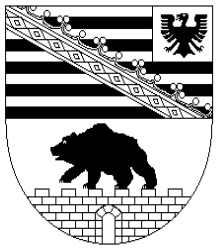
Landesbeauftragter
für den Datenschutz
Sachsen-Anhalt



III. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

**für die Zeit
vom
1. April 1995 bis 31. März 1997**

Inhaltsverzeichnis

Anlagen

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
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS - Innere Sicherheit
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
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

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

E

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

FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit
FRV	Fahrzeugregisterverordnung
FTP	File Transfer Protocol
FVG	Finanzverwaltungsgesetz

G

GBl.	Gesetzblatt der DDR
GBO	Grundbuchordnung
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

HGB	Handelsgesetzbuch
HTML	HyperText Markup Language; Definitionssprache für WWW-Dokumente
HTTP	HyperText Transport Protocol; Protokoll zur Kommunikation zwischen WWW-Client und WWW-Server

I

HK	Handwerkskammer
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
KpS	Kriminalpolizeiliche personenbezogene Sammlungen
KunstUrhG	Kunsturheberrechtsgesetz

L

LAN	Lokal Area Network
LKA	Landeskriminalamt
LKO LSA	Landkreisordnung des Landes Sachsen-Anhalt
LSA	Land Sachsen-Anhalt

M

MAN	Metropolitan Area Network
MBl. LSA	Ministerialblatt des Landes Sachsen-Anhalt
MdE	Minderung der Erwerbsfähigkeit
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

OECD	Internationale Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
OLG	Oberlandesgericht
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgift-handels und anderer Erscheinungsformen der organisierten Kriminalität
OVG	Oberverwaltungsgericht
Owi	Ordnungswidrigkeit
OWiG	Ordnungswidrigkeitengesetz

P

PC	Personal Computer
PersVG LSA	Landespersonalvertretungsgesetz Sachsen-Anhalt
PKH	Prozeßkostenhilfe
PKZ	Personenkennziffer
POLAS	Polizeiliche Auskunftssysteme
POLIS	Polizeiliches Informationssystem
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)
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
TÜV	Technischer Überwachungs-Verein

U

UIG	Umweltinformationsgesetz
UVollzG	Gesetz über den Vollzug der Untersuchungshaft

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
VermG	Vermögensgesetz
VO	Verordnung
VONot	Verordnung über die Tätigkeit von Notaren in eigener Praxis
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

In der Entwicklung des Datenschutzes zeigen sich bundesweit drei Trends:
Die rechtliche Absicherung des Grundrechts auf informationelle Selbstbestimmung in den vom Bundesverfassungsgericht geforderten bereichsspezifischen Regelungen stagniert (z.B. in der StPO), in einigen Bereichen (z.B. im SGB) wurde der gesetzlich gewährte Schutz unter Hinweis auf mehr Verwaltungsökonomie und die Eindämmung von Kosten sogar wieder aufgegeben oder zumindestens aufgeweicht. Vom überzogenen Schutz des einzelnen ist plötzlich wieder die Rede, der sich mit den Interessen der Gesamtheit aller Bürger in einem doch demokratisch gefestigten modernen Rechtsstaat nicht mehr vertrage, der zeit- und personalaufwendig und deshalb im hochverschuldeten Staatswesen Bundesrepublik Deutschland weder zeitgemäß noch zumutbar sei.
Die Argumente stimmen heute so wenig wie vor 15 Jahren. Selbst wenn es so wäre, bliebe zunächst festzuhalten, daß die öffentlichen Stellen in den letzten Jahren bundesweit Milliardenbeträge aufgewendet haben, um den Auf- und Ausbau der automatisierten Datenverarbeitung voranzubringen. Damit haben sie selbst erst einen erheblichen Teil der Gefahren gesetzt, die das Bundesverfassungsgericht schon 1983 zu Recht in seinem sogenannten Volkszählungsurteil skizziert hat. Da dürfte es angesichts der **Pflicht** jeder öffentlichen Stelle zur Beachtung der Grundrechte nicht mehr als recht und billig sein, einen Bruchteil dieser Kosten dafür aufzuwenden, um die Bürgerinnen und Bürger als Träger dieses Staates wenigstens angemessen zu schützen.
Das leitet nahtlos über zu den datenschutzrechtlichen Auswirkungen des zweiten Trends. Die geradezu himmelstürmende Aktivität beim Ausbau der automatisierten Datenverarbeitung hat sich auch im Berichtszeitraum fortgesetzt. War in der Vergangenheit noch die Frage, ob sich mehr der einzelne PC oder mehr die vernetzte Arbeitsstruktur durchsetzen würde, ist nun die Devise: Hauptsache einen irgendwie gearteten automatisierten Arbeitsplatzanschluß, notfalls von außen. Das bringt ganz neue Probleme für den Datenschutz mit sich. Häufig erfolgen Ausbau oder Umstieg ohne schlüssiges rechtliches Anforderungsprofil und mit einer unzureichenden technischen und organisatorischen Sicherheitsstruktur. Gesehen und gezeigt werden nur (schnellebige) neue Anwendungsmöglichkeiten; die damit verbundenen Gefahren verdeutlicht erst ein

eingetretener Schaden.
Nachdem die Vermarktung der automatisierten Datenverarbeitung gut im Trend liegt, zeichnet sich als dritte generelle Linie der Verkauf von Sicherheit und Sicherheitskonzepten aller Art ab. Firewalls und Verschlüsselungssysteme sollen die durch eine unkritische automatisierte Datenverarbeitung erst heraufbeschworenen Gefahren für die Datensicherheit wieder eindämmen. Das kostet neues Geld und bringt in vielen Fällen keine oder jedenfalls nicht die versprochene Sicherheit für die Daten. Kaum hat sich herumgesprochen, daß der codierte Magnetstreifen (z.B. bei EC- und Kreditkarten) ohne großen technischen Aufwand entschlüsselt werden kann, ist in Fachzeitschriften schon nachzulesen, daß die gerade erst als sicherer gepriesene Chipkarte nur unwesentlich mehr Schutz gegen unbefugtes Lesen bietet, und es dürfte nur eine Frage der Zeit sein, bis die jetzt noch hochgepriesene Kryptographie in ihrer Sicherheitsleistung relativiert wird.

Die Entwicklung des Datenschutzes bei den öffentlichen Stellen des Landes Sachsen-Anhalt läßt sich aus dem Spektrum der nachfolgend dargestellten Einzelbeiträge hoffentlich gut erkennen.
Die angesprochenen generellen Trends spiegeln sich mit unterschiedlicher Ausprägung auch im Lande wider. Mit der Verabschiedung des Landesarchiv- und des Landesstatistikgesetzes im Sommer 1995 gab es die letzte große gesetzgeberische Anstrengung zu bereichsspezifischen Regelungen in wichtigen Bereichen der personenbezogenen Datenverarbeitung. Eine Anregung des Landesbeauftragten beim Ministerium der Justiz, die wichtige Einführung des automatisierten Geschäftsstellenbearbeitungssystems SIJUS-Strafsachen bei den Staatsanwaltschaften auf eine landesgesetzliche Grundlage zu stellen, wurde nicht aufgegriffen. Bei der Novellierung des Frauenfördergesetzes im Februar 1997 wurden die noch im II. Tätigkeitsbericht (S. 96) begrüßten datenschutzrechtlichen Verbesserungen bei der Einsichtnahme in Bewerberunterlagen und Personalakten teilweise wieder rückgängig gemacht.
Was den täglichen Umgang der öffentlichen Stellen des Landes mit den personenbezogenen Daten der Bürgerinnen und Bürger angeht, bestätigen sich auch für diesen Berichtszeitraum die grundsätzlichen Feststellungen im II. Tätigkeitsbericht (S. 2 f). Noch immer gibt es einzelne Bedienstete, ja ganze Arbeitsbereiche in einer Verwaltung, die das in Artikel 6 Abs. 1 der Landesverfassung

garantierte Grundrecht auf informationelle Selbstbestimmung nicht kennen und ebensowenig das Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA). Schwierigkeiten bereiten nach wie vor die Beachtung und Umsetzung dieses Grundrechts in der täglichen Arbeit der öffentlichen Stellen beim Vollzug der Gesetze, insbesondere dort, wo es keine bereichsspezifischen Regelungen gibt und die Generalklauseln des geltenden DSG-LSA hilfsweise anzuwenden sind. Beispielhaft sollen hier die Schwierigkeiten der Kommunen bei der Neuberechnung der Gebühren für Kindertagesstättenplätze genannt werden. Für einen einfachen Ermäßigungsantrag wollten einzelne Kommunen auf sechs bis neun DIN A-4-Seiten personenbezogene Daten bei den Antragstellern und ihren Familien erheben; dies hatte wenig mit Verwaltungsökonomie und schon gar nichts mehr mit den datenschutzrechtlichen Grundsätzen der Erforderlichkeit und der Verhältnismäßigkeit zu tun.
Erfreulicherweise nimmt aber die Zahl derjenigen öffentlichen Stellen von Monat zu Monat zu, die sich vom Landesbeauftragten und seinen Mitarbeitern beraten lassen. Im Hinblick auf die schon in der Verfassung festgelegte Eigenverantwortung jeder öffentlichen Stelle wäre aber wünschenswert, daß, vor allem auf den mittleren und unteren Verwaltungsebenen, mehr als bisher die Beratung - auch in datenschutzrechtlichen Fragen - durch die zuständigen Fachaufsichtsbehörden gesucht und seitens dieser auch mehr und qualitativ besser geleistet wird. Auch die entsprechenden Angebote des Landkreistages bzw. des Städte- und Gemeindebundes sollten von der mittleren und unteren Verwaltungsebene mehr genutzt werden.

Zur landesweiten Entwicklung im Bereich der automatisierten Datenverarbeitung sei auf den eingehenden Beitrag unter Ziff. 8 verwiesen.

2. Der Landesbeauftragte

Der Landesbeauftragte kann auch in diesem Berichtszeitraum auf eine intensive und vom Engagement seiner Mitarbeiter getragene Tätigkeit zurückblicken. Die ihm zur Verfügung stehenden Stellen waren durchgängig besetzt; im Herbst 1996 kam es im Sachbearbeiterbereich zu einem im beiderseitigen Interesse begründeten Personaltausch mit einem Ministerium. Das setzt die bereits im

II. Tätigkeitsbericht (S. 6) skizzierte Linie fort, durch einen flexiblen Austausch von Personen und Ideen das gegenseitige Verständnis mit den exekutiven Verwaltungsbereichen zu fördern und möglichen einseitigen Verkrustungen im Personalbereich entgegenzuwirken. Auch bei der Zuweisung der Arbeitsbereiche zu den Referaten hat es leichte Verschiebungen gegeben. Die derzeitige Aufgliederung ergibt sich aus dem als **Anlage 1** ausgedruckten Organigramm der Behörde.

2.1 Tätigkeit im Berichtszeitraum

Auch in den beiden vergangenen Jahren ist das Arbeitsaufkommen beim Landesbeauftragten und seinen Mitarbeitern ständig weiter gestiegen. Die Zahl der schriftlichen Geschäftseingänge stieg von fast 2800 zum Jahresende 1994 auf fast 3 000 im Jahre 1995 und erreichte Ende 1996 die Zahl von 3 500. Dazu haben der Landesbeauftragte und seine Mitarbeiter im Jahre 1995 789 und im Jahre 1996 774 schriftliche Stellungnahmen versandt.
Zugenommen hat auch die Zahl der fernmündlichen Anfragen durch öffentliche und private Stellen; sie liegt z.Zt. bei ca. 720 pro Jahr.
In etwa gleich geblieben sind die Anzahl der persönlichen Anfragen und Vorsprachen in der Behörde des Landesbeauftragten (ca. 30 bis 35 im Jahr) und die Zahl der Bürgereingaben (ca. 150 pro Jahr). Unverändert hoch ist die Erfolgsquote dieser Eingaben; ca. ein Drittel rügen zu Recht Fehler und Rechtsmängel beim Umgang mit ihren personenbezogenen Daten.
Formelle Beanstandungen nach § 24 DSG-LSA sind fünf ausgesprochen worden, in etwa 40 weiteren Fällen hat der Landesbeauftragte nach § 24 Abs. 3 DSG-LSA von einer Beanstandung abgesehen. Damit wurde auch in diesem Punkte die bisherige Verfahrensweise (vgl. II. Tätigkeitsbericht, S. 7) fortgesetzt, wonach nur bewußte, grobe oder hartnäckige Verstöße gegen datenschutzrechtliche Bestimmungen formell beanstandet werden.

Neben einer zweistelligen Zahl gutachterlicher Äußerungen stieg vor allem der Bedarf an Besprechungen mit öffentlichen Stellen stetig an. Gehäuft wahrgenommen wurden auch Beratungen der öffentlichen Stellen vor Ort. Die vom Landesbeauftragten auch für diesen Berichtszeitraum festzustellende erfreulich

hohe Akzeptanz der Behörde führte fast zwangsläufig zu diesem Ergebnis. Auch wenn das Gesetz aus gutem Grund für den Landesbeauftragten keine Beratungs**pflicht** vorsieht, haben sich seine Mitarbeiter und er bemüht, möglichst allen Nachfragen gerecht zu werden.

Insgesamt hat die deutlich gestiegene Arbeitsbelastung, bei gleicher Anzahl von Mitarbeiterinnen und Mitarbeitern, zu Grenzen bei der Arbeitsqualität geführt. Eine weitere Folge sind leichte Einbußen bei den ohne Anlaß durchzuführenden Kontrollen. Schwerpunkte waren in diesem Tätigkeitsbereich die abschließenden Kontrollen bei den Staatsanwaltschaften, die Kontrolle der beiden Industrie- und Handelskammern, eingegrenzte Kontrollen im Bereich der Universitätskliniken sowie Querschnittskontrollen bei den Ausländerbehörden, Meldebehörden und verschiedenen personalaktenführenden Stellen im Lande. Diese werden auch im Verlauf dieses Jahres verstärkt fortgeführt.

Viele seiner Mitarbeiter und der Landesbeauftragte haben wieder als Lehrende, aber auch als Lernende an Aus- und Fortbildungsveranstaltungen teilgenommen.

Einen nicht zu vernachlässigenden Anteil der Arbeitszeit beanspruchen auch die Anfragen und Mitteilungen von bzw. an die Medien. In diesem Bereich gibt es inzwischen einen erfreulich kurzen Draht zwischen Anfragen der Bürger bei Presse und Rundfunk und der gezielten oder allgemein erbetenen Antwort des Landesbeauftragten.

2.2 Zusammenarbeit mit anderen Kontrollorganen

2.2.1 Zusammenarbeit auf Landes- und Bund-Länder-Ebene

Der Landesbeauftragte kann hierzu nahtlos an seine Ausführungen im II. Tätigkeitsbericht (S. 8) anknüpfen.
Die im Hinblick auf § 14 Abs. 1 DSG-LSA besonders wichtige Zusammenarbeit mit den obersten Landesbehörden ist unverändert gut. Das schließt nicht aus, daß im Einzelfall, aufgrund der unterschiedlichen Aufgaben und Interessen-

lagen um rechtlich einwandfreie und praxisbezogene Lösungen in sachlicher Form hart gerungen wird.
Auf der Wunschliste des Landesbeauftragten steht aber für manche Häuser - manchmal auch nur für einzelne Arbeitsbereiche in den Häusern - eine zügigere Beantwortung seiner Fragen. Wartezeiten von im Einzelfall bis zu neun Monaten hindern den Landesbeauftragten an einer effektiven Erledigung seiner gesetzlich vorgegebenen Aufgaben. Gravierende zeitliche Verzögerungen sind auch ein wichtiger Diskussionspunkt bei der von den Ministerien immer wieder gewünschten Beteiligung auf dem Dienstweg. Der Landesbeauftragte ist nach dem Gesetz bewußt nicht an den Dienstweg gebunden, hat aber Verständnis dafür, daß die für ihren Geschäftsbereich verantwortlichen Ministerien, jedenfalls beim Rücklauf der Antworten nachgeordneter Behörden, beteiligt werden wollen. Um diesem Interesse gerecht zu werden und andererseits seinem gesetzlich verbrieften Recht auf unverzügliche Auskunft nicht „nachlaufen“ zu müssen, hat der Landesbeauftragte seinerseits in solchen Fällen die nachrichtliche Beteiligung vorgesehen und dem nachgeordneten Bereich für Rückantworten den zweifachen Berichtsweg empfohlen (ein Berichtsexemplar auf dem Dienstweg, ein Berichtsexemplar direkt an den Landesbeauftragten).
Ein weiterer Wunschpunkt ist die rechtzeitige Übersendung von Gesetzentwürfen des Bundes, bei denen das Land im Bundesratsverfahren beteiligt ist und bei denen vom Landesbeauftragten wegen der Auswirkungen auf die Bürgerinnen und Bürger in Sachsen-Anhalt Äußerungen zu datenschutzrechtlichen Fragen erwartet werden können.
Hervorzuheben ist erneut die besonders gute Zusammenarbeit mit dem Ministerium des Innern. Insbesondere die fortlaufende Abstimmung mit dem für Grundsatzfragen des Datenschutzes zuständigen Referat 41 ermöglicht nicht nur eine schnelle und umfassende Information über aufkommende Problembereiche zum Datenschutz in der gesamten Landesverwaltung, sondern vermeidet häufig Doppelarbeit und führt zu zeitnahen und praxisverträglichen Lösungen.

Sehr gut ist auch die Zusammenarbeit mit dem Landtag. Die bereits in den zurückliegenden Jahren entwickelte vertrauensvolle Zusammenarbeit hat sich auf allen Ebenen bewährt. Die Beratung der Landtagsverwaltung und der Parlamentsausschüsse wird häufig in Anspruch genommen, kann aber manchmal auf

seiten des Landesbeauftragten und seiner Mitarbeiter nur begrenzt geleistet werden, weil die Arbeitskapazitäten erschöpft sind.
Der fortgesetzte Erfahrungsaustausch mit dem Präsidenten des Landtages und sein Informationsbesuch anläßlich einer Arbeitssitzung in der Geschäftsstelle im Dezember 1996 haben auch im Berichtszeitraum das Verständnis für die Arbeit des Landesbeauftragten und dessen Unterstützung gestärkt.

Besondere Erwähnung bedarf auch diesmal wieder die wichtige Zusammenarbeit auf der Ebene der Datenschutzbeauftragten des Bundes und der Länder. Die zweimal jährlich stattfindende Konferenz und die begleitende Sacharbeit in den Arbeitskreisen bilden, abgesehen von der gesetzlichen Verpflichtung (§ 22 Abs. 7 DSG-LSA), eine wichtige Grundlage für die effektive Tätigkeit des Landesbeauftragten und seiner Mitarbeiter. Die Unterstützung besteht nicht nur in der bereits früher herausgehobenen Verteilung von Arbeitsschwerpunkten und in der Möglichkeit zur Nutzung vielfältiger Ideen aus dem föderalen Rechts- und Verwaltungsspektrum, sondern auch in der Zurverfügungstellung eines gebündelten hohen Sachverstandes zur komplexen Sach- und Rechtsmaterie des Datenschutzes. Unabhängig davon gewährleistet diese Zusammenarbeit - auch unter Berücksichtigung landesgesetzlicher Abweichungen und individueller Interpretationsspielräume - im Bundesgebiet einen im wesentlichen ausgewogenen und, gemessen am internationalen Vergleich, hohen Schutz der Persönlichkeitsrechte der Bürgerinnen und Bürger.

2.2.2 Zusammenarbeit im europäischen und internationalen Bereich

Neben der erwähnten bundesweiten Zusammenarbeit gewinnt auch die Zusammenarbeit im europäischen und internationalen Bereich immer mehr an Bedeutung. Der Wegfall der Binnengrenzen in der europäischen Union führt zur fortlaufenden Abstimmung und Anpassung der Rechtsbereiche und damit auch der datenschutzrechtlichen Bestimmungen. Unabhängig davon hat die Technik bei der automatisierten Datenverarbeitung schon längst sämtliche Staats- und Ländergrenzen hinter sich gelassen.
Die im wesentlichen unter deutschem Vorsitz erarbeitete Europäische Datenschutzrichtlinie stellt einen ersten übergreifenden Versuch in diesem Bereich

dar, den Schutz der Menschen angesichts der durch merkantile Anreize ausufernden Technikbestimmtheit ganzer Lebensbereiche europaweit annähernd gleich zu gewährleisten. Ob dies gelingen wird, ist fraglich. Schon heute läuft das Recht der Technik hinterher und kann allenfalls noch Grundwerte absichern.

Der Landesbeauftragte hat deshalb auch im Berichtszeitraum an zwei internationalen Datenschutzkonferenzen teilgenommen.
Die 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat ihn im Herbst 1995 außerdem gebeten, zunächst übergangsweise bis zur bundesgesetzlichen Umsetzung der EUROPOL-Konvention (vgl. Ziff. 7.2), die dort vorgesehenen Aufgaben eines Ländervertreters für die gemeinsame Kontrollinstanz wahrzunehmen. Dazu hat er im Berichtszeitraum an mehreren Sitzungen deutscher und europäischer Arbeitsgremien teilgenommen.

2.3 Dateienregister - Einsichts- und Auskunftsrecht der Bürger

Seit nunmehr fünf Jahren führt der Landesbeauftragte das Register der automatisiert geführten Dateien der öffentlichen Stellen des Landes. Dieses Register enthält **keine** personenbezogenen Daten einzelner Betroffener (vgl. auch II. Tätigkeitsbericht, S. 10).
Obwohl nach § 25 Abs. 2 DSG-LSA das Register von **jedermann** eingesehen werden kann und diese **Einsichtnahme** nach § 25 Abs. 3 DSG-LSA **kostenfrei** ist, haben die Bürgerinnen und Bürger davon auch im zurückliegenden Berichtszeitraum keinen Gebrauch gemacht. Einige wenige schriftliche Anfragen zum Dateienregister von Petenten gingen von der falschen Vorstellung einer allumfassenden Informationsquelle über die zu ihrer Person gespeicherten Daten aus.

