommens die Aufgabe der nationalen Stelle gem. Art. 4 des Übereinkommens wahrnimmt und der Bundesbeauftragte für den Datenschutz die Aufgaben der nationalen Kontrollinstanz gem. Art. 23 des Übereinkommens, doch sind die Landeskriminalämter innerstaatlich befugt, im automatisierten Verfahren über das Bundeskriminalamt selbst Daten in das Informationssystem bei EUROPOL einzugeben und abzurufen und die eingegebenen Daten zu ändern, zu berichtigen oder zu löschen. Auch bleibt - entsprechend den innerdeutschen Zuständigkeiten - die Datenschutzkontrolle durch die Landesbeauftragten unberührt.

Als Vertreter der Bundesländer hat der Referatsleiter 24 im Ministerium des Innern einen Sitz im Verwaltungsrat, und der Landesbeauftragte ist das vom Bundesrat benannte zweite deutsche Mitglied in der Gemeinsamen Kontrollinstanz für EUROPOL.

Die mit Inkrafttreten des EUROPOL-Übereinkommens am 01. Oktober 1998 ins Leben gerufene Gemeinsame Kontrollinstanz nach Art. 24 des Übereinkommens hat nach längeren, sehr sachorientierten Verhandlungen am 23. November 1998 den von ihr erwarteten Entwurf einer Geschäftsordnung für dieses

Gremium verabschiedet und als Vorsitzenden des Gesamtgremiums den Datenschutzbeauftragten der Republik Irland, als Vorsitzenden des Beschwerdeausschusses den Präsidenten der Niederländischen Registratiekamer gewählt.

Der Entwurf der Geschäftsordnung bedarf nun der Ratifizierung durch die Ratsmitglieder der EU-Länder. Diskussionsbedarf besteht auf dieser Seite insbesondere noch seitens Frankreichs und mit Einschränkungen auch Belgiens, Luxemburgs und Dänemarks, ob das Verfahren im Beschwerdeausschuß mehr justiziellen oder mehr verwaltungsverfahrensrechtlichen Charakter erhalten soll. Dabei stehen auch Mehrheitsentscheidungen zur Diskussion.

Da die endgültige Entscheidung über die Fassung der Geschäftsordnung nur im Einvernehmen zwischen den unabhängigen Mitgliedern der Kontrollinstanz und den Vertretern des Rates der Mitgliedsländer getroffen werden kann, soll in einer Sitzung der Gemeinsamen Kontrollinstanz im April 1999 ein Vermittlungsvorschlag der Ratsvertreter diskutiert werden.

Nach dem letzten Stand der Verhandlungen hofft man, daß EUROPOL seine Tätigkeit im Laufe des Sommers aufnehmen kann.

8. Entwicklung der automatisierten Datenverarbeitung

8.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Auch der zurückliegende Berichtszeitraum ist durch eine Erweiterung des Bestandes an PC-Technik und eine Verbesserung der Ausstattungsqualität in den Obersten Landesbehörden gekennzeichnet. Deutlich wird diese Entwicklung im 4. Gesamtplan der Informationstechnik - 1998 dokumentiert, den das Ministerium des Innern entsprechend dem Gem. RdErl. StK u. der übr. Min. vom 01.06. 1992, MBl. LSA, S. 805, jährlich auf der Grundlage der Ressortpläne erstellt.

In seinem III. Tätigkeitsbericht (S. 25 ff) hat der Landesbeauftragte über den damaligen Entwicklungsstand berichtet.

Im Jahr 1998 erreichten 9 von 12 Obersten Landesbehörden einen **Ausstattungsgrad** mit PC-Technik von fast **90 %**. Schließt man in diese Betrachtung auch die nachgeordneten Behörden/Dienststellen der Ressorts ein, verbirgt sich dahinter eine Anzahl von über **17.000** Arbeitsplatzcomputern.

Die Ausstattung mit Hardware bildet aber nur einen Teilaspekt der Entwicklung bei der ADV.

Bei der **lokalen Vernetzung** (LAN) - der Anteil lag 1996 bei ca. 61 % - ist ebenfalls eine Erhöhung zu verzeichnen. Dieser Wert stieg 1998 bei den Obersten Landesbehörden auf im Durchschnitt über **80 %** an. Einzige Ausnahme bildet das Ministerium der Justiz, das selbst einen lokalen Vernetzungsgrad von ca. 58 % und bei Einbeziehung der nachgeordneten Gerichte und Justizbehörden nur einen Wert von 40 % erreicht.

Eine Weiterentwicklung ist auch hinsichtlich der **landesweiten Vernetzung** (WAN), d.h. beim Anschluß von Behörden/Dienststellen der Landesverwaltung - und im geringen Umfang der Kommunalverwaltung - an das ITN-LSA, zu beobachten. Mit Stand Juni 1998 waren **377** Behörden/Dienststellen an dieses Landesnetz angeschlossen.

Neue Dimensionen und damit verbunden Handlungsbedarf im Hinblick auf die Beachtung des Datenschutzes zeichnen sich bei der Planung, Einführung und dem Ausbau von landesweiten bzw. ressortübergreifenden Projekten und Vorhaben ab. Zu nennen sind hier z.B.

- das **H**aushalts-**A**ufstellungs-, -**M**anagement- und **I**nformations-**S**ystem **S**achsen-**A**nhalt (HAMISSA),
- das Projekt "**Uni**x im **F**inanz**a**mt" (UNIFA) und
- das länderübergreifende Projekt "**F**öderales **i**ntegriertes **s**tandardisiertes **c**omputergestütztes **S**teuersystem" (FISCUS) im Bereich der Finanzverwaltung,
- das Projekt "Elektronisches Grundbuch" im Bereich der Justiz sowie
- das **Pol**izeiliche **I**nformations**s**ystem Sachsen-Anhalt (POLIS-neu) im Bereich des Ministeriums des Innern.

In diesem Zusammenhang erinnert der Landesbeauftragte alle Ressorts an die gesetzliche Verpflichtung zu seiner rechtzeitigen Unterrichtung über die Planungen beim Aufbau automatisierter Informationssysteme, wenn in ihnen personenbezogene Daten verarbeitet werden sollen (§ 22 Abs. 4 Satz 2 DSG-LSA).

Das Ministerium der Finanzen nahm diese Verpflichtung beim Projekt HAMISSA erst wahr, als der Landesbeauftragte auf die Verpflichtung zu seiner Beteiligung hingewiesen hatte. Erst dann konnten z.B. die datenschutzrechtlich relevanten Anwendungen in diesem Verfahren herausgearbeitet werden, die nunmehr sowohl unter rechtlichen als auch unter Aspekten des technischen und organisatorischen Datenschutzes geprüft werden müssen.

Neue Wege beschreitet das Land bei seiner Beteiligung am Projekt **"TESTA-Deutschland"**. Kern dieses Projektes ist die Bereitstellung eines **bundesweiten** Intranet für die öffentliche Verwaltung, zu dem neben den Bundesländern auch der Bund sowie seine nachgeordneten Behörden und Einrichtungen und auch der kommunale Bereich zum Beitritt berechtigt sein sollen.

Grundlage bildet ein zwischen dem Thüringer Innenministerium und der Deutschen Telekom AG im Oktober 1998 abgeschlossener Rahmenvertrag zur Erstellung der "TESTA-Plattform Deutschland". Am Pilotversuch beteiligen sich neben Thüringen die Länder Rheinland-Pfalz, Nordrhein-Westfalen, Hessen, Hamburg, Sachsen und Brandenburg.

Das Projekt "TESTA-Deutschland" ist Teil des **europäischen** Projektes **"TESTA"** (**T**rans **E**uropean **S**ervices for **T**elematics between **A**dministrations), welches die Vernetzung von Standorten der öffentlichen Verwaltung der EU-Länder zum Ziel hat. Mit dem Zugang zu "TESTA" wird neben der Kommunikation untereinander innerhalb von Deutschland auch die Nutzung länderübergreifender Dienste ermöglicht werden.

Der Rahmenvertrag, der auch dem Landesbeauftragten vorliegt, beinhaltet z.Zt. **keine** grundsätzlichen Aussagen zur Datensicherheit. Lediglich in den Leistungsbeschreibungen zum Rahmenvertrag (Anhang 2, Teil A, Beschreibung des Kommunikationssystems, Abschnitt 3: Zusätzliche Leistungen) findet sich der Hinweis, daß auf "Kundenwunsch" durch die Deutsche Telekom AG nach vorgegebenen Anforderungen ein Firewall-Konzept erarbeitet werden kann. Ergänzend heißt es weiter, daß eine Firewall zur Zeit in diesem Rahmenvertrag nicht vorgesehen sei, aber in einer weiteren Projektphase angeboten werden könnte.

Auf seine Anfrage zu diesem Projekt wurde dem Landesbeauftragten vom Ministerium des Innern mitgeteilt, daß vorerst im Landesrechenzentrum in Halle eine Anbindung an das TESTA-Deutschland-Netz über ein zweistufiges Verfahren

(Router mit IP-Filterung und ein weiterer Router mit Network-Adress-Translation (NAT)) erfolgt. Über den Einsatz von Krypto-Boxen zur Leitungsverschlüsselung ist noch keine endgültige Entscheidung getroffen worden. Die Integration weiterer Sicherheitseinrichtungen soll verfahrensbezogen und bedarfsorientiert vorgenommen werden.

Der Landesbeauftragte bekräftigt deshalb seine Hinweise und Forderungen aus dem III. Tätigkeitsbericht (S. 28 ff). Der Wahrnehmung der Rechtsverantwortung nach § 14 Abs. 1 DSG-LSA, gerade bei der Planung und Einrichtung neuer bundes- bzw. sogar europaweiter Kommunikationsbeziehungen, kommt hierbei eine Schlüsselrolle zu. Die Beachtung der datenschutzrechtlichen Grundsätze der Erforderlichkeit, der Verhältnismäßigkeit und die Realisierung angemessener Maßnahmen zur Datensicherheit auf der Basis einer entsprechenden Risikoanalyse müssen zum festen Bestandteil bei der Umsetzung von IT-Projekten für **jede** öffentliche Stelle, von der Gemeinde bis zum Ministerium, werden.

Der Landesbeauftragte steht hier im Rahmen seines Beratungsauftrages den öffentlichen Stellen zur Verfügung. Er regt weiterhin an, unter Beachtung der stürmischen Entwicklung im Bereich der Informations- und Kommunikationstechnik, die IT-Grundsätze aus dem Jahr 1992 auch hinsichtlich der Verpflichtungen der öffentlichen Verwaltung zur Sicherstellung des Datenschutzes zu überarbeiten. Auch hierfür bietet er seine Unterstützung an.

8.2 Neue Strukturen und Technologien im Landesnetz

Im ITN-LSA haben sich im zurückliegenden Berichtszeitraum wesentliche Veränderungen vollzogen. Hierzu zählen der Einsatz leistungsfähiger Multiplexer-Knotentechnik, die weitere Erhöhung von Bandbreiten des Leitungsnetzes, die Planung und schrittweise Realisierung von Richtfunkstrecken zur Beseitigung von Belastungsspitzen sowie die Integration der Sprachkommunikation (Einbindung der TK-Anlagen der Landesregierung). Das zuständige Ministerium des Innern als Netzbetreiber faßt seine Aktivitäten unter dem Arbeitsbegriff "Corporate Network der Polizei und der Verwaltung des Landes Sachsen-Anhalt" (CNPV LSA) zusammen.

Anstrengungen der Landesregierung gab es auch zur Weiterentwicklung des "Intranet LSA". Der Landesbeauftragte hat in seinem III. Tätigkeitsbericht

(S. 32 f) auf die damit verbundenen Risiken bei Nutzung der neuen Informations- und Kommunikationstechnologien hingewiesen.

Mittlerweile bietet fast jedes Ministerium auf der Basis der WWW-Technologie Informationen an. Die Zahlen der Zugriffe auf diese sog. "Web-Angebote" von außen belaufen sich im Februar 1999 auf über 250.000, mit steigender Tendenz, und zeugen damit von einem regen Interesse der Öffentlichkeit.

8.2.1 Elektronische Post

Der E-Mail-Dienst, allgemein auch als "elektronische Post" bezeichnet, ist fast flächendeckend in der Landesverwaltung eingeführt. Das Land verfügt seit Mai 1998 hierzu über zwei zentrale "Postämter" (sog. MTA-Kopfstationen), die im Ministerium für Wirtschaft, Technologie und Europaangelegenheiten in Magdeburg und im Landesrechenzentrum (LRZ) in Halle eingerichtet wurden. Die Kopfstation im Wirtschaftsministerium deckt dabei die Nord-Region und die Kopfstation im LRZ Halle die Süd-Region des Landes ab. Gleichzeitig besteht die Möglichkeit, bei Störung einer primären Kopfstelle die andere Kopfstelle alternativ zu benutzen. Für eine gewisse Ausfallsicherheit hat die Landesregierung damit Vorsorge getroffen. Bei Maßnahmen zum Datenschutz besteht aber noch Handlungsbedarf.

Der Landesbeauftragte hat bereits im II. Tätigkeitsbericht (S. 36) und im III. Tätigkeitsbericht (S. 33) auf die noch fehlenden Regelungen zur Nutzung der "elektronischen Post" hingewiesen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung zum Datenschutz bei elektronischen Mitteilungssystemen vom März 1995 die Beachtung von Sicherheitsaspekten wie die Nutzung von X.400-Produkten nach dem 88er-Standard und die Verschlüsselung personenbezogener Daten gefordert (vgl. II. Tätigkeitsbericht, Anlage 16).

Über die spezifischen **Sicherheitsrisiken** beim E-Mail-Dienst, wie die Möglichkeiten zum Mitlesen, Verändern bzw. Verfälschen von elektronischen Nachrichten oder zum Erstellen von Nutzerprofilen, hat der Landesbeauftragte in seinem III. Tätigkeitsbericht (S. 59 ff) berichtet. Die Hinweise haben nichts von ihrer Aktualität verloren.

Eine weitere Gefährdung stellen **Computerviren** dar, die sich in einem Attachment der E-Mail (Anhang in einer E-Mail) befinden können.

Bisher ist es bei einem vom Ministerium des Innern vorgestellten Entwurf einer "Regelung zur elektronischen Post im Ministerium des Innern", die Grundlage für eine landesweite Regelung sein sollte, geblieben.

Der Landesbeauftragte fordert deshalb die Landesregierung auf, noch im Verlauf des Jahres 1999 zur Nutzung der "elektronischen Post" eine landeseinheitliche Regelung zu schaffen, in der auch die Belange des Schutzes personenbezogener Daten Berücksichtigung finden.

8.2.2 Sicherheitskonzept für das ITN-LSA

Auch das seit langem vom Landesbeauftragten geforderte Sicherheitskonzept für das ITN-LSA (vgl. III. Tätigkeitsbericht, S. 31 f) liegt bisher nur als Entwurf vor und läßt auf sich warten. Das Ministerium des Innern begründet die Verzögerung mit "personellen" Engpässen. Dieser Grund entläßt das Ministerium aber nicht aus seiner gesetzlich festgelegten Verantwortung zur Sicherstellung des Datenschutzes, die ihm besonders als Netzbetreiber obliegt. Der Landesbeauftragte fordert deshalb die Landesregierung auf, nach Abschluß der Firewall-Zertifizierung verbindliche Regelungen in einem prüffähigen Sicherheitskonzept vorzulegen.

Eine Verzögerung ist bei der Zertifizierung der Firewall zum Anschluß des ITN-LSA an das Internet eingetreten, deren Inbetriebnahme bereits für April 1998 vorgesehen war. Die Zertifizierung selbst obliegt dem BSI und ist vom Abschluß der Überprüfung durch die dafür zugelassenen Unternehmen abhängig.

Die erfolgreiche Zertifizierung der Firewall bildet die Voraussetzung zur Schaffung eines zentralen und kontrollierten Übergangs vom ITN-LSA zum Internet. Dieser Übergang stellt allerdings nur einen, wenn auch wichtigen, Baustein des Sicherheitskonzeptes für das ITN-LSA dar. Das Netz wird immer nur so stark (sicher) sein, wie die schwächste Stelle seiner Teilnehmer!

Regelungen zum Schutz besonders sensibler personenbezogener Daten bei ihrer Übertragung im Landesnetz fehlen noch in diesem Sicherheitskonzept. Hierzu gehören personenbezogene Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, wie z.B. dem Arzt-, Sozial- und Steuergeheimnis.

Im III. Tätigkeitsbericht (S. 61) hat der Landesbeauftragte seinen Standpunkt zur Möglichkeit der Nutzung kryptographischer Verfahren für Zwecke der Verschlüsselung dargelegt. In der Entschließung vom 9. Mai 1996 (vgl. III. Tätigkeitsbericht, Anlage 6) bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Forderungen nach einer sicheren Übertragung elektronisch gespeicherter personenbezogener Daten.

Mit Besorgnis verfolgt der Landesbeauftragte gegenwärtig die Planung und Realisierung von Maßnahmen zur Erhöhung der Übertragungskapazitäten im ITN-LSA und die Einrichtung von Richtfunkstrecken. Diese führen in ihrem Ergebnis z.Zt. teilweise dazu, daß die bisher verschlüsselte Übertragung, z.B. von Sozialdaten, im ITN-LSA nicht mehr erfolgen kann, weil die dazu erforderliche neue Verschlüsselungstechnik nicht zur Verfügung steht und einzelne öffentliche Stellen bei der Entwicklung von alternativen Lösungen überfordert sind. Die Einführung neuer Übertragungstechnologien im ITN-LSA darf jedenfalls nicht zum Abbau bereits bestehender Datenschutzstandards führen.

Das Ministerium des Innern als Netzbetreiber sollte die Möglichkeiten des Einsatzes zentraler, anwendungsunabhängiger Verschlüsselungstechnik prüfen.

8.2.3 Datenschutz durch Technik - Datenschutzfreundliche Technologien

Die Nutzung der modernen Informations- und Telekommunikationstechnik hat in den zurückliegenden zwei Jahren auch in der öffentlichen Verwaltung zunehmend an Bedeutung gewonnen und ist aus dem "Verwaltungsalltag" nicht mehr wegzudenken. Diese Entwicklung bietet neben den datenschutzrechtlichen Risiken gleichzeitig auch Chancen, die Informationstechnik selbst zur Sicherung des informationellen Selbstbestimmungsrechtes zu nutzen. Auch in Sachsen-Anhalt muß zukünftig bereits bei der Planung der IuK-Systeme, die der Verarbeitung personenbezogener Daten dienen, das Prinzip der **Datensparsamkeit** wesentlich stärker durch die öffentlichen Stellen beachtet werden. Das Ziel muß darin bestehen, so wenig personenbezogene Daten wie möglich zu erheben und zu verarbeiten. Bei der Entwicklung von automatisierten Verfahren sowie bei der Auswahl von Hard- und Softwareprodukten durch öffentliche Stellen müssen diese Prinzipien zunehmend Berücksichtigung finden.

Datenschutzfreundliche Technologien lassen sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit. Datensparsamkeit bis hin zur **Datenvermeidung**, z.B. durch Anonymisierung und Pseudonymisierung personenbezogener Daten, spielt bisher in der Landesverwaltung und auch im kommunalen Bereich noch eine untergeordnete Rolle.

Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff **"Privacy enhancing technology - PET"** eine Philosophie der Datensparsamkeit beschreiben und ein ganzes System technischer Maßnahmen umfassen, sollten zunehmend genutzt werden. Die Datenschutzbeauftragten des Bundes und der Länder forderten im Oktober 1997 in ihrer Entschließung **(Anlage 10)** von den Gesetzgebern, daß sie die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen unterstützen. Als positive Beispiele sind der Mediendienste-Staatsvertrag der Länder und auch das Teledienstedatenschutzgesetz des Bundes zu nennen, die bereits den Grundsatz der Datenvermeidung normieren.

Der Landesbeauftragte regt deshalb an, z.B. die Möglichkeit der Anonymisierung sensibler personenbezogener Daten bei ihrer Übertragung im ITN-LSA als eine Alternative zur Verschlüsselung zu untersuchen.

9. Finanzwesen

9.1 Änderung der Abgabenordnung

Auf die datenschutzrechtlichen Forderungen hat der Landesbeauftragte bereits im I. Tätigkeitsbericht (S. 48), in seinem II. Tätigkeitsbericht (S. 38) und auch in seinem III. Tätigkeitsbericht (S. 33 f) hingewiesen und über die mangelnde Bereitschaft zu datenschutzrechtlichen Verbesserungen bei den obersten Finanzbehörden des Bundes und der Länder informiert.

Bis heute hält das Bundesministerium der Finanzen datenschutzrechtliche Ergänzungen der Abgabenordnung nicht für erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder haben dennoch eine Bestandsaufnahme der wünschenswerten und notwendigen Änderungen der

Abgabenordnung erstellt, weil seit Beginn des Jahres 1999 erste Anzeichen für eine grundsätzlich geänderte Einstellung beim Bundesministerium erkennbar sind.

In Anbetracht fortschreitender technischer Entwicklungen im Bereich der automatisierten Datenverarbeitung werden neue datenschutzrechtliche Vorkehrungen nicht zu vermeiden sein, will man z.B. das auch von den Finanzverwaltungen stets hoch gehaltene Steuergeheimnis nicht gefährden. Dabei geht es nicht nur um die Glaubwürdigkeit der Steuerverwaltung im Umgang mit den ihr anvertrauten Daten, sondern auch um die Frage, wie bei den neuen technischen Risiken mit den Persönlichkeitsrechten der Steuerbürger umgegangen wird. Unerwähnt sollte auch nicht bleiben, daß auch die Umsetzung der EG-Datenschutzrichtlinie Anlaß gibt, die Abgabenordnung zu überprüfen.

Der Landesbeauftragte fordert die Landesregierung auf, mehr als bisher die Bestrebungen zur datenschutzrechtlich gebotenen Überarbeitung der Abgabenordnung zu unterstützen.

9.2 Hundebestandsaufnahme zur Erfassung steuerpflichtiger Hundehalter

Bereits im II. Tätigkeitsbericht (S. 45) hatte der Landesbeauftragte auf datenschutzrechtliche Probleme bei der Regelung einer Hundebestandsaufnahme in einer Hundesteuersatzung hingewiesen. 1998 erfuhr er über eine Pressemeldung von einem neuen Fall. Dabei verteilte die Gemeinde Erfassungs- und Anmeldebogen an alle Haushalte zusammen mit den Wahlunterlagen zur Landtagswahl. Verpflichtet zur Antwort sollte jeder Grundstückseigentümer bzw. sein Vertreter sein.

Eine derartige Erhebung personenbezogener Daten kann nur auf freiwilliger Basis oder aufgrund eines Gesetzes erfolgen. Nachrangiges Satzungsrecht der Gemeinden ist als Grundlage für einen solchen Grundrechtseingriff (vgl. Artikel 6 Absatz 1 LVerf) nicht ausreichend. Zu prüfen blieb nur die Zulässigkeit einer Erhebung nach § 93 AO i.V. mit § 13 Absatz 1 Nr. 3a) KAG-LSA. Diese Vorschriften erlauben aber keine **generellen** Ermittlungen nach unbekannten Steuerpflichtigen. Darüber hinaus führte die Gestaltung des Fragebogens zu

datenschutzrechtlich nicht erforderlichen und daher unzulässigen Doppelerhebungen bei jenen Hundehaltern, die ihren Hund dem Stadtsteueramt bereits gemeldet hatten. Nicht erforderlich war auch, in jedem Fall nach der "Rasse" des Hundes zu fragen, da es für die Besteuerung lediglich darauf ankam, ob ein "Kampfhund" im Sinne der Satzung gehalten wurde.

Der Stadt wurde empfohlen, die Hundebestandsaufnahme abzubrechen, die bereits erhobenen Daten zu löschen und ihr wichtiges Anliegen mit gezielten stichprobenhaften Kontrollen der Hundebesitzer zu verfolgen. Diese waren per Hundesteuersatzung zum Mitführen einer Hundesteuermarke verpflichtet.
Die Stadt folgte dieser Empfehlung.

9.3 Steuergeheimnis und Grunderwerbsteuer

Ein Bürger beschwerte sich darüber, daß ein Finanzamt Einzeldaten aus seinem Grunderwerbsteuerbescheid einem Nachfolgeerwerber übermittelt hatte.

Vorausgegangen war der Zuschlagsbeschluß eines Amtsgerichts im Zwangsversteigerungsverfahren, der die Festsetzung der Grunderwerbsteuer gegen den Bürger als steuerpflichtigen Erwerbsvorgang auslöste.
Da der Bürger das betreffende Grundstück sofort nach dem Zuschlagsbeschluß weiterveräußerte, hatte der Nachfolgeerwerber sich mit dem Finanzamt wegen der zusätzlichen Übernahme der bisher nicht beglichenen Grunderwerbsteuer für den Ersterwerber in Verbindung gesetzt, um eine möglichst schnelle Eigentumsumschreibung im Grundbuch zu erreichen. Der Einfachheit halber übergab das Finanzamt dem Nachfolgeerwerber eine Kopie des Grunderwerbsteuerbescheides des Ersterwerbers. Hiergegen richtete sich die Beschwerde des Bürgers.

Die Offenbarung der nach § 30 Abs. 2 AO erlangten steuerlichen Daten ist nach § 30 Abs. 4 Ziff. 1 AO zulässig, wenn sie der Durchführung eines Verwaltungsverfahrens dient. Dabei reicht es grundsätzlich aus, daß die Offenbarung von Steuerdaten für den Fortgang eines Verwaltungsverfahrens nützlich sein kann.

Mit der Festsetzung der Grunderwerbsteuer war das steuerliche Festsetzungs- und Erhebungsverfahren als steuerliches Verwaltungsverfahren nach § 30 Abs. 4 Ziff. 1 AO eingeleitet worden. Dieses war mit der Erstellung des Grunderwerbsteuerbescheides noch nicht abgeschlossen, denn die Zahlung der Grunderwerbsteuer war noch nicht erfolgt.

Dennoch bestehen erhebliche Zweifel, ob es zur Förderung des Steuerverfahrens durch schnelle Begleichung der Steuerschuld erforderlich ist, dem Nachfolgeerwerber eine Kopie des Grunderwerbsteuerbescheides auszuhändigen. Es hätte bei Beachtung des Grundsatzes der Verhältnismäßigkeit ausgereicht, lediglich die festgesetzte Steuerschuld und das Bearbeitungszeichen des Finanzamtes mitzuteilen.

Die somit in diesem Fall unzulässige Übermittlung der überschüssigen Daten aus dem Grunderwerbsteuerbescheid blieb aber folgenlos, weil das Finanzamt aus besonderen Gründen des Einzelfalls davon ausgehen durfte, daß keine schutzwürdigen Interessen des Petenten mehr berührt wurden.

Auch wenn der Landesbeauftragte im vorliegenden Einzelfall einen Verstoß gegen datenschutzrechtliche Vorschriften letztlich nicht feststellen konnte, hat die OFD die Empfehlung des Landesbeauftragten aufgenommen und eine Ergänzung der entsprechenden Dienstanweisung - wegen der Gefahren für das Steuergeheimnis bei ähnlichen Fallkonstellationen - vorgenommen.

9.4 Steuerfahndung überprüfte Fördermittelunterlagen

Von einem mit der Sache beauftragten Rechtsanwalt erfuhr der Landesbeauftragte, daß sich die Steuerfahndung wegen des Verdachts der Steuerhinterziehung von Baufirmen an einen Landkreis gewandt und dort die für die Wohnungsbauförderung vorliegenden Fördermittelanträge zur Überprüfung abverlangt hatte. Hierzu hatte die Steuerfahndung einen richterlichen Durchsuchungsbeschluß zur Beschlagnahme der Beweismittel bei dem zuständigen Amtsgericht erwirkt.

Der Landkreis war unter diesen Umständen nach den spezialgesetzlichen Vorschriften der StPO zur Übermittlung der Unterlagen mit den personenbezogenen Daten an die Steuerfahndungsstelle verpflichtet.

Von der rechtlichen Möglichkeit einer Beschwerde gegen den Beschlagnahmebeschluß des Amtsgerichts hatte der Landkreis leider keinen Gebrauch gemacht. Dies wäre sinnvoll und mit hoher Wahrscheinlichkeit erfolgreich gewesen, denn der Bundesfinanzhof hat schon in einem früheren Urteil zu Recht entschieden, daß eine "Rasterfahndung oder ähnliche Ermittlungen ins Blaue hinein" durch die Finanzbehörden unzulässig sind. Die Steuerfahndung hätte deshalb eine solche Durchsuchung beim Amtsgericht erst gar nicht beantragen dürfen, weil es ihr an hinreichenden Anhaltspunkten in konkreten Fällen fehlte.

Datenschutzrechtliche Vorschriften wurden dadurch verletzt, daß die Steuerfahndung nach Auswertung der Unterlagen Teilergebnisse ihrer Ermittlungen dem Landkreis mitteilte, ohne daß die Offenbarungsmöglichkeiten nach den §§ 30 Abs. 4 und 31a Abs. 3 AO in jedem Fall vorlagen. Die Datenübermittlungen von der Steuerfahndung an den Landkreis wurden erst 1997 eingestellt, nachdem die Steuerfahndung selbst die Rechtswidrigkeit der Datenübermittlung bei den Fällen erkannte, in denen die Zuwendung nicht an Unternehmen, sondern an Einzelpersonen gewährt worden war.

Der Landkreis sah sich veranlaßt, auf der Grundlage dieser Mitteilungen gegen eine große Anzahl von Betroffenen Rückforderungsbescheide zu erlassen.

Aus datenschutzrechtlicher Sicht ist für die Verfahren des Landkreises folgendes von Bedeutung:

1. Die unter Verstoß gegen Vorschriften über das Steuergeheimnis (§ 30 AO) mitgeteilten Tatsachen dürfen nicht im Verwaltungsverfahren als Beweismittel verwendet werden.

2. Die vorliegenden Mitteilungen der Steuerfahndung sind aber als Indiz für eigene weitere (oder neue) Feststellungen verwertbar - z.B. um eine Überprüfung mit neuer Anhörung durchzuführen.

Ergeben die Anhörung und die weitere Prüfung eigenständige und damit rechtmäßig erlangte Beweismittel, kann auf dieser Grundlage ein Rückforderungsbescheid erlassen werden.

3. Sollten Urteile der Strafgerichte ergehen bzw. ergangen sein, können die Feststellungen des Strafurteils unmittelbar für das Verwaltungsverfahren verwendet werden.

Zwischenzeitlich hat eine Arbeitsgruppe beim Ministerium für Wohnungswesen, Städtebau und Verkehr die Vorgänge unter Beteiligung des Landesbeauftragten aufgearbeitet und entsprechende Hinweise für das weitere Verfahren an den Landkreis weitergeleitet.

Auch die Oberfinanzdirektion Magdeburg hat eine klarstellende Verfügung an die Finanzämter herausgegeben.

9.5 Kontrolle eines Finanzamtes

Im Berichtszeitraum hat der Landesbeauftragte damit begonnen, auch die 21 im Lande bestehenden Finanzämter in die datenschutzrechtlichen Kontrollen einzubeziehen.

Eine erste Prüfung ergab, daß im materiell-rechtlichen Bereich wenige, dafür aber **erhebliche** Mängel im Bereich des technisch-organisatorischen Datenschutzes festzustellen waren. Datenschutzrechtliche Defizite zeigten sich besonders bei:

- der Verschlußsicherheit von Räumlichkeiten und der Organisation der Gebäudereinigung durch eine Fremdfirma,
- der Organisation und dem Ablauf der Vernichtung von dienstlichem Schriftgut,
- den Melde- und Dokumentationspflichten.

9.5.1. Probleme der Zugangskontrolle

Die Gebäudereinigung erfolgte durch eine private Firma. Diese war im **ständigen** Besitz eines Schlüssels für den Haupteingang der Behörde. Über den

Verbleib und die sichere Verwahrung dieses Schlüssels bestanden noch nicht einmal vertragliche Regelungen.

Die Gebäudereinigung selbst erfolgte grundsätzlich **außerhalb** der Dienstzeiten. Das Gebäude wurde nach Beendigung der Reinigungsarbeiten nicht durch einen Bediensteten des Finanzamtes, sondern durch die Reinigungsfirma verschlossen. Eine Kontrolle oder Aufsicht durch Mitarbeiter des Finanzamtes war damit in keinem Fall gegeben. Diese Tatsache war dem Landesbeauftragten besonders unverständlich, da in fast allen Bereichen des Finanzamtes die Steuerakten **offen** aufbewahrt und die Dienstzimmer auch nach Dienstschluß nicht verschlossen wurden. Eine Dienstanweisung, die Regelungen zur Verschlußsicherheit von Diensträumen nach Dienstschluß bzw. bei längerer Abwesenheit der Mitarbeiter vom Arbeitsplatz traf, existierte nicht.

Die Wahrung des Steuergeheimnisses (§ 30 AO) hat das Finanzamt als speichernde Stelle auch durch angemessene Datensicherheitsmaßnahmen im technischen und organisatorischen Bereich zu gewährleisten (§ 6 Abs. 1 DSG-LSA).

Mit den damit bestehenden gesetzlichen Anforderungen, generell den Umgang mit personenbezogenen Daten nachvollziehbar und einschränkend zu gestalten, waren die angetroffenen Zustände nicht vereinbar.

Die Aufbewahrung von Steuerakten in den kontrollierten Diensträumen in offenen Aktenregalen sowie die Aufbewahrung von Steuerfällen in der Verbindungsstelle zum Finanzrechenzentrum (VRZ) in Einlegemappen und offenen Aktenregalen von der Datenerfassung bis zum Abschluß der Rücklaufbearbeitung und der Abgabe in die Arbeitsbereiche entsprach nicht den Mindestanforderungen zur zugangssicheren Aufbewahrung von Akten.

9.5.2 Probleme bei der Schriftgutvernichtung

Bereits beim Sammeln des zu vernichtenden Schriftgutes gab es erhebliche Mängel. Es erfolgte außerhalb der Dienstzeiten des Finanzamtes durch Arbeitskräfte der Reinigungsfirma aus den normalen Papierkörben. Separate und verschließbare Behältnisse, in denen das zu vernichtende dienstliche Schriftgut mit steuerrelevanten Angaben verwahrt werden konnte, existierten nicht.

Mit diesem Einsammeln des zu vernichtenden Schriftgutes durch unbeobachtete und unkontrollierte Arbeitskräfte der Reinigungsfirma war in einer Vielzahl von Fällen die unbefugte Offenbarung von steuerlichen Verhältnissen und damit eine Verletzung des Steuergeheimnisses (§ 30 Abs. 2 AO) nicht auszuschließen.

Die Vernichtung in der behördeneigenen Aktenvernichtungsanlage erfolgte nicht zeitnah, sondern in mehrwöchigen Abständen. Die mit dienstlichem Schriftgut gefüllten Müllsäcke wurden zunächst zur "Zwischenlagerung" in einer völlig unzureichend gesicherten Baracke **außerhalb** des Dienstgebäudes gesammelt.

Das Finanzamt hatte dabei gänzlich vergessen, daß es sich bei der Vernichtung von Schriftgut um die letzte Datenverarbeitungsphase, das **Löschen** von personenbezogenen Daten, handelt, die alsbald zu erfolgen hat (§ 16 Abs. 2 Nr. 2 DSG-LSA).

Auch für diese Phase der Datenverarbeitung hätten die erforderlichen technischen und organisatorischen Sicherungsmaßnahmen getroffen werden müssen, um das Steuergeheimnis zu wahren (§ 30 Abs. 1 AO).

9.5.3 Versäumnisse bei den Melde- und Dokumentationspflichten

Die gesetzliche Übergangsfrist nach § 32 Abs. 2 DSG-LSA für das Anlegen des Verzeichnisses der eingesetzten Datenverarbeitungsanlagen der Behörden, des innerbehördlichen Dateienverzeichnisses und die Erstattung der Dateimeldung automatisierter Dateien zum Dateienregister an den Landesbeauftragten ist bereits am **01.10.1992** abgelaufen. Damit kann sich keine öffentliche Stelle des Landes Sachsen-Anhalt auf einen noch bestehenden "Übergangsbonus" bei einer Kontrolle durch den Landesbeauftragten berufen.

Der Landesbeauftragte mußte feststellen, daß die Dokumentations- und Meldepflichten nur zum Teil erfüllt waren. Das lag aber ursächlich nicht allein in der Verantwortung des Finanzamtes. Für die Dateien des **Integrierten Automatisierten Besteuerungsverfahrens** (IABV) der insgesamt 21 Finanzämter in Sachsen-Anhalt zeichnet die OFD Magdeburg verantwortlich, da die Daten aller Steuerbürger bei den Finanzämtern zentral im Finanzrechenzentrum (FRZ) Magdeburg gespeichert und verarbeitet werden.

Die OFD hatte aber erst mit ihrer Verfügung vom 06.02.1995 hierzu Regelungen getroffen und die Finanzämter zur erstmaligen Abgabe einer Dateienregistermeldung zum 01.06.1995 verpflichtet.

Sie hatte es dann versäumt, die zentralen IABV-Dateien dem Landesbeauftragten für das Dateienregister zu melden. Auch wenn die Finanzverwaltung ihre Daten in einem landesweiten Verfahren zentral im FRZ verarbeiten läßt, bleibt jedes einzelne Finanzamt für seine Steuerdaten die verantwortliche, speichernde Stelle (§ 2 Abs. 8 DSG-LSA) und ist damit auch für die Sicherstellung des Auskunftsanspruches eines Bürgers nach § 15 Abs. 1 DSG-LSA verantwortlich.

Als positiv sieht der Landesbeauftragte die schnelle Reaktion und die eingeleiteten Maßnahmen sowohl des geprüften Finanzamtes als auch der OFD Magdeburg auf die in seinem Prüfbericht aufgezeigten datenschutzrechtlichen Mängel und die daraus abgeleiteten Forderungen an.

Der Landesbeauftragte geht davon aus, daß die Ergebnisse dieser ersten Kontrolle in allen Bereichen der Finanzverwaltung zu den gebotenen Maßnahmen für einen effektiven technischen und organisatorischen Datenschutz im Sinne des Gesetzes führen werden. Der Landesbeauftragte wird dabei im Rahmen seines Beratungsauftrages helfen. Die Kontrollen werden fortgesetzt.

9.6 Unzulässige Datenübermittlungen bei den Steuerberaterkammern

Seit längerem mußte sich der Landesbeauftragte - wie auch seine Kollegen und Kolleginnen in den anderen Bundesländern - mit der Veröffentlichungspraxis der Steuerberaterkammern beschäftigten. Sofern Unbefugte sich steuerberatend betätigen, werden sie abgemahnt und zur Abgabe von strafbewehrten Unterlassungserklärungen "verpflichtet". Diese sicher notwendigen Unterlassungserklärungen werden dann aber im öffentlich zugänglichen Mitteilungsblatt der Kammern (z.B. in den Wartezimmern der Steuerberater) abgedruckt. Das wird mit dem Informationsbedürfnis der Kammermitglieder begründet; nur auf diese Art und Weise könnten die Steuerberaterkammern ihrer Informationspflicht nachkommen und die Einhaltung der Unterlassung überprüft werden.

Der Landesbeauftragte wies in mehreren Schreiben darauf hin, daß es für diese Veröffentlichungspraxis in Sachsen-Anhalt keine gesetzliche Grundlage gibt. Die Verfassung des Landes und auch das DSG-LSA verlangen eine Rechtsgrundlage, weil mit der jedermann zugänglichen Kammerzeitung personenbezogene Daten Dritten übermittelt werden. Das als Grundlage von den Kammern herangezogene Steuerberatungsgesetz enthält nur eine Aufgabenzuweisung, aber keine Befugnis zum Eingriff in das Persönlichkeitsrecht der Betroffenen. Als Körperschaft des öffentlichen Rechts sind die Steuerberaterkammern an Gesetz und Recht gebunden. Keines der Urteile, die die Kammern zur Begründung für ihre Praxis herangezogen haben, hat sich mit der Verletzung der Grundrechte auseinandergesetzt.

Der Landesbeauftragte hat unter Berücksichtigung der Gesamtsituation bis zu einer Klärung angeregt, von den Betroffenen entweder eine separate Zustimmung zur Veröffentlichung zu erhalten oder aber die Erklärung nicht als Abdruck im offen zugänglichen Mitteilungsblatt, sondern nur im Begleitschreiben an die Kammermitglieder direkt zu übermitteln. Dann löst sich das Rechtsproblem ohne großen Aufwand.
Auf eine Antwort auf seinen Vorschlag wartet der Landesbeauftragte seit September 1998.

10. Forschung

Wie bereits im I. Tätigkeitsbericht (vgl. S. 55 ff) und im II. Tätigkeitsbericht (vgl. S. 47 ff) ausgeführt, bestehen Probleme beim Umgang mit personenbezogenen Daten bei Forschungsvorhaben. Häufig wird, wenn die Einwilligungserklärung der Betroffenen erforderlich ist, nicht berücksichtigt, daß § 4 Abs. 2 DSG-LSA Form und Inhalt einer Einwilligungserklärung rechtsverbindlich vorschreibt. So wird oft von der grundsätzlich vorgesehenen Schriftform abgewichen, Nachteile für die Betroffenen werden nicht benannt oder Hinweise auf das Widerrufsrecht (für die Zukunft) unterlassen.

Wie sich im Berichtszeitraum zeigte, werden immer häufiger Forschungsaufträge an private Stellen vergeben. In den dazu ausgehandelten Vertragswerken werden häufig zwingende gesetzliche Vorschriften nicht beachtet. So ist z.B.

vertraglich sicherzustellen, daß die Bestimmungen des DSG-LSA befolgt werden und sich die private Stelle der Kontrolle durch den Landesbeauftragten unterwirft.

Eine entsprechende Regelung findet sich in § 8 DSG-LSA (Auftragsdatenverarbeitung). Hiernach ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung auszuwählen. Der Auftrag ist schriftlich zu erteilen. Im Vertrag sind die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen. Der Landesbeauftragte **ist** von der öffentlichen Stelle über die Beauftragung **zu unterrichten** (§ 8 Abs. 6 Satz 2 DSG-LSA).

Ein weiterer wesentlicher Punkt der Auftragsdatenverarbeitung ist die vertragliche Einräumung eines Weisungsrechtes für den Auftraggeber. Durch dieses Weisungsrecht wird sichergestellt, daß der Auftragnehmer im Sinne des Auftraggebers handelt. Die Verantwortung für die Datenverarbeitung verbleibt beim Auftraggeber, der mithin Herr der Daten bleibt.

Die Verträge mußten entsprechend nachgebessert werden.

10.1 Ausgewählte Forschungsprojekte

1. Studie zur Beschäftigungsförderung

Ein Ministerium beauftragte eine GmbH, das Forschungsprojekt durchzuführen. Die hierzu abgeschlossenen Verträge sahen auch die Befragung von Personen vor, die aufgrund der Beschäftigungsförderung eingestellt worden waren. Hierzu war vorgesehen, daß die Betriebe diese Arbeitnehmer mit Namen und Vornamen benennen. Da eine Übermittlung dieser personenbezogenen Daten an eine private Stelle rechtlich nicht gedeckt war, hat der Landesbeauftragte vorgeschlagen, durch ein im Betrieb zu verteilendes Merkblatt die betreffenden Arbeitnehmer zu bitten, an der Befragung teilzunehmen und sich direkt an die GmbH zu wenden. So kann jede Person selbst entscheiden, ob sie ihre personenbezogenen Daten für den vorgesehenen Forschungszweck preisgeben möchte. Das Konzept wurde dementsprechend geändert.