Der Landesbeauftragte nimmt diesen Punkt zum Anlaß, noch einmal auf das **Auskunftsrecht** jedes Bürgers und jeder Bürgerin hinzuweisen (vgl. § 15 DSG-LSA). Der Antrag auf Auskunft muß bei der jeweils speichernden öffentlichen Stelle (also z.B. beim Meldeamt, beim Gesundheitsamt oder bei der zuständigen Polizeibehörde) gestellt werden und soll die Art der personenbezogenen Daten

näher bezeichnen, über die Auskunft verlangt wird. Jede öffentliche Stelle hat dann Auskunft über die zur Person gespeicherten Daten, deren Herkunft und Übermittlung an Dritte, den Zweck und die Rechtsgrundlage der Speicherung zu erteilen. Wird die Auskunft verweigert, kann sich der Betroffene an den Landesbeauftragten wenden.

Im Hinblick auf die im folgenden unter Ziff. 8 dargestellte Entwicklung der automatisierten Datenverarbeitung, des nicht geringen Zeit- und Verwaltungsaufwandes zur Pflege, Korrektur und Aktualisierung des Dateienregisters und der Tatsache, daß von der Möglichkeit zur kostenfreien Einsichtnahme durch jedermann bisher kein Gebrauch gemacht wurde, sollte über die Notwendigkeit des Fortbestandes dieses Registers nachgedacht werden.
Bei einer Novellierung des DSG-LSA könnte anstelle des § 25 DSG-LSA eine **Vorlagepflicht** der innerbehördlich geführten Dateibeschreibungen und des Verzeichnisses der eingesetzten Datenverarbeitungsanlagen nach Abforderung durch den Landesbeauftragten treten. Soweit diese nicht schon von der bisherigen Regelung des § 23 Abs. 1 Satz 2 Nr. 1 DSG-LSA umfaßt ist, könnte sie als neue Nr. 3 dieser Vorschrift angefügt werden.
Unberührt bleiben sollte allerdings die Verpflichtung für jede öffentliche Stelle zur Führung des innerbehördlichen Verzeichnisses nach § 14 Abs. 2 DSG-LSA.
Die Regelung hat sich in der Praxis in mehrfacher Hinsicht bewährt.
Die bei einem Wegfall dieser Aufgabe verfügbar werdende Arbeitszeit könnte der Landesbeauftragte zielgerichtet für die Beobachtung und Beurteilung der stürmischen Entwicklung im technischen Bereich der Netzwerktechnologien (Internet/Intranet) sowie im Telekommunikationsbereich (neue Tele- und Mediendienste) nutzen.

Deshalb regt der Landesbeauftragte gegenüber dem Ministerium des Innern im Hinblick auf die Verwaltungsreform und die künftigen Umsetzungen der EU-Datenschutzrichtlinie in das Landesrecht an, diese Überlegungen als Diskussionsgrundlage für notwendige Veränderungen des DSG-LSA zu berücksichtigen.

2.3.1 Dateienregistermeldungen

Mit Stand 31.12.1996 beinhaltet das Register annähernd 1300 Dateimeldungen **(Abb. 1)**, ohne Berücksichtigung der Errichtungsanordnungen der Polizeibehörden, die nach § 25 Abs. 2 Satz 2 DSG-LSA einer beschränkten Einsichtnahme unterliegen.
Auch nach einem Zeitraum von fünf Jahren muß der Landesbeauftragte aber feststellen, daß die gesetzlich vorgeschriebene Meldepflicht gem. § 25 Abs. 1 Satz 3 DSG-LSA noch immer nicht von allen öffentlichen Stellen befolgt wird. So liegt bis heute vom Ministerium der Finanzen und dem Ministerium für Wirtschaft, Technologie und Europaangelegenheiten sowie vom Landesrechnungshof trotz der eindeutigen Gesetzeslage keine einzige Dateiregistermeldung vor.

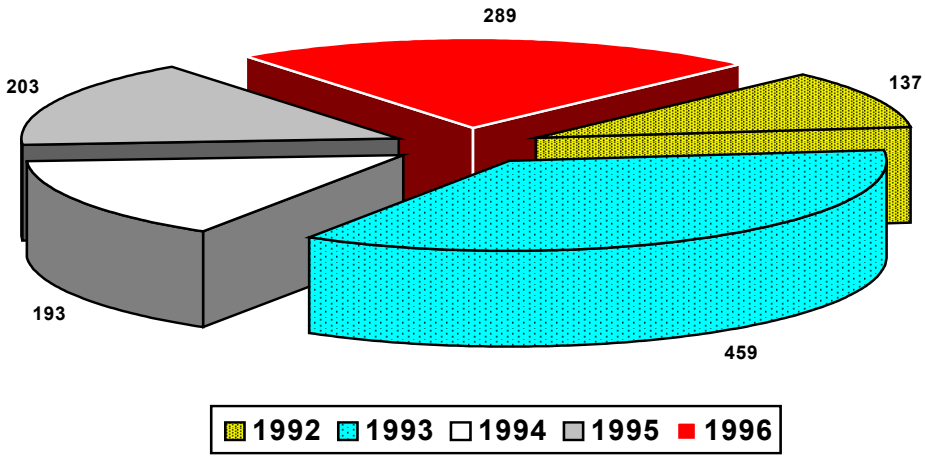


Abbildung 1: Anzahl der Dateimeldungen zum Register der Jahre 1992 - 1996

Im Bereich der Kommunalverwaltung sind z.B. von den insgesamt 215 Verwaltungsgemeinschaften bisher nur 28 % ihrer Meldepflicht nachgekommen.
Die inhaltliche Qualität der Dateimeldungen hat sich gegenüber den bereits im II. Tätigkeitsbericht (S. 12 f) dargestellten Defiziten nicht wesentlich verbessert. Fehlende oder falsche Rechtsgrundlagen für die Verarbeitung der personenbezogener Daten sowie fehlende Prüf- bzw. Löschfristen bilden nach wie vor die

Hauptkritikpunkte des Landesbeauftragten gegenüber den meldenden öffentlichen Stellen.
Legt der Landesbeauftragte als Bezugsgröße die entsprechende Anzahl von öffentlichen Stellen auf der Basis der Verwaltungsstruktur der Landesverwaltung zu Grunde, ergibt sich mit dem Stand 31.12.1996 bezüglich des Meldeverhaltens der öffentlichen Stellen folgende Übersicht:

Verwaltungsbereich	Gemeldete Anzahl	Anteil
oberste Landesbehörden	7	70 %
Behörden der Mittelinstanz	11	38 %
untere Landesbehörden	28	14 %
sonstige Landesbehörden	12	16 %

Bezogen auf den Kommunalbereich ergibt die Übersicht folgendes Meldeverhalten der öffentlichen Stellen:

Verwaltungsbereich	Gemeldete Anzahl	Anteil
Landkreise	21	100 %
kreisfreie Städte	3	100 %
Verwaltungsgemeinschaften	59	28 %

Der Landesbeauftragte erwartet, daß die Ressorts in ihrem unmittelbar nachgeordneten Bereich und insbesondere die Kommunalaufsicht in den Regierungspräsidien und bei den Landkreisen ihre Aufmerksamkeit verstärkt diesem rechtswidrigen Verhalten widmen.

2.3.2 Automatisierte Dateien bei den Staatsanwaltschaften - SIJUS-STRAF-STA

Bereits in seinem I. (S. 131 f) und seinem II. Tätigkeitsbericht (S. 122) hat sich der Landesbeauftragte kritisch mit dem Einsatz dieses Programmsystems bei den Staatsanwaltschaften auseinandergesetzt.

Bis heute fehlt eine bereichsspezifische gesetzliche Grundlage für die Einrichtung dieses Systems (vgl. Ziff. 21.13). Auch die dem Landesbeauftragten seit September 1994 zugeleiteten Dateimeldungen entsprachen in **mehrfacher** Hinsicht nicht den rechtlichen Anforderungen.
Da das Programm zunächst keine Funktion zur Löschung von Daten vorsah, enthielt auch die entsprechende Spalte der Dateimeldungen entgegen § 25 Abs. 1 Satz 3 DSG-LSA keine Angabe. Auch die richtige Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten (§§ 152, 160, 161 StPO i.V. mit § 10 Abs. 1 DSG-LSA) fehlte.
Für eine Antwort auf die damaligen Vorschläge des Landesbeauftragten zur Einhaltung eines datenschutzrechtlichen Mindeststandards in einer Übergangszeit benötigte das Ministerium der Justiz acht Monate.
Die dann avisierte Einführung einer Programmerweiterung zur manuellen Datenlöschung und Datensperre verzögerte sich von 1995 bis Anfang 1997.
Die gesetzlich erforderlichen **Änderungsmeldungen** zu den seit 1995 bemängelten Dateimeldungen der Staatsanwaltschaften haben den Landesbeauftragten bis zum Redaktionsschluß noch immer nicht erreicht.

3. Archivwesen

3.1 Landesarchivgesetz

Die zuletzt im II. Tätigkeitsbericht (S. 14) als wenig erfreulich dargestellte rechtliche Situation im Archivwesen hat sich durch die Verabschiedung des Landesarchivgesetzes (ArchG-LSA) vom 28.06.1995 (GVBl. LSA S. 190) gebessert.
Das Gesetz enthält für Nutzer wie Anwender wichtige bereichsspezifische Regelungen zum Datenschutz. Damit ist in diesem Bereich Rechtssicherheit eingetreten, was sich deutlich in einem Rückgang der Anfragen abzeichnet.

Die nachfolgend aufgeführten Bestimmungen sind mit dem Gesetz aufgehoben worden:

- Verordnung über das staatliche Archivwesen vom 11.03.1976,
- Erste Durchführungsbestimmung zur Verordnung über das staatliche Archivwesen vom 19.03.1976,

- Zweite Durchführungsbestimmung zur Verordnung über das staatliche Archivwesen vom 16.03.1990,
- Beschluß über die Erfassung und Auswertung der in der DDR befindlichen Dokumente über die Zeit der Hitlerdiktatur vom 28.09.1964,
- Beschluß über die Mikroverfilmung von Schrift- und Zeichnungsgut vom 19.09.1972,
- Anordnung über die Verleihung der Titel „Oberarchivar“, „Archivrat“ und „Oberarchivrat“ vom 01.04.1986

sowie:

- § 36 des DSG-LSA (Sperrung personenbezogener Daten aus ehemaligen Einrichtungen).

3.2 Medizinische Unterlagen aufgelöster Einrichtungen

Die Archivarin eines Landkreises hatte sich nach der Wende dankenswerterweise um die Unterlagen (in der Regel Karteikarten u.ä.) aufgelöster Krankenhäuser, (Betriebs-) Polikliniken und anderer Einrichtungen gekümmert und sie so vor dem Untergang bewahrt. Später fragte sie an, ob ihrem Archiv nicht auch die medizinischen Unterlagen, die beim Gesundheitsamt des Landkreises lagerten, zugewiesen werden könnten.

Leider läßt dies § 203 StGB nicht zu. Die medizinischen Unterlagen des Gesundheitsamtes fallen unter das besondere Vertrauensverhältnis Patient/Arzt. Darüber hinaus können Auskünfte aus solchen Unterlagen ausschließlich durch einen Mediziner erteilt werden, der im Einzelfall auch die Zulässigkeit der ärztlichen Schweigepflichtsdurchbrechung zu prüfen hat.
Der Landesbeauftragte regte aber an, daß das Archiv und das Gesundheitsamt die - nicht personenbezogenen - Archivierungsverzeichnisse austauschen, um so bei Bürgeranfragen zu einer umfassenden Auskunftserteilung zu kommen.

3.3 Erstellen von Verdienstbescheinigungen aus Archivunterlagen

Im Zusammenhang mit der Erstellung von Verdienstbescheinigungen aus Archivunterlagen für frühere Mitarbeiter ehemaliger Einrichtungen der DDR wurden wiederholt Anfragen zur datenschutzgerechten Handhabung an den Landesbeauftragten gestellt.
Die Rechtslage beurteilt sich jetzt nach den Bestimmungen des neuen Landesarchivgesetzes.

Soweit die archivführende öffentliche Stelle die Auswertung der archivierten Unterlagen selbst vornehmen will, bestehen nach § 10 Abs. 6 ArchG-LSA keine datenschutzrechtlichen Bedenken. Werden dritte Stellen mit der Auswertung und Verarbeitung beauftragt, sind zusätzlich die Bestimmungen des § 8 DSG-LSA zu beachten.
Im Hinblick darauf, daß innerhalb der Schutzfrist nach § 6 ArchG-LSA nur den Betroffenen ein Auskunftsanspruch zusteht, wurde aber empfohlen, die (komplett) erarbeiteten Verdienstbescheinigungen im Archiv zu belassen, sofern nicht der Betroffene von seinem Auskunftsanspruch Gebrauch macht oder eine Übermittlung (z.B. an einen Rentenversicherer) beantragt.

4. Ausländerangelegenheiten

4.1 Prüfung von Ausländerbehörden

Recht erfreulich verlief die datenschutzrechtliche Prüfung von drei Ausländerbehörden im Berichtszeitraum.

Gravierende datenschutzrechtliche Verstöße konnten nicht festgestellt werden. Neben einigen kleineren Defiziten im technisch-organisatorischen Datenschutz scheint sich aber noch nicht in allen Ausländerbehörden herumgesprochen zu haben, daß zum Zwecke der Speicherung in der Ausländerdatei A das Datum „Staatsangehörigkeit des (früheren) Ehegatten“ nicht erhoben werden darf (vgl. II. Tätigkeitsbericht, S. 20 f).

Schwierigkeiten haben die Ausländerbehörden offensichtlich auch damit, abhängig vom beantragten aufenthaltsrechtlichen Status (Aufenthaltsbewilligung, -befugnis, -erlaubnis, -berechtigung), nur die personenbezogenen Daten zu erheben, die tatsächlich erforderlich sind. So ließ eine Ausländerbehörde ausländische Antragsteller pauschal erklären, „mit Auskünften des zuständigen Leistungsträgers nach § 71 X. SGB, der für mich zuständigen Krankenkasse, des Finanzamtes, des Rentenversicherungsträgers“ einverstanden zu sein, während eine andere von jedem Ausländer wissen wollte, ob der Nachzug Familienangehöriger vorgesehen sei. Auch z.B. die Frage, ob man mit seinem Ehegatten in häuslicher Gemeinschaft lebe, ist datenschutzrechtlich nur zulässig, wenn dazu im Einzelfall ein konkreter Anlaß besteht, z.B. wenn ein im Wege des Familiennachzuges eingereister Ehegatte die Verlängerung seiner Aufenthaltsgenehmigung beantragt.

Der Landesbeauftragte wird die Prüfung in diesem Jahr fortsetzen.

4.2 Übermittlung personenbezogener Daten bosnischer Bürgerkriegsflüchtlinge

Durch den Ausländerbeauftragten der Landesregierung erfuhr der Landesbeauftragte im Herbst 1996 von der Absicht des Ministeriums des Innern, auf Bitten des Bundesinnenministeriums die Ausländerbehörden des Landes anzuweisen, die personenbezogenen Daten (u.a. Personalien und Herkunftsort) aller bosnischen Bürgerkriegsflüchtlinge an eine Projektgruppe beim Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) zu übermitteln, um die freiwillige Rückkehr dieses Personenkreises vorzubereiten und u.a. mit Mitteln der EU fördern zu lassen.

Weder der Bundesbeauftragte für den Datenschutz noch die Länderkollegen wußten etwas von diesen Maßnahmen. Schnell zeigte sich, daß für diese Datenübermittlung weder im Ausländergesetz noch in den Datenschutzgesetzen der Länder eine direkte Rechtsgrundlage existiert. Auch ließ sich die Zuständigkeit des BAFl nicht belegen.

Zwischenzeitlich sind einige Landesbeauftragte und der Bundesbeauftragte für den Datenschutz nach „kräftigem Schütteln“ ihrer Gesetze zu dem Ergebnis gekommen, daß die mehrfache Übermittlung dieser personenbezogenen Daten datenschutzrechtlich noch zulässig, zumindest vertretbar sei.
Der Landesbeauftragte hat in einem Schreiben an seine Kollegen noch einmal deutlich gemacht, daß er nach unserem Landesrecht die Übermittlung der Daten ohne die Einwilligung der Betroffenen nicht für zulässig hält. Vor dem Hintergrund wiederholter Äußerungen des Bundesaußenministers, wonach vor allem statistische Angaben über Zahl und Herkunftsort der in Deutschland lebenden bosnischen Flüchtlinge benötigt würden, ist ihm nicht ersichtlich, warum die Übermittlung hunderttausender personenbezogener Daten „als Voraussetzung für erfolgreiche Verhandlungen mit den internationalen Geldgebern“ erforderlich sein soll. Statistische Aufstellungen, ohne Namensbezug, dürften eigentlich auch für die als „ausufernd“ bekannte EU-Bürokratie reichen. Für deren Tätigkeit gibt es im übrigen bis heute kein angemessenes Datenschutzniveau.
Die in Sachsen-Anhalt gefundene Lösung hält der Landesbeauftragte für datenschutzrechtlich vertretbar. Danach wird jeder Betroffene über die Übermittlungsabsicht schriftlich informiert und erhält Gelegenheit, evtl. schutzwürdige Belange in seinem Fall vorzutragen.

5. Ausweis- und Meldewesen

5.1 Datenübermittlung aus dem Melderegister für eine Diplomarbeit

Eine Diplomandin der Martin-Luther-Universität Halle-Wittenberg begehrte Auskünfte aus dem Melderegister der Stadt Halle für eine wissenschaftliche Arbeit zu Lebensverhältnissen im Alter. Hierfür wurden die Namen und Anschriften einer Vielzahl älterer Personen benötigt, deren Anschrift sich, auf einen bestimmten Zeitraum bezogen, verändert hatte.

Die erbetenen Auskünfte stellen sich rechtlich als Antrag auf Gruppenauskunft aus dem Melderegister gem. § 33 Abs. 3 MG LSA dar. Diese darf nur erteilt werden, wenn ein berechtigtes öffentliches Interesse vorliegt, das die Meldebehörde in eigener Zuständigkeit prüft. Ein geeignetes positives Entscheidungs-

merkmal war in diesem Fall die Vergabe einer Diplomarbeit durch eine Universität und die Verwendung der Arbeitsergebnisse für öffentliche Belange. Dagegen sprach allerdings die große Zahl der betroffenen Einwohner.

Der Landesbeauftragte empfahl deshalb das sog. Adreßmittlungsverfahren. D.h., daß nach statistischer Feststellung der Zahl der Betroffenen, die Diplomandin die entsprechende Anzahl fertig kuvertierter Anschreiben mit Zweck und Hinweis auf die Freiwilligkeit der Teilnahme dem Einwohnermeldeamt vorlegt. Die Behörde versieht diese mit Adreßaufklebern und versendet sie auf Kosten der Diplomandin. Damit werden der Diplomandin keine Einwohnerdaten übermittelt, und es obliegt allein den betroffenen Bürgern, ob sie eine Kontaktaufnahme und damit die Teilnahme an der Analyse wünschen.

5.2 Datenübermittlungen aus dem Melderegister für Forschungsvorhaben

Immer wieder treten Forschungsinstitute an die Meldebehörden heran, um Auskünfte aus den Melderegistern zu erlangen. Meist handelt es sich dabei um Forschungsaufträge, bei denen ein berechtigtes öffentliches Interesse nachgewiesen werden kann.

Ob eine Melderegisterauskunft erteilt wird, prüft in der Regel die Meldebehörde in eigener Zuständigkeit. Häufig wird aber der Landesbeauftragte vorsorglich um datenschutzrechtlichen Rat gebeten.
Rechtlich handelt es sich fast ausnahmslos um Anträge auf Erteilung einer Gruppenauskunft nach § 33 Abs. 3 MG LSA. Der Landesbeauftragte empfiehlt dazu als geeignete Entscheidungshilfe für die Prüfung des berechtigten öffentlichen Interesses die den Forschungsinstituten häufig erteilten Bescheinigungen über eine Unbedenklichkeitsprüfung der zuständigen obersten Landesbehörde des Bundeslandes, in dem das Institut wissenschaftlich tätig ist. Das vom Landesbeauftragten befragte Ministerium des Innern teilt diese Auffassung.
Im übrigen ist vor einer Datenübermittlung aus dem Melderegister stets zu beachten, daß nur solche Daten übermittelt werden, die auch vom Forschungsauftrag gedeckt sind.

Datenschutzrechtliche Verstöße hat der Landesbeauftragte zu diesem Punkt bei seinen Kontrollen von Meldebehörden bisher nicht festgestellt.

5.3 Auskunft über Meldedaten für Adreßverzeichnisse auf CD-ROM

Seit auf dem freien Markt neue Datenspeichermedien, wie z.B. die CD-ROM erschienen sind, treten immer häufiger Hersteller von Adreßverzeichnissen an die Meldebehörden heran, um Einwohnerdaten auch für solche, automatisiert vielseitig auswertbaren Zusammenstellungen zu erhalten.
Der Landesbeauftragte hat gegen das Erstellen einer Adreßsammlung auf CD-ROM gegenüber dem Ministerium des Innern datenschutzrechtliche Bedenken geäußert und empfohlen, den Meldebehörden des Landes Sachsen-Anhalt eine klare Regelung diesbezüglich an die Hand zu geben.