2. Politische Einstellungen und Handlungsorientierungen junger Menschen in Sachsen-Anhalt

Dieses Forschungsprojekt sah die Befragung von ca. 300 jungen Menschen zwischen 18 und 27 Jahren vor. Damit wurde ein privates Forschungsinstitut vom zuständigen Ministerium beauftragt. Das Thema erforderte besondere Sensibilität beim Umgang mit den zu Befragenden. Dennoch war weder die Übermittlung der Daten von den Meldebehörden an das private Institut noch die Freiwilligkeit bei der Datenerhebung rechtlich einwandfrei geregelt.

Zwischenzeitlich wurden die zulässigen Datenübermittlungswege geklärt und entsprechende Merkblätter versandt, so daß jeder Befragte sich nunmehr selbst im Rahmen einer freien Entscheidung an das Forschungsinstitut wenden kann, um an dieser Befragung teilzunehmen.

10.2 Epidemiologie und Datenschutz

In einer Denkschrift der Deutschen Forschungsgemeinschaft wurde u.a. auch gegenüber den Datenschutzbeauftragten des Bundes und der Länder der Vorwurf der Wissenschaftsbehinderung erhoben. Das war Anlaß zu Gesprächen zwischen Vertretern der Deutschen Forschungsgemeinschaft und Teilnehmern aus dem Kreis der Datenschutzbeauftragten, in denen zum besseren Verständnis der gegenseitigen Anliegen die beiderseitigen Problembereiche erörtert wurden. Dabei ergab sich bald Übereinstimmung darin, daß das bereits in der Verfassung angelegte Spannungsverhältnis zweier gleichrangiger Verfassungsgüter - des Persönlichkeitsrechts einerseits und der Forschungsfreiheit andererseits - nur befriedigend gelöst werden kann, wenn sich beide Seiten bemühen, wirkungsvollen Datenschutz zu gewährleisten, ohne die Wissenschaftsfreiheit zu gefährden.

Ein 1998 gemeinsam von der Deutschen Arbeitsgemeinschaft für Epidemiologie und dem Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitetes Papier **(Anlage 23)** zeigt datenschutzrechtlich unproblematische Forschungsbereiche auf und versucht, in anderen

Bereichen typische Problemfelder zu identifizieren und Lösungsvorschläge zu erarbeiten.

10.3 Schutz medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Ein gemeinsames Anliegen der Deutschen Forschungsgemeinschaft und der Datenschutzbeauftragten ist die Ausdehnung des Schutzes der Patientendaten auf den forschenden Arzt gegen die Inanspruchnahme durch Dritte. Die Datenschutzbeauftragten haben diesen Aspekt in ihre Entschließung vom 17./18. April 1997 "Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen" **(Anlage 6)** mit einbezogen. Im Hinblick auf die zunehmende Auslagerung medizinischer Patientendaten sowie die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung halten die Datenschutzbeauftragten es für wünschenswert, in diesem Bereich einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.

11. Gesundheitswesen

11.1 Gesetz über den Öffentlichen Gesundheitsdienst und die Berufsausübung im Gesundheitswesen.

Mit der Verordnung über den öffentlichen Gesundheitsdienst und die Aufgaben der Gesundheitsämter in den Landkreisen und kreisfreien Städten vom 08.08. 1990 (GBl. I, S. 1068) wurde der Staatliche Gesundheitsdienst der ehemaligen DDR in den öffentlichen Gesundheitsdienst überführt und so eine Rechtsgrundlage für die Tätigkeit der Gesundheitsämter in den neuen Bundesländern geschaffen.

Diese Rechtsgrundlage reichte aber nicht aus, um einen den heutigen Anforderungen entsprechenden modernen Gesundheitsdienst im Lande zu schaffen. Eine gesetzliche Grundlage für Rechtsverordnungen zu bestimmten Aufgabenbereichen war in einem der Verfassung entsprechenden Rahmen ebenfalls

nicht vorhanden. Darüber hinaus hatte sich der Aufgabenkatalog des öffentlichen Gesundheitsdienstes zwischenzeitlich so geändert, daß auch dazu eine gesetzliche Regelung unumgänglich wurde. Die ersten Gesetzentwürfe wurden dem Landtag bereits 1994 zugeleitet. Der Landesbeauftragte wurde vom zuständigen Ministerium für Arbeit, Gesundheit und Soziales Ende 1994 beteiligt und konnte so bei der Gestaltung dieses modernen Gesetzes mitwirken.

Die Vorschriften zu den datenschutzrechtlichen Regeln - die sich im übrigen an dem Baden-Württembergischen Gesundheitsdienstgesetz orientierten - wurden übernommen und in das Gesetz eingearbeitet.

Schwierigkeiten - die aber letztendlich im Interesse der betroffenen Bürger gelöst werden konnten - ergaben sich bei der geplanten Meldepflicht aller Ärzte an das jeweilige Gesundheitsamt über die von ihnen vorgenommenen Impfungen bei Kindern. Dazu sollten deren personenbezogenen Daten in ein Impfregister eingestellt werden.

Hier waren sowohl das Recht der Eltern und das Grundrecht ihrer Kinder auf informationelle Selbstbestimmung berührt als auch die ärztliche Schweigepflicht und das Grundrecht auf freie Berufsausübung des Arztes. Nach eingehender, teilweise kontrovers geführter Diskussion zwischen dem Fachministerium, den beteiligten Fachausschüssen des Landtages und dem Landesbeauftragten folgte das Parlament Ende 1997 der Empfehlung des Landesbeauftragten und schrieb in § 4 Abs. 3 GDG-LSA die Einwilligung der Eltern für die Datenerhebung und -verarbeitung der Impfdaten der Kinder vor.

11.2 Chipkarten im Gesundheits- und Sozialwesen

Bereits im II. Tätigkeitsbericht (vgl. S. 54 f) hatte sich der Landesbeauftragte eingehend mit der Problematik der Chipkarte (nicht nur der Krankenversicherungskarte!) auseinandergesetzt.

Die neuere Entwicklung im Bereich des Gesundheits- und Sozialwesens bestätigt, daß das grundsätzliche Mißtrauen gegenüber der Chipkartentechnologie berechtigt ist. Auf die generellen Gefahren haben die Datenschutzbeauftragten

bereits in ihrem Beschluß vom 9./10. November 1995 (Anlage 5 zum III. Tätigkeitsbericht, Ziffer 4) zu datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen sehr deutlich hingewiesen.

Jetzt zeigt sich, daß nicht nur die merkantilen Interessen der Kartenhersteller und in der Folge die der Hardwareproduzenten Gefahren für die Millionen von gesetzlich Versicherten beinhalten, sondern auch die Unberechenbarkeit der Tagespolitik. Die plötzlich entstandene Diskussion über die Beschränkung der Anzahl der Arzt- bzw. Facharztbesuche unter "Zuhilfenahme" der Chipkarte zeigt, wie schnell aus einem Mittel **für** den Bürger ein Mittel **gegen** den Bürger werden kann, indem man den Chip auf der Karte durch Zusatzspeicherungen in seiner Zweckrichtung verändert.

Mit der "Anreicherung" weiterer Daten werden - naturgemäß - auch wieder weitere Begehrlichkeiten entstehen (z.B. bei Aufnahme medizinischer Daten), die dann z.B. das Ausleseverfahren für Berufsbewerber erleichtern. Welcher (z.B. arbeitslose) Arbeitnehmer kann sich dann noch dem Druck der Offenbarung beim Einstellungsgespräch oder der Einstellungsuntersuchung widersetzen, wenn der Blick in die Chipkarte doch so einfach ist?

11.3 Ärztliche Schweigepflicht

Immer wieder muß sich der Landesbeauftragte mit besonderen Problemen im Bereich der ärztlichen Schweigepflicht auseinandersetzen.

So wurde aufgrund einer Kontrolle bei einer Krankenversicherung festgestellt, daß diese, ohne daß eine gesetzliche Grundlage oder eine Entbindungserklärung von der ärztlichen Schweigepflicht vorlag, von Fachärzten (auch Nervenfachärzten!) vollständige Gutachten aufgrund einer einfachen Anforderung erhielt. Der Krankenversicherung ist die Einsichtnahme in fachärztliche Gutachten nur in wenigen im Gesetz genannten Fällen erlaubt (vgl. z.B. § 100 SGB X). Auch eine Einwilligungserklärung des Versicherten berechtigt nicht, das vom Gesetzgeber festgelegte grundsätzliche Verbot dieser Datenerhebung zu umgehen.

Bedenklich erscheint auch das Verhalten der Mediziner, die durch die unbefugte Offenbarung personenbezogener medizinischer Daten nicht ausreichend berücksichtigen, daß sie sich dadurch einer strafrechtlichen Verfolgung aussetzen

(§ 203 StGB). Es ist festzuhalten, daß der Mediziner Sachwalter der Interessen seiner Patienten ist und die ihm bekannten (oft sehr sensiblen) Daten nur dann offenbaren darf, wenn das Gesetz oder der Patient dieses fordern bzw. gestatten.

Rechtlich umstritten ist die auch in § 10 Abs. 2 der Berufsordnung der Ärztekammer Sachsen-Anhalt verankerte Regelung, daß dem Patienten die subjektiven Eindrücke oder Wahrnehmungen des Arztes nicht offenbart werden müssen. Zum einen kann durch eine standesrechtliche Satzung geltendes Bundesrecht (hier § 19 BDSG) nicht außer Kraft gesetzt werden. Zum anderen würde durch diese nicht gesetzeskonforme Interpretation der Wille des Gesetzgebers konterkariert, der gerade beim Auskunftsrecht ausweislich der Beratungsprotokolle zum Entwurf des Bundesdatenschutzgesetzes größten Wert darauf gelegt hat, daß das Auskunftsrecht als wichtigstes Kontrollrecht des Bürgers nicht eingeschränkt wird.

Im übrigen ist festzuhalten, daß das Vorenthalten von Auskünften das Vertrauensverhältnis Arzt/Patient derart belasten dürfte, daß eine gedeihliche Zusammenarbeit zwischen Arzt und Patient bei der Behandlung wohl kaum noch möglich ist.

12. Gewerbe, Handwerk und Wirtschaft

12.1 Novellierung der Handwerksordnung

Der Landesbeauftragte hatte in seinem II. Tätigkeitsbericht (S. 59 f) berichtet, daß in dem seinerzeit in Kraft getretenen (Bundes-)Gesetz zur Änderung der HandwO vom 20.12.1993 im Datenkatalog der Anlage D für die Lehrlingsrolle bei den Handwerkskammern die Aufnahme der Wohnanschrift des Lehrlings vergessen worden war. Der rechtliche Mangel ist nach Intervention der Datenschutzbeauftragten 1998 vom Gesetzgeber im Zuge der Neufassung der HandwO behoben und die Aufnahme der Anschrift des Lehrlings in die Lehrlingsrolle zugelassen worden.

Damit ist in diesem Bereich Rechtssicherheit eingetreten.

12.2 Bekanntmachung öffentlich bestellter Sachverständiger im Internet

Welche Problemfelder sich auftun und was beachtet werden muß, wenn beabsichtigt ist, Register mit personenbezogenen Daten, auch solche mit öffentlichem Charakter, im Internet zum Abruf bereitzustellen, dazu hatte der Landesbeauftragte in seinem III. Tätigkeitsbericht (S. 51 f) ausführlich Stellung bezogen.

Sensibilisiert durch diesen Beitrag hatte eine der IHK'n des Landes bei Beratungen mit den anderen Kammern Bedenken geäußert, ob die Daten Öffentlich bestellter Sachverständiger ohne weiteres ins Internet eingestellt werden dürfen. Als ihr bekannt wurde, daß die mit der Erledigung von Datenverarbeitungsaufgaben nach § 8 DSG-LSA beauftragte IHK-GfI diese Daten gegen ihren ausdrücklichen Willen doch ins Internet einstellte, forderte sie die IHK-GfI auf, sofort die betreffenden Daten aus dem Internetangebot zu nehmen und bat auch den Landesbeauftragten um Prüfung.

Der Landesbeauftragte gab der Kammer in seiner Stellungnahme recht. Weder § 9 IHK-G (für kammerangehörige Sachverständige) noch § 7 der Sachverständigenordnung der betreffenden IHK enthalten eine Rechtsgrundlage für die IHK, die personenbezogenen Daten bestellter Sachverständiger via Internet zu publizieren.

Zwar sind die Bestellung und Vereidigung des Sachverständigen öffentlich bekannt zu machen und dazu Name, Adresse und Sachgebietsbezeichnung des Sachverständigen in geeigneten Publikationsorganen jedermann zur Verfügung zu stellen, doch sprengt das Internet den Rahmen der in Frage kommenden geeigneten Publikationsorgane (z.B. Kammerzeitschrift, örtliche Tagespresse und überregionale Sachverständigenverzeichnisse) bei weitem. Denn in allen Fällen ist dabei der Kreis der möglichen Datenempfänger entweder regional oder personell in gewisser Weise eingeschränkt. Eine Abrufmöglichkeit im weltweit zugänglichen Internet ist damit nicht vergleichbar. Die Datenübermittlung erhält damit eine völlig neue Qualität und wäre von den o.g. Rechtsvorschriften nicht mehr gedeckt. Dazu wurde auch auf die bereits im III. Tätigkeitsbericht beschriebenen zusätzlichen Gefährdungen hingewiesen.

Die IHK-GfI nahm die Einstellung der Sachverständigendaten aus dem Internet zurück.

Die Lösung des Problems war nur durch die informierte Einwilligung der Betroffenen in der in § 4 Abs. 2 DSG-LSA vorgeschriebenen Form möglich.

12.3 Einsicht des Gewerbeaufsichtsamtes in Stundennachweise

Durch eine Wach- und Schließgesellschaft war der Landesbeauftragte informiert worden, daß im Rahmen einer Gewerbeaufsichtskontrolle bei ihr Einsicht in die Stundennachweise der Beschäftigten begehrt wurde.

Diesen Stundennachweisen sei, so teilte die Firma weiter mit, entnehmbar, welche Mitarbeiter wann wie lange bei welchen Kunden eingesetzt waren. Hieraus ergäben sich Sicherheits-, personalrechtliche und Datenschutzbedenken. Die Firma wollte deshalb wissen, ob sie zur Vorlage oder gar Herausgabe der Stundennachweise verpflichtet sei.

Nach Rücksprache mit den beteiligten Ämtern konnte der Landesbeauftragte die Wach- und Schließgesellschaft beruhigen, daß sich das Auskunftsbegehren des Landesamtes für Arbeitsschutz auf § 17 Abs. 4 Satz 2 des Arbeitszeitgesetzes stützt. Dort ist festgelegt, daß sich die Aufsichtsbehörde vom kontrollierten Arbeitgeber u.a. die Stundennachweise vorlegen oder zur Einsicht einsenden lassen kann. Die Vorschrift soll u.a. der Bekämpfung von Arbeitszeitverstößen dienen, eines Anlasses für die Kontrolle bedarf es nicht.

Dennoch war das Verhalten des Landesamtes für Arbeitsschutz nicht ganz korrekt. Denn werden - wie in diesem Fall - personenbezogene Daten aufgrund einer Rechtsvorschrift durch Einsichtnahme erhoben, ist der Betroffene gem. § 9 Abs. 3 DSG-LSA auf seine Auskunftspflicht und die Rechtsgrundlage hinzuweisen. Dies unterblieb leider, hätte aber entscheidend zur Erhöhung der Transparenz des Verwaltungshandelns und zur Vermeidung von Verunsicherungen bei der kontrollierten Firma beigetragen.

12.4 Datenabgleich von Ausbildungsverhältnissen

Dem Landesbeauftragten war bekannt geworden, daß aufgrund einer 1997 getroffenen Vereinbarung zwischen dem DIHT (für die Industrie- und Handelskammern und die Handwerkskammern) und der Bundesanstalt für Arbeit (für die Landesarbeitsämter) zur Verbesserung der Transparenz auf dem Ausbildungsmarkt ein Datenabgleich von noch nicht vermittelten Ausbildungsplatzsuchenden mit bereits eingetragenen Ausbildungsverhältnissen erfolgen sollte. Ziel sollte sein, die Arbeitsmarktstatistik in bezug auf Ausbildungsplatzsuchende und -inhaber zu bereinigen.

Auf der Basis dieser Vereinbarung schlossen die IHK'n und HK'n des Landes selbst Verträge mit dem Landesarbeitsamt über den Datenabgleich. Rechtlich handelte es sich dabei um personenbezogene Datenübermittlungen der Kammern an das Landesarbeitsamt.

Der Landesbeauftragte prüfte die Rechtslage und stellte fest, daß es an der erforderlichen gesetzlichen Grundlage für die Datenübermittlung fehlt. Weder das SGB X noch das IHK-G oder die HandwO bieten hierfür den rechtlichen Rahmen. Die eingangs genannte Vereinbarung und die geschlossenen Verträge haben nicht die nach § 4 Abs. 1 DSG-LSA erforderliche Qualität einer Rechtsvorschrift.

Der Landesbeauftragte hat über die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfohlen, den Bundesgesetzgeber aufzufordern, die arbeitsmarktpolitische Zweckmäßigkeit des Verfahrens zu prüfen und sodann die entsprechenden gesetzlichen Rahmenbedingungen zu schaffen.

12.5 Korruptionsregister

Bereits im vergangenen Berichtszeitraum hatte der Landesbeauftragte aufgrund eines Hinweises aus einem anderen Bundesland das Innen- und das Wirtschaftsministerium befragt, ob es in Sachsen-Anhalt Bestrebungen gibt, ein Register mit solchen Gewerbetreibenden anzulegen, die wegen Preisabsprachen, Bestechung usw. bei der öffentlichen Auftragsvergabe nicht berücksichtigt werden sollen.

Dies war seinerzeit - außer mit fehlender Notwendigkeit - vor allem mit rechtlichen Bedenken verneint worden. Bereits seit einigen Jahren haben Bewerber um öffentliche Aufträge ab 20.000 DM bestimmte Erklärungen abzugeben und einen Auszug aus dem Gewerbezentralregister bzw. ein Führungszeugnis vorzulegen. Die Berücksichtigung bloßer Ermittlungen wegen des Verdachts auf derartige Straftaten dürfte dagegen wegen fehlender Rechtsgrundlagen problematisch sein.

Im nunmehr zuständigen Ministerium des Innern wird erneut über ein solches Register nachgedacht. Allerdings hält man dort, wie der Landesbeauftragte auch, nach wie vor daran fest, daß es einer Rechtsgrundlage für ein solches Korruptionsregister bedarf. Man wolle zunächst ohnehin die Aktivitäten und Erfahrungen auf Bundesebene beobachten.

Im übrigen wird der Nutzen eines landesbezogenen Registers für eher gering gehalten, möglicherweise müßten bestimmte Fälle eines bundesweiten Korruptionsregisters sogar in einen europäischen Nachweis eingestellt werden. Auch dafür fehlt z.Zt. noch die entsprechende Rechtsgrundlage.

12.6 Industrie- und Handelskammern

In seinem III. Tätigkeitsbericht (S. 48 ff) hatte der Landesbeauftragte ausführlich über die Tätigkeiten der beiden in Sachsen-Anhalt ansässigen IHK'n und der dabei festgestellten datenschutzrechtlichen Defizite berichtet.

So war damals bei einer Kontrolle der IHK festgestellt worden, daß diese der IHK-GfI jeweils Aufträge zur Verarbeitung der Daten ihrer Kammerzugehörigen erteilt hatte. Die IHK-GfI sollte die Daten - gemeinsam mit den Kammerzugehörigendaten der anderen IHK im Bundesgebiet - in einer Referenzdatenbank speichern, zum automatisierten Abruf durch alle angeschlossenen IHK'n bereithalten und diese auch als elektronische Datenträger zur Verfügung stellen.

Diese Verfahrensweise war rechtlich gedeckt, allerdings mußte der Landesbeauftragte die Kammern darauf aufmerksam machen, daß das beschriebene Verfahren eine Datenverarbeitung im Auftrag darstellt und § 8 DSG-LSA an die Vertragsgestaltung in den Fällen, in denen das DSG-LSA für den Auftragnehmer nicht gilt, bestimmte Anforderungen stellt.

Eine der Kammern reagierte, wie im III. Tätigkeitsbericht (S. 51) berichtet, schnell, die andere Kammer konnte erst im Berichtszeitraum einen den gesetzlichen Anforderungen entsprechenden Vertrag mit der IHK-GfI vorlegen.

Der Forderung des Landesbeauftragten, für das bei der IHK-GfI eingerichtete automatisierte Abrufverfahren gem. § 7 DSG-LSA ein entsprechendes Gesetz bzw. eine Verordnung in Kraft zu setzen, ist das zuständige Ministerium für Wirtschaft und Technologie auch im Berichtszeitraum nicht nachgekommen.
Allerdings soll inzwischen eine Verordnung erarbeitet werden.

Noch nicht geklärt hingegen ist, ob die mit der Ermittlung von Bemessungsgrundlagen für die Feststellung des Kammerbeitrages der Mitglieder beauftragte

AKB e.V. als Gemeinschaftseinrichtung der Kammern im Sinne von § 9 Abs. 2 IHK-G die erforderliche Datenverarbeitung als eigene Aufgabe erfüllt oder in Form von Datenverarbeitung im Auftrag der Kammern. In letzterem Fall wäre wieder § 8 DSG-LSA zu beachten.

Der Landesbeauftragte wird die weitere Entwicklung beobachtend begleiten.

13. Hinweise zum technischen und organisatorischen Datenschutz

13.1 Datumsumstellung 2000

Der Landesbeauftragte beobachtet schon seit mehreren Jahren die eher zurückhaltenden Aktivitäten der öffentlichen Stellen des Landes in bezug auf die Vorbereitungen zur Datumsumstellung auf das Jahr 2000, welche nicht ganz ohne Grund "Millennium Challenge" genannt wird.

Es dürfte, so einschlägige Erfahrungen von Softwareanwendern, eine Fülle von älterer, aber noch immer verwendeter Software geben, deren Entwickler nicht davon ausgingen, daß ihre Produkte im Jahre 2000 noch in Betrieb sein würden. Um damals teure Speicherkapazität zu sparen, wurden meist nur die letzten zwei Stellen für die Jahreszahl verwendet. Aus diesem Grund wird das Jahr 2000 in vielen Programmen als das Jahr 1900 interpretiert. Hinzu kommt das Problem, daß Algorithmen zur Berechnung von Schaltjahren u.U. zu dem falschen Ergebnis kommen, daß es sich beim Jahr 2000 nicht um ein Schaltjahr handelt.

Mögliche Folgen für die Bürgerinnen und Bürger reichen von Fehlberechnungen im privaten Lebensbereich (z.B. bei Banken und Versorgungsunternehmen, auf Lohnlisten und bei Versicherern) bis zu Sicherheitsproblemen im öffentlichen Bereich (z.B. in Einsatzrechnern der Polizei, bei Verkehrskontrollsystemen oder der Intensivstation einer Universitätsklinik).

Zu Beginn des Berichtszeitraumes richtete der Landesbeauftragte eine Anfrage an die Zentrale Stelle für Informationstechnik (ZIT) beim Ministerium des Innern, um zu erfahren, welche Anstrengungen in der unmittelbaren Landesverwaltung bisher unternommen worden sind, um das Ausmaß der Bedrohung festzustellen

und ggf. koordiniert entsprechende Gegenmaßnahmen zu ergreifen. Aus datenschutzrechtlicher Sicht ist neben Maßnahmen in den genannten besonderen Gefahrenbereichen besonders darauf zu achten, daß es als Folge der "Datums-wirren" nicht zu ungewollten Löschungen oder unrichtiger Verarbeitung personenbezogener Daten bei den öffentlichen Stellen kommt.

Eine Antwort hierauf ist dem Landesbeauftragten zwar nicht zugegangen, aber seiner Empfehlung folgend wurde die Problematik auf einer Sitzung des IMA-IT behandelt. Dabei wurde u.a. mitgeteilt, daß es Probleme bei der Datumsumstellung seitens der Rechenzentren des Landes nicht geben wird. Für den großen Bereich der PC-Anwendungen wurde den Mitgliedern empfohlen, selbständig Überprüfungen und Tests in den Behörden und Dienststellen ihres Geschäftsbereiches durchzuführen.

Auf dem Server der ZIT wurde ein vom Bundesministerium des Innern entwickelter umfangreicher Leitfaden zur Datumsumstellung zum Abruf bereitgestellt:

http://www.zit.mi.lsa-net.de/zitalt/2000/jahr2000.htm
http://www.bsi.de/aufgaben/projekte/2000/inhalt.htm

Der Landesbeauftragte weist zusätzlich auf eine inzwischen vorhandene Vielzahl von herstellerspezifischen Informationsangeboten im Internet hin (z.B. von Microsoft, Novell oder Siemens).

Der Landesbeauftragte fordert **alle** öffentlichen Stellen auf, sich rechtzeitig über die volle Funktionsfähigkeit aller bei ihnen eingesetzten Rechner zu vergewissern. Bei Fehlern in der automatisierten Verarbeitung personenbezogener Daten **haftet** die verantwortliche Stelle **auch ohne** Verschulden nach § 18 DSG-LSA!

13.2 Telefax

Wiederholt hat der Landesbeauftragte in den letzten Jahren darauf aufmerksam gemacht, daß der Einsatz von Telefaxgeräten bei der Übermittlung personenbezogener Daten generell als ein rechtlich und technisch unzuverlässiges Verfahren einzustufen ist. Ein Einsatz kommt deshalb nur in Ausnahmefällen in

Betracht und setzt dann die Beachtung bestimmter Grundregeln voraus (vgl. III. Tätigkeitsbericht, S. 62 ff), wenn der Benutzer nicht gegen § 6 DSG-LSA verstoßen will.

Dennoch häuften sich auch im Berichtszeitraum wieder die Hinweise darauf, daß zahlreiche öffentliche Stellen in allen Verwaltungsbereichen einen gedanken- und sorglosen Umgang mit den Geräten an den Tag legen. Ein prekärer Beispielsfall - ausgerechnet bei der Polizei - hat nun auch das Ministerium des Innern nachdenklich gemacht.

Es sah sich genötigt, mit gesondertem Erlaß die nachgeordneten Polizeibehörden und -einrichtungen für die Problematik der Fax-Telekommunikation zu sensibilisieren und auf die Empfehlungen des Landesbeauftragten aus dem III. Tätigkeitsbericht hinzuweisen.

13.3 Datenübermittlungen im Internet und per E-Mail

Der Einsatz "moderner" Übermittlungswege hat oft seine besonderen Tücken und kann schnell zum Verstoß gegen datenschutzrechtliche Bestimmungen führen, wenn man nicht die gesetzlich geforderten Grundregeln der Datensicherheit (§ 6 DSG-LSA) beachtet.

Wer als öffentliche Stelle personenbezogene Daten über das Internet, z.B. per E-Mail, übermitteln will, muß beachten, daß es sich beim Internet um ein offenes Netz handelt, in dem jeder Teilnehmer offene Dokumente einsehen, die darin aufgeführten personenbezogenen Daten lesen und sie sogar, ohne große Spuren zu hinterlassen, verändern kann. Der Weg der Daten und damit die Zahl der möglichen Leser ist nicht im vorhinein festlegbar und kann auch nicht nachvollzogen werden, weil die Übermittlungen automatisch über freie Netzknoten vorgenommen werden. Dabei ist es nicht ausgeschlossen, daß die Daten auf dem Wege von Hamburg nach München über Netzknoten in z.B. drei anderen europäischen Ländern geleitet werden.

Rechtlich bedeutet dies, daß bei einer offenen Datenübermittlung nicht nur die Vorschriften zur Datensicherheit in § 6 DSG-LSA beachtet werden müssen, sondern auch die Übermittlungseinschränkungen in den §§ 12 und 13 Abs. 2 DSG-LSA. So hat beispielsweise eine (offene) Übermittlung personenbezogener

Daten über das Ausland zu unterbleiben, wenn dort keine gleichwertigen Datenschutzregelungen wie im Geltungsbereich des Grundgesetzes bestehen.

Mindestvoraussetzung für die Übermittlung personenbezogener Daten auf diesen Wegen ist deshalb eine im Verhältnis zur Sensibilität stehende, ausreichend sichere Verschlüsselung der Daten. Anzumerken wäre auch noch, daß - entgegen landläufiger Auffassung - die Übermittlung per E-Mail aus den vorstehend genannten technischen Gründen keineswegs schnell sein muß; Übermittlungszeiten von mehreren Tagen auch innerhalb Deutschlands sind durchaus möglich.

13.4 Auftragsdatenverarbeitung durch nicht-öffentliche Auftragnehmer

13.4.1 Unterrichtung des Landesbeauftragten

Bereits in seinem II. Tätigkeitsbericht (S. 65 ff; Anlage 21) hat der Landesbeauftragte ausführlich auf die Probleme bei der Vergabe von Aufträgen zur Verarbeitung personenbezogener Daten an **nicht-öffentliche** Stellen hingewiesen.

Da die Vorschriften des DSG-LSA nur auf öffentliche Stellen des Landes anwendbar sind, muß der öffentliche Auftraggeber gemäß § 8 Abs. 6 Satz 1 DSG-LSA **vertraglich** sicherstellen, daß der nicht-öffentliche Auftragnehmer die Bestimmungen des DSG-LSA befolgt und sich der Kontrolle durch den Landesbeauftragten unterwirft. Außerdem besteht in diesen Fällen für den öffentlichen Auftraggeber eine **Unterrichtungspflicht** gegenüber dem Landesbeauftragten gem. § 8 Abs. 6 Satz 2 DSG-LSA.

Zur Unterrichtung kann auch das einheitliche Meldeformular (vgl. II. Tätigkeitsbericht, S. 11) genutzt werden. Dieses Meldeformular ist Bestandteil der Verwaltungsvorschriften zum DSG-LSA vom 14.10.1993 (MBl. LSA S. 2485). Außerdem ist es im Excel-Datei-Format verfügbar und kann vom Landesbeauftragten abgefordert werden.

Im Berichtszeitraum erreichten den Landesbeauftragten hauptsächlich Meldungen zur Auftragsdatenverarbeitung bei der Aktenvernichtung, der Datenerfassung sowie dem Versand von Lohnsteuerkarten und Wahlunterlagen.

Im Gegensatz zu den jetzt über 2.300 Meldungen automatisierter Dateien zum Register beim Landesbeauftragten gem. § 25 Abs. 1 DSG-LSA nimmt sich die Zahl von nur 40 Unterrichtungen über eine Auftragsvergabe an eine nicht-öffentliche Stelle bescheiden aus.

Überprüfungen von sog. "Fehlmeldungen" haben gezeigt, daß öffentliche Stellen, welche z.B. Lohn- und Gehaltszahlungen im Auftrag durch eine nicht-öffentliche Stelle automatisiert verarbeiten lassen, nicht erkennen, daß es sich auch in diesen Fällen um Datenverarbeitung handelt, für die sie weiterhin die volle datenschutzrechtliche Verantwortung tragen (vgl. § 8 Abs. 1 Satz 1 DSG-LSA).

13.4.2 Aktenvernichtung durch nicht-öffentliche Stellen

Viele öffentliche Stellen bedienen sich inzwischen bei der Entsorgung entbehrlich gewordenen dienstlichen Schriftgutes privater Dienstleistungsunternehmen. Da es sich bei der Vernichtung von Akten mit personenbezogenen Daten um Datenlöschung, also um eine Phase der Datenverarbeitung handelt, haben die den Vernichtungsauftrag erteilenden öffentlichen Stellen § 8 DSG-LSA - insbesondere dessen Absatz 6 - zu beachten.

Der Landesbeauftragte hat im Berichtszeitraum mehrere große Aktenvernichtungsunternehmen aufgesucht und die Beachtung der datenschutzrechtlichen Bestimmungen - insbesondere die §§ 5 und 6 DSG-LSA - bei der Durchführung der mit den öffentlichen Stellen des Landes geschlossenen Verträge geprüft. Die Unternehmen waren kooperativ und arbeiteten im wesentlichen datenschutzgerecht. Bei einer Firma zeigten sich in einem Punkt Probleme bei der Vertragsgestaltung:

Fehlte im Vertrag die Vereinbarung der tagaktuellen Vernichtung, wurde das Aktenmaterial von dem Unternehmen solange unbearbeitet gelassen, bis die Aktenvernichtungsanlage durch tagaktuelle Aufträge nicht ausgelastet war und damit freie Kapazität entstand. Hierdurch hatte sich ein unbearbeitetes Volumen von mindestens einer Wochenproduktion angehäuft. Dies kann zu Datengefährdung und Datenmißbrauch führen.

Der Landesbeauftragte hat aber nicht mehr feststellen können, ob die Vernichtung öffentlicher Datenbestände von dieser Verfahrensweise betroffen war. Trotzdem sollte dieser Fall Anlaß für die öffentlichen Auftraggeber sein, von

Zeit zu Zeit von ihrem vertraglich zu vereinbarenden Recht Gebrauch zu machen, die beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen selbst zu kontrollieren und sich nicht nur auf den Landesbeauftragten zu verlassen.

Deshalb empfiehlt der Landesbeauftragte, insbesondere den öffentlichen Stellen im kommunalen Bereich, alle Auftragsvergaben an nicht-öffentliche Stellen und die damit verbundene Vertragsgestaltung kritisch zu überprüfen und, wenn erforderlich, diese Verträge gem. § 8 Abs. 6 Satz 1 DSG-LSA nachzubessern und umgehend die Unterrichtung des Landesbeauftragten gem. § 8 Abs. 6 Satz 2 DSG-LSA nachzuholen.

Nur so ist der Landesbeauftragte in der Lage, seinem gesetzlich vorgeschriebenen Kontroll- und Beratungsauftrag nachzukommen.

13.5 Datentransfer zwischen Anwendungsprogrammen unterschiedlicher Sicherheitsdomänen

Eine einfache und trotzdem wirksame Möglichkeit, Datenbestände mit personenbezogenen Daten mehreren privilegierten und berechtigten Nutzern gleichzeitig zugänglich zu machen und außerdem von zentraler Stelle Backup und Datenpflege durchführen zu können, ist bekanntlich die Vernetzung.

Nur der Server muß dann - so die allgemeine Auffassung - wegen der dort gespeicherten sensiblen Daten besonders geschützt untergebracht und ggf. mit zusätzlicher Datenschutzsoftware gesichert werden; für die "leeren" PC an den Arbeitsplätzen hält man dies nicht für erforderlich.

Wer das annimmt, irrt! Denn Standard-Bürosoftware, wie die aus dem Hause Microsoft, bietet z.B. die Menü-Funktionen "Datei - Speichern unter" und "Bearbeiten - Kopieren" bzw. "Bearbeiten - Einfügen". Auf diesem Wege könnten in der Sicherheitsdomäne des geschützten Servers legal zugängliche Daten oder Dateien auf Datenträger ins wenig geschützte Client-Umfeld gelangen. Dies gilt unter den marktüblichen Versionen von MS-Windows auch für DOS-Anwendungen und Terminal-Emulationen.

Der Landesbeauftragte hat bei seinen Beratungen und Kontrollen in geeigneter Weise auf dieses Problem aufmerksam gemacht und empfohlen, entsprechende Schutzmaßnahmen bei den Client-PC zu ergreifen, wenn Bedrohungslage und

Sensibilität des zu schützenden Datenbestandes dies erforderlich erscheinen lassen.

Zu den geeigneten Schutzmaßnahmen neben dem Einsatz von Betriebssystemen mit entsprechenden Sicherheitsmechanismen oder zusätzlicher Sicherheitssoftware, die den Zugriff Unbefugter auf die lokalen Datenbestände verhindert, gehören auch die regelmäßige Kontrolle der Datenbestände, z.B. durch den behördlichen Datenschutzbeauftragten oder eine andere geeignete Person, sowie die regelmäßige Sensibilisierung der Mitarbeiter für diese Problematik.

13.6 Computerviren

Auch im zurückliegenden Berichtszeitraum erhielt der Landesbeauftragte wieder Hinweise darauf, daß Computer in öffentlichen Stellen des Landes mit Computerviren infiziert worden sind. Bei den Viren handelte es sich fast ausschließlich um Makro-Viren, also um Viren, die z.B. in WordBasic oder VisualBasic für Excel erstellt wurden und Teil von Word-Dokumenten oder Excel-Arbeitsmappen sind.

Immer häufiger stellte sich dabei das Internet als Infektionsquelle heraus, aus dem die infizierten Dokumente heruntergeladen worden waren.

Zu Vorsichts- und Gegenmaßnahmen wird auf die Hinweise im II. Tätigkeitsbericht (S.72 f) und III. Tätigkeitsbericht (S. 66) verwiesen.

Allerdings machte in letzter Zeit eine völlig neue "Art" von Viren von sich reden, die Hoax-Viren (Scherz-Viren).

Der ahnungslose Nutzer - ausgerüstet mit der neuesten, in diesem Fall allerdings wirkungslosen Anti-Virus-Software - erhält eine E-Mail mit etwa folgendem Inhalt:

"Virengefahr! Wenn Sie eine Mail erhalten mit dem Betreff 'Win a Holiday' (oder einem beliebigen anderen Betreff), so öffnen Sie diese Mail nicht. Alle Dateien Ihres Computers würden gelöscht. Senden Sie diese Nachricht an jeden weiter, der in Ihrem E-Mail-Adreßbuch steht. Senden Sie diese Nachricht sofort an alle weiter!"

Diese Mail selbst ist der "Virus". Nach dem Prinzip des Kettenbriefes wird die Mail durch das Weitersenden an andere Nutzer wieder und wieder vervielfältigt und dabei auch immer größer. Dies führt letztendlich zu einer starken Be- oder gar Überlastung der Übertragungswege und Mail-Server, bis zu deren zeitweisem Ausfall.

Der Landesbeauftragte rät deshalb davon ab, solcher Art Virenwarnungen in Form von E-Mail weiterzuleiten, genau dies wäre der Schadensmechanismus des Hoax-Virus.

Ende März 1999 wurde zum ersten Mal ein Word-Makro-Virus festgestellt, der diesen Schadensmechanismus, nämlich Unmengen von E-Mail zu produzieren, in sich trägt und selbständig ausführen kann.

Der Virus, der den Namen "Melissa" erhielt, benutzt MS-Outlook, um sich selbst an die Einträge im Outlook-Adreßverzeichnis zu versenden, wenn das Attachment einer infizierten E-Mail geöffnet wird.

Einige Antivirensoftware-Produzenten reagierten schnell und boten im Internet Programme zur Melissa-Beseitigung an.

Der Landesbeauftragte empfiehlt im Fall des Zugangs unangeforderter E-Mail: Öffnen der Nachricht und vor allem Öffnen des Attachment ausschließlich in gesicherter und isolierter Umgebung (Einzel-PC).

13.7 Paßwortgestaltung

Öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben gem. § 6 Abs. 2 DSG-LSA zu gewährleisten, daß die Daten nur von befugten Personen im Rahmen der Erledigung ihrer Amtsgeschäfte gelesen, verarbeitet, genutzt oder gelöscht werden (Speicher- und Zugriffskontrolle). Dies geschieht im allgemeinen in Netzwerken, aber auch bei Einzelplatz-PC durch paßwortgeschützte Nutzerkennungen/-Accounts.

Der Landesbeauftragte ist bei seinen Kontrollen und Beratungen vor Ort, aber oftmals auch telefonisch, um Hinweise in bezug auf die datenschutzrechtlich korrekte Bildung und Verwendung dieser Paßworte für IT-Systeme gebeten worden.

Zusammengefaßt wurden dabei durch den Landesbeauftragten folgende, teilweise auch im Grundschutzhandbuch des BSI nachzulesende Hinweise und Empfehlungen gegeben:

- Jeder Nutzer sollte über ein nur ihm bekanntes Paßwort verfügen, das er jederzeit selbst ändern können muß.

- Das Paßwort sollte mindestens 6 Zeichen lang sein und aus Buchstaben, Ziffern und Sonderzeichen bestehen. Allerdings ist zu beachten, daß mit zunehmender Länge und Komplexizität eines Paßwortes (z.B. "$:#K&m13L" o.ä.) proportional die Gefahr zunimmt, daß der Nutzer sich dieses Paßwort irgendwo notiert.

- Paßworte sollten regelmäßig, jedoch nur in begründeten Fällen öfter als monatlich, geändert werden. Die Mindestbestandsdauer eines Paßwortes sollte einen Tag betragen.

- Den Nutzern sollte bekannt sein, daß Paßworte, die aus Bestandteilen des familiären oder beruflichen Umfeldes bestehen, mittels eines "social engineering" genannten Verfahrens von einem möglichen Angreifer häufig herausgefiltert werden können.
  Dies gilt auch für sog. Trivialpaßworte (z.B. 12345, 4711, admin u.ä.).

- Es sollte nach Möglichkeit softwareseitig ausgeschlossen werden, daß aus Bequemlichkeit als neues wieder das alte Paßwort verwendet wird (Paßwort-Historie).

- Nach einer bestimmten Anzahl (zweckmäßigerweise drei) aufeinanderfolgender fehlerhafter Paßworteingaben sollte eine befristete oder unbefristete Sperrung des Accounts erfolgen.
  Der Systemadministrator muß Kenntnis von dieser Sperrung erhalten und darf erst nach Klärung der Ursache die Sperrung wieder aufheben. Anmeldefehlversuche müssen vom System protokolliert werden.

- Die Paßworte des Systemverwalters und der Personen, die alleinverantwortlich besondere Programmberechtigungen besitzen, sollten an sicherer Stelle

versiegelt aufbewahrt werden, z.B. in einem Safe beim Behördenleiter. Der Vertreter des Systemverwalters sollte dazu nur im Vertretungsfall Zugang haben.

- Bei EDV-Verfahren, die Zugang zu besonders sensiblen Daten ermöglichen, ist das Paßwort nach dem Vier-Augen-Prinzip (d.h. von zwei Personen kennt jede nur das halbe Paßwort) einzugeben.

Die öffentlichen Stellen werden durch den Landesbeauftragten stets darauf hingewiesen, daß aus der Fülle der genannten Maßnahmen gem. § 6 Abs. 1 DSG-LSA nur diese ausgewählt und getroffen werden müssen, deren Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Die Art und Weise der Maßnahmen hat sich dabei am Stand der Technik zu orientieren, d.h. sie sind von Zeit zu Zeit zu überprüfen und ggf. fortzuschreiben.

13.8 Fehlende Datenträgerkontrolle

Ziel der Datenträgerkontrolle ist es, so Ziff. 6.2.2.2 VV-DSG-LSA, die bei der Verarbeitung und Nutzung personenbezogener Daten tätigen Personen mit Hilfe geeigneter Maßnahmen am unbefugten Lesen, Kopieren, Verändern oder an der unbefugten Entfernung von Datenträgern zu hindern.

Gleichwohl kam es in einem Polizeirevier im Berichtszeitraum dazu, daß aus dem rund um die Uhr besetzten Bereich des Dienstabteilungsführers eine vorschriftswidrig nicht unter Verschluß gehaltene Diskettenbox mit 9 Disketten abhanden kam und bisher nicht wieder aufgefunden werden konnte.

Auf den Disketten gespeichert waren das Unfalltagebuch der durch die betreffende Dienstabteilung aufgenommenen Unfälle über eine Frist von mehreren Monaten, Urlaubsplanungen, Stundenabrechnungen der Beamten und deren Adressenverzeichnis.

Bedenklich zunächst, daß sich dort offenbar die Polizeibeamten gegenseitig bestehlen. Aber damit nicht genug:

Auf gezielte Nachfrage wurde dem Landesbeauftragten noch mitgeteilt, daß es sich bei dem Datenbestand auf den Disketten nicht etwa nur um eine Sicherheitskopie der auf der Festplatte vorhandenen Originaldaten handelte, sondern auch noch um den Originaldatenbestand, der damit unwiederbringlich verloren

war. Ein Beweis, wie oberflächlich man selbst mit einfachen Sicherungsmitteln umgeht, wenn die tägliche Routine den Blick verstellt.