Das Ministerium des Innern hat die Anregung aufgegriffen und durch Erlaß klargestellt, daß die Herausgabe von Meldedaten für die Erstellung von Adreßverzeichnissen auf CD-ROM oder in sonstiger automatisierter Form eine mögliche Beeinträchtigung schutzwürdiger Interessen der Betroffenen zur Folge haben kann und deshalb unterbleiben sollte.

Die zuständige Meldebehörde hat sich deshalb vor der Bearbeitung eines Auskunftsersuchens über die in § 34 Abs. 3 MG LSA genannten Einwohnerdaten vom Adreßbuchverlag im Rahmen der Zweckbindung nach § 35 Abs. 1 MG LSA schriftlich bestätigen zu lassen, daß die Daten **ausschließlich** für die Herausgabe von **Adreßbüchern in gedruckter Form** verarbeitet werden und eine anderweitige Verwendung, z.B. zur Verarbeitung auf CD-ROM oder in sonstiger automatisierter Form, unterbleibt.

5.4 Innerbehördliche Datenweitergabe aus dem Einwohnermelderegister

Bei der Prüfung von Meldebehörden im Berichtszeitraum wurde wiederholt festgestellt, daß im Zuge der lokalen Vernetzung zur automatisierten Datenverarbei-

tung bei einigen auch ein uneingeschränkter Zugriff verschiedener Ämter einer Behörde auf Meldedaten **aller** Einwohner möglich war.

Nach Auffassung der betroffenen Behörden ist die hierzu erforderliche Rechtsgrundlage im Meldegesetz vorhanden. Diese Rechtsauffassung wird vom Landesbeauftragten nicht geteilt.

§ 29 Abs. 5 MG LSA erlaubt nur die Weitergabe innerhalb der Behörde im **Einzelfall**. Dabei ist die Erforderlichkeit jedes Datums im Rahmen der Aufgabenerfüllung der anfordernden Stelle grundsätzlich zu prüfen. Wollte man einen stetigen, unkontrollierbaren Online-Zugriff aller Ämter und Stellen einer Behörde auf **alle** Einwohnerdaten zulassen, wäre die vom Verfassungsrecht den betroffenen Bürgern garantierte Zweckbindung nicht mehr zu gewährleisten und der vom Bundesverfassungsgericht betonte Grundsatz der informationellen Gewaltenteilung auch innerhalb einer speichernden öffentlichen Stelle wäre verletzt.
Etwas anderes gilt nur bzgl. der Daten für eine einfache Melderegisterauskunft (§ 33 Abs. 1 MG LSA).

6. Bau- und Bodenrecht

6.1 Übermittlung von Einwendungen im Raumordnungsverfahren

Ein Petent beschwerte sich beim Landesbeauftragten darüber, daß ein Landkreis in einem Raumordnungsverfahren seine Einwendungen in dem Verfahren an einen Unternehmer weitergeleitet hatte.
Wie sich herausstellte, hatte der Unternehmer mit einem von ihm beabsichtigten Bauvorhaben die Einleitung dieses Raumordnungsverfahrens ausgelöst.

Nach § 15 Abs. 1 des Vorschaltgesetzes zur Raumordnung und Landesentwicklung des Landes Sachsen-Anhalt kann ein Raumordnungsverfahren auch auf Antrag des Vorhabenträgers eingeleitet werden. Der Vorhabenträger erhält dann gemäß § 16 Abs. 2 dieses Gesetzes als zu beteiligender Antragsteller grundsätzlich die Verfahrensunterlagen zugeleitet.

Allerdings legt die zuständige Landesplanungsbehörde den Umfang der notwendigen Verfahrensunterlagen fest.
Weil der Landkreis in diesem Fall die Stellungnahme des Betroffenen selbst als „für das vom Landkreis durchzuführende Verfahren unerheblich“ einschätzte, war die Übersendung der Stellungnahme an den beteiligten Unternehmer nicht erforderlich und hätte aus datenschutzrechtlichen Gründen unterbleiben müssen.

In solchen Fällen - und das ist für alle Landkreise als Landesplanungsbehörden von Interesse - verdrängen die Bestimmungen über die Übermittlung personenbezogener Daten nach § 3 Abs. 4 DSG-LSA die Regelungen des allgemeinen Verwaltungsverfahrensrechts.

6.2 Einsichtnahme der Ämter für Landwirtschaft und Flurneuordnung in Grundbücher

Das Ministerium der Justiz des Landes Sachsen-Anhalt wandte sich bezüglich eines Vorhabens des damaligen Ministeriums für Ernährung, Landwirtschaft und Forsten des Landes Sachsen-Anhalt ratsuchend an den Landesbeauftragten.
Es ging um die Rechtsfrage, ob Mitarbeiter der Ämter für Landwirtschaft und Flurneuordnung alle Grundbücher einsehen dürfen, um Grundstücke aus der Bodenreform festzustellen, bei denen möglicherweise Ansprüche des Landes bestehen, die geltend gemacht werden müssen.
Das Ministerium der Justiz wollte die Einsichtnahme von vornherein auf die Abteilung I der Grundbücher beschränken, weil sich daraus der Bodenreformvermerk und die Eigentümereigenschaft ergeben.

Das war datenschutzgerecht.
Als Rechtsvorschriften, die die Datenübermittlung zur Erfüllung der in der Zuständigkeit der Ämter für Landwirtschaft und Flurneuordnung liegenden Aufgaben erforderlich machen und zwingend voraussetzen (§ 11 Abs. 1 i.V. mit § 10 Abs. 2 Nr. 1 DSG-LSA), sind die Regelungen in Artikel 233 § 11 Abs. 3 und § 12 EGBGB anzusehen. Der nach diesen Vorschriften mögliche Übereignungsanspruch gegen den Eigentümer eines Bodenreformgrundstücks kann vom Fiskus

in den Fällen, in denen der Eigentümer keine Verfügung über das Grundstück trifft, nur dann vor Eintritt der Verjährung geltend gemacht oder wenigstens einstweilig gesichert werden, wenn ihm bekannt ist, wessen Grundstück Teil der Bodenreform war oder ist.
Dazu genügt die Einsichtnahme in Abteilung I der Grundbücher.

6.3 Datenübermittlung der Notare an Gemeinden zur Ausübung des Vorkaufsrechts

Aus einem anderen Bundesland kam der Hinweis auf eine datenschutzgerechtere Lösung bei der Übermittlung von Kaufverträgen durch Notare an die Gemeinden zur Ausübung des kommunalen Vorkaufsrechts.

Nach § 28 Abs. 1 Satz 1 BauGB hat der Verkäufer eines Grundstückes der Gemeinde zur Ausübung des Vorkaufsrechts unverzüglich den Inhalt des Kaufvertrages mitzuteilen; die Mitteilung des Verkäufers wird auch durch die Mitteilung des Käufers ersetzt.
In der täglichen Praxis erfolgt diese Mitteilung durch den beurkundenden Notar. In einigen Bundesländern ist man dabei zu einem sog. „zweistufigen Verfahren“ übergegangen, um die Übermittlung „überschüssiger“ personenbezogener Daten zu vermeiden.
Danach werden zunächst nur alle Daten, die die Tatsache des Kaufes, die Kaufvertragsparteien und die genaue Bezeichnung des Grundstücks einschl. der Angabe, ob es bebaut oder unbebaut ist, betreffen, der Gemeinde mitgeteilt. Erst wenn die Gemeinde aufgrund dieser Mitteilung die Ausübung des Vorkaufsrechts in Erwägung zieht, wird in einer zweiten Stufe die Vorlage des vollständigen Kaufvertrages notwendig.

Dieses Verfahren hält der Landesbeauftragte für datenschutzgerecht.
Auch in Sachsen-Anhalt wird nach Auskunft der Notarkammer von den Notaren das „zweistufige Verfahren“ bevorzugt. Allerdings verlangen einige Gemeinden ohne nähere Begründung die sofortige Übersendung einer vollständigen Abschrift des Kaufvertrages.

Der Landesbeauftragte empfiehlt aus datenschutzrechtlichen Gründen allen Gemeinden die Anwendung des zweistufigen Verfahrens. Denn nur die tatsächlich vorgesehene Ausübung des Vorkaufsrechts rechtfertigt die Vorlage des vollständigen Kaufvertrages. Das wird aber die Ausnahme bleiben.

7. Europäischer Datenschutz

7.1 Richtlinie der Europäischen Union

Bereits im I. (S. 40) und im II. Tätigkeitsbericht (S. 30) hatte der Landesbeauftragte über den Inhalt und Stand der Arbeiten am Entwurf einer „Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (EU-Datenschutzrichtlinie) berichtet.
Am 24.07.1995 beschloß der Ministerrat die EU-Datenschutzrichtlinie, das Europäische Parlament verabschiedete sie am 24.10.1995. Bis auf eine Stimmenthaltung durch Großbritannien billigten alle übrigen Mitgliedsstaaten der EU die Richtlinie.

Damit ist nun der Weg frei für ein einheitliches Datenschutzrecht in der Europäischen Union. Die Mitgliedsstaaten haben die Richtlinie binnen drei Jahren - wobei in bestimmten Bereichen längere Übergangsfristen zugestanden werden - in nationales Recht umzusetzen. Dabei liegt die Federführung für die Umsetzung in der Bundesrepublik beim Bundesministerium des Innern.
Soweit aufgrund der Richtlinie auch Datenschutzvorschriften zur Regelung der Datenverarbeitung im öffentlichen Bereich zu ändern sind, werden auch die Länder ihre Datenschutzgesetzgebung anpassen. Auch in Sachsen-Anhalt gibt es dazu erste Vorbereitungen. Es zeichnet sich aber ab, daß die Bundesregierung keine Neigung verspürt, die gesetzliche Anpassung über das unbedingt notwendige Maß hinaus vorzunehmen.
Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb auf ihrer Sitzung am 09./10.11.1995 ihr Anliegen zur Weiterentwicklung des Datenschutzes in der Europäischen Union in einer Entschließung **(Anlage 2)** formuliert sowie am 14./15.03.1996 Eckpunkte zur Modernisierung und europäischen

Harmonisierung des Datenschutzrechts in einer weiteren Entschließung **(Anlage 3)** erarbeitet.

7.2 EUROPOL

Gegen das am 26.07.1995 von den Mitgliedsstaaten der Europäischen Union unterzeichnete Übereinkommen über die Errichtung eines europäischen Polizeiamtes (EUROPOL-Konvention) sind seitens des Landesbeauftragten (II. Tätigkeitsbericht, S. 33) und seiner Kollegen in Bund und in den Ländern aus unterschiedlichen Gründen schon frühzeitig Bedenken erhoben worden. Es ist zu befürchten, daß die in der Konvention vorgesehenen Verwendungsmöglichkeiten der Daten, ohne eine ausreichende direkte Kontrolle, die Polizeibehörden der Bundesländer von ihrer Verantwortung für die von ihnen eingegebenen Personendaten abkoppeln. Dies kann zu erheblichen Gefährdungen der Rechte Betroffener führen. Denn sind die personenbezogenen Daten erst einmal in der EUROPOL-Datenbank, sind ihre weitere Nutzung dort und die Folgen einer Datenübermittlung in andere EU-Staaten, u.U. sogar in Staaten außerhalb der EU, nicht mehr kontrollierbar.

Voraussetzung der Datenspeicherung bei EUROPOL ist keine Einwilligung des Betroffenen und keine staatsanwaltschaftliche oder richterliche Anordnung. Es genügt die - vom Betroffenen oft gar nicht bemerkte - Aufnahme in die polizeiliche Datei eines Vertragsstaates der EU im Zusammenhang mit einer Straftat, für die EUROPOL nach der Konvention zuständig sein soll. EUROPOL nimmt seine Aufgaben und den Umgang mit den Daten „freischwebend“ wahr; kein Staatsanwalt, kein Richter leitet die Ermittlungen, kein Minister ist für die Tätigkeit verantwortlich und kein Parlament kontrolliert es. Der Direktor und die anderen EUROPOL-Bediensteten dürfen von keiner Regierung, Behörde, Organisation oder EUROPOL-fremden Personen Weisungen entgegennehmen. Der von den nationalen Regierungen beschickte Verwaltungsrat darf im wesentlichen nur Rahmenbedingungen festlegen, in die konkrete Aufgabenerfüllung aber nicht eingreifen. Die einzige - eingegrenzte - Kontrolle wird durch eine „Gemeinsame Kontrollinstanz“ wahrgenommen, die von den Regierungen der EU-Mitgliedsstaaten beschickt wird und deren Mitglieder richterliche Unabhängigkeit genießen.

Ein Ausschuß dieser „Gemeinsamen Kontrollinstanz“ verfügt über eine bescheidene richterliche Entscheidungs- und Rechtsgestaltungskompetenz. Sie bezieht sich aber nur auf Beschwerden und Streitigkeiten über den Auskunftsanspruch oder den Berichtigungs- und Löschungsanspruch eines Betroffenen. EUROPOL soll künftig nicht nur Vermittlungsstelle für die EU-Polizeien sein, sondern auch eigenständige Analysen mit den eingespeicherten Daten vornehmen. Dabei ist bislang noch nicht abschließend festgelegt, welche Qualität (harte oder weiche Daten) die in die Analyse einbezogenen personenbezogenen Daten haben müssen und inwieweit sie den Betroffenen „entblättern“ dürfen (Herkunft, Lebensgewohnheiten u.a.).
Schwerwiegende Bedenken ergeben sich auch zu den bisher vorgelegten Entwürfen der Mitgliedsstaaten der EU für Durchführungsbestimmungen zu den Analysedateien. Gemeinsam ist allen Vorschlägen, daß sie vor allem in ihrem Umfang der Datenerhebung sehr weitgehend sind und bisher jegliche Differenzierung zwischen Tatverdächtigen und Tätern einerseits, sowie Zeugen, Hinweisgebern, Opfern, Kontakt- und Begleitpersonen und sonstigen Informanten andererseits, vermissen lassen. Daneben werden Datenkategorien für die Aufnahme in die Analysedateien genannt, die zumindest in dieser Häufung in keiner deutschen polizeilichen Datei vorkommen dürfen: z.B. Namen der Eltern, Ausbildungen, wirtschaftliche Verhältnisse, Verhaltensmerkmale bis hin zu Charaktermerkmalen, DNA-Profile (sog. „genetische Fingerabdrücke“), Verweise auf Speicherungen in nichtpolizeilichen Datenbanken etc..
Hinzu kommt, daß die Speicherung darin nach den vorgelegten Entwürfen bereits dann möglich sein soll, wenn sie für Zwecke „der Analyse“ erforderlich ist. Beurteilungsmaßstab für die Speicherung ist also nicht etwa die Notwendigkeit der Verfolgung oder Verhütung von Straftaten, sondern ein von EUROPOL selbst bestimmter, unklarer Zweck!

Inzwischen hat die Bundesregierung einen Gesetzentwurf zur Ratifizierung und Ausführung der EUROPOL-Konvention vorgelegt. Dieser Entwurf läßt allerdings die klare Tendenz erkennen, daß die polizeirechtlichen Kompetenzen zu Lasten der bisher zuständigen Länder, mit allen datenschutzrechtlichen Konsequenzen, auf den Bund verlagert werden sollen. So ist beispielsweise das Bundeskriminalamt als alleinige Auskunftsstelle vorgesehen. Für die Anlieferung der Daten

aus den Ländern über das BKA an EUROPOL soll ausschließlich Bundesrecht gelten und bei der Datenschutzkontrolle wird dem Bundesbeauftragten für den Datenschutz die maßgebliche Rolle bei den datenschutzrechtlichen Kontrollen eingeräumt.

In die erste Stellungnahme des Bundesrates zu diesem Gesetzentwurf ist ein Antrag Sachsen-Anhalts aufgenommen worden, wonach in der „Gemeinsamen Kontrollinstanz“ in den Fällen, in denen Interessen der Länder berührt werden, die Stellungnahme des Ländervertreters eine **maßgebliche** Berücksichtigung finden soll. Gestärkt werden soll auch die Stellung des Ländervertreters im Verwaltungsrat von EUROPOL. Die Umsetzung dieser Anträge im Gesetz würde die materiellrechtliche Verantwortlichkeit der Länder für ihre Daten stärken.

Das Gesetzgebungsverfahren war bei Redaktionsschluß noch nicht abgeschlossen, so daß die weitere Entwicklung auch künftig vom Landesbeauftragten kritisch begleitet wird.

8. Entwicklung der automatisierten Datenverarbeitung

8.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Die bereits im II. Tätigkeitsbericht (S. 35 f) angesprochene dynamische Entwicklung bei der Ausstattung der Landesverwaltung mit Informations- und Kommunikationstechnik hat sich in den vergangenen zwei Jahren fortgesetzt.
Grundsätzlich erhöht sich mit dieser Entwicklung auch das Gefährdungspotential für die automatisierte Verarbeitung personenbezogener Daten.
Drei Aspekte sind hier besonders zu nennen und zu beachten:

Bezogen auf die Beschäftigtenzahl hat sich insgesamt der Ausstattungsgrad in den obersten Landesbehörden mit PC von ca. 55 % im Jahr 1994 auf ca. 78 % im Jahr 1996 erhöht. In einigen Ministerien ist bereits die „100 %-Grenze“ überschritten, d.h. hier sind bereits mehr Bildschirmarbeitsplätze bzw. PC als Mitar-

beiter vorhanden. Einen differenzierten Überblick zeigt hierzu die nachfolgende Grafik (**Abb. 1**).

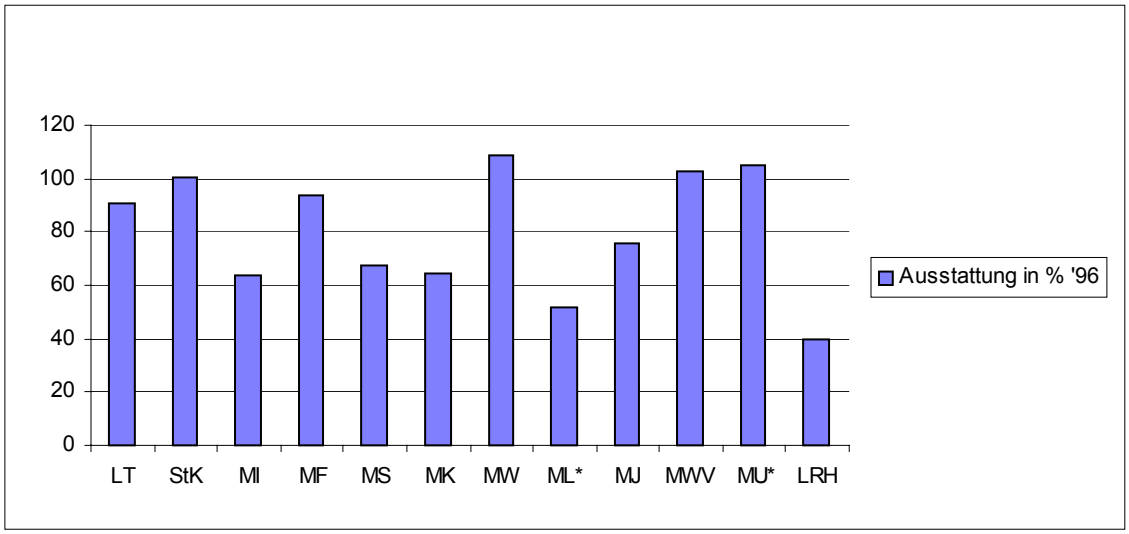


Abbildung 1: Ausstattung der Beschäftigten mit PC bzw. Bildschirmarbeitsplätzen (* seit 11.06.1996 ML und MU zu MRLU zusammengelegt)

Für die nachgeordneten Bereiche der Ressorts liegen dem Landesbeauftragten solche Statistiken nicht vor. Es ist aber davon auszugehen, daß sich auch dort die gleiche Tendenz widerspiegelt.

Der zweite Aspekt betrifft die lokale Vernetzung der Informationstechnik innerhalb der Ministerien. Waren 1994 durchschnittlich ca. 37 % der Bildschirmar-

beitsplätze bzw. PC lokal vernetzt, hat sich dieser Anteil im Jahr 1996 auf ca. 61 % erhöht (**Abb. 2**).

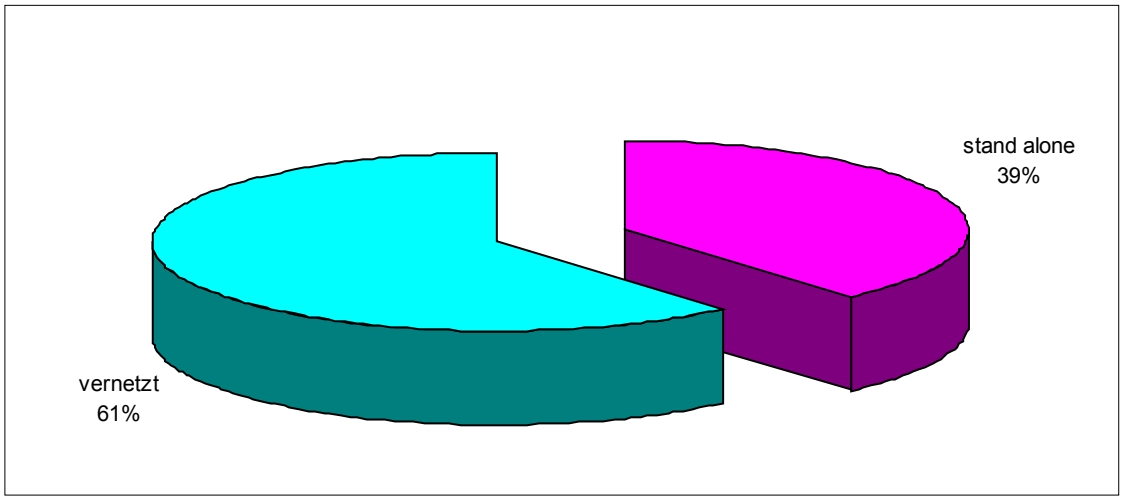


Abbildung 2: Anteil vernetzter Bildschirmarbeitsplätze bzw. PC am Gesamtbestand der obersten Landesbehörden 1996

Von Bedeutung ist schließlich auch die Ausgestaltung der überregionalen Vernetzung (WAN) der Behörden auf der Landesebene. Die Entwicklung ist hier durch den weiteren Ausbau des ITN-LSA bzw. die weitere Anbindung von Landesbehörden an das ITN-LSA gekennzeichnet.
Parallel hierzu erfolgte der Ausbau von Meldungsübermittlungssystemen (MHS) nach dem X.400-Standard, die Anfang des Jahres 1995 als Pilotprojekte begonnen wurden.

Der Landesbeauftragte weist deshalb erneut auf seine Ausführungen zu den Anforderungen beim Einsatz von elektronischen Mitteilungssystemen im II. Tätigkeitsbericht (S. 36 u. Anlage 16) hin. Insbesondere sollten nur solche Produkte eingesetzt werden, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahr 1988 erfüllen.

Die vom Bundesverfassungsgericht herausgestellte Bedrohung der Grundrechte durch die automatisierte Datenverarbeitung kann und muß mit Hilfe der Technik auch wieder eingegrenzt werden.

Für das Jahr 1997 sind durch das zuständige Ministerium des Innern als Netzbetreiber des ITN-LSA die Integration der Fernmeldekommunikation und die Schaffung des „INTRANET LSA“ für die Landesbehörden innerhalb des Landesnetzes vorgesehen. Beim „INTRANET LSA“ handelt es sich um die Bereitstellung von sog. TCP/IP-basierenden „Internet-Diensten“, wie z.B.:

- WWW-Dienst (World Wide Web - als multimedialer Informationsdienst),
- FTP-Dienst (File Transfer Protocol - als interaktiver Dateitransfer) und
- E-Mail-Dienst (Electronic Mail - als elektronische Post oder sog. Internet-Mail).

Werden auf sog. FTP- bzw. WWW-Servern personenbezogene Daten eingestellt, die dann von jedem Zugangsberechtigten abgerufen werden können, handelt es sich aus datenschutzrechtlicher Sicht um die Einrichtung eines automatisierten Abrufverfahrens (§ 7 DSG-LSA). Ein solches automatisiertes Abrufverfahren darf nach § 7 Abs. 1 DSG-LSA nur eingerichtet werden, wenn ein Gesetz dies ausdrücklich zuläßt.
Für die Ministerien besteht nach § 7 Abs. 2 DSG-LSA die Ermächtigung, für die Behörden und Einrichtungen ihres Geschäftsbereiches solche automatisierten Abrufverfahren durch Rechtsverordnung zuzulassen. Der Landesbeauftragte weist deshalb im Vorfeld der Planungen zum INTRANET LSA nachdrücklich auf die Beachtung dieser datenschutzrechtlichen Bestimmung hin.

Die Landesregierung hat bei der weiteren Vernetzung der Landesverwaltung und der Gestaltung des INTRANET LSA unter Berücksichtigung ihrer Rechtsverantwortung nach § 14 Abs. 1 DSG-LSA darauf zu achten, daß im Sinne eines vorgelagerten Grundrechtsschutzes die Kernaussagen des Volkszählungsurteils des Bundesverfassungsgerichts vom 15. Dezember 1983 (BVerfGE 65, 1), insbesondere die Grundsätze der Verhältnismäßigkeit und der Zweckbindung bei der Planung und Herstellung neuer Kommunikationsbeziehungen, beachtet werden.

Nicht alles, was die moderne Technik über ihre Zugangswege anbietet, muß so von jeder öffentlichen Stelle (von der kleinsten bis zur größten) und von jedem Mitarbeiter auch genutzt werden. Maßstab darf rechtlich (und finanziell) nur sein, ob die Herstellung neuer Kommunikationsbeziehungen zur Erfüllung der konkreten Verwaltungsaufgaben **erforderlich** ist. Bei mehreren technisch möglichen Wegen ist stets der für die personenbezogene Datenverarbeitung sicherste zu wählen.
Auch die Zweckbindung bei der Erhebung und Verarbeitung personenbezogener Daten und der damit verbundene Grundsatz der informationellen Gewaltenteilung sollen bei der landesweiten Vernetzung Berücksichtigung finden. Dabei müssen die Erforderlichkeit und das Risiko einer Zusammenführung von personenbezogenen Daten aus verschiedenen Stellen und Quellen durch diese Vernetzung rechtzeitig abgewogen werden.

Die gleiche Verantwortung trifft auch die Gemeinden und Landkreise für ihren jeweiligen Zuständigkeitsbereich bei der Wahrnehmung der eigenen Aufgaben.

Der Landesbeauftragte regt deshalb eine Anpassung der datenschutzrechtlichen Bestimmungen im Hinblick auf verbindliche Regelungen für die Sicherheit und Ordnungsmäßigkeit der automatisierten Verarbeitung personenbezogener Daten, unter Beachtung der sich abzeichnenden Entwicklung der weiteren lokalen und überregionalen Vernetzung innerhalb der Landesverwaltung, an. Als beispielgebend sind hier die Verordnungsermächtigung aus § 7 Abs. 4 Landesdatenschutzgesetz (LDSG) des Landes Schleswig-Holstein vom 30.10.1991 (GVOBl. Schl.-H. S. 555) und die danach erlassene Datenschutzverordnung (DSVO) vom 12.09.1994 (GVOBl. Schl.-H. S. 473) zu nennen.

8.2 ITN-LSA

8.2.1 Entwicklung des Landesverwaltungsnetzes - ITN-LSA

Das ITN-LSA ist im zurückliegenden Berichtszeitraum durch das Ministerium des Innern, als Netzbetreiber, auf 45 X.25-Netzknoten ausgebaut worden. Die Anzahl der an das Landesverwaltungsnetz angeschlossenen Behörden hat sich

weiter vergrößert. Die Übertragungskapazität zwischen den Hauptknoten des Netzes in Magdeburg, Halle und Dessau wurde auf 2 MBit/s erhöht. In den Randbereichen ist eine zunehmende Vermaschung des Landesnetzes zu beobachten. Die Übertragungskapazität wurde teilweise bis auf 64 KBit/s erhöht. Damit wird die Störanfälligkeit des Netzes reduziert und den Übertragungsengpässen entgegengewirkt.

Bei der geplanten bzw. bereits teilweise erfolgten Umsetzung neuer Kommunikationstechnologien, wie z.B. dem Aufbau des INTRANET LSA (vgl. dazu Ziff. 8.3) und der Integration der Sprachkommunikationsdienste für die Landesverwaltung im ITN-LSA, sind wegen der Verarbeitung und Nutzung personenbezogener Daten mit Hilfe dieser Mittel auch die datenschutzrechtlichen Bestimmungen, insbesondere die §§ 6 und 7 DSG-LSA, zu beachten. So unterwirft § 7 DSG-LSA die Einrichtung automatisierter Abrufverfahren, zu denen auch die Internet-Dienste (z.B. WWW, FTP) zählen, strengen Anforderungen.

Der Landesbeauftragte hält im übrigen eine Aktualisierung und Präzisierung des Runderlasses vom 07.02.1994 zum ITN-LSA hinsichtlich der IT-Sicherheitsmaßnahmen (z.B. Firewall-Konzept), der Einführung neuer Kommunikationstechnologien (z.B. Intranetfunktionalität, Integration der Sprachkommunikationsdienste) sowie des Antragsverfahrens zum Anschluß von öffentlichen Stellen an das ITN-LSA für erforderlich. Dabei müssen die im Rahmen des Antragsverfahrens zu einem Netzanschluß festgelegten und zu erfüllenden Mindestvoraussetzungen eine stärkere Beachtung finden. Nach Ziff. 2.1 Buchstabe g) des Runderlasses zählt dazu auch ein Datenschutzkonzept gem. § 6 DSG-LSA. Die Verantwortlichkeit hierfür liegt bei der speichernden öffentlichen Stelle selbst, nicht aber beim Netzbetreiber des ITN-LSA. Der gewährleistet mit seinen Maßnahmen nur im Transportnetz selbst eine Grundsicherheit. Als ein positives Beispiel kann der Landesbeauftragte die Umsetzung seiner Forderung nach der Verschlüsselung der Übertragung von Sozialdaten nennen. Bereits seit September 1995 erfolgt der verschlüsselte Datenaustausch zwischen den Landesämtern für Soziales und Versorgung und dem Landesrechenzentrum mittels vom BSI zertifizierter Verschlüsselungsboxen auf der Netzebene des ITN-LSA.

Eine andere Lösungsmöglichkeit besteht in der sog. Ende-zu-Ende-Verschlüsselung durch die einzelne öffentliche Stelle selbst. Dabei erfolgt durch den Benutzer die Verschlüsselung der Daten mittels des jeweils eingesetzten Programmes auf der Anwendungsebene bereits vor der Datenübertragung im ITN-LSA.
Welche Verschlüsselungsvariante realisiert wird, ist immer vom konkreten Einzelfall abhängig.
Im Rahmen seines Kontrollauftrages wird der Landesbeauftragte sein Augenmerk verstärkt auf die Sicherheitskonzepte und deren Umsetzung richten.

8.2.2 Sicherheitskonzept und Firewall-Konzept

Dem Landesbeauftragten liegt nunmehr der 1. Entwurf eines Gesamtsicherheitskonzeptes für das ITN-LSA vor. Das Ministerium des Innern kommt damit einer langjährigen Forderung des Landesbeauftragten nach (vgl. u.a. II. Tätigkeitsbericht, S. 37).
Der Entwurf beinhaltet neben Aussagen zur Grundsicherheit im ITN-LSA auch die Darstellung eines Lösungskonzeptes für die Übergänge zu Fremdnetzen (Internet, Datex-P, ISDN). Dazu sind die Schaffung kontrollierter zentraler Übergänge und deren Absicherung durch ein entsprechendes Firewall-Konzept vorgesehen.

Die zu Beginn des Jahres 1997 getroffene Grundsatzentscheidung des Ministeriums des Innern für eine höherwertige Zertifizierung der Firewall-Lösung für das ITN-LSA wird vom Landesbeauftragten begrüßt. Bis zur endgültigen Erteilung des Zertifikates durch das BSI sollte der Anwenderkreis, der den Praxistest unterstützt, überschaubar beschränkt bleiben. Ergänzend kann auf die folgenden Ausführungen zum Anschluß von Verwaltungsnetzen an das Internet (Ziff. 13.1) verwiesen werden.
Die mit der höherwertigen Zertifizierung des Firewalls verbundene zeitliche Verzögerung bis zur voraussichtlichen Inbetriebnahme im April 1998 sollte durch das Ministerium des Innern zu einer intensiven Abstimmung des Gesamtsicherheitskonzeptes des ITN-LSA mit allen Ressorts genutzt werden.

Der Landesbeauftragte wird diesen Prozeß aufmerksam begleiten und im Rahmen seines Kontroll- und Beratungsauftrages das Ministerium des Innern unterstützen.

8.3 INTRANET LSA

Die Anwendung von Internet-Prinzipien und die Nutzung von Internet-Diensten in lokalen Netzen (LAN) der Behörden und Dienststellen des Landes sowie innerhalb des Landesverwaltungsnetzes (ITN-LSA), einem sog. Fernnetz (WAN), wird als „INTRANET LSA“ bezeichnet.
Technisch verbirgt sich hinter der Bezeichnung INTRANET LSA der Einsatz von Server-Technik, die, in Verbindung mit einem Domain Name Service (DNS) für die Namen-Domain der Landesverwaltung „lsa-net.de“, diese Internet-Prinzipien und Internet-Dienste auf der Basis des TCP/IP-Protokolls umsetzt.
Mit dem INTRANET LSA sollen nach Planungen des Ministerium des Innern IP-basierte Dienste (z.B. WWW, E-Mail, FTP), wie sie heute bereits zu den Standardtechnologien im INTERNET zählen, auch für die an das ITN-LSA angeschlossenen Behörden verfügbar werden.

Mit der Einführung eines DNS wird ein verteiltes hierarchisches System zur Konvertierung von Rechnernamen in IP-Adressen geschaffen, denn jeder Netzwerk-Rechner in einen TCP/IP-Netzwerk wird durch die 32 Bit lange IP-Adresse identifiziert. Die Aufgabe des DNS besteht im wesentlichen darin, Kommunikationsbeziehungen zu ordnen und dabei jeder IP-Adresse einen Rechnernamen zuzuweisen. In Verbindung mit dem Einsatz von dynamischem Routing („Jeder kann mit jedem kommunizieren“) entstehen neue datenschutzrechtliche Gefährdungspotentiale, denn damit wird die verfassungsrechtlich gebotenen Abschottung von öffentlichen Stellen, die mit verschiedenen Aufgabenstellungen personenbezogene Daten verarbeiten, bereits durch die Bereitstellung technischer Kommunikationsmöglichkeiten in Frage gestellt.
Deshalb fordert der Landesbeauftragte bei der weiteren Umsetzung neuer Kommunikationstechnologien, das Prinzip der „informationellen Gewaltenteilung“ zu beachten und dementsprechende technische Vorkehrungen zu treffen.

Die notwendigen Voraussetzungen für das INTRANET LSA sind zwischenzeitlich geschaffen worden. Dazu gehören neben der fachlichen Ausbildung der Systemverwalter die Einrichtung der innerhalb des ITN-LSA zukünftig den Verwaltungsbehörden zur Verfügung stehenden Server-Technik.
Hierzu zählen der X.400-Server, der DNS-Server und der WWW-Server unter der Namen-Domain „lsa-net.de“.

Der Landesbeauftragte hält es bei der geplanten breiten Anwendung dieser neuen elektronischen Kommunikationstechnologien in der Landesverwaltung für erforderlich, neben den technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit, die generelle Zulässigkeit und die Anwendungsbreite der einzelnen Verfahren auch in den Geschäftsordnungen der Ministerien und der ihnen nachgeordneten Behörden zu regeln.
Den datenschutzrechtlichen Risiken, die mit der Umsetzung der behördenübergreifenden Vernetzung von Informations- und Kommunikationstechnik, **unabhängig** von einer bestimmten Verwaltungsaufgabe, allein aus dem Einsatz solcher Technologien entstehen, muß bereits in der Planungsphase begegnet werden.

Der Landesbeauftragte nimmt an den gemeinsamen Besprechungen zur umfangreichen Problematik INTRANET LSA teil.

9. Finanzwesen

9.1 Änderung der Abgabenordnung

Der Landesbeauftragte hat zu diesem Punkt bereits im I. (S. 48) und II. Tätigkeitsbericht (S. 38) auf die datenschutzrechtlichen Forderungen hingewiesen.

Nach einer Bestandsaufnahme aller Änderungs- und Ergänzungsvorschläge seitens der Datenschutzbeauftragten des Bundes und der Länder wurden diese im Dezember 1996 zwischen den obersten Finanzbehörden des Bundes und der Länder, dem Bundesbeauftragten und einem Vertreter der Landesbeauftragten für den Datenschutz erörtert.

Im Ergebnis konnte kein Konsens erzielt werden, da die Vertreter der obersten Finanzbehörden des Bundes und der Länder jegliche Änderungen bzw. Ergänzungen der Abgabenordnung um datenschutzrechtliche Vorschriften ablehnten, weil nach deren Auffassung dafür keine Notwendigkeit erkennbar sei. Erst ein kurz vor Redaktionsschluß eingegangenes Schreiben des Bundesministeriums für Finanzen läßt eine gewisse Bereitschaft erkennen, einzelne Vorschriften zu ändern.

Die Datenschutzbeauftragten des Bundes und der Länder beabsichtigen, demnächst das weitere Vorgehen miteinander abzustimmen, um dennoch eine Anpassung der Abgabenordnung an die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts zu erreichen.

9.2 Abruf von Steuerdaten im automatisierten Verfahren

Im Anschluß an die Ausführungen im II. Tätigkeitsbericht (S. 39) kann jetzt mitgeteilt werden, daß der Bundesgesetzgeber zwischenzeitlich durch eine Ergänzung der Vorschriften über das Steuergeheimnis und durch die Einbeziehung der Rechnungsprüfungsbehörden in den Kreis der abrufberechtigten Stellen die gesetzlichen Voraussetzungen für einen automatisierten Abruf geschaffen hat (§ 30 Abs. 2 Ziff. 1a und Abs. 6 AO).
Die seitens des Bundesministeriums der Finanzen (BMF) bestehende weitere Absicht, durch eine **Steuerdatenabrufverordnung** die Einzelheiten beim Abruf der steuerlichen Daten zu regeln, wurde aber aufgegeben, weil eine einvernehmliche und einheitliche Regelung sowohl für Bundes- und Landesfinanzbehörden als auch für die Gemeinden nicht zu erreichen war.

Das BMF hat jetzt vorgesehen, für die Bundes- und Landesfinanzbehörden - ohne die Gemeinden - eine **Verwaltungsvorschrift** über den automatisierten Abruf von Steuerdaten des Bundesamtes für Finanzen und der Finanzämter zu erlassen.
Der Landesbeauftragte hat zu dem Entwurf dieser Verwaltungsvorschrift gegenüber dem Ministerium der Finanzen des Landes Stellung genommen und insbesondere darauf hingewiesen, daß schon nach § 9 BDSG bzw. nach den ent-

sprechenden Regelungen der Landesdatenschutzgesetze (hier: § 6 DSG-LSA) die gesetzlich bestimmte Pflicht zu technischen und organisatorischen Maßnahmen der Datensicherung besteht. Insofern haben die dazu im Entwurf vorgesehenen Verwaltungsvorschriften nur konkretisierenden Charakter. Außerdem sind für die öffentlichen Stellen des Landes die Bestimmungen des Landesdatenschutzgesetzes anzuwenden, soweit einzelne Steuerbehörden nicht über ihren Doppelstatus als Bundesbehörde tätig werden.
Nach Landesrecht wäre die Einrichtung von automatisierten Abrufverfahren gem. § 7 Abs. 1 DSG-LSA nur zulässig, soweit ein **Gesetz** dieses ausdrücklich zuläßt. Bei fehlender bundes- oder landesgesetzlicher Grundlage wäre das Finanzministerium des Landes auch gem. § 7 Abs. 2 DSG-LSA unter bestimmten Voraussetzungen ermächtigt, für die Behörden seines Geschäftsbereiches die Einrichtung automatischer Abrufverfahren durch Verordnung zuzulassen.
Das BMF will demnächst den überarbeiteten Entwurf der vorgesehenen Verwaltungsregelung dem Bundesbeauftragten für den Datenschutz zuleiten. Es bleibt abzuwarten, inwieweit die Anregungen und Hinweise des Landesbeauftragten Berücksichtigung finden werden.

9.3 Datenübermittlungen der Finanzämter an die Gewerbebehörden

Bei säumigen Steuerzahlern im Gewerbebereich stellt sich schnell die Frage, ob und welche Maßnahmen das Finanzamt einleitet, um ein weiteres Anwachsen von Steuerrückständen zu Lasten der Allgemeinheit zu unterbinden. Die notwendigen Datenübermittlungen an die Gewerbebehörden stützt die Finanzverwaltung auf § 30 Abs. 4 Nr. 5 der Abgabenordnung (AO). Danach ist eine Offenbarung von Steuerdaten zulässig, wenn hierfür ein zwingendes öffentliches Interesse besteht. Dazu sind in der genannten Rechtsvorschrift drei Regelbeispiele gebildet worden, wann ein solches zwingendes Interesse anzunehmen ist und damit eine Übermittlung der personenbezogenen Daten an die Gewerbebehörden gestattet ist.

Der Landesbeauftragte hält im Interesse der vom Bundesverfassungsgericht geforderten Klarheit für die Betroffenen eine entsprechende bereichsspezifische gesetzliche Regelung für erforderlich.

Er hat außerdem beim Ministerium der Finanzen angeregt, den Gewerbetreibenden durch das Finanzamt vorher in entsprechender Anwendung der Vorschriften über die Anhörung (§ 91 AO) auf die vorgesehene Mitteilung hinweisen zu lassen.

Leider haben die Finanzministerien des Bundes und der anderen Länder eine Gesetzesänderung bisher nicht für erforderlich gehalten.
Aber das Ministerium der Finanzen hat jetzt die Finanzämter des Landes angewiesen, in diesen Fällen dem Steuerschuldner zunächst den Antrag auf Einleitung eines gewerberechtlichen Verfahrens anzudrohen. Erst wenn der auf dieses Schreiben nicht positiv reagiert, wird das Finanzamt bei der zuständigen Gewerbebehörde den Antrag auf Einleitung eines gewerberechtlichen Verfahrens stellen.

9.4 Datenschutz bei der Ausstellung und Versendung von Lohnsteuerkarten

Aufgrund einer Eingabe eines Petenten in einem anderen Bundesland ist der Landesbeauftragte der Frage nachgegangen, wie hier der Datenschutz bei der Ausstellung und Versendung von Lohnsteuerkarten gewahrt wird. Insbesondere wurde geprüft, inwieweit es zulässig ist, private Auftragnehmer an der Ausstellung und Versendung der Lohnsteuerkarten in Anbetracht der engen Grenzen und der Bedeutung der Vorschriften über das Steuergeheimnis (§ 30 AO) zu beteiligen. Grundsätzlich ist die Beauftragung nicht-öffentlicher Stellen durch Steuerbehörden als unzulässig abzulehnen.