Der Landesbeauftragte wird überprüfen, ob die ihm dazu vom Ministerium des Innern avisierten technischen und organisatorischen Maßnahmen in diesem Polizeirevier umgesetzt wurden.

14. Hochschulen

Lebenslauf bei der Veröffentlichung von Dissertationen

Ein Petent, der an einer Universität des Landes eine Dissertation geschrieben hat, hatte am Schluß des Promotionsverfahrens Bedenken, den von der Fakultät angeforderten tabellarischen Lebenslauf über die Beifügung zur Dissertation einer breiten Öffentlichkeit zugänglich zu machen. Deshalb bat er den Landesbeauftragten um datenschutzrechtliche Beurteilung.

In der Tat fand sich für die Forderung der Fakultät keine Rechtsgrundlage. Die Fakultät hat deshalb auf die Beifügung des Lebenslaufes nicht mehr bestanden. Gleichwohl wurde aber zu Recht darauf hingewiesen, daß es in der "wissenschaftlichen Welt" seit langem üblich ist, u.a. mit dem tabellarischen Lebenslauf die Persönlichkeit des Promovenden zu würdigen.

Der Landesbeauftragte teilt die Auffassung des Dekans der Fakultät, daß die Veröffentlichung eines Kurzlebenslaufes, der auch wesentliche Aussagen zum wissenschaftlichen Werdegang des Promovenden enthält, zusammen mit der wissenschaftlichen Arbeit den weiteren beruflichen Werdegang bereichern kann.

15. Kommunalverwaltung

15.1 Veröffentlichung eines Redebeitrages aus einer Stadtratssitzung

Durch den Hinweis einer Kommunalaufsichtsbehörde erfuhr der Landesbeauftragte davon, daß in einer Gemeinde der in nicht-öffentlicher Ratssitzung gehaltene Redebeitrag des Bürgermeisters zu einer Personalangelegenheit in allen

Einzelheiten durch eine Veröffentlichung im Nachrichtenblatt der Gemeinde öffentlich bekanntgemacht worden war.

Die in nicht-öffentlicher Ratssitzung gefaßten Beschlüsse sind nach § 50 Abs. 2 GO LSA in einer öffentlichen Sitzung bekanntzugeben, sofern nicht das öffentliche Wohl oder - wie hier - berechtigte Interessen einzelner dem entgegenstehen. In Personalangelegenheiten ist dies wegen der speziellen Vorschriften des Beamtengesetzes der Regelfall. Dann beschränkt sich die Bekanntgabepflicht grundsätzlich auf die **Ergebnisse** der gefaßten Beschlüsse. Es genügt die genaue Bezeichnung der Vorlage und des Abstimmungsergebnisses.

Durch die Veröffentlichung des gesamten Redebeitrages mit personenbezogenen Daten aus der nicht-öffentlichen Ratssitzung war das gesetzlich zulässige Maß deutlich überschritten worden, indem unter Mißachtung kommunal- und beamtenrechtlicher Vorschriften über die Amtsverschwiegenheit personenbezogene Daten unzulässig Dritten zugänglich gemacht wurden.
Wer dafür im dienstrechtlichen Sinne die Verantwortung trägt, muß nun im Disziplinarverfahren festgestellt werden.

15.2 Personaldaten für Haushaltsberatungen des Gemeinschaftsausschusses

Die Mitglieder des Gemeinschaftsausschusses einer kommunalen Gebietskörperschaft wollten ein Personalkonzept zur Verminderung von Personalkosten der Verwaltung beschließen. Dazu wurde der Leiter der Verwaltungsgemeinschaft aufgefordert, dem Gemeinschaftsausschuß eine detaillierte Aufstellung aller Bediensteten mit deren Namen und Bruttovergütung zur Verfügung zu stellen. Der Leiter der Verwaltungsgemeinschaft entsprach dem Beschluß, obwohl er vom Personalrat der Verwaltungsgemeinschaft auf datenschutzrechtliche Bedenken hingewiesen worden war.

Als Ergebnis einer datenschutzrechtlichen Prüfung wurde einvernehmlich festgestellt, daß die Übermittlung der personenbezogenen Daten aller Bediensteten an den Gemeinschaftsausschuß nicht zulässig war, weil es dafür keine Rechtsgrundlage gab. Weder das nach § 85 i.V. mit § 44 Abs. 5 und 6 der GO LSA gegenüber dem Leiter des gemeinsamen Verwaltungsamtes (vgl. § 44 Abs. 2

GO LSA) bestehende Auskunftsrecht war hier einschlägig noch die von der Verwaltungsgemeinschaft als vermeintliche Rechtsgrundlage herangezogene Aufgabenbeschreibung des Gemeinschaftsausschusses über Ernennung, Einstellung und Entlassung der Bediensteten in § 79 Abs. 1 Nr. 4 GO LSA. Auch die spezialgesetzlichen Vorschriften für Übermittlung und Nutzung der Daten im neuen Beamtenrecht (§ 90 Abs. 1 Satz 3, § 90d und § 90g BG LSA), die auch für die nicht verbeamteten Bediensteten Anwendung finden, ließen keine solche Datenverwendung zu, weil personenbezogene Daten für die vorgesehene Erstellung des Konzeptes zur Einsparung von Haushaltsmitteln nicht erforderlich waren. Eine Gesamtaufstellung der vorhandenen Stellen ohne Einzelausweisung und namentliche Zuordnung von Bruttogehältern hätte ausgereicht.

Aufgrund der nicht ganz einfachen Rechtslage sowie weiterer Einzelgesichtspunkte wurde nach § 24 Abs. 3 DSG-LSA von einer formellen Beanstandung durch den Landesbeauftragten abgesehen.

15.3 Kommunales Sachsen-Anhalt Netz (komsaNet)

"komsaNet", so lautete der Produktname für ein ehrgeiziges Projekt der beiden kommunalen Spitzenverbände des Landes. Der Landesbeauftragte war über einen Beitrag in den "Kommunalnachrichten Sachsen-Anhalt" (KNSA) auf dieses Pilotprojekt aufmerksam geworden.

Die Firma debis Systemhaus sfi (Systemhaus für Informationsverarbeitung GmbH), nachfolgend "debis" genannt, beabsichtigte auf der Grundlage eines am 04.09.1996 abgeschlossenen Rahmenvertrages mit den kommunalen Spitzenverbänden ein landesweites, kommunales Datennetz mit geschlossenen Benutzergruppen aufzubauen. Die Knotentechnik und die Leitungen sollten durch die Deutsche Telekom AG als Wählverbindungen (ISDN) oder als Festverbindungen (Mietleitungen) bereitgestellt werden. Die Betreuung der kommunalen "Kunden" sowie das gesamte Netzmanagement sollten durch die Firma debis erfolgen. Hintergrund der Überlegungen bildete auch die Tatsache, daß im

bestehenden ITN-LSA nur Behörden der unmittelbaren Landesverwaltung eingebunden waren und eine Anbindung der Landkreise, Städte und Verwaltungsgemeinschaften lediglich optional vorgesehen war. Ein solcher Anschluß ist bisher nur für die Landeshauptstadt Magdeburg realisiert worden.

Der Landesbeauftragte wirkte im Rahmen seines Beratungsauftrages gem. § 22 Abs. 4 DSG-LSA an den Besprechungen des von den Vertragsparteien eingerichteten Koordinierungsausschusses mit. Einen wesentlichen Schwerpunkt bei der weiteren Begleitung des Pilotprojekts bildeten die Begutachtung und Beurteilung des Entwurfs eines Sicherheitskonzepts für das komsaNet zur Umsetzung der erforderlichen technisch-organisatorischen Maßnahmen gemäß § 6 Abs. 2 DSG-LSA.

Im vorgelegten Entwurf des Sicherheitskonzepts zeigten sich insbesondere im Anschlußmodell, d.h. im Konzept der Abschottung der einzelnen Kommune als Netzteilnehmer im komsaNet selbst, Defizite. Die Bildung von virtuellen privaten Netzen im komsaNet und damit die Kommunikation der Netzteilnehmer in einer oder mehreren geschlossenen Benutzergruppen mit einer zentralen Firewall zur Sicherung gegenüber Fremdnetzen hielt der Landesbeauftragte für nicht ausreichend.

In einer Beratung mit der Firma debis im Juli 1997 wurden diese Bedenken und die daraus resultierenden Forderungen vom Landesbeauftragten dargelegt. Erst nach dem Vorliegen eines endgültigen Sicherheitskonzepts und der Inbetriebnahme der komsaNet-Firewall sowie der Installation und Administration entsprechender intelligenter Routertechnik bei den kommunalen Stellen wäre eine gesicherte Nutzung möglich geworden. Durch die Firma debis wurde daraufhin die Umsetzung eines neuen Sicherheitskonzepts mit entsprechender Änderung des Anschlußmodells bestätigt. Ein endgültiges Sicherheitskonzept erreichte den Landesbeauftragten aber nicht mehr.

Vielmehr wurde ihm mitgeteilt, daß die neben den Standard-Internet-Diensten beabsichtigten zentralen Dienstleistungen bzw. Verfahren als Kern des komsaNet, nämlich zur Zahlbarmachung von BAföG-Mitteln, Wohngeld sowie der Nutzung von ALB-Daten, wegen unüberwindlicher technischer und organisatorischer Probleme vorerst nicht bereitgestellt werden konnten.

Im Januar 1999 wurde die einvernehmliche Aufhebung des auf drei Jahre begrenzten Rahmenvertrages zum 31.12.1998 und damit die Einstellung des Netzbetriebes in den KNSA bekanntgegeben.

Die Präsidien des SGSA und des Landkreistages haben sich aber gleichzeitig entschlossen, zukünftig gemeinsam einen elektronischen Online-Informationsdienst für ihre Mitglieder aufzubauen und über das Internet bereitzustellen. Als einziges Überbleibsel des alten Pilotprojekts bleibt das leicht veränderte Namenkürzel "komsanet" der Nachwelt erhalten.

Der Landesbeauftragte wird die weitere Entwicklung beobachten und steht auch weiterhin den kommunalen Spitzenverbänden für die Beratung zur Verfügung.

15.4 Personaldatenübermittlung zwischen Stadtverwaltung und Stadtrat

Der Landesbeauftragte wurde um Stellungnahme gebeten, ob es für die Stadtverwaltung zulässig sei, eine personenbezogene Aufstellung von Abfindungszahlungen an ehemalige Mitarbeiter zur Information den Stadträten/-innen zu übermitteln.

Bei der von den Stadträten gewünschten aufgeschlüsselten Aufstellung handelte es sich datenschutzrechtlich um eine Übermittlung personenbezogener Daten zwischen zwei öffentlichen Stellen derselben Körperschaft. Diese bedurfte der Einwilligung der Betroffenen oder einer gesetzlichen Grundlage.

Da die Gemeindeordnung neben einem Auskunftsrecht keine ausdrückliche Regelung für diesen Fall enthält, gilt ergänzend das DSG-LSA.

Gemäß § 11 Abs. 1 DSG-LSA ist die Übermittlung personenbezogener Daten an öffentliche Stellen, wozu auch Organe derselben Körperschaft gehören können, wenn sie wie hier nach der GO LSA mit eigenen Rechten ausgestattet sind, zulässig, wenn dies zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist.

Gemäß § 44 Abs. 4 Satz 2 Nr. 1 GO LSA beschließt der Stadtrat oder ein beschließender Ausschuß im Einvernehmen mit dem Bürgermeister über die Ernennung, Einstellung und Entlassung von Gemeindebediensteten, soweit durch Hauptsatzung dem Bürgermeister nicht die Entscheidung übertragen wurde oder diese zur laufenden Verwaltung gehört.

Im vorliegenden Fall hatte der Stadtrat durch die Hauptsatzung die Befugnis zur Entscheidung über die Einstellung und Entlassung von Angestellten und Arbeitern für die in Rede stehenden Vergütungsgruppen auf den Bürgermeister übertragen. Daraus folgt, daß der Rat als ganzes keine Zuständigkeit mehr für die Entscheidung über die Einstellung und Entlassung von Angestellten und Arbeitern hatte. Im übrigen sprach die Hauptsatzung nur von Einstellung und Entlassung, nicht aber von der Beendigung eines Beschäftigungsverhältnisses durch Vertrag.

Mithin war es in diesem Fall nicht zulässig, dem Stadtrat personenbezogene Daten zu übermitteln.

Der Landesbeauftragte hat aber angeregt, zur Gewährleistung des Kontrollrechtes des Gemeinderates aus § 44 Abs. 2 GO LSA, namentlich des aus dem Etatrecht des Gemeinderates gem. §§ 44 Abs. 3 Nr. 4, 94 GO LSA resultierenden Kontrollrechtes des Haushaltsvollzuges den Stadträten anonymisierte Daten in Gestalt von Zahlenmaterial zur Verfügung zu stellen.

15.5 Personaldatenübermittlung an den Gemeinschaftsausschuß

Zu einer planmäßigen Haushaltsberatung sollte den Mitgliedern eines Gemeinschaftsausschusses auch eine detaillierte und vollständige personenbezogene Übersicht der Vergütung und Gehälter aller Bediensteten der Verwaltung zur Verfügung gestellt werden. Datenschutzrechtlich war zu prüfen, inwieweit die personenbezogenen Vergütungs- und Gehaltsaufstellungen erforderlich und rechtlich zulässig waren.

Angelegenheiten, die sich mit Vergütung/Lohn/Bezüge befassen, sind grundsätzlich auch Personalaktenvorgänge. Nach den personalaktenrechtlichen Bestimmungen im Beamtengesetz ist über jeden Beamten eine Personalakte zu führen, sie ist vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Diese Regelung ist auch auf nichtbeamtete Bedienstete entsprechend anzuwenden.

Zwar sind vom Grundsatz her Gemeinschaftsausschüsse für personelle Angelegenheiten der Bediensteten der Verwaltung zuständig, jedoch ließ schon das

vom Gemeinschaftsausschuß vorgegebene Thema der Haushaltsplanung erkennen, daß es gar nicht um **Personalangelegenheiten** einzelner Bediensteter ging, sondern um die üblichen Haushaltsberatungen zu Kostenansätzen. Damit gab es weder eine Rechtsgrundlage noch die Erforderlichkeit zur Übermittlung von konkreten Personaldaten an den Gemeinschaftsausschuß.

Es war ausreichend, für den Beratungsgegenstand "Haushaltsplanung" die einzelnen Dienst- oder Funktionsbezeichnungen der Mitarbeiter und die dazugehörige Besoldungs- oder Vergütungsgruppe gemäß BBesO bzw. BAT-O mitzuteilen. Damit entfiel auch das datenschutzrechtliche Problem.

15.6 Datenerhebung für Aufgaben des Katastrophenschutzes

Ein Landkreis als Katastrophenschutzbehörde forderte die medizinischen Einrichtungen seines Zuständigkeitsbereiches auf, eine aktuelle namentliche Aufstellung des ärztlichen und nicht ärztlichen Personals mit Wohnanschrift und privater Telefonnummer zur Verfügung zu stellen.

Auf eine Beschwerde hin wurde der Katastrophenschutzbehörde die Rechtslage verdeutlicht, daß gem. § 4 Abs. 1 DSG-LSA die Erhebung und Verarbeitung dieser personenbezogenen Daten nur zulässig ist, wenn das Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

Das Katastrophenschutzgesetz des Landes enthält keine unmittelbare Regelung zum Erheben und Verarbeiten personenbezogener Daten für Planungszwecke des Katastrophenschutzes. Darüber hinaus war auch nicht festzustellen, daß für die Katastrophenschutzvorsorge des Landkreises personenbezogene Daten des gesamten ärztlichen und nicht ärztlichen Personals jeder medizinischen Einrichtung erforderlich sind. Damit entfiel auch die Erhebungs- und Verarbeitungsmöglichkeit ohne Einwilligung der Betroffenen.

Nach Hinweis auf die Rechtsgrundlage verzichtete der Landkreis auf seine Datensammlung.

15.7 Bekanntgabe eines Bestattungstermins

Ein Witwer hatte der Stadtverwaltung den Wunsch seiner verstorbenen Frau mitgeteilt, daß die mit ihr zerstrittene Tochter nicht an der Bestattung teilnehmen solle. Nach dem Tode seiner Ehefrau forderte er die Behörde deshalb auf, der Tochter den Bestattungstermin nicht bekanntzugeben. Diesem Anliegen kam die Stadtverwaltung nach und lehnte eine Auskunft an die Tochter ab.

Der Landesbeauftragte klärte die Behörde auf, daß es sich beim Bestattungsdatum nicht (mehr) um ein personenbezogenes Datum handelt, denn von der Behörde wurde übersehen, daß das DSG-LSA nur auf lebende Personen Anwendung findet. Vielmehr handelt es sich bei dem Bestattungstermin um ein Organisationsdatum der Behörde, dessen Übermittlung jedenfalls nicht aus Gründen des Datenschutzes abgelehnt werden kann.

Der Witwer hätte im vorliegenden Fall lediglich auf dem Zivilrechtsweg den letzten Willen seiner verstorbenen Ehefrau durchsetzen können.

16. Landtag

Datenschutz im Petitionsausschuß des Landtages

Auf Anfrage der Ausschußvorsitzenden, ob jedes Mitglied des Petitionsausschusses grundsätzlich alle vorliegenden Petitionen einsehen darf, hat der Landesbeauftragte wie folgt gutachtlich Stellung genommen:

Die aufgeworfene Frage betrifft sowohl die Rechte der Petenten als auch die der Abgeordneten. Bei der Bearbeitung der Petitionen kann es zu einer Konkurrenz beider Rechte kommen. Die dann von Verfassungs wegen gebotene Abwägung beider Rechte obliegt dem Landtag selbst, soweit nicht schon in der Verfassung selbst oder in einem Gesetz Regelungen dazu getroffen wurden.

Im einzelnen:

1. Sowohl die Eingaben von Petenten als auch zu diesem Zweck durch den Petitionsausschuß angeforderte Akten und Auskünfte enthalten regelmäßig personenbezogene Daten. Diesbezüglich steht jedem Petenten und jedem Drittbetroffenen das Recht auf Schutz seiner personenbezogenen Daten aus Art. 6 Abs. 1 Satz 1 LVerf zu. Diese Grundrechte binden nach Art. 3 Abs. 1 LVerf auch den Landtag. Das Nähere regelt das auch für die Arbeit des Landtages geltende Datenschutzgesetz des Landes. Die personenbezogenen Daten der Petenten dürfen danach im Landtag nur im Rahmen des Grundsatzes der **Erforderlichkeit** erörtert, genutzt oder übermittelt werden. Die Entscheidung, ob und ggf. in welchem Umfang die Erforderlichkeit durch generelle Regelungen oder durch Vorgaben für bestimmte Kategorien von Einzelfällen näher konkretisiert werden soll, obliegt dem Landtag, soweit nicht die Verfassung selbst dem einzelnen Abgeordneten besondere Rechte zuweist.
   Der speziell für die Behandlung von Bitten und Beschwerden verfaßte Art. 61 LVerf trifft zur Fragestellung keine spezielle Regelung.

   Allerdings wird durch den in Art. 61 LVerf enthaltenen Verweis auf die Regelung in Art. 53 Abs. 4 LVerf deutlich gemacht, daß die schutzwürdigen Interessen Betroffener (sie sind Dritte im Sinne der Vorschrift) von Verfassungs wegen bei der Behandlung im Ausschuß zu berücksichtigen sind. Die nähere Ausgestaltung der parlamentarischen Arbeit bleibt der Geschäftsordnung (GO LT) nach Art. 46 LVerf vorbehalten. Diese konkretisiert die "Erforderlichkeit" in den §§ 48 und 49 GO LT. Eine direkte Regelung, einzelne Abgeordnete von bestimmten Vorgängen in Ausschüssen auszuschließen, enthält die Geschäftsordnung nicht.

2. Wichtige Hinweise für die rechtliche Beurteilung enthalten aber die Ziffn. 6 und 7 der Grundsätze des Petitionsausschusses über die Behandlung von Bitten und Beschwerden, die vom Plenum des Landtages beschlossen wurden. Danach obliegt die einleitende Bearbeitung dem Ausschußdienst im Einvernehmen mit dem/der Vorsitzenden des Petitionsausschusses. Wird eine Petition nicht im vereinfachten Verfahren erledigt, so sehen die Grundsätze zwei - verschiedenen Fraktionen angehörende - Ausschußmitglieder

als Berichterstatter vor. Daraus folgt, daß im normalen Bearbeitungsfall die jeweils vorliegende Petition lediglich dem/der Vorsitzenden des Ausschusses und den zwei benannten Berichterstattern im vollen Umfang zur Einsichtnahme zur Verfügung steht. Ihnen und dem Ausschußdienst obliegt nicht nur die Verfügungsgewalt über die Vorgänge, sondern auch die Pflicht zur Verschwiegenheit (vgl. § 5 DSG-LSA). So käme z.B. ein Verbringen der Unterlagen in allgemein zugängliche Fraktionsräume oder die personenbezogene Erörterung mit Abgeordneten, die nicht dem Petitionsausschuß angehören, nicht in Betracht.

Auch aus den getroffenen Regelungen über die weitere Behandlung der Petitionen durch den Ausschuß kann der Wille des Parlaments und die Selbstverpflichtung des Ausschusses entnommen werden, den Umgang mit den gerade bei Petitionen häufig anzutreffenden sensiblen personenbezogenen Daten und die damit verbundenen Darlegungen auf ein Minimum an allgemeiner, offener Diskussion zu beschränken.

Auch wenn die Grundsätze zur Beteiligung des/der stellvertretenden Vorsitzenden des Ausschusses keine definitiven Regelungen treffen, sollte auch dabei die angesprochene vorsichtige und zurückhaltende Weiterleitung der personenbezogenen Informationen praktiziert werden. Kommt es im Einzelfall zu keiner einvernehmlichen Regelung zwischen der/dem Vorsitzenden und dem/der Stellvertreter(in), wäre dazu eine Diskussion und ggf. eine Beschlußfassung im Petitionsausschuß anzuraten.

3. Einen weiteren Sonderweg bei der Bearbeitung der Petitionen läßt § 49 GO LT zu. Durch (Mehrheits-)Beschluß des Petitionsausschusses können einzelnen Mitgliedern besondere Befugnisse übertragen werden. Damit können im Einzelfall aus begründetem Anlaß auch besondere Einsichtsrechte verbunden sein.

Bei Einhaltung der vorstehend dargelegten Grundsätze und Regelungen sind die datenschutzrechtlich zu beachtenden Besonderheiten gewahrt.

17. Landwirtschaft

Nachweis zweckentsprechender Verwendung von Fördermitteln

Immer wieder Anlaß zu Beschwerden von Bürgern geben oft umfangreiche Datenerhebungen der Bewilligungsbehörden im Zusammenhang mit den zahlreichen Förderprogrammen, besonders auf dem Gebiet der Landwirtschaft.

So wollte ein Landwirt, der vom Land Sachsen-Anhalt zinsverbilligte Kredite, öffentliche Darlehen und einen Starthilfezuschuß erhalten hatte, nicht einsehen, warum er dem zuständigen Amt für Landwirtschaft und Flurneuordnung über einen Zeitraum von 10 Jahren einen Auszug seines Jahresabschlusses übermitteln sollte und bat, den "Durchleuchtungen ein Ende zu setzen".

Da konnte ihm der Landesbeauftragte leider nicht helfen.
Zwar fehlt im Zuwendungsrecht oft eine bereichsspezifische Rechtsvorschrift für die Erhebung und Verarbeitung personenbezogener Daten, doch muß dann ergänzend auf die allgemeinen Regelungen des DSG-LSA zurückgegriffen werden. Nach § 9 DSG-LSA ist das Erheben personenbezogener Daten bei Betroffenen mit seiner Kenntnis zulässig, wenn die Kenntnis der Daten zur Erfüllung der Aufgaben der erhebenden Stelle **erforderlich** ist.

Zuwendungen werden im allgemeinen auf der Grundlage des § 44 der Landeshaushaltsordnung (LHO) gewährt. § 44 Abs. 1 LHO verlangt, daß die zweckentsprechende Verwendung der Zuwendungen nachzuweisen und ein Prüfungsrecht der zuständigen Dienststelle oder ihrer Beauftragten festzulegen ist. Wie dieser Nachweis im einzelnen zu erfolgen hat, ist oft in Förderrichtlinien geregelt, und meist wird der Landwirt bereits bei der Antragstellung darauf hingewiesen.
Das zuständige Ministerium hat ergänzend vorgetragen, daß im Regelfall durch die Pflicht zur Vorlage der jährlich gefertigten Buchführungsabschlüsse keine Daten übermittelt werden, die dem Amt für Landwirtschaft und Flurneuordnung nicht schon bekannt sind.

Der Landesbeauftragte sieht keine rechtliche Möglichkeit für eine datenschutzrechtliche Beanstandung, wenn eine Bewilligungsbehörde zum Nachweis der zweckentsprechenden Verwendung der Fördermittel die erforderlichen personenbezogenen Daten, wie hier z.B. in Form von Jahresabschlüssen, beim Zuwendungsempfänger erhebt.

18. Personalwesen

18.1 Personalfragebögen

Für die Gestaltung von Personalfragebögen bestehen in Sachsen-Anhalt keine zwingenden Vorgaben. Deshalb werden in vielen Behörden die unterschiedlichsten Personalfragebögen verwendet. Hierbei zeigt sich immer wieder, daß einzelne Fragestellungen rechtlich unzulässig sind. Der Landesbeauftragte hat dazu bereits im I. Tätigkeitsbericht Hinweise gegeben (S. 85 und 96).

Der Landesbeauftragte weist erneut darauf hin, daß stets die Rechtsgrundlagen für das Erheben, Verarbeiten und Nutzen personenbezogener Daten öffentlicher Stellen bei Dienst- und Arbeitsverhältnissen in den §§ 28 Abs. 1 DSG-LSA und 90 BG LSA einzuhalten sind.

Im übrigen bleibt oft unbeachtet, daß der Landesgesetzgeber der Personalvertretung in den Behörden auch für spezifische Fragen an die Bediensteten ein Beteiligungsrecht eingeräumt hat. Zwar besteht kein formelles grundsätzliches Mitbestimmungs- oder Beanstandungsrecht, doch kann die Beachtung des in § 2 Abs. 1 PersVG LSA verankerten Grundsatzes der vertrauensvollen Zusammenarbeit mit der Personalvertretung das Verständnis und die Akzeptanz bei den Bediensteten deutlich verbessern.

18.2 Ungeschützte Personaldaten bei der Versendung von Lohnsteuerkarten

Mit einer Eingabe rügte ein Petent das Verhalten seiner Bezügestelle bei der Versendung der Lohnsteuerkarte und der Lohnsteuerbescheinigung, weil im Fenster des Briefumschlages neben seinem Vor- und Nachnamen sensible

Daten, wie Geburtsdatum, Steuerklasse, Zahl der Kinderfreibeträge, Kirchensteuermerkmale - einschl. die des Ehegatten - und Beschäftigungszeiten, sichtbar waren und bei der Verteilung der Karten von vielen Dritten gelesen werden konnten.

Bei der unverzüglich vorgenommenen Kontrolle bestätigte sich, daß bei der Versendung in ca. 2.000 Fällen so verfahren worden war. Diese Vorgehensweise wurde damit begründet, daß eine Zuordnung der Karten erleichtert wird, wenn auf der Lohnsteuerkarte die Organisationseinheit erkennbar ist.

Da die Einwilligung der Bediensteten dafür unstreitig nicht vorlag, beurteilte sich die erkennbare Übermittlung der Personaldaten nach § 90 Abs. 1 BG LSA und § 28 Abs. 1 Satz 1 DSG-LSA. Sie wäre nur zulässig gewesen, wenn dies zur Durchführung personeller Maßnahmen erforderlich war oder eine Rechtsvorschrift dies vorsah. Dies war nicht der Fall und von der Bezügestelle auch so nicht gewollt. Die Mitarbeiter dort hatten schlicht die vertrauliche Behandlung der Personaldaten aus Vereinfachungsgründen ignoriert, obwohl die verschlossenen Umschläge mit dem Aufdruck "Vertrauliche Personalsache" versehen waren.

Ganz nebenbei verstieß man dabei auch noch gegen das Steuergeheimnis, denn bei einem Teil der (offenbarten) Daten handelte es sich auch um Steuerdaten.

Bei der Konfrontation mit den Folgen sahen die betroffenen Mitarbeiterinnen der Bezügestelle den fehlerhaften Umgang ein und versuchten, die noch nicht verteilten Umschläge auf vertraulichem Wege weiterzuleiten.

Im Hinblick auf besondere Umstände hat der Landesbeauftragte von der an sich erforderlichen förmlichen Beanstandung abgesehen.

18.3 Personaldaten im sog. Konkurrentenklageverfahren

Bereits im II. und III. Tätigkeitsbericht hatte der Landesbeauftragte Probleme bei der allzu großzügigen Übermittlung der Personaldaten Unbeteiligter an ein Gericht dargestellt (II. Tätigkeitsbericht, S. 92 und III. Tätigkeitsbericht, S. 75 f). Dies hat aber das Personalreferat einer Obersten Landesbehörde wiederum nicht davon abgehalten, nichtbeteiligte Beamte dieser Behörde in einen Zivilrechtsstreit vor dem Landgericht wegen Nichtberücksichtigung bei einer Stellen-

vergabe mit hineinzuziehen, indem sie eine Fülle personenbezogener Daten aus deren Personalakten an das Gericht übermittelte. Hierdurch erhielten sowohl das Gericht, vor allem aber die anderen Prozeßbeteiligten Kenntnis von diesen sensiblen Personaldaten.

Die Datenübermittlung begründete die Behörde damit, daß sie in dem von dem unterlegenen Bewerber angestrengten Schadenersatzprozeß die volle Darlegungs- und Beweislast treffe und sie deshalb die Verteidigungsmittel gem. § 277 ZPO vorbringe, die sie für erforderlich erachte. Dazu gehören auch Personaldaten vergleichbarer fiktiver Mitbewerber.

Dieser Argumentation konnte schon deshalb nicht gefolgt werden, weil die fiktiven Mitbewerber nicht über das vom Dienstherrn bei der Stellenvergabe verbindlich vorgegebene Anforderungsprofil mit wirtschaftswissenschaftlicher Qualifikation verfügten. Folgerichtig hatten sich die Beamten von vornherein auch nicht um den frei gewordenen Dienstposten beworben. Außerdem war es auch nicht nachvollziehbar, weshalb der Dienstherr in die Tabelle auch Einzelheiten des beruflichen Werdeganges aufgenommen hatte, die nach der Rechtsprechung der Gerichte in solchen Fällen keine Rolle spielen (z.B. uralte Zeugnisse).

Auch die spezialgesetzlichen Rechtsgrundlagen der ZPO rechtfertigen nur ausnahmsweise eine Zweckänderung des dem Dienstherrn von seinem Beamten für die Personalakte überlassenen umfangreichen personenbezogenen Datenbestandes. Der Beamte muß nur dann Einschränkungen seines Rechts aus seiner Pflicht zur loyalen Mitarbeit hinnehmen, wenn der Dienstherr im Einzelfall wichtige Interessen und Rechte nicht ohne diesen Eingriff wahrnehmen kann.

Unabhängig davon hätte sich der Dienstherr der milderen Form bedienen und dem Gericht anonymisierte Personaldaten zur Verfügung stellen müssen. Erforderlichenfalls hätte bei Bedarf oder Nachfrage des Gerichts dann eine personelle Zuordnung erfolgen können. Dazu hat der Landesbeauftragte bereits 1994 detaillierte Verfahrenshinweise zum Schutz Unbeteiligter bei der Übermittlung personenbezogener Daten aus Personalakten und -dateien an Gerichte gegeben (vgl. II. Tätigkeitsbericht, S. 216).

Wenn auch die oberste Landesbehörde von der Auffassung des Landesbeauftragten nicht völlig überzeugt werden konnte, so hat sie gleichwohl unter Hinweis auf die Beanstandung durch den Landesbeauftragten das Verwaltungsgericht, an das der Rechtsstreit dann abgegeben worden ist, gebeten, die personenbezogenen Daten der nicht beteiligten Beamten nicht mehr in das weitere Verfahren einzubeziehen.

Der Landesbeauftragte hat den Fall formell beanstandet.

18.4 Datenschutz im Justizministerialblatt

Im Justizministerialblatt des Landes wurde ein nicht rechtskräftiger Beschluß eines Verwaltungsgerichts zu einem beamtenrechtlichen Konkurrentenklageverfahren abgedruckt. In den seitenlangen Ausführungen des Gerichts zur Begründung sind umfangreiche personenbezogene Angaben zum schulischen und insbesondere solche zum beruflichen Werdegang sowie genaue Angaben zur jetzigen Beschäftigungsbehörde sowohl des Antragstellers als auch des "Konkurrenten" aufgeführt. Der Name selbst war nur mit dem Anfangsbuchstaben des Nachnamens angedeutet.

Die Publikation veröffentlichungswürdiger Gerichtsentscheidungen steht nach übereinstimmender Auffassung mit dem Ministerium der Justiz außer Streit. Unabhängig davon gilt aber auch für diese Fälle § 4 Abs. 1 DSG-LSA. D.h., es muß eine Rechtsgrundlage vorhanden sein oder die Einwilligung der Betroffenen vorliegen, wenn aus der Fülle der mit dem Abdruck in einem öffentlich zugänglichen Druckwerk übermittelten personenbezogenen Daten die Betroffenen bestimmbar werden (§ 2 Abs. 1 DSG-LSA). Etwas anderes gilt nur dann, wenn diese Daten schon vor der Übermittlung öffentlich aus (anderen) allgemein zugänglichen Quellen bekannt waren.

§ 2 Abs. 7 DSG-LSA sieht in der ersten Alternative die vollständige, in der zweiten Alternative lediglich eine faktische Anonymisierung vor. Letzteres bedeutet, daß der Personenbezug nicht in jedem Fall völlig beseitigt werden muß, wenn die Bestimmbarkeit des Betroffenen mit dem im Gesetz näher beschriebenen Aufwand wesentlich erschwert wird.

Es kann dahingestellt bleiben, welche Form der Anonymisierung sich das Ministerium der Justiz bei der Veröffentlichung vorgestellt hatte, denn im vorliegenden Fall waren die Mindestanforderungen keiner Variante beachtet worden. Eindeutig waren beide betroffenen Personen für eine Vielzahl Außenstehender ohne großen Aufwand bestimmbar, und durch die sehr ins einzelne gehende Darlegung ihres Lebens- und Berufsweges sind ihre Grundrechte (Art. 6 Abs. 1 LVerf) mißachtet worden.

Das Ministerium der Justiz ist als Herausgeber gehalten, die Wahrung der Grundrechte künftig genauer einzuhalten.

18.5 Datenübermittlung aus Personalakten von Polizeibeamten

Im Zusammenhang mit der Vernehmung einer abzuschiebenden ausländischen Staatsangehörigen ergaben sich vage Hinweise auf einen Verrat von Dienstgeheimnissen durch Polizeibeamte einer bestimmten Dienststelle. Die Vernehmung einer weiteren Zeugin führte zu einer Personenbeschreibung zweier Männer. Obwohl nähere Angaben zu Art, Umfang und Zeit einer möglichen Dienstgeheimnisverletzung fehlten, ordnete daraufhin ein für die Ermittlungen unzuständiger leitender Polizeibeamter, unter Umgehung des Personaldezernatsleiters und des Behördenleiters, die Entnahme von Lichtbildern aus einer Vielzahl von Personalakten von Polizeivollzugsbeamten an. Sämtliche Lichtbilder wurden der Zeugin vorgelegt.

Die Entnahme der Lichtbilder aus den Personalakten und die anschließende Übermittlung durch Vorlage an die Zeugin beurteilte sich nach § 28 Abs. 1 Satz 1 DSG-LSA i.V. mit § 56 Abs. 1 BRRG (jetzt § 90 Abs. 1 BG LSA). Danach dürfen Daten von Beschäftigten nur verarbeitet und genutzt werden, wenn dies zur Durchführung personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift dies vorsieht. Deshalb war zunächst zu prüfen, ob die Lichtbilder von der Personalstelle für dienstrechtliche oder polizeiliche Ermittlungen herausgegeben werden durften und ob es sich schon bei der Herausgabe der Lichtbilder an den leitenden Beamten um eine Datenübermittlung oder (nur) eine Datenweitergabe handelte.

Verschiedene Organisationseinheiten innerhalb einer Behörde sind zwar grundsätzlich zueinander nicht Dritte, weil sie derselben speichernden Stelle angehören. Gleichwohl gebot die Einhaltung des Zweckbindungsgrundsatzes und der von Verfassungs wegen gebotene Grundrechtsschutz der betroffenen Beamten im vorliegenden Fall die Anwendung des sog. funktionalen Behördenbegriffs. Unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts zur informationellen Gewaltenteilung auch innerhalb einer Behörde war die Herausgabe der Lichtbilder aus dem Personaldezernat an den leitenden Beamten der gleichen Behörde eine Datenübermittlung an einen Dritten.

Die Unterscheidung ist z.B. für die strafrechtliche Beurteilung (§ 31 DSG-LSA) wichtig und darf insbesondere bei komplexen Behörden, wie z.B. einer Polizeibehörde oder einem Regierungspräsidium, nicht verwischt werden, wenn die von Verfassungs wegen gebotene Zweckbindung von Daten nicht ins Leere laufen soll.

Der anordnende leitende Beamte war weder unmittelbarer Vorgesetzter für die Personalstelle noch war er in Vertretung des Behördenleiters tätig. Für die von ihm angeordnete Lichtbildherausgabe und deren spätere Vorlage an die Zeugin fehlte eine gesetzliche Übermittlungsgrundlage im Dienstrecht.

Ein konkreter Tatverdacht, der die Einleitung eines strafprozessualen Ermittlungsverfahrens aufgrund eines Anfangsverdachts gem. §§ 160, 163 StPO gerechtfertigt hätte, lag nach der Beurteilung des Sachverhalts aus der Sicht des Landesbeauftragten gegenüber keiner der Personen, deren Lichtbilder aus der Personalakte entnommen worden sind, vor. Die Entnahme und die Verwendung der Lichtbilder diente gerade nicht dazu, einen bereits bestehenden Anfangsverdacht zu bestätigen, sondern erst Verdachtsmomente gegenüber Betroffenen zu finden (sog. Verdachtsschöpfungen). Im übrigen war der anordnende Beamte weder Hilfsbeamter der Staatsanwaltschaft noch lag seitens dieser eine entsprechende Anordnung vor.

Damit war der geschilderte Umgang mit den Lichtbildern auch unter strafprozessualen Bestimmungen unzulässig.

Angesichts der Gesamtumstände war eine förmliche Beanstandung geboten. Der Minister des Innern wollte nicht ausschließen, daß vielleicht doch ein Anfangsverdacht, wenn auch nicht personell konkretisiert, gegeben gewesen sein

könnte. Im Ergebnis hält das Ministerium die Entnahme der Lichtbilder nicht für gelungen und hat den Vorgang zum Anlaß genommen, im Rahmen einer Besprechung auf die Problematik hinzuweisen.

18.6 Formulare und Personenbezug

Ein Lehrer wandte sich an den Landesbeauftragten mit der Frage, ob in einer Dienstberatung ein von ihm fehlerhaft ausgefülltes Formular mit seinem Namen mittels eines Overheadprojektors gezeigt werden darf. Die Fragestellung läßt aus datenschutzrechtlicher Sicht zwei Antworten zu.

Soweit die Formulare personenbezogene Daten des Lehrers (Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person gem. § 2 Abs. 1 DSG-LSA) enthalten, die Personalaktenqualität haben, sind diese nach den dafür geltenden Bestimmungen des Personalaktenrechts (vgl. § 90 BG LSA und § 28 DSG-LSA) nur für Personen bestimmt, die für die Personalbewirtschaftung oder die Personalplanung zuständig sind. Die Bekanntgabe anläßlich einer Dienstberatung an andere Bedienstete wäre rechtlich ohne Einwilligung des Betroffenen eine unbefugte Übermittlung an Dritte und unzulässig.

Handelt es sich aber um ein fehlerhaft ausgefülltes Formular, dessen inhaltliche Angaben im Zusammenhang mit dem allgemeinen Dienstbetrieb stehen, ist die dienstbezogene Namensangabe des Lehrers auf dem Formular aus datenschutzrechtlicher Sicht kein Hinderungsgrund für die Erörterung in der Dienstberatung.

18.7 Anhörung von Beschäftigten vor den Personalkommissionen bei Gauck-Überprüfungsverfahren

Die Landesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR des Landes Sachsen-Anhalt hat den Landesbeauftragten um datenschutzrechtliche Prüfung gebeten, ob Vertrauenspersonen bei Anhörungen von Beschäftigten vor Personalkommissionen hinzugezogen werden dürfen.

Die Hinzuziehung ist aus datenschutzrechtlicher Sicht grundsätzlich unbedenklich, denn in der Hinzuziehung einer Vertrauensperson des Betroffenen liegt eine nach § 4 Abs. 1 DSG-LSA schlüssige rechtsgültige Einwilligung in die Bekanntgabe seiner bei der Anhörung übermittelten Daten für den konkreten Fall.

Allerdings ist darauf zu achten, daß der Vertrauensperson keine personenbezogenen Daten Dritter dabei bekannt werden. Dies kann der Fall sein, wenn vom Betroffenen und der Vertrauensperson Einsicht in Unterlagen der Gauck-Behörde genommen wird, in denen personenbezogene Angaben Dritter nicht unkenntlich gemacht worden sind.

18.8 Vorlage von ärztlichen Bescheinigungen auf dem Dienstweg

Ein Personalrat hat den Landesbeauftragten um rechtliche Bewertung gebeten, ob die Vorlage von ärztlichen Bescheinigungen über die Arbeitsunfähigkeit und Arztrechnungen auf dem Dienstweg zulässig sei.

Derartige Bescheinigungen gehören gem. § 90 Abs. 1 und § 90a BG LSA zu den Personalaktendaten und dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in eine anderweitige Verwendung ein. Zugang zu Personalakten haben gem. § 90 Abs. 3 BG LSA nur Beschäftigte, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Die Vorlage solcher Bescheinigungen auf dem Dienstweg ist deshalb grundsätzlich datenschutzrechtlich bedenklich. Ärztliche Bescheinigungen über die Arbeitsunfähigkeit sollen direkt der personalbewirtschaftenden Stelle vorgelegt werden. Die Dienststellenleitung wird lediglich über die Zeiten der Arbeitsunfähigkeit informiert.

Detaillierte Arztrechnungen sind bei Unfällen auf dem Arbeitswege aus Rechtsgründen ebenfalls nur der Personalstelle der jeweils zuständigen Behörde vorzulegen. Diese hat von Gesetzes wegen Anspruch auf detaillierte Angaben, um in den gesetzlich begründeten Fällen Regreßverfahren führen zu können. Das Einreichen offener Unterlagen über die Leitung der Beschäftigungsstelle ist datenschutzrechtlich unzulässig und soll grundsätzlich nicht praktiziert werden, es sei denn, der oder die Bedienstete wollen dies von sich aus.

19. Personalvertretung

19.1 Fragebögen zur Gesundheitsförderung aller Bediensteten

Der Personalrat einer Kommune hatte in Zusammenarbeit mit einer gesetzlichen Krankenkasse einen umfangreichen Fragebogen für alle Bediensteten erstellt, der vom behördlichen Datenschutzbeauftragten dem Landesbeauftragten zur Prüfung vorgelegt wurde.