Zur Frage der Beteiligung privater Dienstleistungsunternehmen konnte aber einvernehmlich mit dem Ministerium der Finanzen geklärt werden, daß die gesetzliche Ermächtigung zur Offenbarung der dem Steuergeheimnis unterliegenden Verhältnisse in Einzelfällen nach § 30 Abs. 4 Nr. 1 AO zulässig ist, wenn die Offenbarung z.B. der Durchführung eines Verwaltungsverfahrens in Steuersachen dient. Das Ausstellen und Versenden von Lohnsteuerkarten ist als Voraussetzung für das Steuerabzugsverfahren Bestandteil eines solchen Verwaltungsverfahrens.

Das Ministerium der Finanzen wurde darauf hingewiesen, daß es sich bei der insoweit datenschutzrechtlich vertretbaren Beauftragung von privaten Dienstleistungsunternehmen um eine Datenverarbeitung im Auftrag gem. § 8 DSG-LSA handelt. Unterliegt der Auftrag**nehmer** dabei nicht dem DSG-LSA (z.B. weil er eine private Firma ist), so ist der Auftraggeber nach § 8 Abs. 6 DSG-LSA verpflichtet, vertraglich sicherzustellen, daß der Auftragnehmer die Bestimmungen des DSG-LSA befolgt und sich der Kontrolle durch den Landesbeauftragten unterwirft. Außerdem hat der Auftrag**geber** den Landesbeauftragten über die Beauftragung zu unterrichten. Dies wird häufig übersehen!
Die Empfehlungen zu den bei der Vertragsgestaltung nach § 8 DSG-LSA zu beachtenden datenschutzrechtlichen Gesichtspunkten hat der Landesbeauftragte in einem besonderen Merkblatt zusammengefaßt.
Das Ministerium der Finanzen hat inzwischen die OFD Magdeburg angewiesen, die Verfügung zur Ausstellung und Versendung von Lohnsteuerkarten bezüglich eines Hinweises auf datenschutzrechtliche Vorschriften des § 8 Abs. 6 DSG-LSA zu ergänzen.

Geändert wurde die Verfügung der OFD Magdeburg von 1995 auch in einem weiteren Punkt. Sie enthielt in Ziff. 17 Abs. 2 Satz 2 die Regelung, daß bei Abwesenheit des Arbeitnehmers die Lohnsteuerkarte **offen** nur einem Familienmitglied übergeben werden darf.
Dazu war festzustellen, daß eine offene Übergabe der Steuerkarte sich rechtlich als Offenbarung von Steuerdaten an eine Privatperson darstellt und die engen Grenzen des § 30 Abs. 4 AO dies nicht zulassen.

Die OFD Magdeburg hat sich der Auffassung des Landesbeauftragten angeschlossen und die Verfügung zur Ausstellung und Versendung der Lohnsteuerkarten für das Kalenderjahr 1996 entsprechend geändert. Künftig soll die Übergabe der Lohnsteuerkarten in einem **geschlossenen** Briefumschlag erfolgen.

9.5 Satzungsmängel bei der Erhebung einer Kurtaxe

Mehrere „Haare in der Suppe“ fand der Landesbeauftragte bei einem ihm vom Ministerium des Innern zugeleiteten Entwurf eines Satzungsmusters über die Erhebung einer Kurtaxe.

So ist nach dem Satzungsmuster zwar eine teilweise Befreiung für Schwerbehinderte mit einer MdE von **weniger** als 100% und eine vollständige Befreiung von der Abgabepflicht für Begleitpersonen von Schwerbehinderten vorgesehen. Eine Befreiung der Schwerbehinderten mit einer MdE von 100% ist dagegen nicht enthalten.
In diesem Punkt konnte sich das Ministerium des Innern aus bisher nicht dargelegten Gründen noch nicht zu einer Änderung des Satzungsmusters entschließen.
Gestrichen wurde dagegen die Regelung des Musterentwurfes, nach der die Kurkarte bei mißbräuchlicher Verwendung ersatzlos eingezogen wird.
Der Landesbeauftragte hatte darauf hingewiesen, daß bei Entzug der Kurkarte grundsätzlich ein vermögensrechtlicher Erstattungsanspruch besteht, der aber - rechtlich fragwürdig - nach der Formulierung im Satzungsmuster automatisch erlöschen würde. Diese Regelung wäre außerdem nicht verhältnismäßig gewesen, denn sie läßt zum einen keinen Spielraum bei leichten oder wiederholten Verstößen, zum anderen dürfte die nach dem Satzungsmuster ebenfalls vorgesehene Mißbrauchsahndung als Ordnungswidrigkeit ausreichen.
Der Landesbeauftragte hatte außerdem angeregt, die in dem Satzungsmuster enthaltenen Bewehrungsvorschriften unter genauer Bezeichnung der Zuwiderhandlung präziser zu fassen und nicht nur bei Zuwiderhandlungen auf einzelne Paragraphen der Satzung zu verweisen. Auch dabei ist das Ministerium des Innern der Anregung des Landesbeauftragten gefolgt.

9.6 Ratenzahlung bei Verwaltungskosten

Ein Petent hatte bei einem Katasteramt formlos den Antrag gestellt, die von dort für Vermessungsleistungen festgesetzten Kosten in Raten bezahlen zu können.
Das Katasteramt sandte ihm deshalb einen Fragebogen zu, um gem. § 12 Abs. 1 VwKostG LSA prüfen zu können, ob die sofortige Einziehung mit erheblichen Härten für den Anspruchsgegner verbunden wäre.
Diese Prüfung ist legal, das Verfahren sicherlich nicht bürgerunfreundlich und doch hatte der Landesbeauftragte Grund einzugreifen. Der Fragebogen nämlich, mit dem das Katasteramt den Petenten um die Selbstauskünfte ersuchte,

war ohne inhaltliche Änderungen von einem Selbstauskunftfragebogen „Kreditantrag“ einer Sparkasse übernommen worden.
So wurde - außerhalb jeder Erforderlichkeit für das Katasteramt - z.B. erfragt, ob der Betroffene in den letzten 5 Jahren einen Offenbarungseid geleistet hatte, oder ob er von schwebenden Mahnverfahren bzw. anhängigen Klagen betroffen sei.
Das Beispiel zeigt, wie schnell Gedankenlosigkeit dazu führen kann, daß Bürger durch Verwaltungshandeln einer öffentlichen Stelle in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt werden.

Das Katasteramt lenkte auf die Intervention des Landesbeauftragten sofort ein und verwendet künftig nur noch die entsprechenden landeseinheitlichen Vordrucke.

10. Forschung

Auch in diesem Berichtszeitraum hat die Anzahl der Forschungsvorhaben in erheblichem Maße zugenommen. Insgesamt wurden 15 Forschungsvorhaben datenschutzrechtlich beraten. Dabei war festzustellen, daß weiterer Informationsbedarf zur gesetzlich vorgeschriebenen informierten Einwilligung (§ 4 Abs. 2 DSG-LSA) besteht, wenn es um die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten geht.

Bis auf wenige Ausnahmen wurde der Landesbeauftragte aber rechtzeitig zur Beratung oder zur datenschutzrechtlichen Überprüfung der Konzepte hinzugezogen, so daß in den meisten Fällen durch überschaubare Änderungen den datenschutzrechtlichen Anforderungen Genüge getan werden konnte.

Mehrere Forschungsprojekte befaßten sich mit bestimmten Personenkreisen (z.B. festgesetzte Altersgrenzen oder Fördermittelempfänger), dabei war festzustellen, daß die datenschutzgerechte Erreichbarkeit dieses speziellen Personenkreises häufig Probleme bereitete. Teilweise wurde übersehen, daß es sich bereits bei den Anschriften um personenbezogene Daten handelt, und die Übermittlung dieser Anschriften bereits der Einwilligung bedurft hätte.

Der Landesbeauftragte hat daher wiederholt auf die Möglichkeit des Adreßmittlungsverfahrens hingewiesen. Hierbei können die Forscher die Informationsunterlagen zusammenstellen und kuvertieren. Die Kuverts werden der öffentlichen Stelle übergeben, die über die benötigten Adressen verfügt (z.B. Meldeamt). Diese Stellen übertragen dann nur die Anschriften der Probanden auf die Umschläge und versenden sie. Nun kann der Proband selbst entscheiden, ob er sich für den vorgesehenen Forschungszweck zur Verfügung stellen und mit den Forschern Kontakt aufnehmen will.

Im folgenden sollen drei Projekte und ihre datenschutzrechtlichen Problembereiche zur Verdeutlichung näher beschrieben werden.

10.1 Klinische Tumorregister

Die datenschutzrechtliche Überprüfung der ersten Konzepte zur Errichtung der Tumorregister in Magdeburg, Halle und Dessau hatte seinerzeit ergeben (I. Tätigkeitsbericht, S. 53), daß sie in der Rechtsform eines eingetragenen Vereins geführt werden sollten und damit keine öffentlichen Stellen im Sinne des § 3 DSG-LSA gewesen wären. Nach gemeinsamen Beratungen mit der Aufsichtsbehörde, den Leitern der Tumorregister und dem Landesbeauftragten, wurden die Konzepte dahingehend geändert, daß die Tumorregister nunmehr als klinische Register bei den Universitätskliniken Halle und Magdeburg und beim Städtischen Klinikum in Dessau geführt werden. Damit handelt es sich bei ihnen um öffentliche Stellen.

Die datenschutzrechtliche Überprüfung und Überarbeitung der Konzepte wurde im Februar 1996 abgeschlossen.
Zwischenzeitlich wurde am Klinischen Tumorregister der Martin-Luther-Universität Halle eine Kontrolle nach § 22 Abs. 1 DSG-LSA durch den Landesbeauftragten vorgenommen. Bei dieser Kontrolle wurden keine datenschutzrechtlichen Verstöße festgestellt.

10.2 Magdeburger Fehlbildungsregister

Ziel des Fehlbildungsregisters ist die Feststellung der Häufigkeit von Fehlbildungen bei Neugeborenen und deren Konzentration auf bestimmte Regionen oder Bereiche. Anhand dieser Feststellungen soll eine gezielte Ursachenforschung betrieben werden. Anschließend sollen es die gewonnenen Erkenntnisse dem Ministerium für Arbeit, Soziales und Gesundheit ermöglichen, gezielte Hilfen für die betroffenen Kinder und deren Familien anzubieten bzw. zu planen (Ausschließen von Risikofaktoren, bedarfsgerechte Planung von Rehabilitationseinrichtungen, qualifizierte Beratungseinrichtungen).

Nach der Feststellung massiver Verstöße gegen das Grundrecht auf informationelle Selbstbestimmung der Betroffenen wurde die Datenerhebung und -verarbeitung für das erste Projekt im September 1994 eingestellt (I. Tätigkeitsbericht, S. 50).
Nach der Einarbeitung datenschutzrechtlicher Verbesserungen konnte die Datenerhebung im November 1995 wieder aufgenommen werden.

Nunmehr werden die Eltern vorab durch ein Informationsblatt über Inhalt und Zweck der Forschung aufgeklärt. Vor der Datenerhebung wird die gem. § 4 DSG-LSA erforderliche Einwilligung der Sorgeberechtigten eingeholt. Als wissenschaftliche Kontrollmaßnahme werden zu jeder aufgetretenen Fehlbildung die Daten von 2 Neugeborenen ohne Fehlbildung aus dem selben Landkreis erhoben, um Vergleichsdaten zu erhalten, ohne die eine Erforschung von Fehlbildungen nicht möglich ist.

10.3 Studie zur weiteren Entwicklung der Erwachsenenbildung

Das Institut für Strukturpolitik und Wirtschaftsförderung Halle/Leipzig e.V. erarbeitete im Auftrag des Kultusministeriums eine Studie zur weiteren Entwicklung der Erwachsenenbildung. Es war vorgesehen, vor allem inhaltliche Schwerpunkte, zweckmäßige Gestaltungsformen und erforderliche Bedingungen für die Weiterbildung im Lande Sachsen-Anhalt zu untersuchen, mit dem Ziel, die Angebote in der Weiterbildung stärker auf die tatsächlichen Bedürfnisse der

Bürgerinnen und Bürger auszurichten. Insgesamt sollten hierzu bei ca. 4 000 Bürgern aus verschiedenen Bereichen Sachsen-Anhalts mittels Fragebogen Daten erhoben werden.
Der Fragebogen sah zwar eine anonymisierte Datenerhebung vor. Das Konzept ging aber davon aus, sich für den Versand der Fragebögen die erforderlichen Adressen aus den jeweiligen Melderegistern übermitteln zu lassen.

Um die Rechte der betroffenen Bürger und Bürgerinnen besser zu wahren, hat der Landesbeauftragte das Adreßmittlungsverfahren vorgeschlagen. Da damit die Studie vollständig anonymisiert durchgeführt wird, bestehen keine datenschutzrechtlichen Probleme mehr.

11. Gesundheitswesen

11.1 Krebsregistergesetz

Nachdem der Bundesgesetzgeber mit dem Krebsregistersicherungsgesetz vom 21.12.1992 übergangsweise bis zum 31.12.1994 eine Rechtsgrundlage geschaffen hatte, die eine vorläufige Fortführung des ehemaligen Krebsregisters zuließ (I. Tätigkeitsbericht, S. 59), wurde mit dem Krebsregistergesetz (KRG) vom 04.11.1994 (BGBl. I S. 3351) eine Lösung geschaffen, die bis zum 31.12.1999 befristet ist.

Das Krebsregistergesetz regelt die fortlaufende und einheitliche Erhebung, Verarbeitung und Nutzung dieser Daten. Ärzte und Zahnärzte, und in ihrem Auftrag Klinikregister und Nachsorgeleitstellen, sind berechtigt, Daten an das Krebsregister zu übermitteln. Der Arzt oder Zahnarzt hat den Patienten von einer beabsichtigten oder erfolgten Meldung zum frühestmöglichen Zeitpunkt zu unterrichten. Der Patient hat gegen diese Meldung ein Widerspruchsrecht.

Da den Ländern in diesem Gesetz weitergehende Gestaltungsmöglichkeiten eingeräumt worden sind, haben die neuen Bundesländer auf der Grundlage eines Verwaltungsabkommens ein „Gemeinsames Krebsregister“ mit Sitz in Berlin eingerichtet. Wegen der gravierenden Rechtseingriffe und -folgen haben die

Landesbeauftragten für Datenschutz der neuen Bundesländer empfohlen, das dazu abgeschlossene Verwaltungsabkommen durch einen Staatsvertrag zu ersetzen.

Zur Zeit wird der Entwurf eines Staatsvertrages über das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen erstellt. Dazu hat auch eine eingehende Beratung mit dem Landesbeauftragten stattgefunden.

11.2 Organtransplantationsgesetz

Die Fraktionen der CDU/CSU, SPD und FDP einerseits und die Bundestagsfraktion Bündnis 90/Die Grünen andererseits haben jeweils einen eigenen Gesetzentwurf zur Organtransplantation eingebracht, über die der Bundestag bisher nicht abschließend entschieden hat. Inzwischen gibt es noch andere - fraktionsübergreifende - Vorstellungen einer größeren Gruppe von Bundestagsabgeordneten.
Die in der Öffentlichkeit andauernden Diskussionen zu den medizinischen, ethischen und rechtlichen Problemen im Zusammenhang mit der Festlegung und Feststellung des Hirntodes als Voraussetzung für eine Organentnahme geben Anlaß, an das Persönlichkeitsrecht des betroffenen Organspenders zu erinnern. Will er seiner eigenen freien Entscheidung sicher sein, so kann nur der Spender selbst - nach Abwägung aller Umstände - seine Zustimmung zur Organentnahme festlegen. Mit der freien Entscheidung des potentiellen Organspenders wäre es auch vereinbar, wenn dieser die Möglichkeit einer späteren Zustimmung auf eine bestimmte Person seines Vertrauens überträgt. Auch darin liegt eine generelle Zustimmung, die allerdings später von der Vertrauensperson konkretisiert werden muß.

Da hierbei das im Grundgesetz garantierte Persönlichkeitsrecht und die Würde jedes einzelnen Menschen im Kern berührt sind, haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer Konferenz am 14./15.03.1996 eine gemeinsame Entschließung gefaßt **(Anlage 4)**. Danach stellt die ausdrücklich

erklärte Einwilligung des Spenders zur Organentnahme den geringsten Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.

11.3 Selbstbestimmungsrecht der Patienten in Krankenhäusern

Die Anwesenheit von Studenten und Praktikanten bei Untersuchungen und Behandlungen in Universitätskliniken und Krankenhäusern führte zu datenschutzrechtlichen Anfragen und vereinzelten Beschwerden beim Landesbeauftragten.

Er hat dazu wie folgt Stellung bezogen:
Die Anwesenheit von Studierenden und Praktikanten im Klinikbereich der Universität greift erheblich in das grundrechtlich geschützte Persönlichkeitsrecht der Patienten ein. Ohne deren ausdrücklich erklärte Einwilligung ist deshalb die Erhebung und Verarbeitung der persönlichen Daten nur auf einer gesetzlichen Grundlage möglich. Auch bei Universitätskliniken vermag der allgemeine Lehr- und Ausbildungsauftrag einen derartigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung nicht zu begründen. Wenn auch Studierende und Praktikanten Teilnehmer am Lehrbetrieb sind, so stellen sie doch keine Bediensteten des Krankenversorgungsbereiches dar. Allerdings ist der Lehrauftrag der Universitäten gesetzlich geregelt und allgemein öffentlich bekannt. Bei Patienten in den Universitätskliniken genügt es deshalb, wenn sie rechtzeitig vor einer Untersuchung oder Behandlung vom Beisein Studierender oder Praktikanten informiert werden und dagegen widersprechen können. Tun sie dies, ist dies zu respektieren.
Die sog. Vorstellung eines Patienten im Hörsaal ist nur mit seiner vorherigen Einwilligung zulässig.

In allen anderen Krankenhäusern in staatlicher Trägerschaft ist die rechtzeitige Einwilligung des Patienten unabdingbare Voraussetzung für die Anwesenheit von Praktikanten und Studierenden. Eine Regelung in den Allgemeinen Vertragsbestimmungen eines Krankenhauses, die das Einverständnis des Patienten an der Anwesenheit von Studierenden und Praktikanten und damit der Übermittlung der personenbezogenen Daten unterstellt, ist wegen Verstoßes gegen gesetzliche Bestimmungen nichtig.

11.4 Datenschutz im Rettungsdienst

Bereits im II. Tätigkeitsbericht (S. 57) hatte sich der Landesbeauftragte eingehend mit der Problematik der ärztlichen Dokumentation im Rettungswesen und der Übermittlung personenbezogener medizinischer Daten von Patienten an dritte Stellen auseinandergesetzt und darauf hingewiesen, daß der Inhalt und die Aufbewahrung des Notarzteinsatzprotokolles nunmehr datenschutzgerecht geregelt sind.
Trotz dieser klaren Regelungen wandten sich verschiedene Notärzte erneut wegen der unzulässigen Übermittlung medizinischer Daten an den Landesbeauftragten.

Die Prüfung ergab, daß in allen Fällen an die Träger des Rettungsdienstes ohne Rechtsgrundlage oder Einwilligung neben den erforderlichen Daten zur Abrechnung auch medizinische Daten der Patienten übermittelt worden waren. Daß diese Übermittlung mangels Rechtsgrundlage bzw. Einwilligung gegen die datenschutzrechtlichen Vorschriften verstieß, war den Trägern der Rettungsdienste ebensowenig bewußt, wie die Tatsache, daß damit die ärztliche Schweigepflicht verletzt wurde.
Aber auch den Ärzten war nicht klar, daß sie solchen, für sie erkennbar rechtswidrigen Forderungen, nicht nachkommen dürfen, ohne sich selbst der Gefahr der Strafverfolgung auszusetzen.
Die Beratungsgespräche führten in allen Fällen zu einer sofortigen Änderung des praktizierten Verfahrens. Die unzulässig erhobenen personenbezogenen Daten wurden entsprechend § 16 Abs. 2 Nr. 1 DSG-LSA umgehend gelöscht.

11.5 Beitragsveranlagung durch die Landesärztekammer Sachsen-Anhalt

Mehrere Ärzte haben als Petenten die Frage aufgeworfen, ob das von der Ärztekammer Sachsen-Anhalt praktizierte Verfahren, für die Beitragsveranlagung die Kopie eines Auszuges des Einkommensteuerbescheides oder eine schriftliche Bestätigung des Steuerberaters beizufügen, rechtmäßig ist.

Hierzu war aus datenschutzrechtlicher Sicht folgendes festzustellen:

§ 6 Abs. 1 Satz 4 des Gesetzes über die Kammern für Heilberufe Sachsen-Anhalt (KGHB-LSA) verpflichtet die Kammerangehörigen, die erforderlichen Angaben über ihre für die Berechnung der Beiträge maßgebenden Einkünfte oder Umsätze mitzuteilen. Die dazu von der Kammer aufgrund des KAG-LSA erlassende Beitragsordnung sieht in § 5 Abs. 1 eine Beitragsveranlagung durch Selbsteinstufung des Kammerangehörigen vor. Darüber hinaus verpflichtet § 2 BeitrO jedoch den Beitragspflichtigen, der Einstufung einen entsprechenden Auszug des Einkommensteuerbescheides als Kopie beizulegen bzw. diesen durch eine schriftliche Bestätigung des Steuerberaters zu ersetzen.

Die Beitragssatzung ist gesetzeskonform auszulegen und darf keine schärferen Anforderungen an die Mitglieder stellen, als es die gesetzliche Grundlage in § 6 Abs. 1 Satz 4 KGHB-LSA zuläßt. Demnach haben die Kammermitglieder nur die für die Festsetzung der Kammerbeiträge „maßgebenden Einkünfte oder Umsätze“ mitzuteilen.
Maßgebend für die Beitragsfestsetzung sind aber lediglich die Einkünfte aus Berufstätigkeit im Zusammenhang mit der medizinischen Heilkunde. Dementsprechend sind die übrigen Festsetzungen im Einkommensteuerbescheid - das Einkommenssteuergesetz kennt **sieben** verschiedene Einkunftsarten - für die Beitragsveranlagung der Kammer unerheblich. Im übrigen dürfen neben den von den Kammerangehörigen selbst zu machenden Angaben zusätzliche Nachweise lediglich in Einzelfällen verlangt werden, insbesondere wenn begründete Zweifel an den Angaben bestehen. Die Kammer wird sich im Regelfall auf die übliche, stichprobenartige Überprüfung einer gewissen Quote der Mitglieder zu beschränken haben. Eine uneingeschränkte Überprüfung jedes Mitgliedes in jedem Jahr stünde auch mit dem verfassungsrechtlich abgesicherten Grundsatz der Verhältnismäßigkeit nicht mehr im Einklang.
Die Ärztekammer Sachsen-Anhalt teilt zwischenzeitlich die Auffassung des Landesbeauftragten und wird ihre Veranlagungsvordrucke für 1997 entsprechend ändern.

11.6 Datenübermittlung durch einen berufsständischen Ausschuß

Mit Recht beschwerte sich ein Arzt beim Landesbeauftragten über den gesetzwidrigen Umgang mit seinen Daten. Er hatte seine kassenärztliche Zulassung für einen bestimmten Facharztbereich beantragt und war abgewiesen worden. Im daraufhin erfolgten Widerspruchsverfahren hatte der dafür zuständige berufsständische Ausschuß die vollständige Widerspruchsbegründung des Betroffenen allen mit der gleichen Facharztzulassung niedergelassenen Kollegen und Kolleginnen zur Kenntnis- und Stellungnahme zugesandt.

Zulässig war es, den niedergelassenen Kollegen den Antrag und die Bedürfnisbegründung zur Stellungnahme mitzuteilen. Das Widerspruchsschreiben enthielt aber darüber hinaus eine Fülle weiterer Informationen und personenbezogener Angaben, deren Mitteilung von der hier zu beachtenden Vorschrift des § 12 Abs. 1 Satz 1 DSG-LSA nicht gedeckt war. Da eine Einwilligung des Betroffenen erkennbar ebenfalls nicht vorlag, hätte die Übermittlung und damit verbundene Verletzung der Persönlichkeitsrechte des Betroffenen unterbleiben müssen.

Der Ausschuß hat nach dem Hinweis des Landesbeauftragten umgehend sein Anhörungsverfahren den datenschutzrechtlichen Vorschriften angepaßt. Im Hinblick auf Besonderheiten des Falles konnte ausnahmsweise von einer förmlichen Beanstandung Abstand genommen werden.

11.7 Chipkarten

Bereits seit geraumer Zeit verfolgt der Landesbeauftragte gemeinsam mit den Datenschutzbeauftragten des Bundes und der anderen Länder die Entwicklungen auf dem Sektor der Chipkartenanwendungen, vorrangig im Bereich der Medizin (Krankenversichertenkarte, Röntgen-Card, Apotheken-Card - vgl. II. Tätigkeitsbericht, S. 54), aber auch in den Bereichen Kommunikation und Finanzwesen mit wachsender Besorgnis.
Aus diesem Grund wurde durch die Konferenz der Datenschutzbeauftragten des

Bundes und der Länder am 9./10.11.1995 eine Entschließung zu den datenschutzrechtlichen Anforderungen an den Chipkarteneinsatz im Gesundheitswesen gefaßt **(Anlage 5).**
Damit soll allen für Kartenprojekte im Gesundheitswesen Verantwortlichen ein Arbeitsmittel an die Hand gegeben werden, das helfen kann, das Recht der betroffenen Bürgerinnen und Bürger auf informationelle Selbstbestimmung zu gewährleisten.
Für die Gesetzgeber bei Bund und Ländern existiert hier erheblicher Regelungsbedarf, um die rasch fortschreitende Entwicklung rechtlich zu begleiten und zu kanalisieren und - im Interesse der Bürger - Fehlentwicklungen vorzubeugen.

Weiterhin hat der Arbeitskreis Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hierzu eine Orientierungshilfe zu „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten“ (Stand 02.12.1996) erarbeitet. Diese Orientierungshilfe ist beim Landesbeauftragten erhältlich.

12. Gewerbe, Handwerk und Wirtschaft

12.1 Industrie- und Handelskammern

Rechtsgrundlage für die Tätigkeit der Industrie- und Handelskammern bildet das Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern **(IHK-G)**.

Mit der Gesetzesnovelle vom 23.11.1994 (BGBl. I S. 3475) wurden insbesondere die datenschutzrechtlichen Bestimmungen des **§ 9 IHK-G** hinsichtlich der Erhebungs- und Verarbeitungsrechte präzisiert. Sie traten am 1. Dezember 1995 in Kraft. Damit gibt es bereichspezifische Regelungen zur Datenerhebung bei den Kammerzugehörigen und den Finanzämtern (Abs. 1 und 2), zur Datenspeicherung und -nutzung (Abs. 3) und zur Datenübermittlung an **Dritte** (Abs. 4 und 6).

Absatz 4 Satz 1 erlaubt es, personenbezogene Angaben der Kammerzugehörigen „zur Förderung von Geschäftsabschlüssen und zu anderen, dem Wirtschaftsverkehr dienenden Zwecken“ an eine **nicht-öffentliche** Stelle zu übermitteln. Zulässige Übermittlungsdaten sind Name, Firma, Anschrift und der Wirtschaftszweig. Eine weitergehende Übermittlung personenbezogener Daten ist nur zulässig, soweit der Kammerzugehörige nicht widersprochen hat; er ist durch die IHK vor einer erstmaligen Übermittlung auf sein Widerspruchsrecht hinzuweisen.
Weitere Regelungen betreffen die Zweckbindung von übermittelten Daten beim Empfänger (Abs. 5). Für die Veränderung, Sperrung und Löschung sowie die Übermittlung an **öffentliche** Stellen finden die Datenschutzgesetze der Länder Anwendung (Abs. 6).
Diese Regelungen sind ein positives Beispiel für normenklare gesetzliche Bestimmungen, wie sie das Bundesverfassungsgericht in seiner Rechtsprechung für Eingriffe in das informationelle Selbstbestimmungsrecht gefordert hat.

Der Landesbeauftragte hat die Industrie- und Handelskammern (IHK) mit Sitz in Magdeburg und Halle im Berichtszeitraum im Rahmen seiner Kontrollbefugnis nach § 22 Abs. 1 DSG-LSA überprüft.

Die Kontrollen zeigten bei beiden überprüften Kammern datenschutzrechtliche Defizite, insbesondere bei der Gestaltung der Auftragsdatenverarbeitung.

1. Verarbeitung der Daten der Kammerzugehörigen

   Die IHK führt zur Erfüllung ihrer Kammeraufgaben ein Verzeichnis der Kleingewerbetreibenden (KGT) und der im Handelsregister (HR) eingetragenen Firmen.
   Durch die „IHK Gesellschaft für Informationsverarbeitung mbH Dortmund“ **(IHK-GfI)** werden die Daten der Kammerzugehörigen von bundesweit insgesamt 68 Kammern zentral in einer Verwaltungsdatenbank gespeichert. Weitere 15 Kammern, die ihre Daten dezentral verarbeiten, übermitteln monatlich mittels Datenträgeraustausch die Daten ihrer im HR eingetragenen Firmen der IHK-GfI zur Speicherung in der sog. Referenzdatenbank.

Durch dieses Informationssystem werden den an diese Verwaltungsdatenbank angeschlossenen IHK die Stammdaten eines jeden Kammerzugehörigen im Bundesgebiet zur Information und für Auskünfte zur Verfügung gestellt. Zusätzlich erhalten alle IHK im Rücklauf aus Dortmund eine sog. FIS-CD (FIS - Firmeninformationssystem) mit den Anschriften aller HR-Firmen, die eine bundesweite Recherche ermöglicht.
Das Speichern der Daten in der Verwaltungsdatenbank im Rechenzentrum der IHK-GfI in Dortmund und die Bereitstellung der Daten zum Abruf im automatisierten Verfahren sowie die Speicherung der HR-Firmen in der Referenzdatenbank und deren Bereitstellung auf einer FIS-CD sind jeweils als **Auftragsdatenverarbeitungen bei einer nicht-öffentlichen Stelle nach § 8 DSG-LSA** einzuordnen. Da zum Zeitpunkt der Kontrollen die gesetzlich vorgeschriebenen vertraglichen Vereinbarungen nicht vorlagen, fehlte für diese Datenverarbeitungen durch die IHK-GfI eine wesentliche Rechtsgrundlage.

2. Verarbeitung der Daten der Auszubildenden

Im Zuge der Berufsausbildung werden mit dem Berufsausbildungsvertrag auch personenbezogene Daten bei den Auszubildenden erhoben.
Die Auswertung der bundeseinheitlichen schriftlichen Prüfung der Auszubildenden erfolgt ebenfalls durch das Rechenzentrum der IHK-GfI in Dortmund. Aus verfahrenstechnischen Gründen besteht dort - nach Angabe der überprüften Kammern - zur Durchführung des Programmlaufes die Notwendigkeit, neben den anonymisierten Prüfungsdaten, die gesamten Stammdaten des Auszubildenden zu übergeben. Zur weiteren Verwendung dieser personenbezogenen Daten der Auszubildenden durch die IHK-GfI in Dortmund konnten die hiesigen Kammern keine Auskunft geben. Eine vertragliche Vereinbarung mit der IHK-GfI bestand zum Zeitpunkt der Kontrollen hierzu ebenfalls nicht. Auch diese Datenverarbeitung war damit zu diesem Zeitpunkt unzulässig.

Der Landesbeauftragte hat deshalb gefordert:

- Für den Bereich der **Auftragsdatenverarbeitung** durch die IHK-GfI ist von den Kammern vertraglich sicherzustellen, daß die Bestimmungen des Lan-

desdatenschutzgesetzes befolgt werden und sich die IHK-GfI der Kontrolle durch den Landesbeauftragten unterwirft (§ 8 Abs. 6 DSG-LSA),

- das bei der IHK-GfI eingerichtete **automatisierte Abrufverfahren** aus der Verwaltungsdatenbank ist auf eine gesetzliche Grundlage zu stellen (§ 7 Abs. 1 DSG-LSA).

Durch eine IHK wurde dem Landesbeauftragten inzwischen bereits der entsprechende Vertrag zur Auftragsdatenverarbeitung übersandt. Der Landesbeauftragte wurde darüber informiert, daß in Auswertung seiner Kontrolle der DIHT gegenwärtig einen Muster-Vertrag zur Auftragsdatenverarbeitung erarbeitet. Dieser sei dazu geeignet, auch vorhandene Defizite in anderen Bundesländern hinsichtlich der Auftragsdatenverarbeitung abzubauen. Der Landesbeauftragte wird diese Entwicklung weiterhin aufmerksam verfolgen.

3. Datenschutzrechtlich von Bedeutung ist auch das im Aufbau befindliche automatisierte Abgleichverfahren der „Arbeitsgemeinschaft Kammerleitstelle für Bemessungsgrundlagen e.V.“ **(AKB e.V.)**. Mitglieder der AKB e.V. sind neben der AKG GmbH alle IHK und HK. Dieses neue Verfahren soll zukünftig das bisherige Verfahren in den neuen Bundesländern zur Umsatzabfrage bei den Kammerzugehörigen ersetzen und vereinfachen.
   Die AKB e.V. in Dortmund will ab Januar 1998 mit den Finanzämtern in einen Datenabgleich eintreten. Bis zur Einführung dieses neuen Verfahrens, welches seine Rechtsgrundlage im eigenen Erhebungsrecht der IHK bei den Finanzämtern nach § 9 Abs. 2 IHK-G findet, sind auch hierfür durch die IHK die entsprechenden vertraglichen Regelungen mit der AKB e.V. unter Beachtung der Bestimmungen in § 8 DSG-LSA zu schaffen.

12.2 Handelsregisterdaten im Internet

Wie dem Landesbeauftragten bekannt wurde, bestehen in anderen Bundesländern Bestrebungen von Industrie- und Handelskammern, Handelsregisterdaten ihrer Kammerzugehörigen im Rahmen ihres Serviceangebotes in das Internet einzustellen.

Obwohl sich nach Angabe des Ministeriums für Wirtschaft, Technologie und Europaangelegenheiten das Problem in Sachsen-Anhalt zur Zeit noch nicht stellt, weist der Landesbeauftragte vorsorglich auf die datenschutzrechtliche Problematik solcher Verfahren hin:

1. **§ 9 Abs. 4 IHK-G** bildet die bereichsspezifische gesetzliche Grundlage für die Datenübermittlung an nicht-öffentliche Stellen. Dabei ist die Einschränkung in § 9 Abs. 4 Satz 1 IHK-G beachtlich, wonach solche Datenübermittlungen nur zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken erfolgen dürfen.
   Mit der Einstellung der Handelsregister- und womöglich weiterer Daten in das **Internet** zum unkontrollierten Abruf durch jedermann wäre diese Zweckbestimmung nicht mehr gewährleistet.

2. Nach **§ 8 HGB** i.V. mit **§ 125 FGG** liegt die Zuständigkeit zur Führung des Handelsregisters bei den Gerichten bzw. den Amtsgerichten.
   Mit der Einstellung von Handelsregisterdaten durch die Industrie- und Handelskammern in das **Internet** würden unzulässige (Teil-) Handelsregister entstehen. Vom Bundesgesetzgeber ist ein bundesweites und weltweit bekanntes Handelsregister nicht vorgesehen. Ein solches würde aber zwangsläufig entstehen, wenn alle Industrie- und Handelskammern Deutschlands dem Vorhaben folgten.
   Deshalb würden die Handelsregisterdaten mit der Einstellung in das Internet eine völlig neue Qualität erhalten und der vom Bundesgerichtshof getroffenen Entscheidung vom 12.07.1989 zur gewollten Eingrenzung des § 9 HGB widersprechen.

Keine Einwände hätte der Landesbeauftragte gegen die Einstellung von Handelsregisterdaten der Kammerzugehörigen, die dazu nach § 4 Abs. 2 DSG-LSA ihre Einwilligung erteilen. Zuvor müssen den Betroffenen aber die besonderen Gefahren aufgrund der technischen Besonderheiten des Internet deutlich gemacht werden.

12.3 Fortbildungsprüfungsordnungen gem. § 46 BBiG bei den Kammern

Die IHK und die Handwerkskammern können nach § 46 Abs. 1 BBiG Prüfungen zum Nachweis der durch die berufliche Fortbildung erworbenen Kenntnisse, Fertigkeiten und Erfahrungen durchführen. Hierzu erlassen sie auf gesetzlicher Grundlage Prüfungsordnungen, die auch die Prüfungsvoraussetzungen festzulegen haben.
Der Landesbeauftragte ließ sich im Berichtszeitraum die Prüfungsordnungen vorlegen und stellte fest, daß mehrere Kammern in ihren Prüfungsordnungen als eine der Zulassungsvoraussetzungen die Vorlage eines tabellarischen Lebenslaufes vorsahen.
So wie der Landesbeauftragte konnten auch das die Rechtsaufsicht über die genannten Kammern führende Ministerium für Wirtschaft, Technologie und Europaangelegenheiten die Erforderlichkeit für die Erhebung einer solchen Sammlung personenbezogener Daten für Fortbildungsprüfungen nicht erkennen.
Das Bundesverfassungsgericht hat in der Begründung seines Urteils zum Volkszählungsgesetz ausgeführt, daß ein Zwang zur Abgabe personenbezogener Daten, z.B. in einer Prüfungsordnung, voraussetzt, daß der Gesetzgeber (in diesem Fall die betreffende Kammer) den Verwendungszweck bereichsspezifisch präzise bestimmt und daß die Angaben für diesen Zweck geeignet und **erforderlich** sind, wobei sich die erhebende öffentliche Stelle auf das **erforderliche Minimum** zu beschränken hat. Ein tabellarischer Lebenslauf dürfte, jedenfalls bei Fortbildungsprüfungen, nicht mehr zu den erforderlichen Angaben gehören.
Die Intervention des Landesbeauftragten führte dazu, daß die Prüfungsordnungen entsprechend geändert wurden.

13. Hinweise zum technischen und organisatorischen Datenschutz

Jede öffentliche Stelle, die personenbezogene Daten speichert, hat die rechtliche Verpflichtung, die ihr einmal anvertrauten Daten der Bürgerinnen und Bürger sicher, und für den Rechtsverkehr jederzeit vollständig verwendbar, aufzubewahren. Sie wird deshalb sehr genau zu beachten haben, daß zur Aufgaben-

erledigung gespeicherte Daten auf einem richtig ausgesuchten und aufbewahrten Papierträger wahrscheinlich in 3 000 Jahren noch vollständig und in brauchbarer Qualität erhalten sein werden, wenn man sie dann noch benötigt. Vergleichbares ist bei vielen im Markt befindlichen elektronischen Datenträgern nicht gewährleistet. Darauf gespeicherte Daten sind möglicherweise schon nach wenigen Jahren nicht mehr vollständig erhalten und nutzbar. Dabei sind die in ihren Auswirkungen noch gar nicht überschaubaren, systemimmanenten Schwächen bei der Software vieler Rechnersysteme zum bevorstehenden Jahrtausendwechsel noch gar nicht berücksichtigt. Hinweise in der Fachpresse, daß als Folge der nur zweistellig gespeicherten Jahreszahl mit dem Wechsel ins Jahr **2000** ganze Datenbestände systemseitig oder als Folge mangelhafter Programmierung gelöscht werden könnten, sollten deshalb ernstgenommen werden.

13.1 Anschluß von Verwaltungsnetzen an das INTERNET

Die Landesverwaltung nutzt das Internet bereits heute zur Informationsdarstellung von Themen aus dem Umweltbereich, dem Statistikbereich und zur Präsentation des Landes Sachsen-Anhalt. Solange diese Informationen keinen Personenbezug besitzen und die separat betriebenen WWW-Server **nicht** in das lokale automatisierte Verwaltungsnetz einer öffentlichen Stelle eingebunden sind, bestehen gegen diese Form der Nutzung keine datenschutzrechtlichen Bedenken. Auch eine Informationsbeschaffung aus dem Internet mittels lokal angeschlossener PC birgt zunächst nur Gefahren für den einzeln angeschlossenen PC in sich. Seit einiger Zeit verstärkt sich aber in öffentlichen Stellen der Wunsch nach einem generellen Zugang zu diesem globalen Datennetz. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen.
Bevor eine öffentliche Stelle einen solchen Zugang zum Internet schafft, muß sie eine **Analyse des Kommunikationsbedarfs** durchführen. Bei der Beurteilung der rechtlichen Erforderlichkeit eines Internet-Anschlusses ist - jedenfalls wenn datenschutzrechtliche Belange berührt sind - ein strenger Maßstab anzulegen. Auch wenn die Erforderlichkeit generell bejaht wird, ist zu prüfen, ob der

Verwendungszweck nicht schon durch den Anschluß eines isolierten Rechners erreicht werden kann, um die Risiken für die Datensicherheit zu minimieren.

Die Art des technisch zu realisierenden Zugangs hängt wesentlich davon ab, welche **Internet-Dienste** genutzt werden sollen. Dabei ist zu unterscheiden zwischen Diensten, die von lokalen Benutzern im Internet abgerufen werden, und Diensten, die von lokalen Rechnern für Benutzer im Internet erbracht werden. Diese Kommunikationsanforderungen müssen auf Grund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zum Internet als auch für jeden einzelnen Rechner analysiert werden. Es dürfen nur die IP-Pakete weitergeleitet werden, die für den zu nutzenden Dienst bezogen auf den nutzungsberechtigten Rechner notwendig sind.
Wird bei der Analyse des Kommunikationsbedarfs festgestellt, daß die Anbindung an das Internet auf IP-Ebene notwendig ist, das **TCP/IP-Protokoll** also in seiner vollen Funktionalität genutzt werden soll, müssen weitere Sicherheitsbetrachtungen folgen, die Voraussetzung für die Planung und Realisierung von Sicherheitskonzepten sind. Ausgangspunkte einer derartigen Risikoanalyse sind der Schutzbedarf der zu verarbeitenden personenbezogenen Daten und die Sicherheitsziele der öffentlichen Stelle.

Es gilt der Grundsatz: Nichts ist sicher im Internet! Die Sicherheitsrisiken der Nutzung resultieren daraus, daß das Internet **nicht** unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen.
Hierzu gehören z.B. das Fehlen sicherer Mechanismen zur Identifikation und Authentisierung im Netz. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen, manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von z. Zt. schon mehr als 40 Millionen Internet-Teilnehmern die Zahl der Angreifer sich täglich vermehrt.

Eine vom Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder erarbeitete **Orientierungshilfe** soll den öffentlichen Stellen eine Hilfestellung bieten. Die Orientierungshilfe soll den für den Betrieb von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der "internen" Netze bei einem Anschluß an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können.

Die nachfolgenden Empfehlungen sind Bestandteil der o.g. Orientierungshilfe, die wegen ihres Umfanges in diesem Bericht nicht abgedruckt, aber beim Landesbeauftragten abgefordert werden kann.

1. Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und soweit dies **erforderlich** ist. Die Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muß, und ob die Aufgabe mit einem nicht in das Verwaltungsnetz eingebundenen Rechner erfüllt werden kann.