Ziel der Fragebogenaktion war es, sich ein Bild über die berufliche und gesundheitliche Situation und die Arbeitsplatzbedingungen der Beschäftigten zu verschaffen. Der Fragebogen war unterteilt nach beruflicher Situation/Belastung, Arbeitszufriedenheit, Lebensgewohnheiten/Gesundheitsverhalten, Gesundheitsbewußtsein und Angaben zur Person. Insgesamt sollten 34 Fragen beantwortet werden, die zum Teil zahlreiche Unterfragen enthielten.

Es wurde seitens des Personalrates darauf hingewiesen, daß die Mitarbeit freiwillig sei und die Angaben streng vertraulich behandelt sowie die Anforderungen des Datenschutzes genauestens eingehalten werden würden.

Allerdings zeigte sich bei genauer Betrachtung, daß die Fragen doch ihre Tücken hatten.

Da der Personalrat für seine Aktion natürlich über keine Rechtsgrundlage verfügte, mußte - worauf auch hingewiesen wurde - die Beteiligung freiwillig sein, oder die Erhebungen wurden völlig anonym durchgeführt. Der Fragenkomplex mit den Angaben zur Person war allerdings derart engmaschig, daß er bei einer Verknüpfung bzw. Zusammenführung der Antworten mit dem ebenfalls anzukreuzenden Arbeitsbereich der Kommune, ohne weiteres Rückschlüsse auf einzelne Mitarbeiter zugelassen hätte.

Vom Landesbeauftragten wurde deshalb empfohlen, zur Wahrung der Anonymität der Teilnehmer, ein größeres Raster auszuwählen. Im Interesse der Bediensteten erschien es darüber hinaus wünschenswert, die Auswertung der Fragebögen von neutralen, nicht zur Verwaltung gehörenden Personen durchführen zu lassen.

Den datenschutzrechtlichen Bedenken wurde Rechnung getragen.

19.2 Einsichtnahme in Bewerbungsunterlagen durch den Personalrat

Über die Möglichkeiten des Personalrates, Einsicht in die Personalakten bei bereits beschäftigten Bediensteten zu nehmen, hatte der Landesbeauftragte im III. Tätigkeitsbericht berichtet (S. 81 f).

Von personalverwaltenden Stellen wird aber immer wieder beim Landesbeauftragten angefragt, in welchem Umfang der Personalrat bei Auswahl und Einstellung von Bewerbern Einsichtnahme in **Bewerbungsunterlagen** erhalten darf.

Auf der Grundlage von § 90 BG LSA und § 28 Abs. 1 DSG-LSA dürfen personenbezogene Daten zur Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben, verarbeitet oder genutzt werden. Die Personalräte wirken bei derartigen Verfahren nach den §§ 66 Abs. 1 und 67 Abs. 1 PersVG-LSA mit. Ohne die Zustimmung des Personalrates sind die genannten Personalmaßnahmen rechtlich unwirksam.

Folglich hat der Personalrat einen rechtlichen Anspruch, in Mitbestimmungsverfahren auch die Bewerbungsunterlagen zur Einsicht zu erhalten. Dabei kann es bei einer großen Bewerberzahl zweckmäßig sein, die Bewerberdaten seitens der Dienststelle tabellarisch zusammenzufassen und dem Personalrat nur die Bewerberdaten zuzuleiten, die dem in der Ausschreibung aufgeführten Anforderungsprofil entsprechen. Im übrigen ist es pflichtgemäße Aufgabe des Personalrates, sich bei Einsichtnahmen in solche sensiblen Datensammlungen auf das Notwendige zu beschränken, ggf. bei der für die An- oder Einstellung zuständigen Stelle Einzelauskünfte abzufragen, wenn dies ausreicht.

Der Bewerber jedenfalls hat keinen Einfluß darauf, ob seine Unterlagen dem Personalrat zugeleitet oder nicht zugeleitet werden, weil es sich hierbei um ein gesetzlich gestaltetes Verfahren handelt, das einer Disposition durch Dritte nicht zugänglich ist. Derjenige Bewerber, der die Vorlage seiner Unterlagen an den Personalrat von seiner vorher erteilten Einwilligung abhängig macht, riskiert unter Umständen, am weiteren Auswahlverfahren nicht teilzunehmen. Zur Vermeidung von Rechtsnachteilen ist der Bewerber ggf. darauf aufmerksam zu machen.

20. Polizei

20.1 Überprüfung der Kriminalakten

Der Landesbeauftragte hat seine Praxis fortgesetzt, bei den Polizeidirektionen die Führung der Kriminalakten und die Nutzung der Informationstechnik zu überprüfen. 5 der 6 Polizeidirektionen wurden im Berichtszeitraum überprüft.

Positiv war festzustellen, daß die vom Gesetzgeber vorgesehenen differenzierten Prüffristen für die Aussonderung der Kriminalakten in der Praxis beachtet werden, die Anlage unsinniger oder unbrauchbarer Kriminalakten und schwerwiegende Mängel eher die Ausnahme waren.

Schwächen zeigten sich bei der Festsetzung von Aussonderungsprüffristen bei Kindern und Jugendlichen. Oft war festzustellen, daß die vorgeschriebene Beteiligung des Beauftragten für Jugendsachen und die begründete Entscheidung des für die Deliktsart zuständigen Fachkommissariats in der Kriminalakte nicht aktenkundig gemacht worden waren.

Mangelhaft waren häufig die in den Kriminalakten vorgesehenen Lichtbildnachweise. Gelegentliche Mißbräuche zeigten sich bei der Ed-Behandlung. Sie muß und darf nicht ständig wiederholt werden.

In einem besonders krassen Fall waren innerhalb eines Zeitraumes von 3 Jahren 5 Ed-Behandlungen vorgenommen worden, wovon 4 komplette Ed-Behandlungen allein auf 1 Jahr entfielen. Ein rechtzeitiger Blick in das POLIS-System hätte dies verhindert.

Deshalb sei daran erinnert, daß wiederholte vollständige Ed-Behandlungen innerhalb kurzer Zeiträume nicht erforderlich und von der gesetzlichen Grundlage (§ 81b StPO) nicht mehr gedeckt sind. Sie verstoßen zudem gegen das verfassungsrechtlich begründete Verbot der Doppeldatenerhebung.

20.2 ADV und Datensicherheit in den Polizeidirektionen

Mit der im Berichtszeitraum durchgeführten Prüfung der Führung der Kriminalakten bei den Polizeidirektionen hat der Landesbeauftragte auch stets eine

Prüfung der automatisierten Datenverarbeitung verbunden. Dabei sind zwei Problemfelder immer wieder zutage getreten:

1. Aus der Verpflichtung in § 14 Abs. 2 Satz 3 DSG-LSA, die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen, folgt auch, daß die öffentlichen Stellen Vorkehrungen zu treffen haben, um sich vor jeder Art von Computerviren zu schützen (vgl. II. Tätigkeitsbericht S. 72 und III. Tätigkeitsbericht S. 66).

   Die neben einer Reihe von organisatorischen Maßnahmen erforderliche Virenschutzsoftware muß dazu so aktuell wie möglich sein und an all den Stellen zur Verfügung stehen, an denen unter Umständen infizierte Datenträger in den Geschäftslauf gelangen könnten.

   Mehrmals hat der Landesbeauftragte jedoch feststellen müssen oder ist von den Stellen sogar darauf hingewiesen worden, daß die zentral vom Technischen Polizeiamt Magdeburg (TPA) beschaffte Software nicht die wünschenswerte Aktualität besaß.

   Die Verteilung dieser Software, entweder über das ITN-LSA oder mittels Datenträger, sollte deshalb im Interesse einer störungsfreien Datenverarbeitung überdacht und optimiert werden.

2. In den Polizeidirektionen werden in der Regel vernetzte PC betrieben, d.h. es steht für zentrale Aufgaben und Dateidienste ein Server zur Verfügung. Allerdings sollen, so wurde dem Landesbeauftragten bei seinen Kontrollen stets mitgeteilt, mit Standard-Bürosoftware (z.B. Textverarbeitungssystemen) erstellte Dokumente nach einem Erlaß des Ministeriums des Innern nicht auf dem Server in gesicherter Umgebung und mit der Garantie der Wiederherstellung bei Hardwaredefekten gespeichert werden, sondern auf den lokalen Festplatten.

   Damit wird eine Löschungsüberwachung bzw. Überwachung der Speicherungsdauer der Dokumente kaum möglich. Daß für das Backup jeder Beschäftigte selbst sorgen muß, wenn er denn Zugriff auf sein Diskettenlaufwerk hat, das in der Regel durch Sicherheitssoftware gesperrt ist, war bekannt, aber durch die Erlaßvorgabe nicht zu ändern.

Der Landesbeauftragte mußte auch feststellen, daß wegen unzureichender Fortbildung der Beschäftigten in diesem Bereich einfache Tätigkeiten, wie das Speichern eines Dokumentes in einem bestimmten Verzeichnis oder unter einen bestimmten Namen oder dessen späteres Wiederauffinden nicht immer gelangen.

Das Ministerium des Innern sollte deshalb vordringlich dafür sorgen, daß

- die Beamten in den Polizeidirektionen über geeignete aktuelle Antivirensoftware verfügen,
- eine Lösung gefunden wird, Standardsoftware-Dokumente zentral zu speichern und zu sichern und
- die Beschäftigten durch geeignete Fortbildungsmaßnahmen in der Lage sind, die ihnen zur Verfügung stehende Computertechnik richtig zu bedienen.

20.3 Defizite bei der polizeilichen Vorgangsverwaltung

Wie durch Presseberichte öffentlich bekannt wurde, waren einem Mitglied der parlamentarischen Kontrollkommission polizeiliche Unterlagen aus Ermittlungsverfahren anonym zugegangen.

Da sich in diesem Zusammenhang der Verdacht des Verwahrungsbruchs und der Verletzung von Dienstgeheimnissen durch Polizeibeamte ergab, ordnete das zuständige Amtsgericht auf Antrag der Staatsanwaltschaft gem. § 81b StPO an, bei 136 Polizeibeamten einer Polizeidirektion die Abnahme von Fingerabdrücken durchzuführen.

Aufgrund von Beschwerden betroffener Polizeibeamter gegen diese Maßnahme setzte die zuständige Staatsanwaltschaft den Vollzug des Beschlusses des Amtsgerichts zunächst bis zur Entscheidung über die Beschwerde aus. Die Beschwerdeentscheidung erübrigte sich dann.

Der Landesbeauftragte hatte aufgrund der Vorkommnisse eine eingehende datenschutzrechtliche Kontrolle bei der Polizeidirektion durchgeführt und eine Vielzahl von Geschäftsabläufen unter datenschutztechnischen Gesichtspunkten überprüft. Dabei ergaben sich auch Hinweise zur Überführung eines Beamten.

Wie in anderen Fällen auch, zeigten sich Mängel bei der sicheren Abwicklung des Kurierdienstes und der klaren Abgrenzung des vorgesehenen Adressaten (Person oder Dienstbereich).

So wurde u.a. empfohlen, die per Kurier zwischen den o.g. beteiligten Behörden zu transportierenden Unterlagen fortan nur verschlossen zu befördern, um sie zukünftig der absichtlichen oder unabsichtlichen Kenntnisnahme durch unbefugte Dritte zu entziehen. Für ankommende und abgehende Fernschreiben auf Mehrlagenpapier muß festgelegt werden, wieviele Durchschläge erforderlich sind, um unnötige und unzulässige Mehrfachdatensammlungen zu vermeiden und auf den festgesetzten Verteiler zu begrenzen.

Der Verteiler muß außerdem unter dem Blickwinkel der Erforderlichkeit erstellt werden, da viele Fernschreiben personenbezogene Daten übermitteln und dies im Einzelfall einer Rechtsgrundlage bedarf. Dies gilt vor allem in bezug auf die regelmäßige Information dritter, nicht an der Bearbeitung beteiligter Stellen.

Einzelne Vorgänge enthielten zudem Unterlagen, deren Herkunft nicht mehr nachvollziehbar war. Nach den im Verfahrensrecht geltenden Grundsätzen einer nachvollziehbar geordneten Amtstätigkeit muß erkennbar sein, wann, wie und durch wen eine Unterlage in die Akte gelangt ist.

Die unterbreiteten Vorschläge und Empfehlungen sind nach dem Bericht der Polizeidirektion bereits wenig später umgesetzt worden.

20.4 Aufbewahren von Lichtbildern in der Lichtbildvorzeigekartei

Ein Petent beschwerte sich darüber, daß bei einem Polizeirevier im Rahmen von strafrechtlichen Ermittlungsverfahren mehrfach sein Foto gegenüber Dritten vorgezeigt worden sein soll. Das Foto stamme aus einer Ed-Behandlung zu einem strafrechtlichen Ermittlungsverfahren aus dem Jahre 1992, das durch Freispruch 1996 beendet worden sei.

Ein weiteres Ermittlungsverfahren sei 1997 zwar eingeleitet, aber alsbald nach § 170 Abs. 2 StPO eingestellt worden.

Wie die Überprüfung ergab, war in beiden Fällen der von der Polizei mit Abgabe der Akte übersandte Vordruck "Mitteilung über den Ausgang des Verfahrens"

von der Staatsanwaltschaft nicht an die Polizeidienststelle zurückgesandt worden. Deshalb erfuhr die Polizei erst aufgrund der Überprüfung des Landesbeauftragten von dem Ausgang der beiden Verfahren. Daraufhin wurden die Lichtbilder von der Polizeidirektion eingezogen und vernichtet.

Für den betroffenen Bürger eine schlimme Situation und eine grobe Beeinträchtigung seiner Grundrechte. Zwar mußte er im ersten Verfahren zunächst die Anfertigung der Lichtbilder auf der Grundlage des § 81b StPO dulden. Auch die weitere Aufbewahrung der Bilder für "Zwecke des Ermittlungsdienstes" war im Rahmen der Erforderlichkeit gesetzlich zulässig - allerdings nur solange, bis seine Unschuld in diesen Fällen feststand. Dann setzt § 16 Abs. 2 DSG-LSA i.V. mit Ziff. 6 der KpS-Richtlinien eine absolute Grenze, d.h. die Bilder sind mit den gesamten Ed-Unterlagen unverzüglich zu vernichten. Eine Aufbewahrung von Ed-Unterlagen ist im übrigen stets unzulässig, wenn schon die Anordnung unzulässig war.

Der Fehler lag hier schwerpunktmäßig bei der Staatsanwaltschaft, die es unterlassen hatte, die Polizei über den Ausgang der jeweiligen Verfahren zu unterrichten.

Der Landesbeauftragte hat aber in der Vergangenheit wiederholt dargelegt, daß nach den Grundsätzen über die Verpflichtung zur rechtmäßigen Amtsführung auch die für die Kriminalaktenhaltung zuständige Polizeibehörde eine Pflicht zur Aktualisierung ihrer Datensammlungen trifft. Daraus folgt, daß nach Ablauf bestimmter Zeiten ohne Rückmeldung der Staatsanwaltschaft eine Nachfragepflicht der Polizei besteht.

Das aufsichtführende Ministerium des Innern hat zu dem Vorgang Stellung genommen und dem Landesbeauftragten mitgeteilt, es werde zukünftig innerhalb der Polizeidirektion sicherstellen, daß in den polizeilichen Unterlagen neben dem Datum des Abgangs der Akten an die Staatsanwaltschaft insbesondere der Rücklauf der Rückmeldung über den Ausgang des Verfahren dokumentiert wird. Damit soll gewährleistet werden, daß erkennungsdienstliche Unterlagen nicht unzulässig in polizeilichen Sammlungen verbleiben.

Auch das der Staatsanwaltschaft vorgesetzte Ministerium der Justiz hat auf den Hinweis des Landesbeauftragten die beteiligten Stellen auf die Beachtung der Rückmeldepflicht hingewiesen.

20.5 Wahllichtbildvorlagen

Der vom Ministerium des Innern bereits mehrfach angekündigte Erlaß über Wahllichtbildvorlagen liegt dem Landesbeauftragten immer noch nicht vor (vgl. I. Tätigkeitsbericht, S. 110, II. Tätigkeitsbericht, S. 100 und III. Tätigkeitsbericht, S. 89).

Wie bekannt wurde, ist seitens der Polizei künftig die Übernahme der Lichtbildvorzeigekarteien zusammen mit den Lichtbildern aus den Kriminalakten in das neue POLIS-Verfahren beabsichtigt und daher eine nochmalige Aktualisierung des bisherigen vom Ministerium des Innern erst im Entwurf erstellten Erlasses vorgesehen.

Der Landesbeauftragte weist im übrigen darauf hin, daß die moderne Technik die Erstellung von virtuellen realitätsnahen Personenbildern erlaubt, so daß in vielen Fällen die Wahllichtbildvorlage "alten Stils" mit ihren Mängeln und Schwächen nicht mehr erforderlich ist.

20.6 Videoaufzeichnungen

20.6.1 Zur Gefahrenabwehr durch kommunale Stellen

Ein Problem scheint der zunehmende Vandalismus in den Städten und Landkreisen des Landes zu sein.

So erfuhr der Landesbeauftragte von einem Anrufer, daß die in einem Landkreis aufgestellten Abfallsammelbehälter mit dem Hinweis versehen seien, die Abfallentsorgung würde videoüberwacht. Wie sich dann herausstellte, entsprach dieser Hinweis nicht den Tatsachen. Tatsächlich sollte das Schild nur potentielle Übeltäter abschrecken. Das war auch erfolgreich.

Dem Landkreis, der nun wissen wollte, unter welchen Voraussetzungen die (tatsächliche) Videoüberwachung datenschutzrechtlich zulässig sei, mußte der

Landesbeauftragte mitteilen, daß es nach § 16 Abs. 2 SOG LSA - unter den dort bestimmten Voraussetzungen - nur der Polizei erlaubt ist, solche Aufzeichnungen vorzunehmen.

Wie der Landesbeauftragte gehört hat, wird aber im Ministerium des Innern des Landes überlegt, diese Problematik durch eine Änderung des SOG LSA langfristig zu lösen.

20.6.2 Für die Aufgaben der Polizei

Auch in Sachsen-Anhalt werden die Wünsche der Polizei nach dem Einsatz technischer Aufzeichnungsgeräte mit verschiedener Begründung immer lauter. Zum einen wird in Zeiten knapper Kassen die Einsparung beim personellen Aufwand angeführt - ein schlechtes und schwaches Argument, denn der Rechtsstaats darf nicht die Beachtung von Grundrechten gegen billige Münze aufrechnen.

Zum anderen wird die deutlich wirkungsvollere Gefahrenabwehr und die beweissichernde Kraft bei der Strafverfolgung ins Feld geführt. In der Tat sprechen viele Beobachtungen im praktischen Alltag dafür, daß das Aufstellen einer Videokamera an bestimmten Stellen in einer Stadt schlagartig zum Rückgang von Straftaten und damit zu einer für die Bürger sinnvollen Gefahrenabwehr führt. Gelegentlich gelingt mit einer aufgezeichneten Szene auch die (leichtere) Festnahme und Überführung eines Straftäters.

Dies wird aber oft nur möglich, weil gleichzeitig die Grundrechte einer Vielzahl unbeteiligter Bürger auf unbeobachtete, freie Entfaltung ihrer Persönlichkeit zumindest teilweise eingeschränkt werden. Das ist nur auf einer klaren gesetzlichen Grundlage zulässig, die der jeweils zuständige Gesetzgeber unter Abwägung aller Gesichtspunkte für unerläßlich und noch für verhältnismäßig halten durfte.

Solche bereichsspezifischen Rechtsgrundlagen gibt es für das Versammlungsrecht in den §§ 12a und 19a VersammlG, für die sonstige Gefahrenabwehr in § 16 SOG LSA und für die Strafverfolgung in § 100c Abs. 1 Nr. 1 StPO.

Daneben gibt es - ohne spezielle Rechtsgrundlage - die Überwachungswünsche der Polizei für Maßnahmen zur Aufrechterhaltung des fließenden Verkehrs. Angesichts der heute zur Verfügung stehenden Vielfalt optischer und technischer

Möglichkeiten bei Aufzeichnungsgeräten ist dieser Einsatzbereich in dichtbesiedelten Stadtbereichen nicht unproblematisch und für Mißbrauch besonders anfällig.

In den Fällen der Gefahrenabwehr ist der Landesbeauftragte bisher vereinzelt um Beratung und Stellungnahme gebeten worden. Wo die gesetzlichen Anforderungen eindeutig vorlagen, hat er unter zusätzlichen Hinweisen zur Mißbrauchseingrenzung und zum Schutz Unbeteiligter keine Bedenken erhoben.

Es sind aber künftig Konstellationen denkbar, bei denen unter den verschiedensten Rechtsgrundlagen eine Gesamtbeobachtungsszenerie entsteht (z.B. Totalerfassung ganzer Innenstadtbereiche), die mit dem übergeordneten Verfassungsrecht nicht mehr vereinbar ist.

Die Datenschutzbeauftragten des Bundes und der Länder haben wegen der vielfältigen Problematik auf ihrer 57. Konferenz im März 1999 beschlossen, dazu eine spezielle Arbeitsgruppe einzusetzen. Deren Ergebnisse sollen dann nach Beratung in die bundesweite Beurteilung durch die Datenschutzbeauftragten einfließen.

21. Rechtspflege

21.1 Justizmitteilungsgesetz

Wie bereits in den drei vorhergehenden Tätigkeitsberichten (I., S. 117, II., S. 11, III., S. 90 ff) angesprochen, fehlte bislang eine Rechtsgrundlage für die vielen Mitteilungen der Justiz in all ihren Tätigkeitsbereichen.

Zwischenzeitlich ist am 01.07.1998 das Justizmitteilungsgesetz und Gesetz zur Änderung kostenrechtlicher Vorschriften und anderer Gesetze (JuMiG) vom 18.06.1997 in Kraft getreten. Es regelt in einer Vielzahl von bereichsspezifischen Vorschriften, teilweise ausgeformt als Soll-Vorschrift oder als Zulässigkeitserfordernis, die Datenübermittlungsbefugnisse der Justiz.

Kritisch ist aus Sicht des Datenschutzes anzumerken, daß eine regelmäßige Unterrichtungspflicht der Betroffenen über Datenübermittlungen zu ihrer Person keinen Eingang in das Gesetz gefunden hat. Es besteht nur ein Auskunftsanspruch des jeweils Betroffenen. Nicht berücksichtigt wurde auch der Anordnungsvorbehalt für Richter.

Die Konkretisierung der im Gesetz vorgesehenen Übermittlungsbefugnisse wird zum Teil auf Verwaltungsvorschriften abgewälzt. Das bedeutet für den Bürger, daß der vom Bundesverfassungsgericht im Volkszählungsurteil entwickelte Grundsatz, daß aus dem Gesetz heraus klar ersichtlich sein muß, wer was wann über ihn wissen darf, im Justizmitteilungsgesetz nicht vollständig umgesetzt, sondern zum Teil auf die Ebene der Verwaltungsvorschriften verlagert wurde. Verwaltungsvorschriften aber sind den Bürgerinnen und Bürgern nicht so einfach zugänglich wie ein Gesetzblatt.

21.2 Strafverfahrensänderungsgesetz

21.2.1 Generelle Anmerkungen

Zu Beginn des Jahres 1999 hat die Bundesregierung einen weiteren Entwurf für ein Strafverfahrensänderungsgesetz (StVÄG) vorgelegt. Dieser knüpft an den nicht mehr weiter diskutierten Entwurf des Jahres 1996 an (siehe III. Tätigkeitsbericht S. 94 f).

Ziel soll (immer noch) sein, für die bei der strafprozessualen Ermittlungstätigkeit in einem Strafverfahren erhobenen personenbezogenen Unterlagen sowie die Verarbeitung personenbezogener Daten in Dateien und ihre Nutzung präzise und normenklare Rechtsgrundlagen zu schaffen.

Neu ist, daß der Entwurf auch eine Übermittlungsbefugnis des Bundeszentralregisters zur Erteilung von Auskünften an die Staatsanwaltschaften und das Bundeskriminalamt zur Durchführung von § 2 DNA-Identitätsfeststellungsgesetz und entsprechende Anfragebefugnisse schaffen will.

Die im neuen Entwurf vorgesehenen Änderungen enthalten gravierende Eingriffe in das Grundrecht auf informationelle Selbstbestimmung, die, insbesondere bei den Regelungen zur Sicherstellung der Strafverfolgung und Strafvollstreckung, den engen verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichtes zur **Unabweisbarkeit** schwerer Eingriffe in keiner Weise entsprechen (BVerf in st. Rechtspr. E 19, 342 (348); E 45, 400 (420), zuletzt E 88, 203 (309)).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dazu bereits in ihrer Entschließung vom 17./18. April 1997 **(Anlage 2)** eingehend begründete Forderungen erhoben. Davon wurde im vorliegenden Entwurf kaum ein wesentlicher Punkt berücksichtigt. In der jetzt beiliegenden Begründung für die vorgesehenen Eingriffe wird lediglich pauschal auf "Bedürfnisse der Praxis" verwiesen. Belegt oder auch nur ansatzweise nachvollziehbar dargelegt sind solche Bedürfnisse nicht. Erkennbar sind allenfalls "kurzsichtige" Bemühungen, Staatsanwälte mit Hilfe der gesetzlichen Regelungen auf Kosten der Rechte Betroffener von Aufgaben zu entlasten und diese auf die Polizei zu übertragen. Damit wird nicht nur das bewährte Prinzip der justiziellen Kontrolle in wichtigen Bereichen des Ermittlungsverfahrens aufgegeben, sondern es findet auch die vom Bundesverfassungsgericht immer wieder geforderte Prüfung und Beschränkung auf **erforderliche** Eingriffe des Gesetzgebers nicht statt.

Der Landesbeauftragte hat zum Entwurf 1999 Stellung genommen. Seine Bedenken beziehen sich im wesentlichen auf folgende Regelungen:

- die Ausweitung der polizeilichen Befugnisse und die Aufweichung des Richtervorbehaltes durch die Möglichkeit, daß Hilfsbeamte der Staatsanwaltschaft bei Gefahr im Verzug Öffentlichkeitsfahndungen einleiten bzw. längerfristige Observationen anordnen und Tage bis zu einer richterlichen Entscheidung vergehen,
- die unverhältnismäßige Belastung von Zeugen im Rahmen der Öffentlichkeitsfahndung, wo bereits eine "wesentliche Erschwernis" der Ermittlungen ausreichen soll, um eine Öffentlichkeitsfahndung nach ihnen auszulösen sowie die Nichtbeachtung von Zeugnis- und Auskunftsverweigerungsrechten,
- keine Benachrichtigungspflicht an Betroffene bei längerfristigen Observationen,
- die begrifflich zu unbestimmte Akteneinsicht zu "Zwecken der Rechtspflege",
- Doppelspeicherungen von Daten für Zwecke künftiger Strafverfahren, da neben bestehenden Speicherungsbefugnissen nach Landes- und Bundespolizeirecht und des im Aufbau befindlichen staatsanwaltschaftlichen Verfahrensregisters noch weiter die eigenständige Speicherung bei den Staatsanwaltschaften vorgesehen ist,

- die im Hinblick auf das staatsanwaltschaftliche Verfahrensregister entbehrlichen gemeinsamen Dateien und die dazu fehlenden Vorschriften zur datenschutzrechtlichen Verantwortlichkeit.

Der weitere Verlauf des Gesetzgebungsverfahren bleibt abzuwarten.

21.2.2 Anmerkungen zur Öffentlichkeitsfahndung

Wie bereits vorstehend angesprochen, beabsichtigt der Gesetzgeber mit dem Entwurf des StVÄG 1999 auch, die Öffentlichkeitsfahndung im Strafverfahren auf eine gesetzliche Grundlage zu stellen.

Den Anforderungen der bereits im III. Tätigkeitsbericht (S. 100 f) erwähnten Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1995 (Anlage 7 zum III. Tätigkeitsbericht) genügen die vorgesehenen Regelungen des StVÄG 1999 nicht.
Im wesentlichen gilt dies für folgende Punkte:

- Bei der in Art. 1 StVÄG 1999 vorgesehenen Neufassung der §§ 131 bis 131c StPO begnügt sich der Gesetzgeber wieder mit dem dehnbaren Begriff der "Straftat von erheblicher Bedeutung". Auf einen Straftatenkatalog oder vergleichende Kriterien, die eine Öffentlichkeitsfahndung auch bei anderen Straftaten erlauben würden, wird gänzlich verzichtet.

- Bei den weiteren Voraussetzungen für eine Öffentlichkeitsfahndung genügt - entgegen der Forderung der Datenschutzbeauftragten - bereits eine wesentliche Erschwernis der Ermittlungen, um bei Beschuldigten, vor allem aber bei Zeugen, in schwerwiegender Weise in deren Persönlichkeitsrechte einzugreifen.

- Eine im Sinne des Grundsatzes der Verhältnismäßigkeit notwendige Abstufung und die Beschränkung hinsichtlich des Verbreitungsgebietes von Öffentlichkeitsfahndungen sowie des Mediums wurde vom Gesetzgeber nicht aufgegriffen.

Auch Forderungen, wie ein ausschließlicher Richtervorbehalt bei der Öffentlichkeitsfahndung nach Zeugen und für die Fahndung nach Beschuldigten ausnahmsweise eine Eilkompetenz der Staatsanwaltschaft bei Gefahr in Verzug, blieben unbeachtet.

Statt dessen muß nun **jeder** Bundesbürger damit rechnen, daß selbst eine große Öffentlichkeitsfahndung nach ihm als Zeuge künftig von Hilfsbeamten der Staatsanwaltschaft angeordnet werden kann, wenn dies im Gesetzgebungsverfahren nicht noch geändert wird.

Bleiben die derzeit unzulänglichen Schutzregelungen in den §§ 131 und 131c des Gesetzentwurfes bestehen, drohen weitere Rechtsbeeinträchtigungen:

So sollen die Vorschriften zur Öffentlichkeitsfahndung nach der Begründung des Gesetzentwurfes auch für Öffentlichkeitsfahndungen im Internet gelten. Damit wird der derzeitige Rechtszustand sogar verschlechtert, wonach bei Fahndungen im Internet zumindest die gesetzlichen Voraussetzungen für eine Datenübermittlung ins Ausland vorliegen müssen.

Völlig unberücksichtigt sind auch die vielfältigen technischen Mißbrauchsmöglichkeiten im Internet. Namen und Bilder von Beschuldigten und Zeugen können von interessierter Seite beliebig verändert werden. Der Landesbeauftragte erinnert in diesem Zusammenhang besonders daran, daß jeder Nutzer des Internet Informationen, wie z.B. Personenfahndungen, auf seinen Rechner herunterladen kann. Das heißt, selbst wenn Öffentlichkeitsfahndungen im Internet als falsch oder gegenstandslos zurückgezogen werden oder der zuständige Richter die Voraussetzungen für die Öffentlichkeitsfahndung nicht gegeben sieht, bestehen keine technischen Möglichkeiten mehr, Fahndungsaufrufe, die auf jedem PC, in jedem Winkel der Welt gespeichert sein können, zu revidieren.

Deshalb hält es der Landesbeauftragte geradezu für unverantwortlich, Öffentlichkeitsfahndungen im Internet durch Hilfsbeamte der Staatsanwaltschaft anordnen zu lassen. Vielmehr muß die Fahndung in diesem Medium die absolute Ausnahme sein und einem strengen Richtervorbehalt unterliegen.

21.3 Einführung des sog. "Großen Lauschangriffs"

Mit dem Gesetz zur Änderung des Art. 13 des Grundgesetzes vom 26.03.1998 hat der Gesetzgeber nach heftiger rechtspolitischer Debatte die verfassungs-

rechtliche Grundlage zur Einführung des sog. "Großen Lauschangriffs" geschaffen. Anschließend erfolgte im Gesetz zur Verbesserung der Bekämpfung der organisierten Kriminalität vom 04.05.1998 die inhaltliche Ausgestaltung des Abhörens von Wohnraum im strafrechtlichen Ermittlungsverfahren.

Bedauerlicherweise fanden dabei die bereits im III. Tätigkeitsbericht (S. 96 f) angesprochenen Forderungen der Datenschutzbeauftragten des Bundes und der Länder vom 22./23.10.1996 (Anlage 10 zum III. Tätigkeitsbericht) zum Schutz vor allem unbeteiligter Dritter keine angemessene Berücksichtigung.

So wurde weder die Wohnraumüberwachung auf die Verfolgung schwerster Straftaten beschränkt, noch wurde die Forderung, nur ein Kollegialgericht über eine solche Überwachung entscheiden zu lassen, konsequent erfüllt; bei Gefahr im Verzuge kann jetzt auch ein einzelner Richter des Kollegialgerichts entscheiden.

Bandendiebstahl, gewerbsmäßige und Bandenhehlerei, aber auch leichte Vergehen nach dem Betäubungsmittelgesetz gehören nach Auffassung des Landesbeauftragten nicht zu den besonders schweren Straftaten, die einen derart schwerwiegenden Eingriff in Grundrechte rechtfertigen. Die Aufnahme des Geldwäschetatbestandes in den Katalog der zur Wohnraumabhörung berechtigenden Delikte und die Bezugnahme auf § 261 Abs. 1 bis 4 StGB führen groteskerweise dazu, daß beim Verdacht einer versuchten Geldwäsche eine Wohnraumüberwachung zulässig ist, obwohl gleichzeitig das mildere Mittel der Telefonüberwachung (noch) nicht erlaubt ist. Deutlicher kann die unausgewogene Arbeit des Bundesgesetzgebers nicht werden.

Das von den Datenschutzbeauftragten geforderte Kriterium der Aussichtslosigkeit anderweitiger Ermittlungen hat zwar Eingang in das Gesetz gefunden, ist aber für die Praxis kein Hinderungsgrund, da als "aufweichende Alternative" eine "wesentliche Erschwernis der Ermittlungen" für die Wohnraumüberwachung ausreichend sein kann. Diese kann stets leicht belegt werden.

Ein weiteres Problem in der Diskussion war die Zulässigkeit des Abhörens bei Berufsgeheimnisträgern und Angehörigen eines Verdächtigen. Immerhin ist nun nach § 100d Abs. 3 Satz 1 StPO die Überwachung von Wohnraum von Berufsgeheimnisträgern (§ 53 Abs. 1 StPO) unzulässig. Leider ist dieser Schutz nicht auf Abhörmaßnahmen im Zusammenhang mit persönlichen Vertrauten ausgedehnt worden. Dabei gewonnene Erkenntnisse dürfen verwertet werden, wenn

dies unter Berücksichtigung der Bedeutung des zugrundeliegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhaltes oder der Ermittlung des Aufenthaltsortes des Täters steht. In der Praxis wird dieses Abwägungskriterium kaum eine Schutzbedeutung gewinnen.

Auch eine weitere Forderung der Datenschutzbeauftragten in ihrer Entschließung zur akustischen Wohnraumüberwachung ist im Gesetzgebungsverfahren nicht berücksichtigt worden. Eine anderweitige Verwendung der erhobenen Daten (Zweckänderung), die die Datenschutzbeauftragten weder zu Beweiszwecken noch als Ermittlungsansatz für andere als Katalogtaten als zulässig ansahen, ist nunmehr durch § 100f StPO möglich.

Abschließend ist anzumerken, daß mit der gesetzlichen Einführung der akustischen Wohnraumüberwachung der Gesetzgeber eine tiefgreifende Bresche in das Grundrecht auf Unverletzlichkeit der Wohnung geschlagen hat, deren Nutzen und Praktikabilität für die Strafverfolgungsorgane auch nach Meinung vieler Praktiker bei Polizei und Staatsanwaltschaft fraglich ist.

Es wäre wünschenswert gewesen, daß der Gesetzgeber zunächst die erforderliche Rechtstatsachensammlung eingeleitet und ihre Ergebnisse abgewartet hätte. Zumindest hätte aber damit der so beschworene "durchschlagende Erfolg" dieses (vor-)letzten Mittels zum "Einbruch" in die Intimsphäre der Bürger nach einer bestimmten Zeit kritisch überprüft werden müssen. Nun kann nur noch das anhängige Überprüfungsverfahren beim Bundesverfassungsgericht dieses Übermaß an "Schnüffelei" in der Intimsphäre wieder beseitigen.

21.4 Parlamentarische Kontrolle des Einsatzes technischer Mittel in Wohnungen

Gemäß Art. 13 Abs. 6 Satz 1 GG unterrichtet die Bundesregierung den Bundestag jährlich über den Einsatz technischer Mittel. Ein vom Bundestag gewähltes Gremium übt auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus. Nach Satz 3 dieser Vorschrift gewährleisten **die Länder** eine gleichwertige parlamentarische Kontrolle.

Unter den Justizministerien der Länder ist eine Diskussion darüber entstanden, ob auch landesrechtlicher Regelungsbedarf bezüglich einer parlamentarischen Kontrolle von Wohnraumüberwachungsmaßnahmen nach der StPO besteht.

Nach Mitteilung des Ministeriums der Justiz sei die übereinstimmende Auffassung der Justizministerien der Länder, daß bei Wohnraumüberwachungsmaßnahmen nach der StPO die parlamentarische Kontrolle vom Bundestag zu gewährleisten ist. Kontrollbedarf der Länder wird nur bei Wohnraumüberwachungsmaßnahmen nach den Sicherheits- und Ordnungsgesetzen der Länder oder den jeweiligen Landesverfassungsschutzgesetzen gesehen.

Der Landesbeauftragte teilt diese Auffassung nicht. Maßgeblicher Anknüpfungspunkt für die parlamentarische Kontrolle ist, ob eine Stelle des Bundes oder des Landes die Maßnahme ausgeführt hat.

Gemäß Art. 83 GG führen die Länder die Bundesgesetze als eigene Angelegenheiten aus, soweit das Grundgesetz nichts anderes bestimmt. Soweit Wohnraumüberwachungsmaßnahmen nach § 100c Abs. 1 Nr. 3 StPO durch Landesbehörden (Polizei und/oder Staatsanwaltschaft) durchgeführt werden, handelt es sich also um Maßnahmen von Landesbehörden.

Die Verantwortung der Exekutivbehörden der Länder besteht gem. Art. 28 Abs. 1 Satz 1 i.V. mit Art. 20 GG gegenüber dem Landesparlament und ist Ausdruck der allgemeinen politischen Kontrollfunktion des Parlaments im Rahmen seiner Zuständigkeit gegenüber der Exekutive.

Für diese Auffassung spricht, daß auch andere Formen parlamentarischer Kontrolle von Grundrechtseingriffen nicht darauf abstellen, ob sich die Maßnahmen nach einem Bundes- oder Landesgesetz richten. Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses gem. Art. 10 Abs. 2 GG finden fast ausschließlich auf bundesgesetzlicher Grundlage statt. Die Nachprüfung dieser Beschränkung wird durch das Gesetz zu Art. 10 GG nur bei Maßnahmen von Bundesbehörden dem G 10-Gremium des Bundestages zugewiesen. Die Regelung der parlamentarischen Kontrolle der G 10-Eingriffe von Landesbehörden wird gem. § 9 Abs. 5 G 10-Gesetz dagegen dem Landesgesetzgeber überlassen.

Allein die Tatsache, daß nach Art. 13 Abs. 6 Satz 1 GG und § 100e Abs. 2 StPO gegenüber dem Deutschen Bundestag jährlich ein Bericht zu erstatten ist, der auch die Maßnahmen der Länderbehörden umfaßt, ändert nach Auffassung des Landesbeauftragten nichts an der Verantwortlichkeit der Exekutive gegenüber dem Landesparlament. Die Berichtspflicht der Landesjustizverwaltungen soll

lediglich gewährleisten, daß der Deutsche Bundestag als Gesetzgeber in diesem Bereich einen Gesamtüberblick über alle durchgeführten Maßnahmen erhält. Art. 13 Abs. 6 Satz 3 GG bleibt hiervon unberührt.

Folgte man dagegen der Auffassung einiger Justizministerien der Länder, könnten sich die Länderparlamente allenfalls über strafprozessuale Maßnahmen nach § 100c StPO auf Landesebene berichten lassen.

21.5 DNA-Identitätsfeststellungsgesetz

Mit dem DNA-Identitätsfeststellungsgesetz (DNA-IFG) vom 07.09.1998, in Kraft getreten am 11.09.1998, hat der Gesetzgeber die 1997 in die StPO aufgenommenen Bestimmungen der §§ 81e und 81f über die DNA-Analyse (molekulargenetische Untersuchung) ergänzt.

Während die genannten Vorschriften die DNA-Analyse nur in einem anhängigen Strafverfahren erlauben, wird mit dem DNA-IFG die DNA-Analyse ein Mittel zur **vorbeugenden** Verbrechensbekämpfung und ist auch zum Zweck der Identitätsfeststellung in **künftigen** Strafverfahren zulässig.

Voraussetzung ist, daß der Beschuldigte eine Straftat von erheblicher Bedeutung begangen hat, die Maßnahme erforderlich ist (z.B. keine Doppelung) und eine Wiederholungsgefahr (Negativprognose) besteht.

Auch bei bereits früher rechtskräftig verurteilten Personen können in entsprechenden Fällen molekulargenetische Untersuchungen durchgeführt werden. Gleiches gilt, wenn eine Verurteilung nur wegen erwiesener oder nicht auszuschließender Schuldunfähigkeit, auf Geisteskrankheit beruhender Verhandlungsunfähigkeit oder fehlender oder nicht ausschließbar fehlender Verantwortlichkeit (§ 3 JGG) nicht erfolgte und die entsprechende Eintragung im Bundeszentralregister oder im Erziehungsregister noch nicht getilgt ist.

§ 3 DNA-IFG schließlich erklärt die Speicherung der gewonnenen DNA-Identifizierungsmuster in einer beim BKA eingerichteten Verbunddatei für zulässig. Weiterhin wird in dieser Vorschrift auch die Verarbeitung und Nutzung mit weitgehenden Auskunftsmöglichkeiten erlaubt.

Der Landesbeauftragte erachtet es grundsätzlich als positiv, daß diese sog. Gen-Datei auf eine gesetzliche Grundlage gestellt wurde. Allerdings sind die derzeitigen gesetzlichen Regelungen in mehreren Punkten aus datenschutzrechtlicher Sicht unzulänglich.

Das Gesetz enthält keine Sicherungen, welche einwandfrei ausschließen, daß gespeicherte Informationen, die Rückschlüsse auf persönlichkeitsrelevante Eigenschaften zulassen, im Rahmen des Fortschritts der Genforschung nicht doch mißbräuchlich oder zweckändernd genutzt werden können.

Des weiteren bringt das DNA-IFG nicht klar genug zum Ausdruck, daß die molekulargenetische Untersuchung und Speicherung zum Zweck der vorbeugenden Verbrechensbekämpfung immer nur nach richterlicher Entscheidung erfolgen darf. Die freiwillige Zustimmung des Betroffenen zur Entnahme reicht nicht.

Auch wenn in einem vorhergegangenen Strafverfahren eine molekulargenetische Untersuchung nach §§ 81e, 81g StPO durchgeführt wurde, ist eine richterliche Prognoseentscheidung darüber einzuholen, ob aus Gründen der vorbeugenden Verbrechensbekämpfung ein DNA-Identifizierungsmuster gespeichert werden darf.

Weiterhin enthält das DNA-IFG mit § 3 keine datenschutzrechtlich ausreichende Lösung der Rechtsgrundlage für Speicherung, Nutzung und Verarbeitung der erhobenen Daten.

Zur Umsetzung des DNA-Feststellungsgesetzes werden derzeit in einigen Bundesländern Verwaltungsvorschriften erlassen. In Sachsen-Anhalt fehlt es bislang an einer solchen Regelung.

Der im März 1999 bekanntgewordene Gesetzentwurf der Fraktionen von SPD und Bündnis 90/DIE GRÜNEN zur Änderung des DNA-IFG im Deutschen Bundestag könnte diese Mängel ausräumen.