2. Voraussetzung für die Anbindung eines solchen Netzes an das Internet ist das Vorliegen eines schlüssigen **Sicherheitskonzepts** und dessen konsequente Umsetzung. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

3. Die Sicherheit des Verwaltungsnetzes und der Schutz von personenbezogenen Daten, die auf vernetzten Systemen verarbeitet werden, ist durch geeignete **Firewall-Systeme** sicherzustellen, die eine differenzierte Kommunikationssteuerung und Rechtevergabe unterstützen. Dabei sind die Anforderungen, die von den Firewall-Komponenten zu erfüllen sind, vorab zu definieren, wobei sich die Verwaltung ggf. auch externen Sachverstandes bedienen sollte. Auch hier gilt: Es gibt bislang keine absolut sicheren Firewall-Systeme!

4. Der Gefahr von Maskeraden-Angriffen und der Ausforschung der Netzstrukturen des zu schützenden Netzes ist durch die Verwendung einer gesonderten **internen Adreßstruktur** entgegenzuwirken. Die internen Adressen des zu schützenden Netzes sind durch den zentralen Firewall auf externe Internet-Adressen umzusetzen.

5. Der ausschließliche Einsatz einer **zentralen Firewall-Lösung** ist nur dann vertretbar, wenn eine Orientierung am höchsten Schutzbedarf erfolgt, auch wenn dies Nachteile für weniger sensible Bereiche mit sich bringt. Die Frage der Kontrolle interner Verbindungen bleibt bei einer solchen Lösung offen. Ferner ist eine ausschließlich zentrale Lösung mit der Maxime der lokalen Haltung und Verwaltung von sicherheitsrelevanten Daten (Pflege von Benutzerprofilen) schwer vereinbar. Werden solche Daten nicht durch diejenigen verwaltet, die den verwalteten Bereich direkt überschauen können, besteht die Gefahr erheblicher Differenzen zwischen der Realität und ihrem sicherheitstechnischen Abbild.

6. Das Konzept **gestaffelter Firewalls** kommt den Datenschutzanforderungen an Verwaltungsnetze entgegen, die aus einer Vielzahl verschiedener Teilnetze bestehen, in denen Daten unterschiedlicher Sensibilität von unterschiedlichen Stellen für unterschiedliche Aufgaben verarbeitet werden und in denen dementsprechend jeweils unterschiedliche Sicherheitsanforderungen bestehen. Die mit gesonderten Firewalls abgesicherten Subnetze sollten jeweils einen definierten Übergang zu dem Gesamtnetz erhalten. Die Anbindung des Gesamtnetzes an das Internet sollte stets über einen zentralen Gateway erfolgen, der durch einen Firewall geschützt wird.

7. Der **personelle** und **sachliche Aufwand** für Firewall-Lösungen ist generell hoch. Es ist gleichwohl unverzichtbar, hochspezialisierte Kräfte einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein. Dieser Aufwand ist jedoch stets dann gerechtfertigt, wenn Verwaltungsnetze an das Internet angeschlossen werden sollen, in denen sensible personenbezogene Daten verarbeitet werden.

8. Der Betrieb von Firewall-Systemen muß klaren **Richtlinien** folgen. Diese Richtlinien müssen neben Zuständigkeitsregelungen auch Vorgaben über die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und die Sanktionen bei Sicherheitsverstößen enthalten.

9. Auch beim Einsatz von Firewalls bleiben **Restrisiken** bestehen, denen anwendungsbezogen begegnet werden muß. So bleibt es auch beim Einsatz von Firewalls notwendig, sensible Daten nur verschlüsselt zu speichern und zu übertragen; hierzu gehören neben besonders sensiblen personenbezogenen Daten auch Paßwörter und sonstige Authentifikationsdaten.

10. Bei einem **unvertretbaren Restrisiko** muß auf einen Anschluß des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste muß in diesem Fall auf nicht in das Verwaltungsnetz eingebundene Systeme beschränkt werden, auf denen ansonsten keine sensiblen Daten verarbeitet werden.

11. Firewall-Konzepte entlasten die dezentralen **Verwalter** von vernetzten Systemen nicht von ihrer Verantwortung zur Gewährleistung des Datenschutzes; vielmehr erhöhen sich mit der Vernetzung die Anforderungen an die lokale Systemverwaltung, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben können, als bei stand alone betriebenen Rechnern.

Gleichzeitig muß aber darauf hingewiesen werden, daß, selbst wenn Maßnahmen gegen die bekannten Gefährdungen getroffen werden, ein hundertprozentiger Schutz ohne Verzicht auf die Netzanbindung an das Internet nicht zu realisieren ist. Nachfolgende Beispiele von **protokollimmanenten** und **dienstespezifischen Sicherheitsrisiken** häufig genutzter Internet-Dienste sollen die datenschutzrechtlichen Bedenken verdeutlichen:

- **Protokollimmanente Sicherheitsrisiken**

  Sowohl die Nutzerkennung als auch das Paßwort werden bei den gängigen Diensten im Klartext über das lokale Netz und über das Internet übertragen. Mit Programmen, die unter dem Namen „Packet Sniffer“ bekannt sind, kann

der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden. So können diese Abhörprogramme zahlreiche Nutzerkennungen mit den zugehörigen Paßworten ausspähen, mit deren Hilfe sich ein Angreifer einen unberechtigten Zugriff auf andere Rechner verschaffen kann.
Datenpakete können nicht nur abgehört, sondern auch **manipuliert** werden. Da bei vielen Internet-Diensten die Authentisierung der Rechner lediglich über die IP-Nummer des Nutzers erfolgt, kann sich dies ein Angreifer zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen an ein fremdes Rechnersystem schickt (IP-Spoofing). Sofern das System die IP-Adresse für vertrauenswürdig hält, wird dem Eindringling ein Zugang, unter Umständen sogar mit Administratorrechten, gewährt. Ferner kann der Übertragungsweg bei dynamischem Routing geändert werden. Pakete können abgefangen werden, so daß sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch **eigene** Pakete ersetzen. Weiterhin läßt sich die Kommunikation eines autorisierten Nutzers aufzeichnen und später wieder einspielen, wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers verschafft.

- **Dienstspezifische Sicherheitsrisiken**

  E-Mail und Usenet-News (Elektronisches Post- und Diskussionsforum - sog. „Schwarzes Brett“):
  Private Nachrichten können mitgelesen werden, sofern sie nicht verschlüsselt sind. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht verändern oder fälschen. Über den elektronischen Postweg können Programme und Textdokumente mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz. Die Informationen über Datum und Uhrzeit der Erstellung einer Nachricht können zu einem Persönlichkeitsprofil des Absenders ausgewertet werden. Daneben forschen Adreßsammler nach E-Mail- und Post-Adressen, um unaufgefordert Werbung zuzuschicken. „Sendmail“, das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post, weist zudem eine ganze Reihe von sicherheitsrelevanten Fehlern auf, die zu einer Zugangsmöglichkeit mit Administratorrechten

führen können. Zudem ist nicht sicherzustellen, daß eine E-Mail den Empfänger überhaupt erreicht und daß der Absender einen Nachweis der Zustellung erhält.

Telnet (Aufbau einer Terminal-Sitzung auf einem entfernten Rechner):
Ist der Telnet-Dienst nicht eingeschränkt, sondern von beliebigen Adressen aus zu beliebigen Ports auf dem eigenen Rechner möglich, wird die Zugangskontrolle gefährdet. Auch ein Angreifer, dem es nicht gelingt, sich einen Zugang mit Administratorrechten zu verschaffen, hat häufig die Möglichkeit, einen nichtprivilegierten Account auf dem Rechner zu nutzen. Dieser Account kann dann als Ausgangsbasis für den Angriff auf weitere Rechner verwendet werden.

FTP (interaktiver Dateitransfer von oder zu einem entfernten Rechner):
Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen des FTP-Server-Programms Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Besondere Vorsicht ist geboten, da viele Beschreibungen zur Installation und Konfiguration von „Anonymous-FTP“-Servern sicherheitsrelevante Fehler enthalten. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, die Datei mit den verschlüsselten Paßwörtern aller Benutzer auf seinen Rechner zu laden und dort in aller Ruhe zu entschlüsseln.

WWW (multimedialer Informationsdienst; Integration von beliebigen Text-, Bild-, Ton-, Videodokumenten auf Basis HTML und mittels HTTP):
Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) läßt sich die Kommunikation abhören. Außerdem weisen CGI-Skripte (Common Gateway Interface) häufig Sicherheitslücken auf. Zur Zeit sind WWW-Browser in der Entwicklung, die das Ablegen von Dateien auf dem Server erlauben. Dies kann zu weiteren Sicherheitsproblemen führen. Beim Nutzen des WWW können zahlreiche Daten über den Anwender und sein Verhalten (was hat wer wann aufgerufen und wie lange gelesen?) protokolliert werden, so daß ein umfassendes Persönlichkeitsprofil erstellt werden kann.

13.2 Kryptographie

Sichere kryptographische Verfahren für Zwecke der

- digitalen Signatur (elektronische Unterschrift),
- Identifikation/Authentisierung und Zugriffskontrolle (z.B. als „digitaler Ausweis“ in Netzen) und
- Verschlüsselung

sind Voraussetzungen für einen wirksamen Datenschutz beim Einsatz von Informationstechnik mit lokaler (LAN) wie auch überregionaler (MAN, WAN) Vernetzung. Es wird jedoch weltweit in unterschiedlicher Ausprägung kontrovers diskutiert, inwieweit die mit der Kryptierung verbundene Erhöhung der IT-Sicher-heit - und damit auch des Datenschutzes - sich staatlichen Sicherheitsinteressen unterzuordnen hat.
Auch in Deutschland existiert dieser Zwiespalt; einerseits will man dem Bürger - das zeichnet den demokratischen Rechtsstaat aus - die Möglichkeit der vertraulichen Kommunikation geben, andererseits sehen sich die Sicherheits- und Strafverfolgungsbehörden, ohne eine Öffnung kryptografischer Verfahren zu ihren Gunsten, in ihrer Aufgabenwahrnehmung eingeschränkt bzw. behindert.
Als Beispiel sei hier das Argument genannt, es sei eine Gefährdung des Rechtsstaates, falls durch eine Kryptierung kriminelle Machenschaften im Telefon- oder im Datenverkehr nicht mehr aufgedeckt und damit auch deren Inhalte als Beweismittel nicht mehr genutzt werden könnten.

Der Landesbeauftragte hat sich gemeinsam mit den Datenschutzbeauftragten des Bundes und der anderen Länder frühzeitig an einer entsprechenden Diskussion beteiligt, in deren Ergebnis die Entschließung zu „Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten“ vom 09.05.1996 **(Anlage 6)** entstand.
Für den Landesbeauftragten ist z.Zt. nicht nachvollziehbar, warum im gegenwärtigen Briefverkehr für jedermann Verschlüsselungsmethoden zumindest theoretisch möglich und zulässig sind, demgegenüber bei modernen Kommunikationstechnologien ein Kryptographiegesetz die Bürger ohne Unterschied bevormunden und sogar kriminalisieren soll.

13.3 Optische Datenspeicherung

Im Berichtszeitraum sind auch in Sachsen-Anhalt vermehrt Anwendungsgebiete für die optische Datenspeicherung (z.B. CD-ROM, WORM-Platte) entstanden. Grund ist häufig die Umstellung von Archivierungssystemen wegen Platzmangels. Markanter Unterschied zwischen herkömmlichen magnetischen Speicherungsmethoden auf Festplatten, Disketten oder Magnetbändern und den o.g. Speichermedien ist, daß diese Speichermedien (außer ROD-MO) nur einmal beschreibbar sind und gespeicherte Daten ausschließlich durch Vernichten des gesamten Datenträgers physisch gelöscht werden können. Soll der Datenträger weiter genutzt werden, bietet die WORM-Technologie gewisse Möglichkeiten. Enthält die Indexdatei des übergeordneten Dateiverwaltungssystems einen Sperrvermerk, kann ein Zugriff auf die gespeicherten gesperrten Daten ausgeschlossen werden; allerdings sind hierzu außerdem flankierende Organisationsanweisungen erforderlich. Der Landesbeauftragte mußte wiederholt öffentliche Stellen darauf aufmerksam machen, daß die an die Stelle der Löschung tretende Sperrung nach § 16 Abs. 3 Ziff. 3 DSG-LSA bisweilen die in Spezialgesetzen geforderte physische (unumkehrbare) Löschung der Daten nicht ersetzen kann, eine solche Speicherung also unzulässig sein könnte.
Eine Möglichkeit, hier doch Recht und Technik in Einklang zu bringen, besteht darin, unter Verwendung des alten Datenträgers einen neuen Datenträger zu beschreiben, der die zu löschenden Daten nicht mehr enthält.
Im Zusammenhang mit der optischen Datenspeicherung hat der Arbeitskreis Technische und organisatorische Datenschutzfragen der Ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe herausgegeben, die beim Landesbeauftragten abgefordert werden kann.

13.4 Datenschutz und Telefax

Bereits in seinem II. Tätigkeitsbericht (S. 91) hatte der Landesbeauftragte darauf aufmerksam gemacht, daß der Einsatz von Telefaxgeräten zur Übermittlung

personenbezogener Daten generell als ein rechtlich und technisch unzuverlässiges Verfahren einzustufen ist. Auch in diesem Berichtszeitraum mußte der Landesbeauftragte wiederholt öffentliche Stellen auf die besonderen Gefahren und Risiken für die Vertraulichkeit der per Telefax übermittelten Informationen hinweisen.

Der Benutzer eines Telefaxgerätes sollte sich stets vor Augen halten, daß

- die Informationen grundsätzlich unverschlüsselt übertragen werden,
- der Empfänger sie damit in offener Form - wie eine Postkarte - erhält,
- Telefaxverkehr wie ein Telefon abhörbar ist,
- die Adressierung nur durch eine Ziffernfolge erfolgt, damit Fehler wahrscheinlicher werden und Übertragungen an den falschen Empfänger nicht oder zu spät bemerkt werden,
- bei modernen Telefaxgeräten vom Hersteller Fernwartungen durchgeführt werden können, ohne daß der Besitzer diesen Zugriff bemerkt (u.U. kann der Seitenspeicher ausgelesen werden und Manipulationen am Rufnummernspeicher sind möglich),
- ein „OK-Sendebericht“ keinerlei Gewähr für die richtige und vollständige Ankunft bietet.

a) Beim Betrieb von Telefaxgeräten ist deshalb für die Übermittlung personenbezogener Daten mit dieser Technik **mindestens** zu beachten:

1. Die Übertragung sensibler personenbezogener Daten per Telefax sollte nur im Ausnahmefall und dann unter Einhaltung zusätzlicher Sicherheitsvorkehrungen erfolgen.
2. Was am Telefon aus Gründen der Geheimhaltung nicht gesagt werden darf, darf auch nicht ohne besondere Sicherheitsvorkehrungen (z.B. Verschlüsselungsgeräte) gefaxt werden. Das gilt insbesondere für rechtlich besonders geschützte personenbezogene Daten, beispielsweise solche, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (Sozial-, Steuer-, Personal- und medizinische Daten).
3. Telefaxgeräte sollten nur auf der Grundlage schriftlicher Dienstanweisungen eingesetzt werden. Die Bedienung darf nur durch eingewiesenes Personal erfolgen.

4. Das Telefaxgerät ist so aufzustellen, daß Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Schreiben erhalten können.
5. Bei der Übertragung sensibler personenbezogener Daten ist zusätzlich mit dem Empfänger eine Sendezeit abzustimmen, damit Unbefugte am Empfängergerät keinen Einblick nehmen können. So kann auch eine Fehlleitung z.B. durch veraltete Anschlußnummern oder beim Empfänger aktivierte Rufumleitungen bzw. Weiterleitungen vermieden werden.
6. Alle vom Gerät angebotenen Sicherheitsmaßnahmen (z.B. Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nach Paßwort, Fernwartungsmöglichkeit sperren) sollten genutzt werden.
7. Bei Telefaxgeräten, die an Nebenstellen angeschlossen sind, ist das Risiko einer fehlerhaften Absendung besonders groß, da vor der Nummer des Teilnehmers zusätzlich Zeichen zur Steuerung der Anlage eingegeben werden müssen. Beim Umgang mit derartigen Geräten ist deshalb besondere Sorgfalt geboten.
8. Die Dokumentationspflichten müssen eingehalten werden (z.B. Vorblatt mit Hinweis auf Ansprechpartner des Absenders bei Fehlleitung oder entsprechend aussagekräftige Aufkleber verwenden, Zahl der Seiten angeben, Protokolle aufbewahren).
9. Die am Telefaxgerät eingestellten technischen Parameter und Speicherinhalte sind regelmäßig zu überprüfen, damit beispielsweise Manipulationsversuche frühzeitig erkannt und verhindert werden können.
10. Verfügt das Telefaxgerät über eine Fernwartungsfunktion, sollte sie grundsätzlich durch den Nutzer deaktiviert werden. Nur für notwendige Wartungsarbeiten ist diese Funktion freizugeben. Nach Abschluß der Wartungsarbeiten sollten die eingestellten Parameter und Speicherinhalte kontrolliert werden.
11. Vor Verkauf, Weitergabe oder Aussonderung von Telefaxgeräten ist zu beachten, daß alle im Gerät gespeicherten Daten (Textinhalte, Verbindungsdaten, Kurzwahlziele usw.) gelöscht werden.

b) PC mit Standard- oder Bürokommunikationssoftware können um Hard- und Softwarekomponenten erweitert werden, mit deren Hilfe Telefaxe gesendet und empfangen werden können (integrierte Telefaxlösungen). Lösungen für den

Faxbetrieb werden sowohl für Einzelplatzrechner als auch für Rechnernetze angeboten.

Der Betrieb (Installation, Konfiguration, Bedienung und Wartung) integrierter Telefaxlösungen birgt gegenüber dem konventionellen Telefaxgerät **zusätzliche** Gefahren, da beispielsweise die verwendeten Faxmodems bzw. -karten oft nicht nur für Telefaxsendung und -empfang geeignet sind, sondern auch andere Formen der Datenübertragung und des Zugriffs ermöglichen.

Daher sollten die folgenden Empfehlungen beim Umgang mit **integrierten** Telefaxlösungen **zusätzlich** beachtet werden:

1. Das verwendete Rechnersystem muß sorgfältig konfiguriert und gesichert sein. Die IT-Sicherheit des verwendeten Rechners bzw. Netzes ist Voraussetzung für einen datenschutzgerechten Betrieb der Faxlösungen. Dazu gehört u.a., daß kein Unbefugter Zugang oder Zugriff zu den benutzten Rechnern und Netzwerken hat.
2. Beim Absenden ist auf die korrekte Angabe der Empfänger zu achten. Dazu sind die durch die Faxsoftware bereitgestellten Hilfsmittel wie Faxanschlußlisten, in denen Empfänger und Verteiler mit aussagekräftigen Bezeichnungen versehen werden können, zu benutzen.
3. Die vielfältigen Nutzungsmöglichkeiten integrierter Faxlösungen erfordern die regelmäßige und besonders sorgfältige Überprüfung der in der Faxsoftware gespeicherten technischen Parameter, Anschlußlisten und Protokolle.
4. Der Einsatz kryptographischer Verfahren ist bei integrierten Faxlösungen unkompliziert und kostengünstig möglich, sofern beide Seiten kompatible Produkte einsetzen. Deshalb sollten personenbezogene Daten möglichst verschlüsselt und digital signiert übertragen werden, um das Abhören zu verhindern und um den Absender sicher ermitteln und Manipulationen erkennen zu können.
5. Schon bei der Beschaffung integrierter Telefaxlösungen sollte darauf geachtet werden, daß ausreichende Konfigurierungsmöglichkeiten vorhanden sind, um die notwendige Anpassung an die datenschutzrechtlichen Erfordernisse des Nutzers zu gewährleisten.

13.5 Computerviren

Zum Thema Computerviren wird in einschlägigen Fachpublikationen regelmäßig über die sich Jahr für Jahr verschärfende Virenproblematik berichtet, und die Medien suchen mit vielen Beiträgen, die Sensibilität der Computerbenutzer für Fragen des Schutzes vor Computerviren zu wecken. Auch der Landesbeauftragte hat in seinem II. Tätigkeitsbericht (S. 72) und bei seinen Beratungen und Kontrollen stets eindringlich vor dem leichtfertigen Umgang mit möglicherweise virusinfizierten Dateien gewarnt. Dennoch erhielt er im vergangenen Zeitraum wiederum mehrfach Berichte öffentlicher Stellen über festgestellte Virusinfektionen.
Der Landesbeauftragte wiederholt deshalb noch einmal seine Hinweise.

Neben der regelmäßigen Fortbildung der für die Computersicherheit Verantwortlichen in den öffentlichen Stellen sind zum Schutz vor Computerviren und zur Schadensminimierung folgende Grundregeln einzuhalten:

- regelmäßige Datensicherung,
- regelmäßiger Einsatz von aktuellen Virenscannern, in Verbindung mit der Benutzung von Prüfsummenprogrammen,
- Ausschluß der Verwendung privater Hard- und Software sowie Public-Domain- bzw. Shareware-Programmen,
- Überprüfung aller eingehenden Datenträger vor ihrer Verwendung auf Virusinfektionen, das gilt auch für via **Internet heruntergeladene** Dateien.

Sollten sich doch virenverdächtige Aktivitäten zeigen, ist zur Virusbeseitigung und Schadensminimierung stets ein Spezialist zu Rate zu ziehen.

14. Hochschulen

Gefundene Matrikellisten

Ein Mitarbeiter einer Universität übersandte dem Landesbeauftragten personenbezogene Auszüge aus dem Matrikelbuch mit dem Hinweis, diese Listen auf einem Tisch des Speisesaales gefunden zu haben.