Die in diesem Entwurf enthaltenen weiteren Ergänzungsvorschläge zu Abfragen aus dem Bundeszentralregister und zur Verarbeitung der nach § 81e StPO gewonnenen Identifizierungsmuster bedürfen noch einer eingehenden rechtspolitischen Diskussion.

21.6 Aufbewahrungsbestimmungen im Bereich der Justiz

Der Forderung des Landesbeauftragten nach einer gesetzlichen Grundlage für die Aufbewahrung von Schriftgut, wie in den vergangenen drei Tätigkeitsberichten erörtert (I., S. 120, II., S. 111 und III., S. 93), wurde bislang nicht entsprochen.

Das Ministerium der Justiz vertritt auch weiterhin die Ansicht, daß eine gesetzliche Regelung für das Schriftgut der Gerichte und Staatsanwaltschaften nicht erforderlich ist. Auch die Landesregierung hat in ihrer Stellungnahme zum III. Tätigkeitsbericht eine gesetzliche Regelung abgelehnt.

Die 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 05./06. Oktober 1998 in einer einstimmigen Entschließung fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz, darunter auch zur Aufbewahrung von Akten, Karteien und sonstigen Unterlagen, sowie für die Dauer der Speicherung personenbezogener Daten(sammlungen) in automatisierten Dateien angemahnt **(Anlage 14).**

21.7 Öffentlichkeitsfahndung mit Mängeln

Im Süden des Landes drang ein Mann in ein Privathaus ein, tötete zwei Menschen und vergewaltigte zwei Frauen. Trotz der durchgestandenen qualvollen Stunden waren die Frauen in der Lage, eine relativ detaillierte Täterbeschreibung abzugeben. Staatsanwaltschaft und Polizei legten den beiden Opfern aufgrund eines Fahndungshinweises des Bundesgrenzschutzes im Rahmen einer Wahllichtbildvorlage auch das Lichtbild eines entflohenen Strafgefangenen vor. Nachdem die Frauen meinten, ihren Peiniger erkannt zu haben, löste der Staatsanwalt, ohne einen Haftbefehl durch den erreichbaren Bereitschaftsrichter abzuwarten, eine breite Öffentlichkeitsfahndung aus.

24 Stunden später stand nach Abschluß der Tatortuntersuchung und Auswertung der ersten Spuren fest, daß der bundesweit in den Medien gesuchte Mann nicht als Täter in Frage kam, sondern ein weiterer, ebenfalls entwichener Straftäter. Die Falschfahndung wurde durch einen gravierenden Mangel im

bundesweiten INPOL-Fahndungssystem begünstigt. Der ermittelnden Polizeibehörde standen aufgrund eines Strukturfehlers bei diesem System Beschreibungen und Lichtbilder anderer Personen nicht als Vergleichsgrundlage zur Verfügung.

Unabhängig davon ist der Landesbeauftragte der Auffassung, daß die groß angelegte und mit schweren Rechtseingriffen verbundene Öffentlichkeitsfahndung nicht ohne die im Verfahren nach § 131 StPO notwendige Beteiligung eines Richters erfolgen durfte.

Entgegen der Auffassung des Ministeriums der Justiz und der zuständigen Staatsanwaltschaft ist die Regelung in den Richtlinien für das Straf- und Bußgeldverfahren (RiStBV), welche bei Gefahr in Verzug auch ohne Haftbefehl eine Öffentlichkeitsfahndung zuläßt, als einfache Verwaltungsvorschrift nicht die von der Verfassung geforderte Rechtsgrundlage für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 1 Abs. 2 i.V. mit Art. 2 Abs. 1 GG und Art. 6 Abs. 1 LVerf). Diese Voraussetzungen erfüllt nur eine gesetzliche Regelung. Dafür steht in der StPO z.Zt. nur § 131 zur Verfügung; dieser wurde vom Staatsanwalt ignoriert.

Wegen bestimmter Besonderheiten dieses Einzelfalls hat der Landesbeauftragte von einer förmlichen Beanstandung trotz des schwerwiegenden Rechtsmangels abgesehen.

Die rechtlichen Meinungsverschiedenheiten könnten sich für die Zukunft erledigen, weil der zuständige Bundesgesetzgeber im Entwurf des StVÄG 1999 (vgl. vorstehende Ziff. 21.2) vorgesehen hat, die Öffentlichkeitsfahndung auf eine (neue) spezielle gesetzliche Grundlage zu stellen.

21.8 Verdachtsanzeigen nach dem Geldwäschegesetz

In seinem III. Tätigkeitsbericht (S. 105 f) hat der Landesbeauftragte zur Problematik der registermäßigen Behandlung von Verdachtsanzeigen nach dem Geldwäschegesetz Ausführungen gemacht. Kernfrage war, ob Verdachtsanzeigen nach dem Geldwäschegesetz (GwG) wegen ihrer Besonderheiten grundsätzlich

wie normale Strafanzeigen in das Js-Register (eingehende Anzeigen, die sich gegen eine bestimmte Person richten) eingetragen werden sollen oder eine zunächst neutrale Form der (AR-)Registrierung erhalten sollen.

Die Landesregierung hat in ihrer Stellungnahme zum III. Tätigkeitsbericht die Auffassung vertreten, daß nach der im wesentlichen ländereinheitlichen Aktenordnung eingehende Schriftstücke und Vermerke über mündliche Mitteilungen das Aktenzeichen Js ohne Rücksicht auf das Vorhandensein eines Anfangsverdachtes im Sinne von § 152 Abs. 2 StPO erhalten. Nach Auffassung der Landesregierung bedeutet die Vergabe des Registerzeichens nicht, daß damit ein solcher Verdacht automatisch angenommen wird. Zahlreiche substanzlose Strafanzeigen, die nicht in ein strafrechtliches Ermittlungsverfahren münden, erhalten ebenso ein Js-Registerzeichen wie begründete Strafanzeigen.
Bei den Verdachtsanzeigen sieht die Landesregierung keine anders zu bewertende Situation. Insbesondere sieht sie keine Belastung des Betroffenen durch die Eintragung einer Verdachtsanzeige in das Js-Register.

Auf das im III. Tätigkeitsbericht angesprochene Schreiben des Landesbeauftragten vom 20.06.**1995** hat das Ministerium der Justiz mit Datum vom 26.07.**1998** geantwortet und zu den Bedenken des Landesbeauftragten klargestellt, daß GwG-Anzeigen in das zentrale staatsanwaltschaftliche Verfahrensregister nicht aufgenommen werden, wenn die Staatsanwaltschaft die Einleitung eines Ermittlungsverfahrens ablehnt, mithin ein Anfangstatverdacht verneint wird.
Der Landesbeauftragte hält dieses Verfahren für akzeptabel.

21.9 Länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Die Landesregierung hat in ihrer Stellungnahme zu den Ausführungen des Landesbeauftragten im III. Tätigkeitsbericht (S. 98 f) mitgeteilt, daß die Bedenken des Landesbeauftragten in die weiteren Beratungen eingeflossen und ihnen im beträchtlichen Maße Rechnung getragen worden sei, so bei der Zuordnungsproblematik und der verschlüsselten Übermittlung von Mitteilungen und Auskünften auf dem Leitungsweg.

Inzwischen hat das Ministerium der Justiz mit Stand 24.11.1998 die aktuellen organisatorisch-technischen Leitlinien übersandt. Leider ist unter Ziff. 3.2.6 der Leitlinien noch immer keine sichere Lösung für die telefonische Auskunftserteilung bzw. die Beantwortung per Telefax gefunden worden.

Die datenschutzrechtlichen Bedenken bleiben insoweit bestehen. Der Landesbeauftragte wird das Verfahren weiterhin kritisch begleiten.

21.10 Postbedienstete als Hilfsbeamte der Staatsanwaltschaft?

In seinem III. Tätigkeitsbericht (S. 104 f) hatte der Landesbeauftragte moniert, daß mit Inkrafttreten des Postneuordnungsgesetzes keine Grundlage mehr für die Bestellung von Mitarbeitern des Betriebssicherungsdienstes der nunmehr privatisierten Deutschen Post AG zu Hilfsbeamten der Staatsanwaltschaft besteht.

Dem Ministerium der Justiz war empfohlen worden, die notwendigen Änderungen der Verordnung über die Hilfsbeamten der Staatsanwaltschaft des Landes Sachsen-Anhalt vorzunehmen.

Das Ministerium der Justiz hat mitgeteilt, daß die Auffassung des Landesbeauftragten geteilt wird, und die Landesregierung hat in ihrer Stellungnahme zum III. Tätigkeitsbericht am 09. Dezember **1997** ausgeführt, daß der Empfehlung des Landesbeauftragten, die Verordnung über die Hilfsbeamten der Staatsanwaltschaft neuzufassen, entsprochen wird.

Geschehen ist aber seither nichts!

21.11 Übermittlung personenbezogener Daten aus Ermittlungsakten

Im Rahmen einer Petition wurde anhand der vorgelegten Unterlagen folgender Sachverhalt festgestellt:

Eine Staatsanwaltschaft beantragte im Zuge eines Ermittlungsverfahrens mit einem Sammelantrag für insgesamt 24 Beschuldigte, darunter dem späteren Petenten, beim zuständigen Amtsgericht Beschlüsse für die Entnahme von Speichelproben und deren molekular-genetische Untersuchung (DNA-Analyse).

Die Beschlüsse wurden antragsgemäß erlassen. Keiner der Betroffenen war der Spurenleger. Das Ermittlungsverfahren gegen den Petenten wurde deshalb eingestellt.

Der Petent fühlte sich aber zu Recht durch die Maßnahme als Unschuldiger betroffen und beauftragte ca. 7 Monate später einen Rechtsanwalt. Dieser bat unter Vorlage einer Vollmacht nach einer Akteneinsicht um eine Kopie des Antrags der Staatsanwaltschaft für den Beschluß gegen seinen Mandanten und erklärte, ein Fax sei für die Übersendung ausreichend.

Der zuständige Staatsanwalt verfügte daraufhin eine Ablichtung des Sammelantrages und dessen Übersendung per Telefax. Dabei wurden die umfangreichen personenbezogenen Daten der weiteren 23 im Antrag aufgeführten Beschuldigten mit übermittelt, obwohl sie seitens des aktenkundigen Rechtsanwalts weder angefordert noch für dessen Aufgabenwahrnehmung erforderlich waren.

Der Landesbeauftragte ist der Auffassung, daß die Übersendung des Antrags ohne die erforderliche Rechtsgrundlage und unter Verstoß gegen die Schutzvorschrift des § 6 DSG-LSA erfolgte.

Nach § 147 Abs. 1 StPO ist ein **Verteidiger** befugt, die Akten, die dem Gericht vorliegen oder diesem im Fall der Erhebung der Anklage vorzulegen wären, einzusehen sowie amtlich verwahrte Schriftstücke zu besichtigen. Es ist aber nach der eindeutigen Aktenlage klar, daß der Rechtsanwalt sich im Verfahren nicht als Verteidiger des Petenten legitimiert hat (warum auch, das Verfahren war längst eingestellt), sondern, ausweislich der ordnungsgemäßen Vollmacht, um als Rechtsanwalt Ansprüche auf Schadenersatz und Schmerzensgeld gegen die Polizei eines anderen Bundeslandes geltend zu machen. Damit entfiel § 147 Abs. 1 StPO als Rechtsgrundlage für die Datenübermittlung.

Auch wenn man dem Rechtsanwalt einen Verteidigerstatus zugestehen wollte, ist § 147 StPO keine schrankenlose Vorschrift zur Datenübermittlung. Die Norm und die darauf gestützten Rechtseingriffe in die Grundrechte der Betroffenen sind vielmehr anhand der Vorgaben des Bundesverfassungsgerichts zur Geeignetheit und Erforderlichkeit der zur Übermittlung vorgesehenen Daten verfassungskonform auszulegen und anzuwenden.

Die Vorschrift dient dem Zweck einer wirksamen Verteidigung. Dem Anspruch des Rechtsanwaltes des Petenten zur Ermöglichung einer wirksamen Verteidigung wäre mit der Übersendung des Beschlusses betreffend seines Mandanten

oder des Antrages der Staatsanwaltschaft unter Schwärzung der personenbezogenen Angaben zu weiteren Beschuldigten genüge getan gewesen. Erkenntnisse zu anderen Beschuldigten oder sonstigen Beteiligten können vom Anspruch auf wirksame Verteidigung nur dann erfaßt werden, wenn sich hieraus schuld- oder rechtsfolgenrelevante Umstände ergeben würden. Dies war hier unstreitig nicht der Fall. Der Petent sowie die weiteren 23 Personen standen in keinerlei persönlichen oder sachlichen Beziehungen zueinander, sondern waren völlig unabhängig voneinander vom staatsanwaltschaftlichen Ermittlungsverfahren erfaßt worden. Die Übersendung des Gesamtantrages mit einer Vielzahl von Drittdaten wäre damit auch im Rahmen des § 147 StPO unverhältnismäßig gewesen.

Der Landesbeauftragte weist seit Jahren darauf hin, daß Telefaxgeräte wegen ihrer vielen Fehlerquellen nur in Ausnahmefällen zur Übermittlung personenbezogener Daten eingesetzt werden dürfen (II. Tätigkeitsbericht, S. 91, III. Tätigkeitsbericht, S. 62 und Ziff. 13.2 dieses Tätigkeitsberichtes). Dann sind besondere Schutzvorkehrungen zu treffen.

Dies ergibt sich aus § 6 Abs. 1 Satz 1 und Abs. 2 Nr. 9 DSG-LSA i.V. mit den dazu ergangenen Verwaltungsvorschriften (MBl. 1993, 2485, und 1995, 388). Einen Spielraum gibt es nur bei der gebotenen Abwägung zwischen Arbeitsablaufverzögerungen und Kosten einerseits und der Sensibilität und Schutzwürdigkeit der personenbezogenen Daten andererseits.

Im vorliegenden Fall waren weder der Arbeitsaufwand noch der geringe Zeitverlust bei der vergleichsweise viel sicheren Briefversendung eine berücksichtigenswerte Größe. Besondere Eile bestand ebenfalls nicht. Der Anwalt hatte den Übermittlungsweg offen gelassen.

Der Landesbeauftragte hat diesen Fall angesichts der Schwere der Rechtseingriffe in die Grundrechte einer Vielzahl Betroffener förmlich beanstandet.

Das Ministerium der Justiz hat in wenig überzeugender Weise versucht, dem Rechtsanwalt den Status als Verteidiger zukommen zu lassen und die Übermittlung auch der Fremddaten verteidigt. Hinsichtlich der Benutzung von Telefaxgeräten hat es immerhin der betroffenen Staatsanwaltschaft künftig einen vorsichtigeren Umgang mit diesem Übermittlungsweg nahe gelegt.

21.12 Datenschutz beim Täter-Opfer-Ausgleich

Im III. Tätigkeitsbericht (S. 107) wurde bereits über die unter datenschutzrechtlichen Gesichtspunkten positive Durchführung des Täter-Opfer-Ausgleichs in Sachsen-Anhalt berichtet. Sie wird z.Zt. allein auf der Basis von Verwaltungsvorschriften erreicht.

Zwischenzeitlich liegt der Referentenentwurf eines (Bundes-)Gesetzes zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs vor.

Nach diesem Entwurf soll § 153a StPO um die Möglichkeit ergänzt werden, das Verfahren einzustellen, wenn der Täter sich ernsthaft bemüht, einen Ausgleich mit dem Verletzten zu erreichen. Der neu in die StPO einzufügende § 160a gibt in seinem ersten Absatz Staatsanwaltschaft und Gericht auf, in jedem Stadium des Verfahrens die Möglichkeiten eines Ausgleichs zwischen Beschuldigten und Verletzten zu prüfen und regelt in den folgenden beiden Absätzen die Übermittlung personenbezogener Daten an Stellen, die mit der Durchführung des Täter-Opfer-Ausgleichs befaßt werden, und die Zweckbindung bei der Verarbeitung der übermittelten Daten.

Zu diesem Gesetzentwurf ist aus datenschutzrechtlicher Sicht folgendes anzumerken:

- In § 160a Abs. 2 StPO-E sollte vor einer Datenübermittlung zumindest an nicht-öffentliche Stellen die Einwilligung des Beschuldigten und des Verletzten geregelt werden. Die vorherige Einwilligung ist nach Auffassung des Landesbeauftragten unter dem Gesichtspunkt, daß jeder Bürger wissen können muß, was wo wann zu welchem Zweck über ihn gespeichert ist, ein Beitrag zur Akzeptanz der Ausgleichsbemühungen bei den Betroffenen.

- Die Übermittlung sollte nur für Zwecke der Rechtspflege erfolgen.

- Es fehlen in § 160a StPO-E noch Regelungen zur Vernichtung der Unterlagen bei der beauftragten Stelle und zur aufsichtsbehördlichen Kontrolle nach dem Bundesdatenschutzgesetz in den Fällen, bei denen die mit dem Täter-Opfer-Ausgleich beauftragte Stelle dem nicht-öffentlichen Rechtsbereich angehört.

Der weitere Verlauf des Gesetzgebungsverfahrens bleibt abzuwarten.

21.13 Ein bissiger Hund - und seine Bewältigung durch die Staatsanwaltschaft

Aufgrund einer Eingabe hatte der Landesbeauftragte sich mit folgendem Sachverhalt zu befassen:

Ein Kind war von einem aus einem eingezäunten Grundstück gesprungenen Hund gebissen worden, und die Mutter erstattete Anzeige bei der Polizei. Diese kannte bereits den nicht ungefährlichen Hund und die Sorglosigkeit seiner "Halterfamilie" aus früheren Beschwerden. Befragungen und Vernehmungen von Zeugen ergaben unterschiedliche Angaben dazu, wer in dieser Familie eigentlich der rechtlich verantwortliche Hundehalter sein sollte. Ohne dies weiter aufzuklären, suchte sich der zuständige Amtsanwalt die Petentin in der Halterfamilie als Schuldige heraus und beantragte gegen diese zunächst einen Strafbefehl. Als die Petentin dagegen Einspruch mit der Begründung einlegte, sie sei für den Hund nicht verantwortlich, veranlaßte auch dies den Amtsanwalt nicht zur Sachaufklärung, sondern er firmierte den falschen Strafbefehl gegen die Petentin kurzerhand in eine Anklage vor dem Amtsgericht um. In der Hauptverhandlung ergab sich dann, daß nicht die Petentin, sondern ihr Sohn Halter des Hundes war. Die Petentin wurde freigesprochen.

Im Rahmen der Durchführung eines neuen Strafverfahrens gegen den Sohn der vermeintlichen Halterin wurden Ablichtungen aus deren Strafakte gefertigt, u.a. der Strafanzeige der Mutter des Geschädigten, der Zeugenvernehmung des Geschädigten, des Vermerks des Polizeireviers, des Strafbefehls gegen die Petentin sowie deren Einspruch, des Protokolls der Hauptverhandlung und des freisprechenden Urteils.

Keinen datenschutzrechtlichen Bedenken unterlag die dazu getroffene Verfügung der Staatsanwaltschaft, wonach Ablichtungen aus dem vorherigen Verfahren gegen die Petentin gefertigt und in das neue Verfahren gegen ihren Sohn übernommen wurden. Auch wenn in diesem Falle eine Zweckänderung der personenbezogenen Daten vorliegt, beruht diese auf gesetzlicher Grundlage und

war zulässig. Das der Petentin zustehende Zeugnisverweigerungsrecht (§ 52 Abs. 1 Nr. 3 StPO) wurde dadurch nicht berührt.

Allerdings hat die Staatsanwaltschaft nach Auffassung des Landesbeauftragten zum Nachteil der Petentin gegen die umfassende Sachaufklärungspflicht gem. §§ 160 Abs. 2, 161 StPO verstoßen. Danach ist es Amtspflicht der Staatsanwaltschaft, einen Sachverhalt umfassend zu erforschen. Dabei sind nicht nur zur Belastung, sondern auch zur Entlastung dienende Umstände zu ermitteln.

Die Vorschriften der §§ 160 Abs. 2, 161 StPO sind insoweit als bereichsspezifische Vorschriften über den Datenschutz zu qualifizieren, die der datenschutzrechtlichen Pflicht entsprechen, nur richtige personenbezogene Daten zu erheben und zu verarbeiten (§ 16 DSG-LSA). Jeder unbeteiligte Bürger hat von Verfassungs wegen einen Anspruch darauf, nicht leichtfertig, ohne genügenden Grund oder ohne Beachtung der zu seinem Persönlichkeitsschutz getroffenen gesetzlichen Regelungen in der Strafprozeßordnung mit einem Strafbefehlsantrag oder einer Anklage überzogen zu werden.

Da bereits durch Zeugenaussagen sowie die Aussage der Anzeigenerstatterin selbst unklar war, wer rechtlich die Verantwortung für den Hund trug, hätte allein die Tatsache, daß der Hund zu einem Grundstück gehörte, das von mehreren Familienmitgliedern bewohnt wurde, Anlaß geben müssen, den Halter oder die Halterin oder den Aufsichtspflichtigen sorgfältig zu ermitteln. Ermittelt wurde zu diesen Punkten schlicht nichts.

Der Landesbeauftragte sieht es nicht als seine Aufgabe an, im Rahmen des ihm obliegenden eigenständigen Kontrollauftrages (Art. 63 Abs. 1 LVerf) eine fachspezifische Wertung im Ermittlungsverfahren vorzunehmen. Wird aber eine Grundregel des Prozeßrechtes nicht ansatzweise beachtet und kommt es in der Folge zu einem schweren Eingriff in das Persönlichkeitsrecht, kann ein solcher Verstoß nicht übersehen werden.

Der Landesbeauftragte hat angesichts der besonderen Rechtspflichten einer Staatsanwaltschaft eine formelle Beanstandung für geboten gehalten.

Das Ministerium der Justiz hat die Beanstandung zurückgewiesen. Es hält die genannten Bestimmungen der StPO, insbesondere § 160 Abs. 2 StPO, nicht für vom Landesbeauftragten prüffähige Vorschriften über den Datenschutz. Des

weiteren hat das Ministerium angeführt, die Entscheidung der Staatsanwaltschaft sei unter einem anderen rechtlichen Gesichtspunkt (Unterlassungsdelikt) jedenfalls noch vertretbar.

21.14 Organisatorische und andere Mängel bei einem Amtsgericht

Wegen Büromängel bei der Bearbeitung einer Mahnsache in einem Amtsgericht hatte sich ein Petent an den Landesbeauftragten gewandt. Der Landesbeauftragte forderte daraufhin von dem Amtsgericht eine Stellungnahme zur Sach- und Rechtslage an.

Erstaunlich fiel die Antwort der zuständigen Rechtspflegerin aus, die "um die Nachweisung der Bevollmächtigung sowie um Überlassung einer Kopie des Gesetzes zu § 23 Abs. 1 DSG-LSA" bat, da "dies leider im Hause nicht vorliege".

Nun mag es ja noch sein, daß auch eine gut ausgebildete Rechtspflegerin Aufgaben und Funktion des Landesbeauftragten nicht kennt. Daß diese aber behauptet, in ihrem Gericht gäbe es kein Gesetz- und Verordnungsblatt, ist schon verwunderlich und im übrigen unglaubwürdig.

Dennoch wurde dem Amtsgericht der erbetene Gesetzestext zu § 23 DSG-LSA in Kopie übersandt und dabei auch darauf hingewiesen, daß sich die Auskunftspflicht gegenüber dem Landesbeauftragten unmittelbar aus dem Gesetz ergibt.

Die Merkwürdigkeiten aber gingen weiter. Der Landesbeauftragte wurde kurze Zeit später freundlich schriftlich daran erinnert, daß die Beantwortung des Schreibens der Rechtspflegerin noch ausstehe. Erst nach telefonischer Rücksprache und dem Hinweis, die Beantwortung sei längst erfolgt, fand man im Gericht das Antwortschreiben des Landesbeauftragten in dem entsprechenden Sachvorgang.

Der vom Landesbeauftragten auf diese Mängel hingewiesene Direktor des Gerichts war offensichtlich so erstaunt, daß er bis heute darauf keine Antwort fand.

21.15 Zusammenarbeit zwischen Justiz und Presse

Wie bereits im III. Tätigkeitsbericht (S. 102) berichtet, enthalten die Richtlinien für die Zusammenarbeit der Justiz mit der Presse vom 24.01.1997 trotz datenschutzrechtlicher Verbesserungen noch Mängel.

Der Landesbeauftragte hatte die als bedenklich verbleibenden Punkte gegenüber dem Ministerium der Justiz deshalb nochmals dargelegt.

Das Ministerium der Justiz hat dazu im Februar 1998 und Februar 1999 Stellung genommen.

Im Ergebnis bleibt für den Landesbeauftragten zur Berichterstattung festzuhalten, daß im Bereich der Datensicherheit (zu Ziff. 3.7 der AV) vermeidbare Risiken seitens der Justiz durch den z.Zt. nicht ausreichend sicheren Einsatz der Telefaxübermittlung zu den Medien verbleiben (§ 6 DSG-LSA).

Materiell-rechtlich lückenhaft bleibt der Schutz Betroffener vor Gericht, wenn dort bei der Informationsübermittlung personenbezogener Daten zwischen den Spruchkörpern und der Pressestelle die detaillierte Akteneinsicht nicht restriktiv gehandhabt wird. Vor allem aber bleibt rechtsbedenklich eine ungefragt offene Datenübermittlung an die Medien in "für die Öffentlichkeit bedeutsamen Fällen".

Zum einen ist für die Betroffenen eine solche Einstufung oft nicht erkennbar - und damit die rechtzeitige Ergreifung von Schutzmaßnahmen nicht möglich -, zum anderen liegt gerade dabei ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 6 Abs. 1 LVerf) durch die Presseverantwortlichen nahe, weil oft die gesetzlich vorgeschriebene Berücksichtigung privater schutzwürdiger Interessen (§ 4 Abs. 2 Satz 3 Landespressegesetz) nicht gesehen und beachtet wird.

Eine bereichsspezifische gesetzliche Regelung dieser Materie - wie in anderen Bundesländern - würde den verfassungsrechtlichen Anforderungen gerechter.

In diesem Zusammenhang sei noch einmal an die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995 zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien (Anlage 8 zum III. Tätigkeitsbericht) erinnert.

21.16 Erstellung eines Vermögensverzeichnisses im Betreuungsverfahren

Eine Petentin, die vom Vormundschaftsgericht für ihren Ehemann zur Betreuerin bestellt worden war, wollte vom Landesbeauftragten wissen, ob sie in einem Verzeichnis des Vermögens "detaillierte Angaben zu Sparguthaben, wertvollen Gegenständen, wie Porzellan, Silber u.a., Immobilien" machen müsse.

Tatsächlich hat gem. §§ 1908i i.V. mit 1802 Abs. 1 Satz 1 BGB der vom Vormundschaftsgericht bestellte Betreuer das Vermögen, das zum Zeitpunkt der Anordnung der Betreuung vorhanden ist oder später dem Betreuten zufällt, zu verzeichnen und das Verzeichnis, nachdem es mit der Versicherung der Richtigkeit und Vollständigkeit versehen worden ist, dem Vormundschaftsgericht einzureichen.

Das Vermögensverzeichnis bildet damit die Grundlage für die Vermögensverwaltung durch den Betreuer und die Aufsicht des Vormundschaftsgerichts. Es dient als Unterlage für Rechnungslegung und Schlußbericht und als Beweisstück bei einem eventl. Herausgabeanspruch des Betreuten.

Aus datenschutzrechtlicher Sicht bestehen nach alledem keine Bedenken gegen dieses Verzeichnis.

21.17 Abdrucke aus dem Schuldnerverzeichnis

Bereits in seinem II. Tätigkeitsbericht (S. 112 f) hat der Landesbeauftragte darauf hingewiesen, daß mit der Änderung der ZPO und der Einführung der SchuVVO detaillierte Regelungen über den Inhalt des Schuldnerverzeichnisses, die Aufbewahrungsmodalitäten und Löschfristen sowie das Bewilligungsverfahren zum Bezug von Abdrucken und Listen getroffen wurden.

Über die Bewilligung ist gem. § 6 Abs. 4 SchuVVO die für die datenschutzrechtliche Kontrolle über den Bezieher der Abdrucke **zuständige Stelle** zu informieren. In Sachsen-Anhalt sind dies für den **öffentlichen** Bereich der Landesbeauftragte für den Datenschutz und für den **nicht-öffentlichen** als Aufsichtsbehörden gem. § 38 BDSG die regional zuständigen Regierungspräsidien in Dessau, Halle und Magdeburg.

Trotz dieser eindeutigen Regelung erreichen den Landesbeauftragten von Amts- und Landgerichten immer wieder Mitteilungen über erteilte Bewilligungen aus dem nicht-öffentlichen Bereich (z.B. an Unternehmen).

Das ist um so verwunderlicher, als dem Präsidenten des OLG Naumburg auf seine Bitte hin bereits 1995 vom Landesbeauftragten eine Übersicht der Datenschutz- und Aufsichtsbehörden in Sachsen-Anhalt und den übrigen Bundesländern zur Verfügung gestellt wurde. Dieser hat sie auch den Amts- und Landgerichten zur Kenntnis gegeben.

Um zukünftig unnötigen Verwaltungsaufwand zu vermeiden, weist der Landesbeauftragte nochmals auf die Beachtung der gesetzlichen Zuständigkeiten hin. Dazu sollte diese Übersicht auch genutzt werden.

21.18 Datenschutz bei Notaren

Nach der Änderung der Notarordnung durch das Dritte Gesetz zur Änderung der Bundesnotarordnung und anderer Gesetze vom 31.08.1998 (siehe III. Tätigkeitsbericht S. 112 f) steht nunmehr die Neufassung der Dienstordnung für Notare auf der Tagesordnung des Gesetzgebers. Dazu liegt ein Diskussionsentwurf des Bundes vor, der derzeit auf Länderebene beraten wird.

Der Landesbeauftragte hat gegenüber dem Ministerium der Justiz eine erste Stellungnahme abgegeben.

Der elektronischen Datenverarbeitung wird im Entwurf der Dienstordnung nur eine Hilfsfunktion zugewiesen. Allerdings fehlen in der Vorschrift zur EDV-gestützten Sachbearbeitung in den Notariaten Konkretisierungen zur Löschung der in Personalcomputern gespeicherten Daten sowie Vorschriften über Zugangs- und Bearbeitungsrechte.

Zu begrüßen ist die im Entwurf der Dienstordnung (§ 5) vorgesehene Klarstellung, daß Notarinnen und Notare öffentliche Stellen im Sinne der Datenschutzgesetze der Länder sind und der Kontrolle der Datenschutzbeauftragten unterliegen. Darüber gab es in anderen Bundesländern wiederholt Streit.

Die weitere Entwicklung in diesem Bereich bleibt abzuwarten.

22. Schulen

22.1 Wahlen zum Landeselternrat und Landesschülerrat

Im letzten Tätigkeitsbericht (III., S. 121) hatte der Landesbeauftragte auf die Problematik der Veröffentlichung der privaten Anschriften des gewählten Landeselternrates hingewiesen. Das Kultusministerium hatte vorgesehen, den Umfang der bekanntzumachenden Daten in die ElternWO aufzunehmen.

Zwischenzeitlich ist eine eindeutige Regelung zur Veröffentlichung der personenbezogenen Daten des Landes**elternrates** getroffen worden (GVBl. LSA S. 819).

Dem Hinweis des Landesbeauftragten, gleichzeitig die Veröffentlichung der privaten Anschriften des gewählten Landes**schülerrates** zu regeln, ist das Kultusministerium ebenfalls gefolgt.

22.2 Schulentwicklungsplanung

Eine Verwaltungsgemeinschaft wandte sich an den Landesbeauftragten und wies darauf hin, daß eine Gemeinde auf Anweisung des Regierungspräsidiums personenbezogene Auskünfte von zukünftigen Schülerinnen und Schülern aus dem Melderegister angefordert hatte, um diese zum Zwecke der Schulentwicklungsplanung zu übermitteln.

Hierzu hat der Landesbeauftragte ausgeführt, daß für die Gemeinde keine Rechtsverpflichtung bestand, sich die geforderten personenbezogenen Daten bei der Meldebehörde zu besorgen, um sie an das Regierungspräsidium zu übermitteln. Nach §§ 84a Abs.1 i.V. mit 22 SchulG können statistische Erhebungen für Zwecke der Schulverwaltung und der Schulaufsicht durchgeführt werden. Die Vorschriften enthalten aber weder die für die Anweisung des Regierungspräsidiums erforderliche Erhebungsgrundlage für die personenbezogenen Daten künftiger Schülerinnen und Schüler noch eine Rechtsgrundlage zur Übermittlung dieser Daten durch die Gemeinde. Statistisch aufbereitetes Material (nach Geburtsjahrgang, Wohnort mit Ortsteil und Straße) reicht in allen Fällen aus.

Aus diesen Gründen scheidet auch die Übermittlung personenbezogener Daten zur Schulentwicklungsplanung an eine Schulbehörde aus.

Da bereits personenbezogene Daten ohne Rechtsgrundlage übermittelt und gespeichert worden waren, waren diese gem. § 16 Abs. 2 Nr. 1 DSG-LSA zu löschen.

22.3 Antrag auf Schulwechsel

Eine Familie beschwerte sich beim Landesbeauftragten über die "falsche" Bearbeitung des Antrages auf Schulwechsel für ihr Kind. Das für die Entscheidung zuständige Staatliche Schulamt hatte den Antrag ohne Begründung abgelehnt und die ablehnende Entscheidung mit dem Antrag der Eltern der bisherigen und auch künftigen Schule des Schülers zugeleitet.

Da der Antrag der Eltern eine Fülle sehr sensibler familieninterner Informationen enthielt, war nach datenschutzrechtlichen Vorschriften zu prüfen, ob die Übersendung des an das Staatliche Schulamt gerichteten Elternantrages an die Schule rechtlich zulässig war.

Nach § 84a Abs. 3 SchulG dürfen Schulbehörden und Schulträger personenbezogene Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten u.a. verarbeiten (hierzu zählt auch die Übermittlung des Antrages), soweit dies zur Erfüllung des Erziehungs- und Bildungsauftrages und der Fürsorgeaufgaben erforderlich ist.

Das Staatliche Schulamt begründete seine Entscheidung gegenüber dem Landesbeauftragten damit, daß aufgrund der von den Eltern vorgetragenen Fakten und Befürchtungen die Schule durch die Kenntnis des Elternantrages auf den erhöhten Zuwendungsbedarf des Schülers aufmerksam gemacht werden sollte. Die Datenübermittlung war daher nach dem Gesetz unbedenklich.

Bei dieser Gelegenheit hat der Landesbeauftragte das Staatliche Schulamt aber darauf hingewiesen, daß das Verfahren gegenüber den Eltern aus verwaltungsverfahrensrechtlichen Gründen geändert werden mußte. Bereits die unzulässige Adressierung des ablehnenden Bescheides an die "Familie" hatte zu einem fehlerhaften Verwaltungsakt geführt. Auch wäre nach § 39 Abs. 1 VwVfG LSA

eine Begründung mit den wesentlichen tatsächlichen und rechtlichen Gründen, die zur Ablehnung des Antrages und die Übersendung des Antrages an die Schule geführt haben, mit aufzuführen gewesen.

Das Schulamt folgte der Empfehlung und änderte seinen Bescheid.

23. Sozialwesen

23.1 Probleme mit Jugendlichen

In einer kleineren Gemeinde schlug ein Jugendlicher derart über die Stränge, daß sich die Bürgermeisterin genötigt sah, tätig zu werden.

Sie lud dabei mit einem an "verantwortungsvolle Bürger der Gemeinde" gerichteten Rundschreiben zu einem offenen Gespräch ein, um zu beraten, wie mit dem unter voller Namensnennung bezeichneten Jugendlichen und seinen Eltern in Zukunft "sachlich zu befinden" sei. Gleichzeitig wurde in der Einladung angemerkt: "Jedem ist die Möglichkeit zu verbaler Anklage- und Verteidigungsäußerung gegeben."

Der Landesbeauftragte wies die Gemeinde darauf hin, daß für die Angabe des Vornamens und des Namens des Jugendlichen, die Hinweise auf seine Eltern und die von ihm gezeigten möglicherweise sozialschädlichen Verhaltensweisen weder die erforderliche gesetzliche Befugnis für die Offenbarung noch die Einwilligung der Betroffenen vorlag. Folglich wurden diese personenbezogenen Daten durch die Bürgermeisterin in rechtlich unzulässiger Weise an Dritte übermittelt.

Weiterhin mußte festgestellt werden, daß die mit dem Rundschreiben ins Auge gefaßten Maßnahmen nach den Bestimmungen des Sozialgesetzbuches nicht einmal in den Zuständigkeitsbereich der Gemeinde, sondern den des Landkreises fielen.

Der Landesbeauftragte hat deshalb nicht nur die betroffene Gemeinde zur sofortigen Einstellung der Briefversendung und deren Rückabwicklung aufgefordert, sondern auch die Kommunalaufsicht gebeten, die Veranstaltung mit den ihr zur Verfügung stehenden Mitteln zu untersagen. Dies geschah auch.

Der Gemeinde bleibt es unbenommen, eine allgemeine Veranstaltung(sreihe) zum Problembereich der Jugendgewalt und des Vandalismus durchzuführen. Allerdings müßte die Leiterin der Veranstaltung dann ihr besonderes Augenmerk auf die Persönlichkeitsrechte der betroffenen Personen richten.

Auch ein auf freiwilliger Basis geführtes Gespräch zwischen der Bürgermeisterin, den Eltern und dem Jugendlichen, um die aufgelaufenen Probleme zu erörtern und zu beseitigen, wäre rechtlich unbedenklich.

23.2 Ermäßigungs-/Erlaßanträge zu Kindertagesstätten

Im III. Tätigkeitsbericht (S. 123 f) hatte der Landesbeauftragte ausführlich auf die Bestimmungen des KiBeG hingewiesen und Ausführungen zur datenschutzgerechten Bearbeitung von Erlaß- und Ermäßigungsanträgen gemacht.

Trotzdem zeigte sich auch im Berichtszeitraum, daß weiterhin bei nicht wenigen Behörden noch Unsicherheiten bei der Anwendung der Bestimmungen des KiBeG vorhanden waren.

Dadurch, daß die Bestimmungen des BSHG zur Berechnung heranzuziehen sind, gerieten die Sachbearbeiter immer wieder in die "Bearbeitung von Sozialhilfefällen". Demzufolge wurden Bestimmungen des BSHG zugrunde gelegt, die durch das KiBeG ausdrücklich ausgeschlossen sind. So wurden weiterhin Lebenspartner aus eheähnlichen Gemeinschaften bei der Berechnung mit herangezogen (§ 122 BSHG), obwohl das KiBeG ausdrücklich die Heranziehung von Eltern vorsieht. Festgestellt wurde auch, daß Unsicherheiten bei der Bescheiderstellung vorhanden waren.

Zwischenzeitlich konnte der Landesbeauftragte durch viele Einzelberatungen diesen Problembereich jedenfalls aus datenschutzrechtlicher Sicht abschließen.

23.3 Aufweichung des Sozialgeheimnisses

Zunächst unbemerkt von der Öffentlichkeit und den Fachleuten hat der Bundestag 1998 im Zusammenhang mit der Änderung des Medizinproduktegesetzes (Erstes MPGÄndG) auch § 68 SGB X geändert.

Die Änderung dieser Bestimmung soll es den Sozialbehörden erlauben, weit über den bisher zulässigen Umfang hinaus, der Polizei gegenüber Angaben über Klienten zu machen, insbesondere ob und wann sie sich in den Räumen eines Sozialleistungsträgers aufhalten. Dabei betrifft § 68 SGB X nur Fälle, in denen die Polizei Personen **ohne** den Zusammenhang mit Sozialleistungen sucht. Bei Verstößen gegen Sozialgesetze - etwa Sozialhilfebetrug - ist die Information der Polizei seit jeher nach § 69 SGB X unproblematisch.

Die Gesetzesänderung hat ein starkes Presseecho ausgelöst. Der Landesbeauftragte und die überwiegende Zahl seiner Kolleginnen und Kollegen haben in einer Presseerklärung scharfe Kritik an den Regelungen geäußert.

Das Gesetz ist jetzt soweit gefaßt, daß jedwede Abwägung bei der polizeilichen Aufgabenerfüllung fehlt und **alle** Sozialleistungsträger (Rentenversicherungsträger wie auch die Jugendbehörden) davon erfaßt sind. Diese tiefgreifende Änderung des sozialen Datenschutzes stört künftig das besonders sensible Vertrauensverhältnis Klient/Sozialarbeiter bzw. Sozialleistungsträger und konterkariert so auch den Sinn des Sozialdatenschutzes.

Allerdings obliegt die Mitteilung der freien Entscheidung der Sozialbehörde im Einzelfall - bei schutzwürdigen Belangen des Betroffenen kann die Behörde von einer Auskunftserteilung absehen.

23.4 Ein Antrag auf Wohnberechtigung und die Sammelwut einer Behörde

Eine Petentin berichtete dem Landesbeauftragten, ihre Familie habe beim Wohnungsamt einen Antrag auf Erteilung einer Bescheinigung über die Wohnberechtigung nach § 10 Belegungsbindungsgesetz (Wohnberechtigungsschein) gestellt. Der Antrag sei mit der Begründung abgelehnt worden, das Gesamteinkommen der Familie der Petentin übersteige die sich aus dem Zweiten Wohnungsbaugesetz ergebenden Einkommensgrenzen.

Die Familie akzeptierte diese Entscheidung, forderte aber vom Wohnungsamt ihre mit dem Antrag eingereichten Unterlagen, u.a. die Einkommensnachweise, zurück. Dies wurde mit wechselnden Gründen verwehrt.

Die datenschutzrechtliche Prüfung ergab, daß die Zurückbehaltung der nicht mehr erforderlichen Belege unzulässig war, weil es dafür keine gesetzliche Grundlage gab.

Die Aufbewahrungspflicht nach dem Haushaltsrecht als sog. leistungsbegründende Unterlagen entfiel, da die beantragte Leistung ja abgelehnt worden war. Die Zurückhaltung der Belege wäre danach lediglich noch solange erforderlich gewesen, bis die für eine Anfechtung gesetzlich vorgeschriebene Rechtsbehelfsfrist abgelaufen war. Die Familie hatte jedoch keinen Rechtsbehelf eingelegt. Die Unterlagen waren auch für zukünftige Anträge nicht mehr erforderlich.

Zu prüfen blieb letztlich, ob die Unterlagen z.B. für den Fall einer Geschäftsprüfung zurückbehalten werden mußten.

Richtig ist, daß alle - also auch negative - Entscheidungen der Leistungsverwaltung durch die zuständigen Stellen nachprüfbar sein müssen. Deshalb sind die Entscheidungsgründe nachvollziehbar zu dokumentieren. Dafür reicht es aber aus, im Sachvorgang zu vermerken, daß eine bestimmte (Original-)Unterlage, z.B. ein Steuerbescheid, vorlag, aus der entnommen wurde, daß eine durch ein Leistungsgesetz vorgeschriebene Einkommensgrenze überschritten worden war und deshalb die Leistung verwehrt wurde.

Folglich waren die Unterlagen für die Aufgabenerfüllung des Wohnungsamtes als speichernde Stelle nach § 10 Abs. 1 DSG-LSA nicht mehr erforderlich und, da spezialgesetzliche Aufbewahrungsfristen nicht existieren, zurückzugeben oder datenschutzgerecht zu vernichten.

Dies gefiel dem Wohnungsamt nicht. Erst mit Hilfe des Regierungspräsidiums und des Fachministeriums konnte das Wohnungsamt schließlich zum Einlenken und zur Rückgabe der Unterlagen gebracht werden. Für zukünftige Fälle vergleichbarer Art traf das Regierungspräsidium eine entsprechende Regelung.

23.5 Anforderung von Krankenhausentlassungsberichten

Wiederholte Anfragen von Krankenhäusern veranlaßten den Landesbeauftragten darauf hinzuweisen, daß die pauschale Anforderung von Krankenhausentlassungsberichten durch Krankenkassen nicht zulässig ist.

Sofern unklare Abrechnungsfälle es (im Einzelfall!) erfordern, hat die Krankenkasse den MDK mit der gutachtlichen Prüfung zu beauftragen bzw. Stellungnahmen anzufordern (§ 275 SGB V). In diesem Fall sind die Leistungserbringer

(= Krankenhäuser) entsprechend § 276 Abs. 2 SGB V verpflichtet, die erforderlichen Sozialdaten unmittelbar an den MDK zu übermitteln.

Vom Gesetzgeber ist aus gutem Grund nicht gewollt, daß ärztliche Befunde generell in den Besitz der Krankenversicherung gelangen. Diese Absicht bekräftigt § 277 Abs. 1 SGB V. Danach hat der MDK dem betroffenen Leistungserbringer und der Krankenkasse **das Ergebnis** der Begutachtung **und** der Krankenkasse **die erforderlichen Angaben über den Befund** mitzuteilen.

Da der Gesetzgeber das Verfahren abschließend im SGB V geregelt hat, ist in diesen Fällen auch die Anforderung einer Einwilligungserklärung vom Versicherten durch die Krankenkasse bzw. die Forderung auf Entbindung des behandelnden Arztes von der Schweigepflicht unzulässig.
Eine Übermittlung personenbezogener medizinischer Daten über den vorgenannten Rahmen hinaus verletzt die ärztliche Schweigepflicht und ist strafbewehrt.

23.6 Werbemaßnahmen der Krankenkassen

Bereits im III. Tätigkeitsbericht (S. 129) wies der Landesbeauftragte auf problematische Werbemaßnahmen der gesetzlichen Krankenkassen hin.
Im Zuge des immer härter werdenden Wettbewerbs bemühen sich einzelne Kassen verstärkt darum, verlorengegangene Versicherte zurückzugewinnen.
Dabei werden auch ehemalige Versicherte angeschrieben und aufgefordert, den Versicherungswechsel zu überdenken. Immer wieder kommt es dann zu Beschwerden der Versicherten, die eine mißbräuchliche Verwendung ihrer Daten vermuten.
Die Überprüfungen des Landesbeauftragten haben dies so generell nicht bestätigt.

Nach § 304 SGB V sind die personenbezogenen Daten über Leistungsvoraussetzungen bei den Krankenkassen erst nach zehn und alle übrigen personenbezogenen Daten nach zwei Jahren zu löschen. Damit sind die Krankenkassen durchaus berechtigt, noch über einen längeren Zeitraum im Besitz der personenbezogenen Daten zu sein.

Wenn ein ehemaliger Versicherter Wert darauf legt, daß er von seiner früheren Versicherung keine Werbematerialien erhält, so muß er von seinem Recht der Sperrung seiner personenbezogenen Daten bei der jeweiligen Krankenversicherung Gebrauch machen.

23.7 Übermittlung von Patientendaten zwischen Krankenhaus und gesetzlicher Krankenversicherung

In der letzten Zeit häufen sich Anfragen der Krankenhäuser beim Landesbeauftragten, demzufolge gesetzliche Krankenkassen medizinische Daten ihrer Patienten von den Krankenhäusern abfordern. Oft ist die Aufforderung mit dem "zarten" Hinweis verknüpft, daß die Zahlungen an das Krankenhaus zurückgestellt werden, bis die gewünschten Daten vorliegen.

Aus datenschutzrechtlicher Sicht ist dazu folgendes zu bemerken:

Nach § 67b Abs. 1 SGB X sind die Verarbeitung von Sozialdaten und deren Nutzung nur zulässig, soweit die nachfolgenden Vorschriften oder eine andere Rechtsvorschrift in diesem Gesetzbuch es erlauben oder anordnen oder soweit der Betroffene eingewilligt hat.

Dieses Verbot der Datenverarbeitung mit Ausnahmevorbehalt gilt für alle Leistungsträger. Für die Anforderung der Patientendaten durch die Krankenversicherung muß also eine gesetzliche Befugnis ebenso vorhanden sein, wie für die Übermittlung dieser Daten durch die Krankenhäuser.

Die Erhebungsbefugnis für die Krankenversicherung ist in § 284 SGB V und die Übermittlungsbefugnis der Krankenhäuser in § 301 SGB V abschließend geregelt. Mehr personenbezogene Daten als dort bezeichnet dürfen weder von der Krankenversicherung erhoben noch von den Krankenhäusern übermittelt werden. In diesem Zusammenhang ist auf einen entsprechenden Beschluß des Landessozialgerichts Rheinland-Pfalz vom 11.09.1995 hinzuweisen.

Die mehr oder weniger zarte Verknüpfung mit der Zahlungsbereitschaft der Kasse ist rechtlich bedenklich.

23.8 Fehlbelegungsprüfungen in Krankenhäusern

Verschiedene Krankenhäuser und auch ein Petent wandten sich an den Landesbeauftragten und baten um Beurteilung, ob die Prüfung der Krankenakten in den Krankenhäusern durch den MDK über die in § 275 SGB V ff. genannten Aufgaben hinaus zulässig sei.

Hintergrund für die Anfragen war eine verstärkte Prüftätigkeit des MDK nach der Neufassung des Krankenhausfinanzierungsgesetzes (KHG). Mit § 17a KHG ist eine Aufgabenzuweisung eingeführt worden, die es den Krankenkassen gestattet darauf hinzuwirken, daß unter Zuhilfenahme des MDK Fehlbelegungen vermieden und bestehende Fehlbelegungen zügig abgebaut werden.
Zu diesem Zweck darf der MDK Einsicht in die Krankenunterlagen nehmen. Der Krankenkasse sind das Ergebnis der Begutachtung und ggf. die erforderlichen Angaben über den Befund mitzuteilen.

Leider ist die Einordnung dieser Regelung in das Gesetz mißlungen und hinsichtlich ihrer rechtlichen Bedeutung unklar, insbesondere, ob sie Eingriffe in die Persönlichkeitsrechte der Patienten zuläßt.
Bei der derzeitigen Umsetzung der Regelung in die tägliche Praxis ist aus datenschutzrechtlicher Sicht zu beachten, daß nach dem Wortlaut der Vorschrift eine "gezielte" Einschaltung des MDK erfolgen muß. Dies schließt eine flächendeckende allgemeine Prüfung (Ausforschungsprüfung) aus. Es muß ein inhaltlicher wie zeitlicher Zusammenhang zwischen der von den Kassen in einem Krankenhaus - eher wohl in einer Fachabteilung - festgestellten Auffälligkeit und der dort durchgeführten Prüfung gegeben sein. Auch müssen Umfang und Art und Weise der Prüfung vorher festgelegt sein (z.B. im Prüfauftrag).

Die 8. Kammer des Verwaltungsgerichts Aachen hat in ihrem Beschluß vom 29.01.1998 diese bereits 1997 vom Landesbeauftragten vertretene Rechtsauffassung bestätigt.

23.9 Einsichtnahme in Unterlagen der ehemaligen Krankenversicherung

Ein Petent wollte zur gerichtlichen Durchsetzung seiner Ansprüche Einsicht in die Unterlagen seiner ehemaligen gesetzlichen Krankenkasse nehmen. Diese wurde ihm unter Hinweis auf datenschutzrechtliche Bestimmungen vorenthalten. Man schickte ihm lediglich ein paar Kopien. Den Mitarbeitern der Krankenkasse mußte erst klargemacht werden, daß nach § 25 SGB X dem Betroffenen grundsätzlich Akteneinsicht zu gewähren ist. Dabei ist das Akteneinsichtsrecht nicht beschränkt auf Unterlagen - wie in diesem Fall - die nach Ansicht der öffentlichen Stelle für die Durchsetzung der Ansprüche des Betroffenen erforderlich sind. Welche Unterlagen dafür benötigt werden, entscheidet ausschließlich der Betroffene selbst.

Bei der anschließend durchgeführten Beratung stellte sich heraus, daß die gesetzliche Krankenkasse nervenfachärztliche Stellungnahmen zur Vorlage beim MDK angefordert hatte. Bevor die Unterlagen aber an den MDK weitergeleitet wurden, fertigte man noch schnell Kopien davon und nahm sie zur Leistungsakte.

Diese unzulässige, aber offensichtlich weit verbreitete Praxis führte zu einer gemeinsamen Erörterung zwischen Ärztekammer, MDK, Krankenkasse und dem Landesbeauftragten mit dem Ergebnis, daß künftig zur Vermeidung solcher Mißbräuche die erforderlichen Unterlagen von dem behandelnden Arzt direkt an den MDK adressiert werden.

Die Krankenkasse hat nach Intervention des Landesbeauftragten die ohne Rechtsgrundlage erhobenen Daten entsprechend § 84 Abs. 2 SGB X gelöscht und im übrigen dem Petenten Akteneinsicht ohne Einschränkungen gewährt.

23.10 Entbindung von der ärztlichen Schweigepflicht in der Pflegeversicherung

Eine Pflegeeinrichtung beschwerte sich beim Landesbeauftragten darüber, daß eine Mitarbeiterin des MDK Einblick in medizinische Unterlagen ohne die erforderliche Einwilligung des Betreuers nehmen würde. Da nach Angaben der Einrichtung das kein Einzelfall sei, wurde beim MDK eine Prüfung durchgeführt. Diese ergab keine datenschutzrechtlichen Mängel.

Zu den Aufgaben des MDK gehört es, den Versicherten nach § 18 SGB XI zu untersuchen und eine Stellungnahme über das Ergebnis der Untersuchung der Pflegeversicherung gegenüber abzugeben. Der MDK hat den Pflegebedürftigen in seinem Wohnbereich zu untersuchen und soll - selbstverständlich mit Einwilligung des Pflegebedürftigen - die behandelnden Ärzte in die Begutachtung einbeziehen.

Was die Einrichtung nicht bedachte war, daß der MDK nur im Auftrag der Pflegeversicherung tätig wird und in dem Antrag auf Leistungen nach der Pflegeversicherung die Einwilligungserklärung des Versicherten enthalten ist. So auch in diesem Fall. Pikanterweise hatte die Pflegeeinrichtung ausweislich der vorliegenden Unterlagen von der Einwilligungserklärung Kenntnis.

23.11 "Datenabgleich" zwischen zwei Sozialleistungsträgern

Ein Petent beschwerte sich gleichzeitig beim Bundesbeauftragten für den Datenschutz und beim Landesbeauftragten darüber, daß das Jugendamt sich mit dem Arbeitsamt in Verbindung gesetzt und seine Daten (nach seiner Ansicht unzulässig) ausgetauscht hätte.

Tatsächlich hatte das Jugendamt das Arbeitsamt um Auskunft gebeten, ob der Petent Unterhaltsleistung oder Arbeitslosenhilfe erhalte.

Die Mitarbeiter des Jugendamtes sahen den Petenten fast täglich in einem direkt neben dem Jugendamt befindlichen Gebäude, wo die Arbeitsverwaltung Umschulungsmaßnahmen durchführte. Deshalb keimte schnell der Verdacht auf, daß die Angaben des Petenten beim Jugendamt nicht richtig sein konnten. Als "Umschüler" erhält er nämlich keine Arbeitslosenhilfe, sondern (die höheren) Unterhaltsleistungen.

Da hier ein begründeter Verdacht bestand, daß die Angaben des Petenten zur Leistungserlangung nicht der Realität entsprachen, durfte das Jugendamt das Arbeitsamt unter Hinweis auf § 74 SGB X um Auskunft ersuchen.

Die für den Petenten unerfreuliche Rechtsfolge war, daß seine Unterhaltsleistungen den tatsächlichen Einkommensverhältnissen angepaßt wurden.

24. Statistik

24.1 Volks- und Wohnungszählung 2001

Die Europäische Gemeinschaft beabsichtigt, im Jahre 2001 in den Mitgliedsländern eine Volks- und Wohnungszählung (Zensus 2001) durchführen zu lassen. Die frühere Absicht, dies aufgrund einer Verordnung durchzuführen, wurde fallengelassen. Um den Mitgliedsstaaten mehr Freiheiten zu gewähren, wurden statt dessen 1997 unverbindliche EU-Leitlinien für das Programm erarbeitet.

Diese lassen für die nationalen Behörden auch zu, daß die Vollerhebung ganz oder teilweise durch die Nutzung und Verknüpfung von Verwaltungsregistern oder anderen Verwaltungsquellen ersetzt werden kann. Das kommt den Intentionen der Bundesregierung nach einer weitestmöglichen Kostenreduzierung bei der Zählung sehr entgegen.

Die wichtigsten dieser sogenannten Verwaltungsregister sind neben denen der Bundesversicherungsanstalt für Angestellte und anderer Behörden und Gebietskörperschaften die Melderegister, die jedoch eine für die Statistiken nicht akzeptable Fehlerquote von schätzungsweise ein bis sechs Prozent besitzen. Auch aus diesem Grunde laufen bereits seit Jahren Bestrebungen, die Melderegister zu konditionieren.

Dazu hat der Landesbeauftragte bereits frühzeitig auf das verfassungsrechtliche Gebot der Trennung von Verwaltung und Statistik hingewiesen. Den gleichen erheblichen Bedenken begegnet die Forderung von seiten der Statistik, die Melderegister um weitere für die Zwecke des Zensus 2001 bestimmte Daten, wie z.B. Angaben zur Haushaltszugehörigkeit, dem höchsten Schulbildungsabschluß und dem Pendlerverhalten zu Erwerbszwecken zu erweitern.

Im Verfahren der Entwicklung eines nationalen Konzeptes zur Umsetzung der Leitlinien wurde eine Arbeitsgruppe "Gemeinschaftsweiter Zensus 2001" aus Vertretern des Bundes und der Statistischen Ämter der Länder gebildet. Dabei wurden, ausgerichtet am entsprechend unterschiedlichen Datenbedarf auf Basis der Kernvariablen der EU-Leitlinien, ein Bundes- und ein Ländermodell entwickelt und 1998 durch die o.g. Arbeitsgruppe in einem Bericht dargestellt.

Zu diesem Bericht, der ihm durch das Ministerium des Innern vorgelegt worden war, nahm der Landesbeauftragte ausführlich Stellung.

Tenor der Stellungnahme war, daß

- es zur Umsetzung des Zensus 2001 und der Verwirklichung der erweiterten nationalen Ziele einer Art Volkszählungsgesetz bedarf,
- dieses Gesetz gleichermaßen klar für die rechtsanwendende Verwaltung wie für betroffene Bürgerinnen und Bürger erkennen lassen muß, welche Daten aus welchen Registern entnommen, wo sie wie verknüpft, wann sie gelöscht, wie sie weitergegeben bzw. übermittelt werden und wo welche Daten in Registern schließlich zu anderen Zwecken zurückbleiben und
- es keinesfalls hinnehmbar ist, wenn zu Zwecken der "einfacheren Verknüpfung" der Datenbestände ein individuelles Merkmal nach Art der hinlänglich bekannten Personenkennzahl eingeführt wird.

Das Ministerium des Innern sicherte zu, die Anregungen des Landesbeauftragten bei der Diskussion des zu erwartenden Volkszählungsgesetz-Entwurfes zu berücksichtigen und zu vertreten.

24.2 Ausländereigenschaft kein Erhebungsmerkmal der Einkommens- und Verbrauchsstichprobe (EVS) 1998

In der nach dem Gesetz über die Statistiken der Wirtschaftsrechnungen privater Haushalte zu erhebenden repräsentativen EVS sind auch die "sozialen Verhältnisse" der aus "allen Bevölkerungskreisen" ausgewählten Haushalte zu erfragen. Der Begriff "soziale Verhältnisse" ist im Gesetz nicht näher beschrieben.

Der Landesbeauftragte stellte fest, daß, ebenso wie in anderen Bundesländern, auch das SLA Sachsen-Anhalt den Begriff unzulässig ausgedehnt hat und bei den Befragten auch das Merkmal der Ausländereigenschaft erhob. Das, so das SLA, sei aus fachlicher Sicht unverzichtbar.

Dennoch mußte der Landesbeauftragte dem SLA mitteilen, daß der im § 2 des o.g. Gesetzes enthaltene Erhebungsmerkmalskatalog abschließend und nicht beliebig erweiterbar ist. Der Status der Ausländereigenschaft jedenfalls ist nicht Bestandteil der dort genannten sozialen Verhältnisse. Auch der Hinweis des SLA auf die Freiwilligkeit der Teilnahme der Haushalte an der Erhebung ging

fehl, da in § 15 Abs. 1 des Bundesstatistikgesetzes vorgeschrieben ist, daß die die Statistik anordnende Rechtsvorschrift festzulegen hat, in welchem Umfang (Erhebungsmerkmalskatalog) die Erhebung mit oder ohne Auskunftspflicht erfolgen soll.

Der Landesbeauftragte argumentierte letztlich auch, daß es dem Bundesgesetzgeber frei stand, daß seit 1961 existierende Gesetz zu ändern und den Merkmalskatalog entsprechend zu erweitern, wenn die Ausländereigenschaft wirklich unverzichtbar war. Als Beispiel, daß die Ausländereigenschaft legitimes Erhebungsmerkmal sein kann, nannte der Landesbeauftragte das Mikrozensusgesetz.

Das SLA verzichtet nunmehr auf die Verwendung der Ausländereigenschaft als Erhebungsmerkmal. Bereits gewonnene Daten werden nicht veröffentlicht.

24.3 Mikrozensus

Jahr für Jahr werden auch in Sachsen-Anhalt Bürgerinnen und Bürger, d.h. eigentlich deren Haushalte, neu für die Teilnahme am Mikrozensus ausgewählt. Nicht selten führt dies angesichts des erheblichen Umfangs des Fragenkatalogs zu Irritationen unter den Betroffenen, obwohl das SLA seine Interviewer nunmehr schon lange beauftragt hat, sich einige Tage vor dem Interview schriftlich anzumelden und gleichzeitig ein förmliches Anschreiben und eine "Kurzinformation für die Befragten" beizulegen. Außerdem wird die Befragung regelmäßig in der Presse angekündigt.

Der Landesbeauftragte hatte gleichwohl viele Fragen der Bürgerinnen und Bürger in bezug auf die Zulässigkeit, die gesetzlichen Hintergründe der Befragung und die weitere Verwendung vor allem der Hilfsmerkmale zu beantworten.

Die Tätigkeit des SLA war dabei aus datenschutzrechtlicher Sicht in keinem Fall zu beanstanden.

25. Strafvollzug

25.1 Gesetz zur Änderung des Strafvollzugsgesetzes

Das 4. Gesetz zur Änderung des Strafvollzugsgesetzes (4. StVollzGÄndG) vom 26.08.1998 ist am 01.12.1998 in Kraft getreten.

Wie bereits im III. Tätigkeitsbericht (S. 136 ff) bemerkt, enthält das Gesetz datenschutzrechtliche Verbesserungen bei der Verarbeitung von personenbezogenen Daten der Gefangenen, leider sind aber auch datenschutzrechtliche Defizite zu verzeichnen.

§ 29 Abs. 2 StVollzG schreibt die schon bisher in Sachsen-Anhalt geübte Verwaltungspraxis fest, daß die Datenschutzbeauftragten des Bundes und der Länder zu dem Personenkreis gehören, deren Schriftverkehr mit Gefangenen nicht überwacht wird.

Keinen Eingang in das Gesetz hat die Forderung gefunden, in § 86 StVollzG eine Regelung zu verankern, nach der erkennungsdienstliche Unterlagen nach einer Entlassung von Amts wegen zu vernichten sind. Nach der jetzigen Fassung können gem. § 86 Abs. 3 StVollzG Gefangene nach der Entlassung verlangen, daß die erkennungsdienstlichen Unterlagen, mit Ausnahme von Lichtbildern und Beschreibungen körperlicher Merkmale, vernichtet werden.

Der Gesetzgeber hat sich auch nicht dazu durchringen können, bei kurzen Freiheitsstrafen und Ersatzfreiheitsstrafen gänzlich auf die Anfertigung von erkennungsdienstlichen Unterlagen zu verzichten.

Regelungen zum Inhalt und zur Führung von Personalakten der Gefangenen sind in der neuen Gesetzesfassung ebenfalls nicht zu finden. § 180 Abs. 6 und 7 StVollzG regeln diesen Bereich nur fragmentarisch. Das Ministerium der Justiz hat auf Nachfrage des Landesbeauftragten hin mitgeteilt, daß Verwaltungsvorschriften für diesen Bereich geplant sind.

Hinsichtlich der Aufbewahrung von Akten (Personal- und Krankenakten) sieht das Gesetz nunmehr eine Aufbewahrungsfrist von 20 Jahren gegenüber noch 30 Jahren im ersten Gesetzentwurf vor. Der Landesbeauftragte hatte 10 Jahre für ausreichend erachtet.

Auch die Regelung des § 186 StVollzG zur Übermittlung von Gefangenendaten zu Forschungszwecken ist aus der Sicht des Datenschutzes nicht befriedigend ausgefallen.

Wie bereits im III. Tätigkeitsbericht angemerkt, sieht nun auch der geltende Gesetzestext keine generelle Einwilligung des Gefangenen vor einer Datenübermittlung zu Forschungszwecken vor. Die Regelung zur Aktenübersendung ist dabei so allgemein gefaßt, daß dies in der Praxis häufig auf die Übersendung der gesamten Gefangenenakten hinauslaufen könnte. Die Aktenübersendung darf aber nur ausnahmsweise in Frage kommen, wenn anderweitig der Forschungszweck nicht zu erfüllen wäre.

25.2 Entwurf eines Untersuchungshaftvollzugsgesetzes (UVollzG-E)

Das Ministerium der Justiz übersandte kurz vor Redaktionsschluß zu diesem Tätigkeitsbericht den neuen Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft - Stand 22.02.1999 - (vgl. zum früheren Entwurf III. Tätigkeitsbericht, S. 138 f).

Der Landesbeauftragte begrüßt ausdrücklich die beabsichtigte gesetzliche Regelung des Vollzuges der Untersuchungshaft. Die Landesbeauftragten und der Bundesbeauftragte für den Datenschutz haben in diesem Bereich immer eine gesetzliche Regelung angemahnt, zuletzt in ihrer Entschließung zu "Fehlenden bereichsspezifischen Regelungen bei der Justiz" vom 05./06.10.1998 **(Anlage 14).**

Zu dem vorliegenden Entwurf ist datenschutzrechtlich folgendes zu bemerken:

Der Entwurf fällt bei der Bewertung dadurch auf, daß er ganz offensichtlich die für die Haftanstalt möglichst einfachen Handlungsabläufe favorisiert und die Persönlichkeitsrechte des U-Häftlings weitgehend verdrängt. Dies steht weder mit dessen Rechtsstatus und seinen Grundrechten im Einklang noch mit der bekannt gering ausfallenden Verurteilungsquote im Anschluß an die U-Haft zu maßgeblichen Freiheitsstrafen.

- Die in § 6 Abs. 2 Satz 3 UVollzG-E vorgesehene Übersendung einer Mehrausfertigung der Anklageschrift sollte nur bei Erforderlichkeit für die Aufgabenerfüllung der Anstalt erfolgen, da eine Anklageschrift in der Regel eine Fülle personenbezogener Daten enthält, deren Kenntnis für die Anstalt nicht notwendig ist.

- § 7 Abs. 4 UVollzG-E sieht vor, daß andere Gefangene bei der Aufnahme in die Anstalt, dem Aufnahmegespräch und der ärztlichen Untersuchung nicht anwesend sein dürfen. Dies ist positiv zu bewerten. Ausnahmen bedürfen der Zustimmung des betroffenen Gefangenen, soweit die Hinzuziehung eines anderen Gefangenen nicht lediglich der Verständigung dient. Diese Regelung in § 7 Abs. 4 Satz 2 UVollzG-E ist nicht unbedenklich, denn durch die Hinzuziehung bei Sprachproblemen entsteht die Gefahr, daß hochsensible Gefangenendaten in der Anstalt bekannt werden. Im übrigen ist nicht auszuschließen, daß ein Gefangener infolge der Streßsituation bei einer vielleicht erstmaligen Aufnahme in eine Anstalt, sich der Tragweite seiner Zustimmung nicht bewußt ist.
  In der Stellungnahme des Landesbeauftragten gegenüber dem Ministerium der Justiz wurde daher vorgeschlagen, bei Verständigungsproblemen auf vereidigte Dolmetscher zurückzugreifen.
  Weiterhin fehlt eine Regelung, was geschehen soll, wenn der Gefangene seine Zustimmung nicht erteilt.

- Die Überwachung aller Besuche gem. § 17 Abs. 1 UVollzG-E begegnet verfassungsrechtlichen Bedenken. Mit dieser Regelung werden selbst vertrauliche Besuche nächster Angehöriger unmöglich, ohne daß dies in jedem Inhaftierungsfall zwingend geboten ist. Hier sollte in Absatz 1 ein Satz angefügt werden, nachdem das Gericht mit Zustimmung der Staatsanwaltschaft Ausnahmen für Besuche von Angehörigen zulassen kann. Eine solche Regelung würde auch der prinzipiellen Unschuldsvermutung zugunsten von Untersuchungsgefangenen entsprechen.

- Bei der Überwachung des Schriftwechsels gem. § 19 UVollzG-E wird vorgeschlagen, in Anbetracht des massiven Eingriffs in das verfassungsrechtlich geschützte Briefgeheimnis zumindest eine Unterrichtung des betroffenen Gefangenen vorzusehen.

- Zu § 20 Abs. 2 UVollzG-E wird angeregt, zumindest für die in Abs. 1 Nr. 2 bis 4 vorgesehenen Sachverhalte einen Richtervorbehalt zu verankern. Gerade das Anhalten von Schreiben nach Abs. 1 Nr. 2 und 3 setzt Wertungen voraus, die Personen vorbehalten sein sollten, die über die notwendige Distanz und Neutralität gegenüber der Anstalt verfügen. Die Abfassung eines Schreibens in "fremder Sprache" - was immer das bedeuten soll - ist ohnehin kein rational begründeter Zurückweisungsgrund bei U-Haft. Im Strafvollzug mag das andere Bedeutung haben.

- In § 36 Nr. 2 UVollzG-E sollte mit aufgenommen werden, daß auch eine Verarbeitung und Nutzung personenbezogener Daten nach § 180 Abs. 2 Strafvollzugsgesetz unterbleibt. Die dort aufgeführten öffentlichen Belange werden zwar regelmäßig höher zu bewerten sein als die entgegenstehenden Belange des Untersuchungsgefangenen, allerdings kann es in Einzelfällen durchaus geboten sein, von der Verarbeitung und Nutzung besonders schutzwürdiger personenbezogener Daten Abstand zu nehmen.

- In § 36 Nr. 3 UVollzG-E sollte klargestellt werden, daß eine Mitteilung nur an öffentliche Stellen zulässig ist. Die Unschuldsvermutung zugunsten von Untersuchungsgefangenen gebietet es, daß eine Mitteilung über den Anstaltsaufenthalt eines Gefangenen nur an solche Stellen geht, für deren Arbeit diese Kenntnis zwingend notwendig ist. Im übrigen fehlt eine Regelung für den Fall, daß ein Untersuchungsgefangener rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt wurde. In diesen Fällen wären die Stellen, die gem. § 180 Abs. 5 Satz 1 Strafvollzugsgesetz eine Mitteilung vom Anstaltsaufenthalt erhalten haben, zu informieren.

Der Landesbeauftragte hat gegenüber dem Ministerium der Justiz in diesem Sinne Stellung genommen.

26. Verfassungsschutz

Im Berichtszeitraum fanden beim Landesamt für Verfassungsschutz mehrere Überprüfungen aufgrund der Eingaben von Petenten statt.

Insgesamt zeigten die Überprüfungsergebnisse, daß die datenschutzrechtlichen Bestimmungen eingehalten wurden.

27. Verkehr

27.1 Neues Mammutregister im Straßenverkehrsrecht

Über den Stand der Aktivitäten des Bundesgesetzgebers zur Novellierung des StVG und anderer Gesetze hat der Landesbeauftragte zuletzt in seinem III. Tätigkeitsbericht (S. 141 ff) berichtet. Der damalige Gesetzentwurf vom November 1996 beinhaltete eine Reihe von datenschutzrechtlichen Verbesserungen. Erinnert sei nur an die Entwürfe hinsichtlich der unentgeltlichen Selbstauskunft für Betroffene und der Zweckbindung von Abrufprotokolldaten aus dem VZR und ZFR sowie die Harmonisierung der Verwertungsregel des Bundeszentralregisters (§ 52 Abs. 2 BZRG) mit denen des VZR bei Verfahren zur Erteilung oder Entziehung einer Fahrerlaubnis.

Das nun am 01. Januar 1999 in Kraft getretene "Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze" vom 24. April 1998 (BGBl. I S. 747) beinhaltet datenschutzrechtliche Verbesserungen im Artikel 1 (Änderungen des StVG), die insbesondere die Regelungen des neuen Fahrerlaubnisrechts (§§ 2 bis 6 StVG) betreffen.

Aus datenschutzrechtlicher Sicht zu begrüßen ist, daß für die Datenverarbeitung in Führerscheinakten erstmalig gesetzliche Festlegungen getroffen wurden, auch wenn sie nicht umfassend sind. Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse sind nunmehr nach spätestens **zehn** Jahren zu vernichten, es sei denn, die Unterlagen stehen im Zusammenhang mit einer Eintragung im VZR oder im Zentralen Fahrerlaubnisregister (ZFER) (vgl. § 2 Abs. 9 StVG). Unterlagen, die sich bereits am 1. Januar 1999 in "Altakten"

befunden haben, müssen allerdings erst dann berichtigt werden, wenn die Fahrerlaubnisbehörde aus anderem Anlaß mit dem Vorgang befaßt ist. Die Überprüfung und etwaige "Bereinigung" aller Führerscheinakten muß fünfzehn Jahre nach Inkrafttreten des Gesetzes, also bis zum 1. Januar 2014, erfolgt sein (vgl. § 65 Abs. 1 StVG).

Positiv sind aus datenschutzrechtlicher Sicht auch die Regelungen zur **unentgeltlichen** Auskunft über eigene Daten für Betroffene aus dem VZR (§ 30 Abs. 8 StVG) und den Fahrerlaubnisregistern (§ 58 StVG).

Mit Artikel 5 (Änderung des BZRG) wurde in § 52 Abs. 2 BZRG eine Harmonisierung der Verwertungsregelungen unter Beachtung der Verwertungsfristen der §§ 28 bis 30b StVG vorgenommen.

In Verfahren, die die Erteilung oder die Entziehung einer Fahrerlaubnis zum Gegenstand hatten, galt bisher eine unbefristete Verwertungsmöglichkeit, selbst wenn die Eintragungen in beiden Registern getilgt waren (vgl. II. Tätigkeitsbericht, S. 164 f).

Nunmehr erfolgte im BZRG die Korrektur. Danach dürfen nun die Tat und die Entscheidung nach der Tilgung im VZR im Verfahren über die Erteilung oder Entziehung der Fahrerlaubnis nicht mehr zum Nachteil des Betroffenen verwertet werden.

Dennoch bleiben die auch vom Landesbeauftragten früh angesprochenen Bedenken gegen das neue "Mammutregister" (§ 48 Abs. 2 StVG). Da **alle** Fahrerlaubnisinhaber gespeichert werden, wird dieses Register letztendlich auf ca. **50 Millionen Datensätze** anwachsen. Erfaßt werden in ihm die unveränderbaren Personalien und Führerscheindaten der Betroffenen. Immerhin werden die Anschriften nicht gespeichert. Damit wird auf die Einführung eines neuen bundesweiten "Melderegisters" von Führerscheininhabern verzichtet.

Zusätzlich werden in das ZFER die Daten über die Fahrlehrer und die Kraftfahrsachverständigen übernommen, die bisher beim KBA in eigenständigen Fahrlehrer- und Kraftfahrsachverständigenregistern geführt wurden (vgl. Artikel 2 - Änderung des Fahrlehrergesetzes; Artikel 6 - Änderung des Kraftfahrsachverständigengesetzes).

Neben zahlreichen deutschen Stellen erhalten viele öffentliche Stellen der EU-Mitgliedstaaten im automatisierten Verfahren Zugriff auf das ZFER (vgl. §§ 52 bis 56 StVG).

Der Landesbeauftragte ist aber nach wie vor **nicht** von der Notwendigkeit eines Zentralen Fahrerlaubnisregisters im Sinne eines überwiegenden Allgemeininteresses überzeugt. Angesichts der zahlreichen **europaweiten** Abrufmöglichkeiten öffentlicher Stellen besteht mit der Einrichtung des ZFER jederzeit die Möglichkeit, ein umfassendes elektronisches Überwachungssystem nicht nur für den Verkehrsbereich zu schaffen. Ist das Register erst da, kommen auch neue Begehrlichkeiten zu neuen Übermittlungs- und Nutzungsmöglichkeiten.

Zudem ist kritisch anzumerken, daß die örtlichen Fahrerlaubnisbehörden bei ihrer Aufgabenerfüllung zukünftig auf ein zentrales Register einer Bundesbehörde angewiesen sind. Den Bundesländern ist mit dieser Neuregelung jegliche Einflußnahme und Kontrollkompetenz entzogen.

Auch ist es fraglich, ob in der täglichen Arbeit die Fahrerlaubnisbehörden ohne "eigene" automatisierte Datenverarbeitung auskommen werden. Auch wenn mit der festgelegten Auflösung der örtlichen Fahrerlaubnisregister bis zum 31. Dezember 2005 das Problem der "Doppelspeicherung" gesetzlich gelöst wurde, liegt der Schluß nahe, daß andere örtliche Dateien entstehen könnten, die zwar nicht mehr den Namen "Örtliches Fahrerlaubnisregister" tragen, gleichwohl aber in letzter Konsequenz eine Doppelspeicherung von Fahrerlaubnisdaten beinhalten würden.

Bislang wurden Abrufe aus dem VZR und dem ZFR protokolliert und durften nur für Zwecke der Datenschutzkontrolle genutzt werden. Nunmehr wird die Nutzung der Protokolldaten über Abrufe aus dem VZR, dem ZFR und dem ZFER auch zur Aufklärung oder Verhütung von schwerwiegenden Straftaten gegen Leib, Leben oder Freiheit einer Person zugelassen. Die Aufbewahrungsfrist der Protokolldaten wurde von drei auf **sechs Monate** verlängert (vgl. §§ 30a Abs. 3; 36 Abs. 6; 53 Abs. 3 StVG). Damit erhalten die Protokolldateien den Charakter polizeilicher Fahndungsdateien.

27.2 Neues Fahrerlaubnisrecht - die Fahrerlaubnis-Verordnung

Auf der Grundlage der vom Gesetzgeber umfassend ausgestalteten Ermächtigungsnorm über die Zulassung von Personen zum Straßenverkehr (§ 6 Abs. 1 Nr. 1 StVG) ist die **Fahrerlaubnis-Verordnung** (FeV) vom 18. August 1998 am

01. Januar 1999 (BGBl. I S. 2214) in Kraft getreten. Sie konkretisiert die im StVG grundsätzlich getroffenen Regelungen und ersetzt damit das gleichzeitig durch Artikel 2 (Nr. 1, 2) der FeV aufgehobene Kapitel "A. Personen" (§§ 1 bis 15l a.F.) der Straßenverkehrs-Zulassungs-Ordnung (StVZO).

Da bisher wesentliche Fragen der Datenverarbeitung im Zusammenhang mit der Fahrerlaubnis nicht geregelt waren, ist die Neufassung des Fahrerlaubnisrechts grundsätzlich zu begrüßen. Die bisherige Situation war aus datenschutzrechtlicher Sicht nicht vereinbar mit den Forderungen nach einer normenklaren, gesetzlichen Regelung für die Bürgerinnen und Bürger zur Verarbeitung ihrer Daten. Schon in seinem II. Tätigkeitsbericht (S. 165 f) hatte der Landesbeauftragte auf diese nur unzulänglichen bereichsspezifischen Regelungen aufmerksam gemacht.

Erinnert sei in diesem Zusammenhang daran, daß z.B. für die Verarbeitung personenbezogener Daten von Führerscheininhabern in den §§ 8 und 10 Abs. 2 der StVZO (a.F.) nur ansatzweise Regelungen enthalten waren. So regelte § 8 lediglich die für einen Fahrerlaubnisantrag durch den Bürger der zuständigen Behörde einzureichenden Unterlagen. Der § 10 Abs. 2 verpflichtete die zuständige Behörde nur, die von ihr vorbereiteten Führerscheine vor der Übersendung an einen Sachverständigen oder Prüfer in eine "Liste" mit laufender Nummer einzutragen und diese Nummer im Führerschein anzugeben. Die Behörde hatte des weiteren die nicht näher eingegrenzte Befugnis, über die ausgehändigten Führerscheine eine namentlich, alphabetisch geordnete "Kartei" der Führerscheininhaber zu führen.

Die jetzige FeV regelt im wesentlichen die Einteilung der neuen Fahrerlaubnisklassen (§ 6 FeV), die Voraussetzungen für die Erteilung (§§ 11 bis 14 FeV) der Fahrerlaubnis, die Entziehung, die Beschränkungen, die Anordnung von Auflagen zur Fahrerlaubnis (§ 46 FeV), die Bewertung nach dem Punktesystem (§ 40 FeV; Anlage 13) sowie die Voraussetzungen für die Erteilung einer Fahrerlaubnis zur Fahrgastbeförderung (§ 48 FeV). Darüber hinaus präzisiert die FeV die im ZFER (§ 49 FeV) und in den örtlichen Fahrerlaubnisregistern (§ 57 FeV) zu speichernden Daten. Auch für diese genannten Bereiche hat sich mit der FeV eine deutliche Verbesserung aus datenschutzrechtlicher Sicht im Verhältnis zur früheren Rechtslage ergeben.

Bisher waren wichtige Rechtsbereiche in Form von Verwaltungsvorschriften geregelt. So z.B. das "Punktesystem" (Allg. VwV zu § 15b StVZO (a.F.)), die "Fahrerlaubnisprüfung" (Prüfungsrichtlinie vom 21.01.1987 zu § 11 StVZO (a.F.)) und die Beurteilung der "Eignung" (Eignungsrichtlinien vom 01.12.1982 zu § 12 StVZO (a.F.)).

Die im StVG neu geschaffene gesetzliche Grundlage für das Verfahren zur Anforderung medizinisch-psychologischer Gutachten (§ 2 Abs. 7 und 8 StVG) über die Eignung der Betroffenen zur Führung von Kraftfahrzeugen und die damit verbundene Datenverarbeitung wird durch die FeV (§§ 2, 3, 11-14; 48 Abs. 4 und 5; Anlagen 4, 5 (Teil I, II), 6, 15) konkretisiert.

Positiv zu erwähnen ist auch die Vorgabe eines **bundeseinheitlichen** Musters der ärztliche Bescheinigung (Anlage 5 der FeV), die Bewerber um eine Fahrerlaubnis zur Fahrgastbeförderung zum Nachweis ihrer körperlichen und geistigen Eignung der Fahrerlaubnisbehörde vorzulegen haben.

Bisher gab es keine Regelungen darüber, welchen Inhalt und Umfang das z.B. von Bus- und Taxifahrern vorzulegende ärztliche Zeugnis haben mußte. Dies hatte dazu geführt, daß ärztliche Beurteilungen oft detaillierte Angaben zur Krankengeschichte von Bewerbern beinhalteten und damit der Fahrerlaubnisbehörde bekannt wurden, obwohl diese medizinischen Einzeldaten zur Aufgabenerfüllung nicht erforderlich waren. Solche vollständigen medizinisch-psychologischen Untersuchungsberichte finden sich natürlich auch in den "Altakten" der Führerscheinbehörden wieder.

Das vorgegebene Muster "Bescheinigung über die ärztliche Untersuchung" (Anlage 5 der FeV) gliedert sich in **zwei** Teile. Der "Teil I" mit einzelnen Untersuchungsergebnissen verbleibt beim Arzt und nur der "Teil II" mit den Schlußfolgerungen des Arztes wird dem Bewerber ausgehändigt und ist zur Vorlage bei der Fahrerlaubnisbehörde bestimmt.

Der Landesbeauftragte begrüßt diese Regelung zur Datenverarbeitung, weist aber gleichzeitig daraufhin, daß eine vollständige normenklare Regelung nicht gelungen ist. Zwar wird die Datenübermittlung der Fahrerlaubnisbehörden an Stellen und Personen, welche die Eignung und Befähigung beurteilen oder prüfen, in § 2 Abs. 14 StVG geregelt. Zur Datenverarbeitung und Datenübermittlung der begutachtenden Stellen und Personen selbst **fehlen** jedoch nähere Angaben.

An anderer Stelle der FeV sind bereits erreichte und abgestimmte datenschutzrechtliche Verbesserungen im Zuge des Gesetzgebungsverfahrens wieder zurückgenommen worden. So enthält z.B. § 11 Abs. 6 Satz 2 FeV nicht mehr die Ergänzung, daß der Betroffene **vor** Übersendung der Fahrerlaubnisunterlagen an eine begutachtende Stelle diese einsehen kann.

Außerdem geht die FeV hinsichtlich der Übergabe der Unterlagen an die begutachtende Stelle über die Ermächtigungsnorm im StVG (§ 2 Abs. 14 Satz 1) hinaus. Während das StVG lediglich die Übermittlung der Daten vorsieht, die zur Aufgabenerfüllung **benötigt** werden, bestimmt die FeV (§ 11 Abs. 6 Satz 4) die Übersendung der **vollständigen** Unterlagen. Dies ist rechtlich unzulässig.

Der Landesbeauftragte empfiehlt deshalb dem Ministerium für Wohnungswesen, Städtebau und Verkehr, bis zu einer Novellierung der FeV auf dem Erlaßwege sicherzustellen, daß die Fahrerlaubnisbehörden regelmäßig die Akteneinsicht in diesen genannten Fällen anbieten und nur die **erforderlichen** Fahrerlaubnisunterlagen an die begutachtenden Stellen übersandt werden.

28. Vermessungs- und Katasterwesen

Datenübermittlung an einen Öffentlich bestellten Vermessungsingenieur

Ein Petent wandte sich an den Landesbeauftragten mit der Bitte um Überprüfung einer, seiner Meinung nach, willkürlichen und unzulässigen Übermittlung von Daten zu seiner Person vom Katasteramt an einen Öffentlich bestellten Vermessungsingenieur (ÖbVermIng).

Er hatte seinerzeit einen Bauantrag beim zuständigen Bauordnungsamt gestellt und das Gebäude mittlerweile errichtet. Da der Neubau noch nicht im Liegenschaftskataster erfaßt war, wurde er durch ein Schreiben eines ÖbVermIng auf seine Pflicht zur Veranlassung der Gebäudevermessung hingewiesen. Diesem Schreiben war gleich ein Antrag zur Vermessung durch eben diesen ÖbVermIng beigefügt.

Auf Anfrage des Landesbeauftragten teilten das Katasteramt und das zuständige Ministerium des Innern mit, daß eine Vielzahl von Eigentümern ihrer Pflicht zur Veranlassung der Gebäudevermessung gemäß § 14 Vermessungs- und Katastergesetz (VermKatG LSA) noch nicht nachgekommen seien. Deren Anzahl werde auf ca. 30.000 Fälle beziffert. Aus diesem Grund sei hierzu durch

einen gemeinsamen Runderlaß des MI und des MWV vom 31.03.1995 ein entsprechendes Mitteilungsverfahren festgelegt worden, welches die Unterrichtung der zuständigen Katasterämter über genehmigte Bauvorhaben durch die Bauordnungsämter regele.

Die ÖbVermIngenieure, die gem. § 1 Abs. 2 VermKatG LSA an der Führung des Liegenschaftskatasters mitwirken, erhalten vom Katasteramt Auszüge aus der Liegenschaftskarte, Luftbilder und eine Liste der Flurstücke mit genehmigten Bauvorhaben. Nach einem Feldvergleich teilen sie dem Katasteramt alle Flurstücke mit neu errichteten Gebäuden mit. Da hierbei weder personenbezogene Daten der Bauantragsteller noch der Grundstückseigentümer übermittelt werden, bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

Der Landesbeauftragte wird die geschilderte Verfahrensweise im Rahmen seiner zukünftigen Kontrollen prüfen und hat im übrigen zu diesem Einzelfall das Ministerium des Innern daran erinnert, daß gem. § 14 Abs. 2 VermKatG LSA die Aufforderung an den Eigentümer, einen Antrag auf Gebäudevermessung zu stellen, durch das jeweilige Katasteramt zu erfolgen hat. Da der Petent im vorliegenden Fall durch den ÖbVermIng selbst angeschrieben wurde, entstand neben der Vermutung, daß seine personenbezogenen Daten ohne gesetzliche Grundlage übermittelt wurden, auch der Eindruck unlauteren Wettbewerbs.

In seiner Antwort an den Petenten hat der Landesbeauftragte ergänzend zum eigentlichen Sachverhalt auch den Hinweis gegeben, daß die vom Bürger kritisierte Vorgehensweise nicht erforderlich wäre, wenn alle Eigentümer von Gebäuden ihrer gesetzlichen Verpflichtung nachkommen und die Gebäudevermessung unverzüglich nach Beendigung der Baumaßnahme veranlassen würden.

29. Wahlen

Ausschluß vom Wahlrecht und die datenschutzrechtlichen Folgen

Ein Häftling aus einer Justizvollzugsanstalt des Landes hatte sich zu Recht beim Wahlprüfungsausschuß des Landtages beschwert, daß ihm keine Gelegenheit zur Teilnahme an der Landtagswahl 1998 gegeben worden war, obwohl er wahlberechtigt gewesen sei.

Im Zuge der Nachforschungen wurde festgestellt, daß dem Strafgefangenen lediglich das passive Wahlrecht aberkannt worden war. Die Justizvollzugsanstalt hatte dazu zulässigerweise dem Ministerium der Justiz eine vom Einwohnermeldeamt erstellte "Liste über Wahlrechtsentzug" mit einer Vielzahl personenbezogener Daten von insgesamt 32 Strafgefangenen übersandt. Leider waren darauf nur die Einzeldaten von 16 Gefangenen unleserlich geschwärzt.

Nicht mehr zulässig war dann die weitere Übersendung der nur teilweise geschwärzten Gesamtliste vom Ministerium der Justiz an den Landeswahlleiter, statt an den Wahlprüfungsausschuß des Landtages. Bekanntlich schützt Art. 6 Abs. 1 LVerf jeden der auf der Liste genannten, nicht betroffenen Strafgefangenen vor unzulässigen Übermittlungen seiner personenbezogenen Daten an andere Stellen ohne gesetzliche Grundlage.

Die gesetzlich zugelassene Verfahrensweise ergibt sich aus § 54 LWG i.V. mit dem Wahlprüfungsgesetz vom 11.12.1992, insbesondere dessen §§ 3 und 4. Danach waren im konkreten Verfahren Beteiligte nur der einspruchführende Strafgefangene und der Wahlprüfungsausschuß des Landtages.

Die Übermittlung der Datenliste an den Landeswahlleiter war demnach schon deshalb unzulässig, weil die Prüfung eines Wahleinspruches nicht in seine Zuständigkeit fällt und davon ohnehin nur der Petent Gebrauch gemacht hatte. Der Landeswahlleiter war auch für die anderen aufgelisteten 31 Fälle nicht die zuständige Überprüfungsinstanz.

So führte dieser Fehler prompt zum nächsten. Der Landeswahlleiter übersandte seinerseits die Gesamtliste der Gefangenen an den Wahlprüfungsausschuß, anstelle die Übersendung nur auf den dort zu entscheidenden Einzelfall zu beschränken.

Der die Arbeit des Wahlprüfungsausschusses begleitenden Landtagsverwaltung unterlief dann der nächste Fehler. Dem Schreiben des Ausschusses an den einspruchführenden Gefangenen legte man wiederum die Gesamtliste bei.

Dieser war dann der erste, dem rechtliche Bedenken kamen. Er fragte beim Landesbeauftragten, ob das bis dahin abgelaufene Verfahren wohl datenschutzgerecht sei; immerhin habe er von den gesetzlichen Einschränkungen bei den anderen Gefangenen nichts gewußt, und ihre Daten gingen ihn wohl nichts an.

So war es, und der Landesbeauftragte hätte sich gewünscht, die in der Sache beteiligten öffentlichen Stellen hätten beizeiten auch etwas von dieser Datensensibilität bewiesen.

30. Waffenrecht

Übermittlung personenbezogener Informationen aus Stasi-Unterlagen

Immer wieder Probleme macht die Verwendung personenbezogener Informationen aus Stasi-Unterlagen im Waffenrecht. Vor allem für das Bewachungsgewerbe sind diese Informationen von großer Bedeutung.

So hatte ein Landkreis datenschutzrechtliche Bedenken, zur Begründung der Ablehnung von Waffenscheinen für Angestellte eines Bewachungsunternehmens personenbezogene Informationen aus Stasi-Unterlagen zu verwenden, weil diese dann dem Bewachungsunternehmer bekanntgeworden wären.

Da konnte der Landesbeauftragte eine datenschutzbewußte Behörde auch einmal beruhigen:

Zu den wesentlichen **tatsächlichen** und rechtlichen Gründen der Ablehnungsentscheidung im Sinne von § 39 Abs. 1 Satz 2 VwVfG LSA gehört nach der obergerichtlichen Rechtsprechung mehr als nur die Mitteilung, die "genannten Beschäftigten seien aufgrund ihrer früheren Tätigkeit für das MfS der ehemaligen DDR unzuverlässig". Deshalb mußte die Entscheidung konsequenterweise mit näheren Einzelheiten aus den Gauck-Unterlagen gegenüber dem Bewachungsunternehmer begründet werden. Insofern tragen die Beschäftigten im Bewachungsgewerbe ein gesetzlich vorher absehbares Risiko (vgl. § 30 Abs. 1 i.V. mit § 5 Abs. 1 Nr. 2 WaffG), daß für die Beschäftigung maßgebliche Einzelheiten ihres persönlichen Vorlebens dem Arbeitgeber bekannt werden.

Im übrigen wurden die personenbezogenen Informationen entsprechend den Vorschriften des Stasi-Unterlagen-Gesetzes auch für den Zweck verwendet, für den sie übermittelt worden sind (vgl. §§ 6 Abs. 9, 20 Abs. 1 Nr. 8, 29 Abs. 1 Satz 1 StUG).

31. Wasserrecht

Auskünfte an Bürgermeister über Gebührenschuldner

Ein Abwasserzweckverband wandte sich mit einer Anfrage an den Landesbeauftragten, ob es zulässig sei, eine namentliche Aufstellung von Beitrags- und

Gebührenschuldnern an die Bürgermeister der angeschlossenen Verbandsgemeinden zu übermitteln, um diesen die persönliche Einflußnahme auf die Zahlungsmoral bei den Säumigen zu ermöglichen.

Der Landesbeauftragte hat deutlich gemacht, daß eine solche Datenübermittlung als unzulässig anzusehen ist, und zwar aus folgenden Gründen:

Jeder Bürgermeister einer Mitgliedsgemeinde ist gegenüber dem Abwasserzweckverband als Dritter anzusehen. Eine Datenübermittlung ist nur zulässig, wenn das DSG-LSA oder eine andere Rechtsvorschrift die Übermittlung erlauben oder die Betroffenen darin einwilligen (§ 4 Abs. 1 DSG-LSA).

Bereichsspezifische Regelungen zur Übermittlung waren nicht ersichtlich. Das DSG-LSA (§ 11 Abs. 1 Nr. 1) kommt als Ermächtigungsgrundlage für eine Datenübermittlung nicht in Betracht, weil die Übermittlung weder zur Aufgabenerfüllung des Abwasserzweckverbandes noch der jeweiligen Bürgermeister erforderlich ist.

Erforderlichkeit setzt rechtlich zunächst eine zulässige und geeignete konkrete Maßnahme voraus, um das angestrebte Ziel erreichen zu können. Das Ziel ist aber nicht konkret definiert, wenn die Bürgermeister persönlich Einfluß auf die Gruppe der Gebühren- und Beitragsschuldner nehmen wollen. Fernziel ist zwar die Beitreibung ausstehender Gebühren und Beiträge. Diese ist aber im Verwaltungsvollstreckungsgesetz (VwVG LSA) speziell und verbindlich geregelt. Die Ausübung sozialen Druckes innerhalb der Gemeinden durch die Bürgermeister wäre hingegen kein legitimes Ziel, das eine Übermittlung erforderlich machen könnte.

Der Abwasserzweckverband wurde aber darauf hingewiesen, daß es ihm nicht verwehrt ist, den Bürgermeistern eine abstrakte Zahlenauflistung der säumigen Schuldner ihrer Gemeinde zu übergeben. Diese könnten dann bei Informationsveranstaltungen und auch auf sonst geeigneten Wegen die Bürger allgemein über ihre Zahlungspflichten aufklären und zur Zahlung anhalten.

Anlage 1

Organisationsplan

Landesbeauftragter für den Datenschutz Sachsen-Anhalt

Herr Kalk

Referat 1	Referat 2	Referat 3
Grundsatzfragen des Datenschutzes, Internationaler Datenschutz, Öffentlicher Dienst, Personalvertretung, Landtag, Rundfunk- und Presserecht, Religionsgemeinschaften, Geschäftsstellenleitung	Rechtspflege, Justizverwaltung, Justizvollzug, Rechtshilfe, Allgemeines Ordnungswidrigkeitenrecht, Einigungsvertrag	Grundsatzfragen der Technik und Organisation des Datenschutzes und der Informationstechnik, Wirtschaft, Verkehr, Raumordnung und Landesplanung
Hochschulen, Sozialwesen, Gesundheitswesen, Jugendhilfe	Polizei, Verfassungsschutz, Nachrichtendienste, Finanzen, Kommunalrecht	Betriebs- und Datenbanksysteme, Statistik, Handwerk und Gewerbe, Wohnungswesen
Personenstandswesen, Kultur, Denkmalschutz, Archivwesen, Wissenschaft und Forschung, Schulen	Gefahrenabwehrrecht, Bau- und Bodenangelegenheiten, Natur- und Umweltschutz, Landwirtschaft und Forsten, Ausländer, Aussiedler, Staatsangehörigkeit --- Europäischer Datenschutz	Telekommunikation, Netze, Neue Medien, Vermessungs- und Katasterwesen, Dateienregister,

Verwaltungsangelegenheiten der Geschäftsstelle, Wahlen, Ausweis-, Meldewesen, Feuerwehr, Katastrophenschutz, Personalaktenrecht, Gleichstellungsfragen

Registratur

Bücherei

Dienstgebäude: Berliner Chaussee 9
39114 Magdeburg

Postanschrift: Postfach 1947
39009 Magdeburg

Telefon: (0391) 8 18 03 - 0

Telefax: (0391) 8 18 03 33

Stand: 01.04.1999

Anlage 2

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997:

Beratungen zum StVÄG 1996

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

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

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

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

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

Die Regelungen über Inhalt, Ausmaß und Umfang von Dateien und Informationssystemen mit personenbezogenen Daten bei Staatsanwaltschaften sind unzureichend. Das hat zur Folge, dass nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet und Daten ohne Berücksichtigung der Begehungsweise und Schwere von Straftaten

gespeichert werden können. Die Zugriffsmöglichkeiten der Strafverfolgungs- und Strafjustizbehörden auf diese Daten gehen zu weit. Darüber hinaus werden Standardmaßnahmen des technischen und organisatorischen Datenschutzes (z.B. Protokollierung, interne Zugriffsbeschränkungen etc.) weitgehend abgeschwächt.

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

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

Beispiele hierfür sind:
Der Richtervorbehalt für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation soll gestrichen werden.

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

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

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

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

Speicherungs- und Löschungsfristen für personenbezogene Daten in Dateien sollen ersatzlos gestrichen werden.
Kontrollverfahren für automatisierte Abrufverfahren sollen aufgehoben werden und die Verwendungsbeschränkungen für Protokolldaten sollen entfallen.

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

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

Anlage 3

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997:

Genetische Informationen in Datenbanken der Polizei für erkennungsdienstliche Zwecke

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

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

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

Die automatisiert gespeicherten Informationen aus DNA-Merkmalen, die zum Zweck der Identitätsfeststellung erstellt worden sind, ermöglichen derzeit tatsächlich zwar keine über die Identifizierung hinausgehenden Aussagen zur jeweiligen Person oder deren Erbgut. In Einzelfällen können die analysierten nicht codierenden persönlichkeitsneutralen DNA-Merkmale jedoch mit codierenden Merkmalen korrespondieren. In Anbetracht der weltweiten intensiven Forschung im Bereich der Genom-Analyse ist es nicht ausgeschlossen, dass künftig auch auf der Basis der Untersuchung von bisher als nicht codierend angesehenen Merkmalen konkrete Aussagen über genetische Dispositionen der betroffenen Personen

mit inhaltlichem Informationswert getroffen werden können. Dieses Risiko ist deshalb nicht zu vernachlässigen, weil gegenwärtig weltweit mit erheblichem Aufwand die Entschlüsselung des gesamten menschlichen Genoms vorangetrieben wird.

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

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

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

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

Wenn zum Zweck des Abgleichs mit Daten aus anderen Verfahren (also zu erkennungsdienstlichen Zwecken) DNA-Informationen automatisiert gespeichert werden sollen (DNA-Datenbank mit der Funktion, die bei Fingerabdrücken die AFIS-Datenbank des BKA

besitzt), müssen darüber hinaus folgende Regelungen geschaffen werden:

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

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

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

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

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

Anlage 4

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997:

Geplante Verpflichtung von Telediensteanbietern, Kundendaten an Sicherheitsbehörden zu übermitteln

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

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

Mit guten Gründen haben deshalb die Länder davon abgesehen, in den inzwischen von den Ministerpräsidenten unterzeichneten Staatsvertrag über Mediendienste eine vergleichbare Vorschrift aufzunehmen. In der Praxis werden sich aber für Bürger und Online-Dienstanbieter schwierige Fragen der Abgrenzung zwischen den Geltungsbereichen des

Mediendienste-Staatsvertrags und des Teledienstedatenschutzgesetzes ergeben. Auch aus diesem Grund halten die Datenschutzbeauftragten eine Streichung der Vorschrift des § 5 Absatz 3 aus dem Entwurf für ein Teledienstedatenschutzgesetz für geboten.

Anlage 5

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997:

Achtung der Menschenrechte in der Europäischen Union

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

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

Anlage 6

Entschließung der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. April 1997:

Sicherstellung des Schutzes medizinischer Datenbestände außerhalb von ärztlichen Behandlungseinrichtungen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für sehr problematisch, dass in Folge technischer und gesellschaftlicher Veränderungen in einer zunehmenden Anzahl von Konstellationen personenbezogene medizinische Patientendaten außerhalb des ärztlichen Bereiches verarbeitet werden. Sie fordern, dass zunehmend die Möglichkeiten einer anonymen oder pseudonymen Datenverarbeitung mit Verschlüsselung genutzt werden. Soweit dennoch Patientendaten personenbezogen weitergegeben werden, ist ein wesentliches Problem, dass außerhalb des ärztlichen Gewahrsams der von der Strafprozeßordnung vorgesehene Schutz personenbezogener Patientendaten vor Inanspruchnahme als Beweismittel durch Zeugeneinvernahme oder Beschlagnahme nicht mehr zweifelsfrei sichergestellt ist bzw. überhaupt nicht existiert.

Die folgenden Beispiele machen dies deutlich:

Ärzte bzw. Krankenhäuser haben z.B. keinen Gewahrsam an den personenbezogenen Patientendaten, die der Patient auf einer (freiwilligen) Patientenchipkarte bei sich trägt/besitzt oder die von einer dritten Stelle außerhalb des ärztlichen Bereichs im Auftrag verarbeitet werden, wie z.B. bei Mailbox-Systemen, externer Archivierung oder der Vergabe von Schreibarbeiten an selbständige Schreibbüros.

Fraglich ist auch die Aufrechterhaltung des ärztlichen Gewahrsams, wenn Hilfspersonal des Arztes oder Krankenhauses Patientendaten in der Privatwohnung bearbeitet.

Zunehmend werden einzelne Unternehmensfunktionen bzw. fachliche Aufgaben ausgelagert und einer externen Stelle - in der Regel einem Privatunternehmen - übertragen (sog. Outsourcing), z.B. bei Einschaltung eines externen Inkassounternehmens, bei externem

Catering für stationäre Patienten, bei externer Archivierung oder bei Vergabe von Organisationsanalysen an externe Beratergesellschaften.

Medizinische Daten mit Patientenbezug sollen an Forscher oder Forschungsinstitute zu Zwecken wissenschaftlicher Forschung übermittelt werden. Je umfassender und komplizierter der Einsatz automatisierter Datenverarbeitung für Forschungszwecke vorgesehen wird, desto weniger werden die personenbezogenen Patientendaten ausschließlich durch ärztliches Personal verarbeitet. Hier setzt sich vielmehr die Verarbeitung durch Informatiker und Statistiker immer mehr durch. Aber auch bei Verarbeitung durch Ärzte, die in der Forschung tätig sind, ist keineswegs sichergestellt, dass die personenbezogenen Patientendaten diesen Ärzten „in ihrer Eigenschaft als Arzt“ bekannt geworden sind, wie dies durch die Strafprozeßordnung für den Beschlagnahmeschutz als Voraussetzung festgelegt ist.

Die zunehmende Verlagerung personenbezogener Patientendaten aus dem Schutzbereich des Arztgeheimnisses nach außen verstößt nach Ansicht der Datenschutzbeauftragten massiv gegen Interessen der betroffenen Patienten, solange nicht ein gleichwertiger Schutz gewährleistet ist.

Die Datenschutzbeauftragten des Bundes und der Länder bitten daher den Bundesgesetzgeber - unabhängig von weiteren Fragen des Datenschutzes, die mit der Verarbeitung medizinischer Daten im Rahmen der Telemedizin verbunden sein können - für die sich zunehmend entwickelnden modernen Formen der Auslagerung medizinischer Patientendaten sowie für die Weitergabe medizinischer Patientendaten für Zwecke wissenschaftlicher medizinischer Forschung einen dem Arztgeheimnis entsprechenden Schutz der Patientendaten zu schaffen.

Anlage 7

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20. Oktober 1997 zu den Vorschlägen der Arbeitsgruppe des ASMK

„Verbesserter Datenaustausch bei Sozialleistungen“

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

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

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

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

Dieses System der Differenzierung des Verfahrens der Datenerhebung entspricht dem Grundsatz der Verhältnismäßigkeit. Ferner ist zu differenzieren, ob Daten aus dem Bereich

der Sozialleistungsträger oder Daten außerhalb dieses Bereichs erhoben werden.

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

Datenabgleichsverfahren sollen nur in Frage kommen bei Anhaltspunkten für Missbrauchsfälle in nennenswertem Umfang. Deshalb müssen etwaige neue Datenabgleichsverfahren hinsichtlich ihrer Wirkungen bewertet werden. Daher ist parallel zu ihrer Einführung die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfasst. Dies ermöglicht, Aufwand und Nutzen zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen.

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

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

Mitwirkung bei der Ahndung des Missbrauchs (für alle Leistungsträger) und Verbesserungen für die Leistungsempfänger (zu D.II.10.1 und B.I) (S. 30 u. S. 2)

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

Die mit der Datenerhebung verbundene Offenlegung des Kontaktes bzw. einer Leistungsbeziehung zu einem Sozialleistungsträger stellt einen erheblichen Eingriff für den

Betroffenen dar, u.a. da sie geeignet ist, seine Stellung in der Öffentlichkeit, z.B. seine Kreditwürdigkeit, wesentlich zu beeinträchtigen. Anfragen bei Dritten ohne Kenntnis des Betroffenen lassen diesen im Unklaren, welche Daten wann an wen übermittelt wurden.

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

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

Nachfrage beim Wohnsitzfinanzamt des Hilfesuchenden und Schenkungen und Erbschaften (zu D.I.1.1) (S. 6)

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

Auskunftspflicht der Banken und Lebensversicherungen (zu D.II.1.6) (S. 13)

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

Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünfte gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben. Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, dass dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, dass der Betroffene desavouiert wird.

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

Akzeptanz des Datenaustausches (zu E.IV) (S. 36)

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

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

Anlage 8

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997:

Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.
Noch immer gibt es keinen Kabinettsbeschluss; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

Verbesserungen des Datenschutzes der Bürger, z.B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich; dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.
Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

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

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

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

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

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

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

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

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

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

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

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

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

- Regelungen für Chipkarten-Anwendungen;

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

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

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

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

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

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

Anlage 9

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997:

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

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

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

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und

aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten („Vermeidung kognitiver Dissonanzen“). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

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

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

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

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

Vorbehaltlich des o.g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen

erlaubt sein, da nur so ein wirksamer Schutz vor Missbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fairen, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zulässt, müssen jedenfalls wirksame Vorkehrungen gegen Missbrauch gewährleistet sein, z.B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.

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

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

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

Anlage 10

Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997:

Erforderlichkeit datenschutzfreundlicher Technologien

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

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

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

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

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

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

Anlage 11

Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998:

Datenschutz beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, dass bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, dass erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, dass auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen ("Free TV" und "Pay TV") muss die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, dass die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:
Die Gestaltung technischer Einrichtungen muss sich an dem Ziel ausrichten, dass so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;
die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;
personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;
wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d.h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

Anlage 12

Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998:

Datenschutzprobleme der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen "Schattenkonten" der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese "Schattenkonten" noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluss der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, dass auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

Anlage 13

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998:

Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, dass in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlass von Unsicherheiten ist. Sie weisen daher darauf hin, dass die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u.a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, dass Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

Anlage 14

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998:

Fehlende bereichsspezifische Regelungen bei der Justiz

Derzeit werden in allen Bereichen der Justiz - bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern – im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, daß sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, daß die Rechtsprechung des Bundesverfassungsgerichts zum sogenannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluß an ihren Beschluß der 48. Konferenz vom 26./27.09.1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und –nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentlichen Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien

namentlich die
Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;

Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.

Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;

Datenübermittlung zu wissenschaftlichen Zwecken;

Datenverarbeitung in der Zwangsvollstreckung;

Datenverarbeitung im Jugendstrafvollzug;

Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und
-verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein "StVÄG 1996" erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z.B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück. Zu kritisieren sind vor allem:

Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung

Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte

Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

Anlage 15

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998:

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

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, vor dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlass an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlass an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

Anlage 16

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998:

Weitergabe von Meldedaten an Adressbuchverlage und Parteien

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, dass sie persönlich adressierte Wahlwerbung der Parteien bekommen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen – erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

Anlage 17

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998:

Entwicklungen im Sicherheitsbereich

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z.B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, dass die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

Anlage 18

Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 5./6. Oktober 1998:

Dringlichkeit der Datenschutzmodernisierung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefaßten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.

Die anlaßfreie Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muß in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.

Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.

Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.

Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

Anlage 19

Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 1999:

Modernisierung des Datenschutzrechts jetzt - umfassende Novellierung des BDSG nicht aufschieben

Die deutschen Datenschutzbeauftragten haben bereits früh gefordert, die Novellierung des BDSG zur Umsetzung der EG-Datenschutzrichtlinie zu einer gründlichen Modernisierung des veralteten deutschen Datenschutzrechts zu nutzen. Da die dreijährige Anpassungsfrist im Oktober 1998 verstrichen ist, besteht jetzt ein erheblicher Zeitdruck. Für die Neuregelung, die derzeit in der Bundesregierung und in Koalitionsgremien vorbereitet wird, ist daher ein „Zwei-Stufen-Konzept“ vorgesehen. Einem ersten, in Kürze vorzulegenden Novellierungsgesetz soll zu einem späteren Zeitpunkt eine zweite Änderung folgen, die weitere Verbesserungen enthalten soll. Die Konferenz geht davon aus, daß das Zweistufenkonzept von dem festen politischen Willen getragen wird, die zweite Stufe nach Einbringung des ersten Gesetzentwurfes zügig in Angriff zu nehmen und noch in dieser Legislaturperiode abzuschließen. Auch der in dieser Stufe bestehende Handlungsbedarf duldet keinen Aufschub.

Die Konferenz begrüßt, daß jetzt mit Hochdruck an der BDSG-Novellierung gearbeitet wird und Verantwortliche in Regierung und Fraktionen zugesagt haben, die erste Stufe der Neuregelung werde sich nicht auf das von der Richtlinie geforderte Minimum beschränken. Sie unterstützt die Vorschläge, Regelungen zur Videoüberwachung, zu Chipkarten und zum Datenschutzaudit aufzunehmen. Gleiches gilt für die Übernahme der zukunftsweisenden Bestimmungen zur Datenvermeidung sowie zur anonymen bzw. pseudonymen Nutzung von Telediensten aus dem Multimediarecht. Diese sind wichtige und dringend notwendige Regelungen zur Modernisierung des Datenschutzrechts. Die Konferenz drückt daher ihre Erwartung darüber aus, daß diese Vorschriften in der ersten Stufe des Gesetzgebungsverfahrens zügig verabschiedet werden.

Zu den Punkten, die keinen Aufschub dulden, gehört auch die Verbesserung der Voraussetzungen für eine effektive Datenschutzkontrolle. Die völlig unabhängige Gestaltung der

Kontrolle im nichtöffentlichen Bereich muß institutionell sichergestellt und durch eine sachgerechte finanzielle und personelle Ausstattung unterstützt werden. Gegenwärtig noch bestehende Einschränkungen der Kontrollkompetenzen im öffentlichen Bereich müssen abgebaut, den Aufsichtsbehörden müssen wirksamere Befugnisse an die Hand gegeben werden.

Zum Schutz der Bürgerinnen und Bürger sind bei massenhaften Datenerhebungen mit unkalkulierbaren Datenverarbeitungsrisiken oder ungeklärter Zweckbestimmung klare materielle Grenzen durch den Gesetzgeber zu ziehen.

Die bereichsspezifischen Gesetze, z.B. die Sicherheitsgesetze, dürfen nicht vom Bundesdatenschutzgesetz mit den dort zu erwartenden substantiellen Fortschritten für die Bürgerinnen und Bürger, wie beispielsweise einem verbesserten Auskunftsrecht, abgekoppelt werden.

Notwendig ist nach Auffassung der Konferenz, daß das Datenschutzrecht auch in Zukunft bürgerfreundlich und gut lesbar formuliert ist. Dies ist eine unverzichtbare Akzeptanzvoraussetzung für den Datenschutz bei Bürgern, Wirtschaft und Verwaltung.

Anlage 20

Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 1999:

Transparente Hard- und Software

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt für die Nutzung datenschutzfreundlicher Technologien eingesetzt. Sie sehen jedoch mit Sorge die Entwicklung im Bereich der Informationstechnik, die zu neuen Industriestandards und Produkten führt, die für die Benutzerinnen und Benutzer kaum durchschaubar und selbst für Fachleute nur noch eingeschränkt revisionsfähig sind.
Beispielsweise sind seit kurzem mit dem Intel Pentium III-Prozessor bestückte PC auf dem Markt, deren Prozessor bei der Herstellung mit einer eindeutigen Nummer (Processor Serial Number - PSN) versehen wurde. Intel sieht vor, das Auslesen der PSN durch die Nutzerinnen und Nutzer kontrollieren zu lassen. Die mittlerweile bekannt gewordenen Manipulationsmöglichkeiten der dafür erforderlichen Software machen deutlich, daß die Existenz einer solchen eindeutigen Kennung kaum kontrollierbare Nutzungsmöglichkeiten eröffnet, die dem Datenschutz diametral zuwider laufen.
Die durch den Intel Pentium III initiierte Debatte um eindeutige Kennungen brachte ans Tageslicht, daß Softwarehersteller Nutzern neuerer Office-Produkte ohne deren Wissen eindeutige Kennungen zuordnen. Diese Kennungen können in Dokumenten versteckt sein und bei der Nutzung des Internets von Softwareherstellern verdeckt abgefragt werden.
Werden Daten der Nutzerinnen und Nutzer übermittelt, ohne daß sie dies bemerken, kann deren mißbräuchliche Verwendung die Anonymität der Anwender von Informationstechnik weiter aushöhlen. Den Erfordernissen des Datenschutzes wird aber nur dann ausreichend Rechnung getragen, wenn zum Schutz der Privatheit transparente und von den Nutzerinnen und Nutzern in eigener Verantwortung bedienbare Sicherheitsfunktionen zur Verfügung stehen.
Deshalb erwarten die Datenschutzbeauftragten des Bundes und der Länder von Herstellern von Informations- und Kommunikationstechnik, Hard- und Software so zu entwickeln und herzustellen, daß Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit von Sicherheitsvorkehrungen überzeugen können.

Den Anwendern moderner Technik empfehlen die Datenschutzbeauftragten, nur solche Produkte einzusetzen, welche auch eine Transparenz der Verfahrensabläufe gewährleisten.

Anlage 21

Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 1999:

Zur geplanten erweiterten Speicherung von Verbindungsdaten in der Telekommunikation

Die Bundesregierung und der Bundesrat werden demnächst über den Erlaß der seit längerem überfälligen Rechtsverordnung zum Datenschutz in der Telekommunikation auf Grund des Telekommunikationsgesetzes zu entscheiden haben.

Im Gegensatz zur früheren analogen Vermittlungstechnik erzeugt und verarbeitet das digitalisierte Telekommunikationsnetz (ISDN-Netz) in großem Umfang personenbezogene Verbindungsdaten. Dies zwingt zu begrenzenden, am Grundsatz der Datensparsamkeit orientierten Regelungen, um das Fernmeldegeheimnis und das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation zu garantieren.

Die bisher geltende Telekommunikationsdienstunternehmen-Datenschutzverordnung von 1996 sieht vor, daß die Verbindungsdaten unter Kürzung der Zielrufnummer regelmäßig bis zu 80 Tagen nach Versendung der Rechnung gespeichert werden dürfen. Über diese Frist hinaus dürfen Verbindungsdaten nur gespeichert bleiben, wenn Streit zwischen dem Telekommunikationsunternehmen und den Kunden über die Richtigkeit der Abrechnung entsteht.

Demgegenüber gibt es Überlegungen für eine neue Telekommunikations-Daten-schutzverordnung, daß alle Verbindungsdaten in der Regel selbst bei unbestrittenen oder bezahlten Rechnungen zwei Jahre lang nach Ende der Verbindung gespeichert bleiben können. Da die Speicherungsfrist erst am Ende des Jahres beginnen soll, in dem die Verbindung stattfand, kann dies in Einzelfällen dazu führen, daß die Daten bis zu drei Jahre lang vorgehalten werden.

Hiergegen wenden sich die Datenschutzbeauftragten des Bundes und der Länder mit Entschiedenheit. Sie sehen darin einen unverhältnismäßigen Eingriff in das Grundrecht der Telefonkundinnen und -kunden auf unbeobachtete Kommunikation.

Auch das Telekommunikationsgesetz hebt die Grundsätze der Verhältnismäßigkeit und der Zweckbindung ausdrücklich hervor. Personenbezogene Daten, die für Zwecke der Telekommunikation erhoben und verarbeitet werden, dürfen nur solange gespeichert bleiben, wie es zu diesen Zwecken erforderlich ist. Auch die vom Gesetz geforderte Höchstfrist für die Speicherung von Verbindungsdaten muß sich am Grundsatz der Datensparsamkeit orientieren, solange sich die Kundin und der Kunde nicht ausdrücklich für eine längere Speicherung entscheiden.

Die Dauer einer zivilrechtlichen Verjährungsfrist kann ebenfalls kein rechtfertigender Anlaß für eine solche Datenspeicherung sein. Jedenfalls müssen die Daten unverzüglich gelöscht werden, wenn die Rechnung beglichen und unbestritten ist und damit der vertragliche Speicherzweck erledigt ist.

Da eine telekommunikations- oder zivilrechtlich bedingte Notwendigkeit für eine derart lange Speicherfrist der Verbindungsdaten somit nicht ersichtlich ist, würde sie eine unzulässige Datenspeicherung auf Vorrat zu unbestimmten Zwecken darstellen.

Diese Speicherung von Kommunikationsdaten wäre auch nicht mit der Überlegung zu rechtfertigen, daß diese Daten zum Zwecke eventueller künftiger Strafverfolgung benötigt werden könnten. Die mit einer solchen Speicherung verbundene vorsorgliche Überwachung unverdächtiger Bürgerinnen und Bürger wäre unzulässig.

Anlage 22

Entschließung der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 1999:

Entwurf einer Ratsentschließung zur Überwachung der Telekommunikation (ENFOPOL ‘98)

Gegenwärtig berät der Rat der EU über den Entwurf einer Entschließung zur grenzüberschreitenden Überwachung der Telekommunikation und der Internet-Nutzung (ENFOPOL ‘98).

Die Konferenz der Datenschutzbeauftragten hält es für inakzeptabel, daß der entsprechende Entwurf bisher geheimgehalten und ohne Einbeziehung der Datenschutzbeauftragten beraten wird.

Sie fordert die Bundesregierung auf, der Schaffung gemeinsamer Standards zur grenzüberschreitenden Überwachung der Telekommunikation nur insoweit zuzustimmen, als damit nicht zusätzliche Eingriffe in das Grundrecht auf unbeobachtete Kommunikation und das Fernmeldegeheimnis verbunden sind und die Nutzung datenschutzfreundlicher Technologien (z.B. prepaid cards) nicht konterkariert wird.

Anlage 23

Deutsche Arbeitsgemeinschaft für Epidemiologie (DAE)
Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

Epidemiologie und Datenschutz

Einleitung

Die epidemiologische Forschung zielt nicht auf personenbezogene, sondern auf bevölkerungsbezogene wissenschaftliche Aussagen. Hierbei stützt sie sich jedoch in der Regel auf personenbezogene Daten zum Gesundheitszustand der Probanden, soziodemographische Angaben, Informationen über Risikofaktoren und oftmals medizinische Untersuchungsbefunde und Ergebnisse aus der Analyse biologischer Materialien. Die individuellen Untersuchungsergebnisse werden üblicherweise den Probanden mitgeteilt. Zur Durchführung der Forschungsprojekte werden vielfach Namen und Anschriften zur Kontaktaufnahme benötigt. Darüber hinaus muß eine korrekte Zuordnung von Follow-up-Ergebnissen sowie die Zusammenführung von Daten aus verschiedenen Quellen sichergestellt werden.

Epidemiologie und Datenschutz stehen traditionell im Spannungsfeld des Schutzes der Persönlichkeitsrechte der von der Datenverarbeitung Betroffenen und dem wissenschaftlichen Anliegen, durch das Auswerten von Gesundheitsdaten zu wichtigen und auf andere Weise nicht erreichbaren Kenntnissen zu gelangen.

Im Anschluß an eine Diskussion der datenschutzrechtlichen Fragen zwischen der Deutschen Forschungsgemeinschaft und dem Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben Epidemiologen und Datenschützer versucht, typische Problemfelder zu identifizieren und zu gemeinsamen Lösungsvorschlägen zu kommen. Die folgenden Vorschläge sollen den mit Datenschutzfragen bei epidemiologischen Studien befaßten Wissenschaftlern, Datenschützern, Ethikkommissionen, Behörden und Forschungsförderern zur Information und Orientierung dienen, um Probleme zu vermeiden, die durch fehlende Kenntnis der datenschutzrechtlichen Vorschriften, ungeeignet formulierte Einverständniserklärungen oder durch eine falsche oder

übervorsichtige Interpretation der Rechtsvorschriften zur Datenübermittlung für Forschungszwecke etc. bedingt sind.

1. Rechtliche Rahmenbedingungen für die Forschung mit personenbezogenen Daten

1.1 Forschung mit anonymisierten Daten

Die datenschutzrechtlichen Bestimmungen finden nur Anwendung, wenn für ein Forschungsprojekt personenbezogene Daten benötigt werden. Forschung mit anonymisierten Daten ist jederzeit ohne datenschutzrechtliche Vorgaben möglich. Ob es sich im konkreten Fall um personenbezogene oder um anonymisierte Daten handelt, bedarf allerdings sorgfältiger Prüfung. § 3 Abs. 7 BDSG enthält eine gesetzliche Definition des Anonymisierens. Dieser Definition zufolge ist Anonymisieren das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (sog. "faktische Anonymisierung"). Anonymisierung wird in der wissenschaftlichen bzw. datenschutzrechtlichen Diskussion ganz überwiegend im Sinne einer faktischen Anonymisierung verstanden. Einzelangaben sind z.B. dann keine anonymisierten Daten, wenn beim Forschungsinstitut bzw. beim Forscher lediglich eine organisatorische Trennung der Hilfsmerkmale von den übrigen Daten vorgenommen wurde oder wenn lediglich Name und Adresse der Betroffenen weggelassen wurden und die Betroffenen anhand der weiteren Angaben noch identifizierbar sind. Auch aggregierte Daten können nicht immer als anonymisiert qualifiziert werden. Im Einzelfall muß eine Risikoanalyse unter Berücksichtigung insbesondere des eventuellen Wertes der in Frage stehenden Daten für potentielle Interessenten sowie der dem Empfänger oder den potentiellen Interessenten zur Verfügung stehenden Ressourcen (Zusatzwissen, technische Möglichkeiten der Datenverarbeitung etc.) durchgeführt werden.

In einigen wenigen Bundesländern wird Anonymisierung im Sinne einer absoluten Anonymisierung verstanden, d.h. Einzelangaben werden nur dann als anonym qualifiziert, wenn sie unter keinen Umständen mehr zuzuordnen sind.

1.2 Forschung mit Einwilligung der Betroffenen

Personenbezogene Daten können im Rahmen der epidemiologischen Forschung auf der Basis einer Einwilligung der Betroffenen verarbeitet werden. Nach den datenschutzrechtlichen Regelungen muß die Einwilligung der Betroffenen bestimmte inhaltliche und formale Voraussetzungen erfüllen, damit sie rechtswirksam ist. Insbesondere müssen die Betroffenen über die vorgesehene Verarbeitung ihrer Daten informiert werden (Träger und Leiter des Forschungsprojekts, Zweck des Forschungsvorhabens, Art und Weise der Datenverarbeitung, Personenkreis, der von den personenbezogenen Daten Kenntnis erhält, Zeitpunkt der Löschung der personenbezogenen Daten etc.), damit sie die Tragweite ihrer Entscheidung erkennen können. Die Einwilligung muß in der Regel schriftlich erteilt werden, die gesetzlichen Regelungen sehen jedoch Ausnahmen vor. Ferner ist ein Hinweis erforderlich, daß die Einwilligung freiwillig ist, aus der Verweigerung der Einwilligung keine Nachteile entstehen und ein Widerruf der Einwilligung möglich ist. Einzelheiten sind den jeweils einschlägigen Regelungen zu entnehmen.

Verfügt die Forschungsstelle nicht über die Namen und Adressen der Personen, bei denen Einwilligungen eingeholt werden sollen, und kann sie sich diese Daten aufgrund der rechtlichen Regelungen (z.B. Meldegesetz) nicht beschaffen, so kann die Forschungsstelle die Betroffenen in der Weise kontaktieren, daß sie ihre Anschreiben, Merkblätter etc. in verschlossenen Umschlägen der Stelle übergibt, die über die Daten verfügt, damit letztere auf die Umschläge Namen und Adressen schreibt und die Anschreiben dann versendet. Auf diese Weise wird vermieden, daß die Daten Dritten zur Kenntnis gelangen. Dabei sollte für die Betroffenen in dem Anschreiben eindeutig erkennbar sein, daß ihre geschützten Daten von der Stelle, die über die Daten verfügt, nicht an die forschende Stelle weitergegeben wurden.

1.3 Forschung mit personenbezogenen Daten ohne Einwilligung der Betroffenen

Das Grundgesetz gewährleistet das Recht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts im Sinne von Artikel 2 i.V.m. Artikel 1 Grundgesetz. Ebenso gewährleistet das Grundgesetz die Freiheit von Wissenschaft und Forschung in Artikel 5 Grundgesetz. Diese beiden Grundrechte können bei Forschungsvorhaben, für die - zumindest vorübergehend - personenbezogene Daten benötigt werden, miteinander in Konflikt geraten. In dieser Situation ist es - wie auch

bei anderen Grundrechtskonflikten - in erster Linie Aufgabe des Gesetzgebers, diese potentiellen Konflikte so zu regeln, daß beide Grundrechte möglichst weitgehend realisiert werden können. Der Gesetzgeber muß die rechtlichen Rahmenbedingungen festlegen, unter denen personenbezogene Daten zu Forschungszwecken ohne Einwilligung der Betroffenen verwendet werden dürfen. Dabei sind auch die besonderen Schweigepflichten wie z.B. die ärztliche Schweigepflicht i.S.d. Berufsordnung und des § 203 StGB zu beachten. Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine Einschränkung des Rechts auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse und unter Beachtung des Grundsatzes der Verhältnismäßigkeit zulässig. Die Verarbeitung personenbezogener Daten muß für den angestrebten Zweck geeignet und notwendig sein und es darf keine Alternative geben, die die Betroffenen weniger belastet (z.B. Anonymisierungs- bzw. Pseudonymisierungsverfahren, Einwilligung der Betroffenen).

Gesetzliche Forschungsregelungen, die das Recht auf informationelle Selbstbestimmung und die Freiheit von Wissenschaft und Forschung in diesem Sinne zuordnen, sind z. B. in Landeskrankenhausgesetzen, Meldegesetzen, im Sozialgesetzbuch X, Krebsregistergesetzen, im Bundesdatenschutzgesetz und in Landesdatenschutzgesetzen enthalten. Entgegen dem allgemeinen Grundsatz der Zweckbindung personenbezogener Daten können nach diesen Regelungen unter bestimmten Voraussetzungen Daten, die zu einem anderen Zweck als wissenschaftlicher Forschung erhoben wurden, zu Forschungszwecken weiterverwendet werden.

2. Forschungsansätze in der Epidemiologie, Datenbedarf und Rechtsgrundlagen der Datenverarbeitung

Die Epidemiologie ist die Lehre von der Verteilung der Krankheiten und ihrer Risikofaktoren in der Bevölkerung. Aussagen epidemiologischer Forschung betreffen nicht das Individuum, sondern eine Bevölkerungsgruppe. Daher werden personenbezogene Daten nur für die Datenerfassung und ggf. spätere Kontaktaufnahmen sowie für die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen benötigt.

Als wichtigste epidemiologische Studientypen sind beispielhaft anzusehen:

- Bei Querschnittserhebungen wird typischerweise einmalig eine Befragung und/oder Untersuchung von Probanden durchgeführt. Diese werden persönlich um ihr Einverständnis gebeten. Die epidemiologische Fragestellung umfaßt z. B. die Charakterisierung von Erkrankungshäufigkeiten in der untersuchten Bevölkerungsgruppe oder den Zusammenhang zwischen dem Auftreten von Erkrankungen und Risikofaktoren. Aus datenschutzrechtlicher Sicht sind hier – wie auch bei den anderen Studienformen – die formalen und inhaltlichen Voraussetzungen der Einwilligungserklärung der Betroffenen zu beachten, ferner die jeweils einschlägigen Vorschriften zur Verarbeitung und Nutzung personenbezogener Daten durch die Forschungseinrichtungen (z.B. § 40 BDSG).

- Als zweiter Studientyp ist die Kohortenstudie zu nennen. Hierbei werden - z.B. ausgehend von einer Querschnittstudie - wiederholt Untersuchungen an denselben Probanden durchgeführt. Für diese Follow-up-Untersuchungen ist es erforderlich, personenbezogene Daten zu speichern, Anschriften zu aktualisieren etc. Diese Datenverarbeitung muß von den Einwilligungserklärungen umfaßt sein. Als epidemiologische Fragestellungen werden das Auftreten neuer Erkrankungen oder bestimmter Todesursachen im Zusammenhang mit bestimmten Risikofaktoren bearbeitet. Im letzteren Fall ist es zusätzlich erforderlich, über Einwohnermeldeämter und Gesundheitsämter den Vitalstatus sowie im Falle des Versterbens die Todesursache zu erheben. Als Rechtsgrundlage hierfür kommen die gesetzlichen Forschungsregelungen oder die Einwilligung der Betroffenen in Betracht.

- Einen Spezialfall von Kohortenstudien stellen retrospektive Kohortenstudien (mit zurückverlagertem Beginn) dar, die insbesondere im Bereich der Berufsepidemiologie häufig eingesetzt werden. Bei solchen Studien wird typischerweise aufgrund von betrieblichen Unterlagen die Exposition gegenüber bestimmten Arbeitsstoffen am Arbeitsplatz erhoben. Häufig interessiert das Auftreten von Krebserkrankungen oder das Versterben an bestimmten Todesursachen im Zusammenhang mit den beruflichen Expositionen. Hierbei ist es nicht ungewöhnlich, daß die Personen selbst nicht befragt werden, sondern daß ihre Exposition aus den betrieblichen Unterlagen bestimmt wird und die Krebserkrankung oder Todesursache durch Auswertung

eines Krebsregisters oder über Einwohnermeldeamt und Gesundheitsamt in Erfahrung gebracht wird. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kommen die gesetzlichen Forschungsregelungen oder die Einwilligung der Betroffenen in Betracht.

- Als weiterer epidemiologischer Studientyp ist die Fall-Kontroll-Studie zu nennen. Hierbei werden als Fälle Personen mit bestimmten Erkrankungen bezeichnet, die Kontrollpersonen gegenübergestellt werden. Fälle und Kontrollen werden im Hinblick auf in der Vergangenheit liegende Risikofaktoren befragt. Häufig ist es sinnvoll, Fälle aus Registern, z.B. Krebsregistern, einzubeziehen. Als Rechtsgrundlage kommen die gesetzlichen Forschungsregelungen, z.B. in Krebsregistergesetzen, oder die Einwilligung der Betroffenen in Betracht.

3. Typische Problemfelder

3.1 Zweckbindung von personenbezogenen Daten

Problem:

Personenbezogene Daten werden auf der Grundlage einer Einwilligung der Betroffenen oder einer gesetzlichen Forschungsregelung zu einem bestimmten Zweck, d.h. für eine konkrete epidemiologische Studie, erhoben. Aus wissenschaftlicher Sicht kann es allerdings später wichtig werden, diese Daten für die Bearbeitung neuer Fragestellungen zu nutzen, die zum Zeitpunkt der Einwilligungserklärung der Betroffenen bzw. der Übermittlungen der Daten noch nicht bekannt waren und daher in die Angaben zum Zweck der Verwendung der Daten nicht einbezogen wurden. Eine erneute Kontaktierung der Probanden ist häufig nicht möglich oder wäre mit zusätzlichem hohem Aufwand und Kosten verbunden und könnte wegen Umzug, Tod, Desinteresse etc. der Betroffenen auch zu Problemen im Hinblick auf die Repräsentativität der Daten führen.

Lösungsansätze:

- Soweit es sich um anonymisierte Daten handelt, unterliegt eine Zweckänderung der Daten keinen rechtlichen Beschränkungen. Die datenschutzrechtlichen Regelungen sind nicht anzuwenden. Dies gilt entsprechend für die Verwendung biologischer Materialien.

- Es besteht die Möglichkeit, Einwilligungserklärungen so zu formulieren, daß eine eventuelle inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mit umfaßt ist. Grundsätzlich muß eine Einwilligungserklärung hinreichend bestimmt sein. Die Anforderungen an die Vollständigkeit und Präzision der Einwilligungserklärungen können jedoch je nach der konkreten Verarbeitungssituation variieren. Bei der Verarbeitung personenbezogener Daten für eine wissenschaftliche Studie ist eine weitere Formulierung des Zwecks vertretbar und angemessen. Es ist die Entscheidung der Betroffenen, inwieweit sie auch eine Einwilligungserklärung mit einer weiteren Formulierung des Zwecks der Studie unterschreiben, d.h. es handelt sich um eine Frage der Akzeptanz. Die Einwilligungserklärung kann auch verschiedene Varianten der Verwendung der Daten enthalten, über die die Betroffenen entscheiden.

- Bei einer Übermittlung personenbezogener Daten auf der Grundlage einer gesetzlichen Forschungsregelung ist es vertretbar und angemessen, den Zweck der Übermittlung der Daten (d.h. die Darstellung des Forschungsvorhabens) so zu formulieren, daß eventuelle inhaltliche Änderungen bzw. Ausweitungen der Fragestellungen der Studie mit umfaßt sind.

- In Betracht kommt auch eine Anwendung der datenschutzrechtlichen Regelungen über die Zweckänderung personenbezogener Daten. Die rechtlichen Voraussetzungen für eine Zweckänderung sind im Einzelfall zu prüfen.

- Verfahrensrechtliche Lösungen wie z. B. Einschaltungen von Ethikkommissionen, Datenschutzbeauftragten etc. kommen im Regelfall nur dann in Betracht, wenn Rechtsvorschriften vorhanden sind, die grundsätzlich eine Zweckänderung der Daten unter bestimmten Voraussetzungen zulassen, denn weder Ethikkommissionen noch Datenschutzbeauftragte können ihre Entscheidung an die Stelle der Entscheidung der Betroffenen setzen.

3.2 Löschung der Daten nach Beendigung des Forschungsvorhabens

Problem:

Es ist offen, in welchem Umfang die Daten nach Beendigung des Forschungsvorhabens gelöscht werden müssen.

Lösungsansätze:

- Soweit die Daten anonymisiert sind, sind die datenschutzrechtlichen Regelungen nicht anzuwenden und die weitere Verarbeitung der Daten unterliegt keinen rechtlichen Beschränkungen.

- Werden personenbezogene Daten verarbeitet, sollte der Zeitpunkt der Löschung der personenbezogenen Daten in dem Text der Einwilligungserklärung bzw. dem Antrag auf Übermittlung der Daten konkret benannt werden. Ist im Einzelfall eine Speicherung anonymisierter Daten für die wissenschaftliche Nachprüfbarkeit der Forschungsergebnisse nach ihrer Publikation nicht ausreichend. so kann eine Speicherung der personenbezogenen Daten für einen bestimmten Zeitraum nach der Publikation der Forschungsergebnisse zur wissenschaftlichen Nachprüfbarkeit der Forschungsergebnisse zulässig sein. Der Zeitpunkt für die Löschung der personenbezogenen Daten sollte in der Einwilligungserklärung bzw. in dem Antrag auf Übermittlung der Daten möglichst konkret benannt werden.

3.3 Weitergabe anonymisierter Daten

Problem:

In einem Forschungsvorhaben erweist es sich als sinnvoll, anonymisierte Daten aus mehreren Studien zu poolen, d.h. zusammenzuführen und gemeinsam statistisch auszuwerten, weil sich für viele Fragestellungen nur dadurch ausreichend große Fallzahlen erreichen lassen. Auch eine Weitergabe von anonymisierten Daten in Form von Public Use Files kann sinnvoll sein, um die Daten anderen Wissenschaftlern für ihre Forschung zugänglich zu machen.

Lösungsansätze:

- Grundsätzlich können anonymisierte Daten ohne rechtliche Beschränkungen weitergegeben werden. Es muß allerdings im Einzelfall geprüft werden, ob es sich tatsächlich um anonymisierte Daten handelt und ob die Daten auch nach der Zusammenführung mit den Daten aus den anderen Studien noch als anonymisiert qualifiziert werden können. Eine Zusammenführung anonymisierter Daten aus mehreren Studien führt häufig dazu, daß eine Deanonymisierung der Daten noch schwieriger wird. Im Einzelfall kann es jedoch durchaus auch die Konstellation geben, daß anonymisierte Daten durch ihre Zusammenführung mit Daten aus anderen Studien leichter deanonymisiert werden können und dann u.U. als personenbezogen

qualifiziert werden müssen. In diesem Fall sind die datenschutzrechtlichen Regelungen zu beachten.

- Eine Übermittlung personenbezogener Daten ist nicht in jedem Fall ausgeschlossen. Es gilt das oben unter 3.1 Gesagte entsprechend.

3.4 Optimale Gestaltung der Einverständniserklärung bzw. des Antrags auf Übermittlung der Daten

Problem:

Einerseits sollten in der Einverständniserklärung bzw. in dem Antrag auf Übermittlung der Daten möglichst präzise die zu untersuchende Fragestellung, die Vorgehensweise und die an der Studie beteiligten Institutionen angegeben werden. Andererseits kann es sich im Laufe einer Studie ergeben, daß Kooperationspartner wechseln und sich Fragestellungen erweitern bzw. neue Fragestellungen auftauchen. Wie kann dies in der Einverständniserklärung bzw. in dem Antrag optimal berücksichtigt werden?

Lösungsansätze:

- Die Formulierung des Zwecks der epidemiologischen Studie kann so erfolgen, daß eine evtl. inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mit umfaßt ist (vgl. oben 3.1).

- Die datenverarbeitende Stelle - im Regelfall die Institution (Klinikum, Institut etc.) - muß in der Einwilligungserklärung bzw. in dem Antrag auf Übermittlung personenbezogener Daten konkret und verbindlich benannt werden. Aus datenschutzrechtlicher Sicht ist es von zentraler Bedeutung, daß die Verantwortlichkeit für die personenbezogenen Daten dauerhaft klar geregelt ist und der Bürger eindeutig darüber informiert ist, an wen er sich wo bei Auskunftsersuchen, Widerruf seiner Einwilligung etc. wenden kann. Die Namen der Kooperationspartner müssen nur dann konkret aufgeführt werden, wenn sie mit einer eigenständigen Auswertung der personenbezogenen Daten befaßt sind.

- Im Einzelfall ist es auch möglich, eine Klausel dahingehend aufzunehmen, daß Abweichungen von der angegebenen Vorgehensweise und Erweiterungen der

Fragestellungen nur nach Rücksprache mit dem zuständigen Datenschutzbeauftragten bzw. der Ethikkommission erfolgen.

3.5 Verknüpfung personenbezogener Datensätze (record linkage), z. B. bei Kohortenstudien

Problem:

Es soll eine Studie durchgeführt werden, bei der ein Abgleich verschiedener Datenbestände vorgenommen wird, die Betroffenen jedoch zu keinem Zeitpunkt direkt kontaktiert bzw. um Einwilligung gebeten werden. Ein Beispiel hierfür ist eine Studie, bei welcher die Expositionsbedingungen am Arbeitsplatz aus betrieblichen Unterlagen der dort tätigen Arbeitnehmer zusammengestellt werden. Die Erhebung der aufgetretenen Erkrankungen erfolgt über vorhandene Krankheitsregister (z.B. Krebsregister) oder über Einwohnermeldeämter und Gesundheitsämter zur Erhebung des Vitalstatus und der Todesursache.

Lösungsansätze:

- In einzelnen gesetzlichen Regelungen wie z. B. Krebsregistergesetzen ist ein Abgleich verschiedener Datenbestände vorgesehen. Im übrigen sehen die bundes- bzw. landesrechtlichen Regelungen - mit Unterschieden im einzelnen - grundsätzlich die Möglichkeit von Datenübermittlungen durch Betriebe, Einwohnermeldeämter, Gesundheitsämter, Krebsregister etc. vor (vgl. z.B. § 28 Abs. 2 Nr. 2 BDSG, Meldegesetze, Gesetze über den öffentlichen Gesundheitsdienst, Krebsregistergesetze, Forschungsregelungen im Bundesdatenschutzgesetz und in den Landesdatenschutzgesetzen). Die rechtlichen Voraussetzungen dieser Übermittlungsbestimmungen müssen im Einzelfall geprüft werden.

  Vor der Durchführung einer Studie sollte der Einsatz eines Treuhänders, d.h. eines vertrauenswürdigen Dritten, geprüft werden, der insbesondere personenbezogene Daten aus verschiedenen Quellen zuordnet, speichert und anonymisiert an die Forschungsinstitution übermittelt. Die Übermittlung personenbezogener Daten an einen Treuhänder bedarf ebenso wie die Übermittlung personenbezogener Daten an die Forschungsinstitution selbst einer Rechtsgrundlage. Der Einsatz eines Treuhänders kann jedoch im Einzelfall den Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung minimieren, indem der Kreis derjenigen

Personen, die personenbezogene Daten zur Kenntnis erhalten, reduziert wird und die Datensicherheit umfassender gewährleistet wird. Diese Aspekte haben Relevanz für die in vielen Forschungsregelungen vorgesehene Abwägung zwischen den schutzwürdigen Belangen der Betroffenen und dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens.

3.6 Nutzung der amtlichen Statistik

Problem:

Häufig werden von den statistischen Ämtern des Bundes und der Länder in der Praxis nur Daten übermittelt, bei denen eine Mindestzahl auftretender Konstellationen pro Zelle erfüllt ist. Hierdurch werden bestimmte Aussagen unmöglich gemacht, z.B. die Unterteilung einer Untersuchungsgruppe nach Altersklassen oder nach genaueren diagnostischen Einheiten wie Todesursachen.

Lösungsansätze:

Die statistischen Ämter des Bundes und der Länder dürfen faktisch anonymisierte Einzelangaben für wissenschaftliche Vorhaben an Hochschulen und andere Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung übermitteln, wenn die Empfänger Amtsträger, für den öffentlichen Dienst Verpflichtete oder nach § 16 Abs. 7 Bundesstatistikgesetz Verpflichtete sind (§ 16 Abs. 6 BStatG). Die Daten sind zu löschen, sobald das Vorhaben durchgeführt ist, eine verbindliche Löschungsfrist besteht nicht (§ 16 Abs. 8 BStatG).

Es besteht die Möglichkeit, aus bereits vorliegenden Individualdaten faktisch anonymisierte Einzelangaben zu bestellen. Von diesem Weg wird jedoch häufig aus Kostengründen Abstand genommen. Für einige Bereiche sind faktisch anonyme Daten auf Vorrat erstellt worden, z.B. aus dem Mikrozensus 1995 und der Einkommens- und Verbrauchsstichprobe 1993. Einzelangaben aus solchen Beständen können gegen geringe Gebühr bezogen werden, die breite Anwendung dieser Verfahren wird aber durch Geldmangel behindert.

Leichter verfügbar sind statistische Tabellen, die i.a. dadurch anonymisiert sind, daß Felder mit geringen Belegungen so zusammengefaßt wurden, daß Zahlen kleiner als 3 nicht mehr auftreten. Dies ist für Forschungszwecke oft hinderlich. Soweit jedoch die Angaben aus Feldern mit zu geringer Belegung nicht mehr erkennen lassen, als

nach § 16 Abs. 6 BStatG übermittelt werden darf, und auch die weiteren Bedingungen dieser Vorschrift erfüllt werden, bestehen keine datenschutzrechtlichen Bedenken gegen die Übermittlung auch solcher Tabellen mit faktisch anonymisierten Einzelangaben.

3.7 Aufbewahrung von Daten der amtlichen Statistik

Problem:

Die Löschung älterer Datenbestände kann der epidemiologischen Forschung unwiederbringlich Grundlagen entziehen.

Lösungsansätze:

Abgesehen von den Hilfsmerkmalen (insbesondere Namen und Anschriften) gibt es i.a. keine gesetzlichen Löschungsfristen für statistische Einzelangaben. Die Löschungspraxis richtet sich nach der Einschätzung des zu erwartenden Nutzens aus der weiteren Aufbewahrung im Verhältnis zu deren Kosten. Datenschutzrechtlich zulässig wäre eine weitere Speicherung statistischer Einzelangaben auch für zukünftig erwartete, aber noch nicht im einzelnen bekannte Zwecke. Vor Löschung der Daten sind diese nach den jeweils geltenden archivrechtlichen Bestimmungen den zuständigen Archiven anzubieten. Zur Dauer der Speicherung der Daten bei den statistischen Ämtern bzw. bei den Archiven sollte aus dem Wissenschaftsbereich der Bedarf dargelegt werden. Die Aufbewahrung der Totenscheine (im Original) richtet sich nach dem jeweiligen Landesrecht.

3.8 Nutzung von Krebsregistern für Fall-Kontroll-Studien

Problem:

Bei Fall-Kontroll-Studien wird häufig ein (möglichst repräsentativer) Zugang zu bestimmten Erkrankungsgruppen benötigt. Dieser kann unter hohen Kosten auf der Grundlage von Einwilligungen der Betroffenen oder gesetzlichen Forschungsregelungen über Krankenhäuser erfolgen, in denen diese Patienten behandelt werden. Ein effektiverer und vollständigerer Zugang ist aber derjenige über Krankheitsregister (z.B. Krebsregister). Der Zugang über das Register dient dabei nur der Auffindung des Patienten und der Kontaktaufnahme mit ihm, alles weitere kann durch die Einverständniserklärung der beteiligten Personen abgedeckt werden. Diesen Patienten

werden dann Kontrollpersonen aus der Bevölkerung gegenübergestellt, die auf anderem Wege kontaktiert und in die Studie einbezogen werden.

Lösungsansätze:

- Gemäß § 8 des Krebsregistergesetzes des Bundes (KRG) können für Maßnahmen des Gesundheitsschutzes und bei wichtigen und auf andere Weise nicht durchzuführenden, im öffentlichen Interesse stehenden Forschungsaufgaben die zuständigen Behörden der Vertrauensstelle des Krebsregisters die Abgleichung Personen identifizierender Daten mit Daten des Krebsregisters und die Entschlüsselung der erforderlichen verschlüsselten Identitätsdaten und deren Übermittlung im erforderlichen Umfang genehmigen.

  Vor der Übermittlung personenbezogener Daten hat die Vertrauensstelle über den meldenden behandelnden Arzt oder Zahnarzt die schriftliche Einwilligung des Patienten einzuholen. Ist der Patient verstorben, hat die Vertrauensstelle vor der Datenübermittlung die schriftliche Einwilligung des nächsten Angehörigen einzuholen, soweit dies ohne unverhältnismäßigen Aufwand möglich ist.

- Die Länder können in ihren Gesetzen zur Ausführung des Krebsregistergesetzes abweichende Regelungen treffen (§ 13 Abs. 5 Nr. 2 KRG). Einige Länder haben vom Krebsregistergesetz des Bundes abweichende datenschutzrechtliche Modelle (z.B. keine Aufgliederung des Registers in Vertrauensstelle und Registerstelle) gewählt. Im Einzelfall sind die einschlägigen Übermittlungsbestimmungen zu prüfen und zu beachten.

3.9 Datenschutzfragen bei bundesweiten Studien

Problem:

Bei Studien, die in mehreren Bundesländern stattfinden, sind häufig die unterschiedlichen datenschutzrechtlichen Regelungen der Bundesländer zu berücksichtigen.

Lösungsansätze:

Zur Vereinfachung des Verfahrens kann der Studienleiter den für ihn zuständigen Datenschutzbeauftragten bzw. denjenigen Datenschutzbeauftragten, in dessen Bundesland die zentrale Speicherung der Daten des Forschungsprojekts erfolgen soll,

darum bitten, die Stellungnahmen der anderen Datenschutzbeauftragten (soweit von dem konkreten Forschungsprojekt betroffen) zu koordinieren.

Redaktion: Wichmann, H. E.; Raspe, H. H.; Jöckel, K. H. für die Deutsche Arbeitsgemeinschaft für Epidemiologie; Hamm, R.; Wellbrock, R. für den Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Stichwortverzeichnis *

A

Abgabenbescheid	II/81
Abgabenordnung	I/48, 52, 160; II/39; III/33f; IV/29
Abrufverfahren, automatisiertes	III/28, 30, 35, 51, 95, 113f; IV/13
Abschottung	III/32, 134; IV/61
Abwasserzweckverband	III/146; IV/135
A-Card	II/55
Adreßbücher	I/39; II/24; III/18
Adreßmittlungsverfahren	III/17, 40, 42
Akteneinsicht in Strafakten	IV/87, 106
- an Krankenkassen	III/94, 111
- an Versicherungen	III/94; IV/118
Akteneinsichtsrecht	IV/118
- der Gleichstellungsbeauftragten	I/90; III/76
- in Krankenakten	I/64
- in Umweltakten	II/157
Aktenvernichtung	II/64, 73, 107; IV/52
Aktenvollständigkeit	II/94
Altakten	II/14, 64
- bestände	II/16; III/83
ALB	IV/17
Altdatenbestände	I/24; II/14, 15, 107, 124; III/83
Altenheime	III/124, 125
Ämter für Landwirtschaft und Flurneuordnung	III/20, 73f
Ämter zur Regelung offener Vermögensfragen	I/159; II/169, 170
Amtsverschwiegenheit	II/81
Anonymisierung	I/55, 124; IV/27, 72
APIS	I/111
Arbeitnehmerdatenschutz	I/83
Arbeitsunfähigkeitsbescheinigungen	IV/76
Architektenkammer	II/59
Archivwesen	I/23; II/14; IV/9
Ärzte	I/59, 60, 61, 65
- Attest	II/76; IV/76
- Schweigepflicht	I/61; III/13, 45; IV/40, 114, 118
- Standesrecht	III/45, 47
Asylverfahren	I/31; II/20
Aufbewahrungsbestimmungen der Justiz	I/120; II/111; III/93; IV/96
Aufsichtsbehörden nach § 38 BDSG	I/10, 19
Auftragsdatenverarbeitung	I/47; II/65, 67; III/36, 49, 131; IV/1, 37, 51
Ausgleichsabgabe nach SchwbG	II/147

* Fundstelle zitiert nach Tätigkeitsbericht und Seite

Auskünfte
- an Ausländerbehörde III/14f
- aus dem Gewerberegister I/67
- durch Kommunalverwaltung II/77
- nach dem Vermögensgesetz III/145f
Auskunftsersuchen
- der Behörden aus dem Melderegister II/24
- der Steuerfahndung I/52
Ausländer
- Auslandsstraftaten I/32; II/21
- beauftragter III/71
- behörde III/5, 14f; IV/11
- datei III/14
- dateienverordnung II/20
- gesetz I/30, 33; II/19
- Kostenabrechnungsverfahren IV/10
- zentralregister II/19
Ausreiseunterlagen der ehemaligen DDR I/28,29
Ausweiswesen I/35; II/22
Autobahnmaut II/162; III/140

B
Bauordnungsamt II/27, 29
Behinderte II/42; III/38, 80
Beitrags- und Gebührenschuldner IV/135
Beratung der Kommunen I/77
Berufsschulwesen II/136
Beschäftigungsförderung IV/38
Bestattungstermin IV/65
Besucherverkehr II/69
Betriebe
- gärtnerische III/73f
- landwirtschaftliche III/73f
Bewachungsgewerbe IV/135
Bewerberdaten I/89; II/91; III/76; IV/78
Bewertungsgesetz III/74
Bewertung von land- u. forstwirtsch. Vermögen I/50
Bezügedaten
- der Lehrer III/75
BKK-Card II/55
Bodenreform III/20f
Bodenschätzung III/73f
Bosnische Bürgerkriegsflüchtlinge III/15f
Bundesamt für die Anerkennung ausländischer Flüchtlinge III/15
Bundeskriminalamt (BKA) II/98
Bundesnotarordnung III/112
Bundeszentralregister I/114, 122; II/128
Bußgeldstelle, Zentrale II/76
Bußgeldverfahren I/43; II/76, 168

C

CD-ROM III/18, 62
Chipkarten II/55; III/2, 47, 117; IV/41
Computerviren II/72; III/66; IV/25, 54, 79

D

Dateienregister I/21, 134; II/44; III/8; IV/6
- meldung I/22; II/12, 44; III/10; IV/6, 35
Datenabgleich von Ausbildungsverhältnissen IV/45
Datenlöschung II/71,107; III/12
Datenschutzfreundliche Technologien IV/24, 27
Datenschutz im nicht-öffentlichen Bereich I/19
Datenschutzrichtlinie der EU IV/18
Datensicherheit I/71, 75; II/64; IV/1, 21
Datensparsamkeit IV/27
Datenträger
- aufbewahrung I/71
- austausch II/72
- kontrolle IV/57
Datenübermittlung im Internet IV/50
Datenverarbeitung
- in der Landesverwaltung I/43; II/35; III/25; IV/21, 24, 48, 60
Datenvermeidung IV/1, 27
Datumsumstellung IV/48
Deanonymisierung II/151
Denkmalschutz II/29
DiagnostiX-Card II/55
Diebstahl
- von Hardware II/65
Dienstordnung für Notare III/112
Diplomarbeit III/16
Dissertation IV/58
DNA
- Identitätsfeststellungsgesetz IV/94
Domain Name Service III/32
Drogen I/105, 115; II/102
Duplikatakten I/109; II/106; III/90

E

Ehescheidungsverbundurteile II/113
Einbürgerungsverfahren
- Mitwirkung des Verfassungsschutzes II/162
Eingriffsbefugnisse, staatliche III/103, 170
Einigungsvertrag I/3, 24, 26, 29, 37, 50, 59, 66, 93; II/167
Einkommensteuerbescheid III/45f
Einkommens- und Verbrauchsstichprobe IV/121

Einstellungsbescheid, staatsanwaltschaftlicher III/109f
Einwendungen
- im Raumordnungsverfahren III/19
Einwohnermeldeamt I/63; II/25; IV/11, 12, 13 133
Einzelnutzer-Betriebssystem I/70
Elektronisches Grundbuch IV/21
Elektronisches Mitteilungssystem II/36; III/27
Elternbeiträge in Kindertageseinrichtungen III/123
E-Mail III/28, 32, 59; IV/1, 25, 50, 54
Entwicklungsträger im Städtebau III/145
Epidemiologie IV/39
Erhebungsmerkmal IV/121
Erkennungsdienstliche Behandlung I/32, 114; II/100; III/185; IV/79, 82
Errichtungsanordnung III/10, 84f, 98
Ersatzwirtschaftswert I/50
Erwachsenenbildung III/41
EUROCAT-Registration II/51
Europäische Union II/30; III/7, 22, 23; IV/18
Europol II/33; III/8, 23ff, 152, IV/5, 19

F
Fahrerlaubnis I/157; II/164; IV/127
Fahrerlaubnisregister, Zentrales IV/127
Fahrerlaubnis-Verordnung IV/129
Fahrzeugregister II/167; III/141
Familiennachzug III/15
Fehlbildungsregister, Magdeburger II/50; III/41
Fernmeldegeheimnis III/103, 151
Fernmeldeüberwachung III/136, 138
Fernschreiben III/83
Fernwartung II/67
Finanzämter I/44, 50; II/42; IV/33, 34
Finanzrechenzentrum I/44
Firewall IV/21, 26, 60
FISCUS IV/21
Flurbereinigungsgesetz III/73; IV/16
Fördermittel
- zweckentsprechende Verwendung IV/68
Forschungsdaten aus Melderegister IV/39
Forschungsvorhaben III/17, 39; IV/37, 38
Fragebogen
- für Bezüge I/86
- für Personal I/85, 96; III/2, 78; IV/69
Frauenfördergesetz II/96; III/76
Frontfoto III/143
Führerschein I/105; II/102, 164
- akte II/166
- stelle II/165

G
Gauck
- Bescheide III/78
- Mitteilungen III/81
- Überprüfungsverfahren vor Personalkommission IV/75
Gebäude- und Wohnungszählung III/130
Gebäudevermessung IV/132
Gebührendatenerfassung II/70
Gefangene III/100, 136ff, 164; IV/123, 124
- Personalakten II/156; III/136f
Geldwäschegesetz II/119; III/105f, 117; IV/97
Gemeindeverwaltung II/77
Gemeinschaftsausschuß IV/59, 63
Gerichte
- Aufbewahrungsbestimmungen für das Schriftgut I/120; II/110
- Mitteilungen der I/117; II/111
Gerichtsvollzieher I/128; II/115, 116
Gerontologische Studie II/49
Geschäftsstelle des Landesbeauftragten I/15
Gesundheitsamt I/57, 61, 63, 66; II/56; III/120
Gesundheitswesen I/59; IV/40, 41
Gewerbe
- aufsicht IV/45
- ordnung I/67; II/60
- register I/67
- steuer I/53
- zentralregister IV/46
GEZ I/136; II/132; III/118
Gleichstellungsbeauftragte I/90; III/76
Großer Lauschangriff III/94, 96, 172f; IV/90
Großrechenzentren I/44
Grundbedrohungen der IT I/69
Grundbuch I/126, 161; II/46, 114; III/20f; IV/17, 21
- archiv II/75
Grunderwerbsteuer IV/30
Grundsteuer I/51, 161; II/38, 46, 82

H
HAMISSA IV/21
Handbuch der Justiz I/91
Handelsregister III/49, 51
Handwerksordnung II/59; IV/43
Hauptsatzung der Gemeinden I/80
Heimarbeitsrecht I/68
Hilfsbeamte der Staatsanwaltschaft III/88, 104f; IV/99
Hoax-Virus IV/54
Hochschule I/75; II/76; III/66; IV/58
Hotelmeldepflicht II/22

Hundesteuer II/45; IV/29

I

Identitätsfeststellung I/32
Impfdaten (von Kindern) IV/40
Industrie- und Handelskammer II/61; III/5, 48; IV/47
Informationsgesellschaft III/103
Informationstechnisches Netz Sachsen-Anhalt (ITN-LSA) I/43; II/37; III/29; IV/21, 26, 60, 79
Innerbehördlicher Datenschutzbeauftragter I/73
Insolvenzstatistik I/148
Institut für Datenschutz und Datensicherheit I/75
Integriertes Verwaltungs- und Kontrollsystem (InVeKoS) I/81; II/88; III/72
Interministerieller Arbeitskreis IT I/41
Internet III/9, 31, 51f, 54,103; IV/1, 26, 44, 50, 54, 60, 89
Internet-Dienste III/28, 30, 32, 55, 58
INTRANET LSA III/28, 32
INPOL I/102; II/107
IT-Grundsätze I/42; IV/21
ITN-LSA IV/21, 26, 60, 79
IuK-Arbeitsgruppe I/42

J

Jahr 2000 IV/48
Jugendamt II/145; III/129
Jugendhilfe II/144; III/123; IV/111
Juristenausbildung I/124, 126; II/130, 131; III/116

Justiz
- akten I/120, 121; II/109, 131
- beitreibungsordnung III/116
- ministerialblatt IV/72
- mitteilungsgesetz I/117; II/111; III/90f; IV/86

Justizvollzugsanstalt I/150; II/155, 156; III/136

K

Katasteramt I/45; II/47; III/38; IV/132
Katastrophenschutz IV/64
Kaufvertrag III/21f
Kfz
- Halterdaten III/86
- Zulassungsstelle II/165, 166

Kindergeld II/146
Kindertagesstätten II/143; III/3, 123; IV/112
Kirchen I/136; II/25
- steuer II/41
- Datenschutz II/131

Klassentreffen
- Adressen II/140

Klinisches Tumorregister II/53; III/40
Kommunalabgabengesetz III/147
Kommunalaufsicht II/78
Kommunale Gebietsrechenzentren I/47
Kommunalstatistik III/133
komsaNet IV/60
Konferenz der DSB des Bundes und der Länder I/20
Konkurrentenklage IV/70, 72
Kontrollkompetenz des Landesbeauftragten I/128, 132; IV/108
Kontrollsystem zur Landwirtschaftsförderung I/81; II/88; III/72
Korruptionsregister IV/46
KpS I/108, 113; II/106; III/88f; IV/82
Krankenakten I/64; II/157
Krankenhaus I/61, 64, 66; II/56; III/44, 128; IV/116, 117
Krankenhausentlassungsbericht IV/114
Krankenkassen I/141; III/111, 126, 129; IV/115, 116, 118
Krankenversicherungskarte II/54
Krankmeldungen IV/76
Krebsregister I/59; III/42
Kreisarchiv II/18
Kreisbereisungen I/17, 74, 77
Kriminalakten I/112; II/103, 106, 107; IV/79
Kriminalstatistik I/106
Kryptographie III/2, 61
Kündigungen II/95
Kurtaxe III/37

L

Länderübergreifendes staatsanwaltschaftliches Verfahrensregister III/98, 105f
Landesamt f. Landesvermessung u. Datenverarbeitung I/45
Landesarchivgesetz III/12, 14
Landeselternrat III/121; IV/109
Landesjustizprüfungsamt III/116
Landeskriminalamt III/117
Landespressegesetz III/101; IV/106
Landesrechenzentrum I/44; II/74
Landesrechnungshof I/96, 129; II/40
Landesschülerrat IV/109
Landesstatistikgesetz II/150; III/2, 130
Landeszuwendungen II/143
Landtag I/1ff, 11, 16ff; II/82; III/69, 71; IV/65
Landtagsausschuß II/84
Landwirtschaft I/50, 81; II/88, 89; III/20, 72, 73f
- Fördermittel IV/68
Lauschangriff I/116; II/109; IV/90

Lebenslauf IV/58
Lehrer
- ausbildung II/92
- gehälter III/75
- personaldaten IV/75
Lehrlingsrolle IV/43
Leitstelle für IT I/42
Lichtbildvorlage im Ermittlungsverfahren I/111; II/100; IV/84, 96
Liegenschaftsinformationssystem (SOLIS-G) II/62
Lohnsteuerkarte II/25, 41, 42; III/36f; IV/51, 69

M
Magnetstreifenkarte II/55
Mainzer Modell II/50
Maßregelvollzugsgesetz I/151
Matrikelbuch III/66
MDR I/137
Medizinische Daten IV/40
Medizinische Unterlagen III/13, 45
Medizinischer Dienst IV/114, 117, 118
Mehrfachtäter III/27, 145
Meldebehörde II/23; IV/11, 12, 13, 133
Meldeformular I/21; II/11
Meldegesetz I/33, 39, 63; II/22
- Meldedatenübermittlungsverordnung I/35; II/23; IV/13
Meldepflicht bei Auslandsstraftaten III/104
Melderegister II/23
Melderegisterauskunft
- automatisiertes Abrufverfahren IV/13
- für Verkehrssicherheitsaktion IV/11
- für Wahlen IV/12
Meldungsübermittlungssystem III/27
Methadonbehandlung II/57
Mikrofilme II/17
Mikrozensus I/147; II/151, 152; III/132; IV/122
MiStra I/117; II/111, 195; III/91
Mitbestimmung II/96
MiZi I/117; II/195; III/91
MS-DOS/WINDOWS I/46
Mütterberatung I/61

N
NADIS III/140
- Richtlinien II/159
Netze
- Landesnetz (ITN-LSA) I/43; II/37; III/28, 30; IV/21, 26, 60, 79
- lokale II/35
Notare I/132ff; III/21, 112
- Dienstordnung III/112; IV/108

Notarzteinsatzprotokoll II/57; III/45
NUB-Richtlinien II/56

O
Öffentlichkeitsfahndung III/94f, 100ff, 167; IV/87, 89, 96
Öffentlich-rechtliche Religionsgesellschaften II/131
Öffentlich-rechtliche Rundfunkanstalten I/136; III/118
Ökologischer Landbau III/139
Optische Datenspeicherung III/62
Ordnungswidrigkeiten II/168
Organisationskontrolle I/71
Organisierte Kriminalität I/115
Organtransplantationsgesetz III/43

P
Paßwort IV/55
Patientendaten IV/40, 116
PC
- Einsatz I/46
- Sicherheitsprodukte I/70
Personal
- akten I/83, 87; II/92, 94, 96; III/75 ff; IV/63, 70, 73, 76, 78, 123
- auswahlverfahren II/79, 95; IV/78
- daten IV/58, 59, 62, 69
- der Kommunen I/79
- fragebogen I/85, 96; IV/69, 75, 77
- Kontrollkarten - Schule II/136
- nachrichten II/89
Personalausweis II/26
Personalcomputer, private III/87
Personalvertretung II/96; III/81; IV/69, 77
Personenstandsfälle III/68
Petitionen II/85; IV/65, 99
Petitionsgesetz II/87
Pfändungs- und Überweisungsbeschlüsse II/115
Pflegeversicherung IV/118
PIOS I/111
Planfeststellungen IV/14
POLIS-neu IV/21, 79, 84
Polizei
- Aktenbehandlung IV/81
- Computerviren IV/79
- Datenverarbeitung, automatisiert IV/79
- Duplikatakten I/109; II/106; III/90
- Praktika von Jurastudenten II/130; III/116
- Praktika von Schülern II/108; III/116
- Strukturreform III/85, 89; IV/24
- Vorgangsbearbeitung I/106
Posteingangsstellen II/56

Postprivatisierung III/88, 105; IV/99
Praktikanten III/44, 116
Presse- und Öffentlichkeitsarbeit III/101f; IV/106
Prozeßkostenhilfe III/115f
Prüffristen II/104, 107; IV/79
Prüfungsakten I/124; II/131
Prüfungseinrichtungen III/126
Prüfungsordnung III/53
Prüfungsunfähigkeit II/76
Pseudonymisierung IV/27

R
Ratenzahlungen III/38
Ratssitzung IV/58
Raumordnungsverfahren III/19
Rauschgifthandel I/115
Realsteuer I/53, 160
Rechnungshof I/96; II/40
Rechtsanwalt I/123; II/169
Rechtsextremistische Gewalt II/48
Regierungsbezirkskasse III/115
Regreßverfahren III/127
Reisepaß II/26
Reihenuntersuchungen an Schulen III/120
Religionsgesellschaft II/131
Religionsmerkmale II/25, 41
Rettungsdienst II/57
Rettungswesen I/60
Rheumadokumentation II/50
RiVASt I/32, 118; II/120; III/104
Röntgen-Card II/55
Rundfunkgebührenpflicht II/134; III/119

S
Sachverständige IV/44, 127, 129
Schengener Durchführungsübereinkommen (SDÜ) II/31
Schriftgut der Justiz I/120; II/117, 127
Schriftgutvernichtung IV/34
Schuldnerverzeichnis I/127; II/109, 112; III/113f; IV/107
Schulentwicklungsplan IV/109
Schüler
- akten II/141
- Daten auf privaten Rechnern I/139; II/142
- Daten im Internet III/121
- fotos II/138; III/122
- praktika II/108
Schulgesetz II/135
Schulwechsel IV/110
Schutzstufenkonzept II/68
Schwangerschaftsabbruchstatistik III/135
Schwerbehinderte II/42, 148; III/38, 80

Sicherheitsdienste	II/61
Sicherheitsdomäne	IV/53
Sicherheitskonzept	IV/26, 60
Sicherheitsrisiken im Internet	III/55, 58
Sicherheitsüberprüfung	II/161
Signierblatt (Vergütung)	III/78
SIJUS	
- Strafsachen	I/131; II/122; III/2, 11, 108f
SOG LSA	I/99, 105, 113; II/105
Sozialgeheimnis	I/140; II/148; IV/112
Sozialhilfe	
- dynamik	II/52
- empfänger	I/142
- statistik	II/155
Sozialleistungen	I/74, 143; II/147; IV/119
Spielbank	II/43
Staatsanwaltschaft	I/117, 118, 120, 131; II/118, 121ff, 124; III/2, 5, 11f, 85f, 88, 90, 93f, 104ff, 117, 165, 173; IV/98, 99f, 102, 103,
Staatsanwaltschaftliches Informationssystem (SISY)	II/118
Städtebau	
- Entwicklungsmaßnahme im	III/145
Stadtratssitzung	IV/58
Standesamt	I/63
Stasi-Unterlagen-Gesetz	I/37, 144, 146; II/149; IV/135
Statistik	I/147; II/150
- geheimnis	II/150
- Verknüpfungen verschiedener	II/153
Statistisches Landesamt	I/147
Statistisches Veröffentlichungsprogramm	II/150
Stellenbesetzungslisten	II/78
Steuer	
- akten	IV/33
- beraterkammer	IV/36
- bescheid	I/54
- datenabrufverordnung	II/39; III/34
- fahndung	I/52; IV/31
- geheimnis	I/48, 51; II/38, 39; IV/28, 30, 69
- meßbetrag	I/51
- verwaltung	I/44
Strafverfahrensänderungsgesetz	III/89, 94; IV/87
Strafvollzug	I/150; II/155, 156
Strafvollzugsgesetz	III/136; IV/123
Straßenbenutzungsgebühr	II/162
Straßenverkehrsgesetz	I/156; III/141; IV/127

Studierende III/44
- Daten I/76
- Praktikum III/116

T
Täter-Opfer-Ausgleich II/129; III/107; IV/102
Telefax II/91; III/62ff, 98, 117; IV/49, 98
Telefon
- Ab-/Mithören II/110
- gesprächsaufzeichnung II/101; III/83
- verzeichnis III/79
Territoriale Grundschlüsseldaten (TGS) II/46
Tierseuchengesetz I/82
Transportkontrolle II/74
Tumorregister II/53; III/40

U
Überwachung
- des Besuchs III/137f
- des Schriftverkehrs III/124, 137f
- von Telefonaten III/137f
Umgangsrecht mit Kindern II/145
Umweltinformationsgesetz III/139
UNIFA IV/21
Unterhalt
- Auskunft des Ehegatten I/141
- Auskunftspflicht des Unterhaltspflichtigen III/129
Unterrichtung III/91
Unterrichtungspflicht IV/51, 86
Untersuchungshaft III/138f; IV/124

V
Verdachtsanzeigen III/105f, 117; IV/97
Verdienstbescheinigungen III/14
Verfahrensregister II/118; III/98, 105f; IV/98
Verfassungsschutz IV/127
Verkehr
- Ordnungswidrigkeit I/154; III/143, 145
- Zählung I/158
- Zentralregister I/157; II/164; III/141f
Vermessungsingenieur IV/132
Vermögensgesetz I/159; II/169, 170; III/145f
Vermögensverzeichnis
- im Betreuungsverfahren IV/107
Vernetzung
- lokal III/26, 29, 61
- überregional III/27, 29, 61, 88
Verpflichtungsgesetz III/116
Verschlußsachen III/84, 140

Verschlüsselung III/2, 30f, 61, 63, 117; IV/25, 26, 50
Vertrauenspersonen (V-Personen) II/99
Verwaltungsvorschriften zum DSG-LSA I/9
Videoüberwachung IV/84
VitalCARD II/55
Vorkaufsrecht III/21

W
Waffenrecht IV/135
Wählerverzeichnis II/172
Wahllichtbildvorlagen I/110; II/100; III/89; IV/84, 96
Wahlrechtsausschluß II/172; IV/133
Wahlvorschlag II/171
Wartung von Datenverarbeitungsanlagen II/67
Wassergesetz II/173
Wohnberechtigungsschein IV/113
Wohngeldempfänger I/143
Wohnraumüberwachung
- parlamentarische Kontrolle IV/92
Wohnungsstatistikgesetz II/154

Z
Zensus 2001 IV/120
Zentrale Stelle IT I/41
Zentrales Einwohnermelderegister (ZER) I/36
Zentrales Fahrerlaubnisregister III/142; IV/127
Zerlegungsmitteilungen I/53
ZEVIS III/86
Zugangskontrolle
- im ADV-Bereich I/71; II/74
- kriminalpolizeiliche Beratungsstelle II/65
Zustellung
- von Unterlagen einer Ratssitzung III/67f
Zwangsversteigerung III/114f