Die datenschutzrechtliche Überprüfung ergab, daß die Listen durch eine Aushilfskraft, die diese Unterlagen im Rahmen ihrer Tätigkeit erhalten hatte, liegengelassen wurden. Auch im Anschluß an diese „Nachlässigkeit“ war niemandem aufgefallen, daß eine Vielzahl personenbezogener Daten bei der Bearbeitung plötzlich fehlte.

Der Landesbeauftragte nahm diesen Vorfall zum Anlaß, der Universität zu empfehlen, ihre organisatorischen Maßnahmen zu überprüfen und künftig sicherzustellen, daß ihre innerbehördliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle gemäß § 6 DSG-LSA i.V. mit Ziff. 6.3.1.2.3 ff VV-DSG-LSA). Eine geeignete Maßnahme beim Einsatz von Aushilfskräften wäre z.B. die kontrollierte Aushändigung und Rückgabe der Datenträger.
Der Fall hat deutlich gemacht, daß die vorgenommene Belehrung auf das Datengeheimnis allein, ohne eine entsprechende Kontrolle, nicht ausreicht, um den Schutz der personenbezogenen Daten sicherzustellen.
Der Landesbeauftragte hat empfohlen, künftig in einem solchen Fall auch einen Strafantrag nach § 31 Abs. 4 DSG-LSA wegen unbefugter Datenübermittlung zu prüfen.

15. Kommunalverwaltung

15.1 Falsch zugestellte Unterlagen zur Vorbereitung einer Ratssitzung

Durch die Eingabe eines Bürgers erfuhr der Landesbeauftragte davon, daß in einer Stadt vor einer Ratssitzung durch Selbstzustellung Sitzungsunterlagen mit personenbezogenen Daten über einen Grundstücksverkauf, die für ein Ratsmitglied bestimmt waren, fälschlicherweise in den Nachbarbriefkasten eingeworfen wurden.
Erst durch die vom Landesbeauftragten bei der Stadt angeforderte Stellungnahme ist dem Bürgermeister, der die Zustellung selbst ausgeführt hatte, klargeworden, daß dem betreffenden Stadtrat offenbar schon früher fälschlicherweise über den Briefkasten eines anderen Bürgers amtliche Unterlagen zugestellt wurden. Dies war nur deshalb nicht aufgefallen, weil dieser die Briefe

dann jeweils ohne viel Aufhebens in den benachbarten Briefkasten des Stadtrates gesteckt hatte.

Der Landesbeauftragte hat die fehlerhafte Zustellung der Unterlagen durch den Bürgermeister wegen des Verstoßes gegen die Amtsverschwiegenheit (§ 68 GO LSA und § 61 BG LSA) gerügt.
In Anbetracht der besonderen Umstände dieses Falles hat er aber gem. § 24 Abs. 3 DSG-LSA von einer formellen Beanstandung abgesehen.

15.2 Öffentliche Bekanntgabe von Geburten und Eheschließungen

Eine Kommunalverwaltung veröffentlichte in der örtlichen Presse unter der Rubrik „Meldungen des Standesamtes“ 17 Geburten und 8 Eheschließungen. Die Veröffentlichung enthielt neben Vor- und Familiennamen sowie den jeweiligen Wohnorten auch die Geburts- und Eheschließungsdaten der Betroffenen.

Der Landesbeauftragte hat die betreffende Kommunalverwaltung darauf hingewiesen, daß für eine öffentliche Bekanntgabe (Übermittlung) dieser Daten das Personenstandsgesetz keine Rechtsgrundlage enthält. Also wäre diese nur mit der Einwilligung des betroffenen Personenkreises bzw. deren gesetzlichen Vertreter zulässig gewesen. Darüber hinaus wurde der Kommunalverwaltung empfohlen, auch bei Vorliegen einer formellen Einwilligung nach § 4 Abs. 2 DSG-LSA, die Daten lediglich im Rahmen des RdErl. des Ministerium des Innern vom 21.05.1992 Az.:- 42.12 -11103 - (nicht veröffentlicht) bekanntzugeben.

Die Kommunalverwaltung wird die bisherige Verfahrensweise bei künftigen Veröffentlichungen umstellen.

16. Landtag und Landesregierung

16.1 Datenschutz im Landtag

Personenbezogene Daten werden von den Parlamenten in zunehmenden Maße auch unter Einsatz moderner Informations- und Kommunikationstechnik verarbeitet und damit einem breiten Kreis von Interessenten erschlossen. In den anderen Bundesländern ist deshalb im Auftrag der Konferenz der Präsidenten der deutschen Landesparlamente eine Empfehlung für ein „parlamentsspezifisches Datenschutzrecht“ erarbeitet worden.

Für Sachsen-Anhalt ist die Rechtslage schon seit 1992 zufriedenstellend geregelt.
Artikel 6 Abs. 1 der Landesverfassung Sachsen-Anhalt räumt jedermann das Recht auf Schutz seiner personenbezogenen Daten ein. Daran orientiert sich auch der Landtag. Mit der 1992 verabschiedeten Fassung des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) hat er sich selbst unter den Anwendungsbereich des Gesetzes gestellt (§ 3 Abs. 1 DSG-LSA). Damit gelten dessen Bestimmungen, soweit nicht bereichsspezifische Regelungen in der Landesverfassung, insbesondere die verfassungsrechtlichen Rechte des einzelnen Abgeordneten oder des Parlaments als ganzes dem vorgehen.

16.2 Immunität von Mitgliedern des Landtages von Sachsen-Anhalt

Das Ministerium der Justiz hat die Frage aufgeworfen, ob Artikel 58 der Verfassung des Landes Sachsen-Anhalt, der im übrigen Artikel 46 GG nachgebildet ist, als Rechtsgrundlage für eine Mitteilung der Justiz in Strafsachen herangezogen werden kann, mit der z.B. dem Landtag der Abschluß eines Verfahrens gegen einen Abgeordneten mitgeteilt wird.
Hierzu war aus datenschutzrechtlicher Sicht folgendes aufzuführen:

1. Aus Artikel 58 Landesverfassung ergibt sich unmittelbar, daß nicht dem einzelnen Abgeordneten besondere Rechte eingeräumt werden, etwa mit der

Folge, daß dieser rechtswirksam auf seine Immunität verzichten oder auch nur bindend vom Landtag ihre Aufhebung verlangen könnte. Die Immunität der Abgeordneten ist vielmehr ein Privileg des Parlaments, über das nur dieses selbst disponieren kann.

2. Damit ist aber von Verfassungs wegen noch nichts darüber ausgesagt, ob der betroffene Abgeordnete in bestimmten Fällen eine Einschränkung seiner Grundrechte hinnehmen muß. Das Grundrecht auf informationelle Selbstbestimmung (Artikel 6 Abs. 1 Landesverfassung und Artikel 2 Abs. 1 i.V. mit Artikel 1 Abs. 1 GG) gilt für jeden Staatsbürger, auch für den Abgeordneten. Dessen Grundrecht wird durch Artikel 58 Landesverfassung auch nicht eingeschränkt, denn die Bestimmung richtet sich nicht gegen die Rechte des einzelnen Abgeordneten.
   Der Eingriff in das Grundrecht geht von den personenbezogenen Übermittlungen der Exekutivbehörden bzw. der Gerichte an das Parlament aus. Eingriffs- und Übermittlungsgrundlage für deren Tätigkeit ist entweder eine bereichsspezifische gesetzliche Regelung oder § 11 Abs. 1 i.V. mit § 10 Abs. 2 Nr. 1 DSG-LSA.

3. Artikel 58 Landesverfassung kommt in dem Verfahren allerdings insoweit Bedeutung zu, als er nach Inhalt und Sinn dem Parlament ein Recht zur Nachfrage und damit zur Bestimmung des Umfanges der von der Exekutive zu übermittelnden personenbezogenen Daten des betroffenen Abgeordneten gibt. Artikel 58 gibt dem Parlament aber keinen generellen Informationsanspruch über den Ausgang eines den Abgeordneten betreffenden Ermittlungsverfahrens.

Aus alledem folgt, daß das Parlament im Einzelfall eine Schlußmitteilung für sich nur in den Fällen reklamieren kann, in denen seine Arbeits- und Funktionsfähigkeit weiter tangiert sein könnte. Das ist aber dann nicht der Fall, wenn z.B. ein Abgeordneter aus der vorangegangenen Legislaturperiode inzwischen dem Parlament nicht mehr angehört. Den Behörden und Gerichten fehlt in einem solchen Fall auch die gesetzliche Grundlage für eine Übermittlung an das Parlament, denn es mangelt sowohl an der in § 11 Abs. 1 DSG-LSA vorgesehenen

„Erforderlichkeit“, wie auch an der vom Gesetz geforderten Aufgabe der einen wie der anderen Seite.

16.3 Ständige Teilnahme des Ausländerbeauftragten bei Beratungen über ausländerrechtliche Petitionen im Landtag

Der Petitionsausschuß des Landtages beabsichtigte eine Beschlußfassung mit dem Inhalt, daß der von der Landesregierung bestellte Ausländerbeauftragte künftig zu allen Beratungen über ausländerrechtliche Petitionen hinzugezogen wird. Hiergegen bestanden aus datenschutzrechtlicher Sicht Bedenken.

Die ständige Beteiligung des Ausländerbeauftragten stellt sich - soweit dabei personenbezogene Daten berührt sind - rechtlich als Datenübermittlung von einer öffentlichen Stelle an eine andere öffentliche Stelle dar. Sie wäre nur zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist **und** eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt (§ 10 Abs. 2 Nr. 1 DSG-LSA).

Der einfache Beschluß der Landesregierung über die Stellung des Ausländerbeauftragten vom 07.03.1995 (MBl. LSA S. 428) begründet weder dessen generelle Zuständigkeit für ausländerrechtliche Petitionen noch seine ständige Vertretung der Landesregierung in allen Petitionsverfahren. Ein betroffener Petent darf deshalb bis zu einer ihn bindenden anderen **gesetzlichen** Regelung davon ausgehen, daß auf Seiten der Exekutive nur das in Ausländerangelegenheiten zuständige Ministerium des Innern und seine für diese Verwaltungsaufgabe zuständigen nachgeordneten Behörden beteiligt sind. Zwar muß ein Petent im Rahmen der Bearbeitung seiner eingereichten Petition mit einer sachgerechten Beteiligung anderer öffentlicher Stellen im Einzelfall rechnen und für die damit zusammenhängenden Arbeitsabläufe eine Übermittlung seiner personenbezogenen Daten in Kauf nehmen, doch dient das formenstrenge Verfahren der Festlegung von Zuständigkeiten auf Seiten der Exekutive auch der Überschaubarkeit der beteiligten Stellen für den Betroffenen. Deshalb muß sich im Hinblick auf den im Verfassungsrang stehenden Grundsatz der Verhältnismäßigkeit der

Kreis der Empfänger auf das unbedingt notwendige Maß beschränken. Der Petitionsausschuß des Landtages hat diese Hinweise des Landesbeauftragten aufgegriffen und die Datenübermittlung an den Ausländerbeauftragten von der vorherigen Einwilligung durch den Petenten abhängig gemacht.

17. Landwirtschaft

17.1 Das Kontrollsystem InVeKoS

Bereits in seinem I. (S. 81 f) und seinem II. Tätigkeitsbericht (S. 88 f) hatte der Landesbeauftragte das Integrierte Verwaltungs- und Kontrollsystem (InVeKoS) zur Landwirtschaftsförderung wegen seiner offensichtlichen datenschutzrechtlichen Risiken problematisiert. Dieses Thema ist ein Dauerbrenner geblieben. Mittlerweile hat das Ministerium für Raumordnung, Landwirtschaft und Umwelt des Landes Sachsen-Anhalt eingesehen, daß der Abgleich der Flächenangaben der Antragsteller mit den Daten des automatisierten Liegenschaftsbuches ohne Einwilligung der Betroffenen nicht geht. Eine entsprechende Einwilligungserklärung wurde mit dem Landesbeauftragten abgestimmt.

Doch wer geglaubt hatte, daß diese Geschichte damit zu einem guten Ende gebracht worden wäre, der hatte sich geirrt. Denn im Januar 1997 erfuhr der Landesbeauftragte durch das Ministerium von der Existenz eines gemeinsamen „Mantelbogens 1997 für die Agrarförderung im Bereich Flächen und Tiere für die Bundesländer Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Sachsen-Anhalt“.
Die darin vorgesehenen „Erklärungen zum Datenschutz“ werden den Anforderungen des § 4 Abs. 2 DSG-LSA an eine Einwilligungserklärung leider nicht gerecht.

Der Landesbeauftragte unterstützt die Bestrebungen der Bundesländer durch gemeinsame Formulare Verfahren zu vereinheitlichen und Kosten zu senken. Das darf jedoch nicht dazu führen, daß zwingende gesetzliche Vorgaben im Lande mißachtet werden.

Das Ministerium hat die datenschutzrechtlichen Bedenken des Landesbeauftragten aufgegriffen und ist zuversichtlich, seine konstruktiven Vorschläge für eine datenschutzgerechte Einwilligungserklärung auch bei diesen Vordrucken in die Verwaltungspraxis umsetzen zu können.

17.2 Austausch von personenbezogenen Daten zwischen den Ämtern für Landwirtschaft und Flurneuordnung und der Finanzverwaltung

Nach dem Flurbereinigungsgesetz haben die Ämter für Landwirtschaft und Flurneuordnung der Ermittlung des Wertverhältnisses landwirtschaftlicher Grundstücke die Ergebnisse einer Bodenschätzung zugrunde zu legen. Bodenschätzungen führt die Finanzverwaltung durch. Deshalb war das damalige Ministerium für Ernährung, Landwirtschaft und Forsten (MELF) der Meinung, daß bei Grundstückseigentümern, die die Ergebnisse der Bodenschätzung vergessen haben, die Finanzämter verpflichtet seien, die erforderlichen Daten an die Ämter für Landwirtschaft und Flurneuordnung zu übermitteln. Das Ministerium der Finanzen sah das nicht so, wollte aber seinerseits von den Ämtern für Landwirtschaft und Flurneuordnung die Daten aller landwirtschaftlichen und gärtnerischen Betriebe (in Form von Gesamtverzeichnissen) übermittelt haben, wogegen sich wiederum das MELF sperrte.

Der Landesbeauftragte mußte - um Rat gefragt - wieder einmal auf eine der gesetzlichen Grundvoraussetzungen jedes Umganges mit personenbezogenen Daten hinweisen.
Wer als öffentliche Stelle um eine Datenübermittlung ersucht, muß die begehrten personenbezogenen Daten selbst auch erheben dürfen! Sonst ist schon die Anfrage unzulässig. Nach § 9 Abs. 1 DSG-LSA ist das Erheben personenbezogener Daten zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.
Das war in diesem Fall wegen der Aufforderung im Flurbereinigungsgesetz, Bodenschätzungsergebnisse zu verwenden, unproblematisch. Doch war übersehen worden, daß gem. § 9 Abs. 2 Satz 1 DSG-LSA personenbezogene Daten grundsätzlich **beim Betroffenen mit seiner Kenntnis** zu erheben sind. Eine der Ausnahmevorschriften des § 9 Abs. 2 Satz 2 DSG-LSA kam nicht in Betracht, so

daß die Ämter für Landwirtschaft und Flurneuordnung auf die Datenerhebung beim Eigentümer angewiesen sind.
Um zu einer praxisnahen Lösung zu kommen, schlug der Landesbeauftragte folgendes Verfahren vor:
Stellt sich nach Befragung der Grundstückseigentümer heraus, daß diesen im Einzelfall die Ergebnisse der Bodenschätzung und ihrer Fortschreibung nicht bekannt sind, bleibt es ihnen überlassen, ob sie die Ergebnisse selbst bei der Finanzverwaltung erfragen wollen oder sich auf einem Vordruck damit einverstanden erklären, daß die Ämter für Landwirtschaft und Flurneuordnung bei der zuständigen Finanzbehörde nachfragen.

Was die Übermittlung der Daten aller landwirtschaftlichen und gärtnerischen Betriebe an die Finanzverwaltung angeht, besteht die Besonderheit, daß Vorschriften des Bewertungsgesetzes (BewG) i.V. mit § 1 Abs. 2 AO Anwendung finden, die als bereichsspezifische Rechtsgrundlagen den Bestimmungen des DSG-LSA vorgehen.
Die Finanzverwaltung stützt ihr Auskunftsverlangen offensichtlich auf § 29 Abs. 3 BewG, wonach die nach Bundes- oder Landesrecht zuständigen Behörden den Finanzbehörden die ihnen im Rahmen ihrer Aufgabenerfüllung bekanntgewordenen rechtlichen und tatsächlichen Umstände mitzuteilen haben, die für die Feststellung von Einheitswerten des Grundbesitzes oder für die Grundsteuer von Bedeutung sein können.
Aber auch die Finanzverwaltung muß sich auf den Grundsatz der Erhebung **beim Betroffenen** verweisen lassen und § 29 Abs. 1 Satz 1 BewG ausschöpfen, indem sie sich **von den Eigentümern** alle erforderlichen Angaben machen läßt, die sie braucht. Nur wenn diese **im Einzelfall** nicht ausreichen, kann sie auf die **nachrangige** Vorschrift des § 29 Abs. 3 Satz 1 BewG zurückgreifen, um Unklarheiten auszuräumen, Angaben zu überprüfen oder Unrichtigkeiten zu korrigieren.

18. Personalwesen

18.1 Veröffentlichung von Lehrergehältern in der Presse

Im Rahmen der von der Landesregierung vorgesehenen Kürzung der Gehälter für Lehrer wurden zur Veranschaulichung und Information der Öffentlichkeit beispielhaft Lehrergehälter aus einer Tabelle in der Presse veröffentlicht. Ein Petent sah darin eine unzulässige Übermittlung seiner Gehaltsdaten und wandte sich deshalb an den Landesbeauftragten.
Unter den Schutzbereich der datenschutzrechtlichen Bestimmungen fallen nur Einzelangaben über persönliche oder sachliche Verhältnisse einer **bestimmten** oder **bestimmbaren** natürlichen Person. Die in der Presse verwendeten Beispiele ohne konkreten Personenbezug verstießen also nicht gegen das Recht.
Im übrigen sind die Vergütungstabellen des Tarifvertrages eine für jedermann zugängliche öffentliche Quelle (z.B. Ministerialblatt des Landes Sachsen-Anhalt, Broschüren der Berufsverbände und im Buchhandel) und daher jederzeit und von jedem einsehbar.

18.2 Vorlage von Personalakten an das Gericht

Ein Beamter beschwerte sich beim Landesbeauftragten über die seiner Ansicht nach unkorrekte Vorlage seiner Personalakten an das Verwaltungsgericht.
Er hatte selbst beim Verwaltungsgericht eine sog. Konkurrentenklage erhoben. Daraufhin verfügte das Gericht entsprechend den Vorschriften der Prozeßordnung (hier: § 99 VwGO) die Vorlage der Personalakte. So geschah es.
Der Betroffene bemängelte, die Personalstelle hätte vorher dazu sein Einverständnis einholen, zumindest ihn von der Vorlage informieren müssen.

Der Landesbeauftragte konnte dem Betroffenen nicht helfen. Wer selbst Verfahrensbeteiligter in einem gesetzlich geregelten Gerichtsverfahren ist, kann sich unmittelbar aus dem Gesetz informieren oder sich ggf. auch vom Dienstherrn beraten lassen. Es bedurfte weder einer vorherigen Benachrichtigung des Beamten über die Versendung seiner Akten noch seiner Genehmigung.

Unabhängig von diesem Einzelfall ist aber jede personalverwaltende Stelle gut beraten, in solchen Fällen zu prüfen, ob der Prozeßgegenstand die Vorlage der **gesamten** Personalakte notwendig macht oder ob es nicht ausreicht, prozeßrelevante Teile dem Gericht zuzuleiten.
Grundsätzliche Ausführungen zum Schutz Unbeteiligter bei der Übermittlung personenbezogener Daten aus Personalakten und -dateien an die Gerichte hat der Landesbeauftragte in seinem II. Tätigkeitsbericht gemacht (S. 92 u. 216).

18.3 Einsichtnahme in Bewerbungsunterlagen und Personalakten durch Gleichstellungsbeauftragte

Mit der Verabschiedung eines Zweiten Gesetzes zur Änderung des Frauenfördergesetzes im Februar 1997 sind die Rechte der Gleichstellungsbeauftragten erweitert worden. Damit ist der vom Landesbeauftragten noch im II. Tätigkeitsbericht aufgeführte Schutz (S. 96) in der alten Gesetzesfassung teilweise wieder aufgegeben worden.
Nach der bisherigen Regelung hatte der Gesetzgeber wegen des besonderen Schutzes von Personal-/Bewerberdaten ein Einsichtsrecht für die **hauptamtliche** Gleichstellungsbeauftragte an die **Zustimmung** der davon betroffenen Personen geknüpft. Der Gesetzentwurf wollte diese Einschränkung wieder aufheben. Im Gesetzgebungsverfahren hat der Landesbeauftragte darauf hingewiesen, daß der Landesgesetzgeber, wenn er die Rechte der Gleichstellungsbeauftragten zu Lasten des in Artikel 6 Abs. 1 der Landesverfassung garantierten Grundrechtes auf informationelle Selbstbestimmung der Bewerber bzw. der Bediensteten erweitern will, von Verfassungs wegen in vielfältige Entscheidungs- und Begründungszwänge gerät. Bedenklich waren die vorgesehenen Änderungen insbesondere, weil zum einen nicht hinreichend belegt werden konnte, daß die bisherige Verfahrensweise mit der Einholung der Einwilligung der jeweils Betroffenen zu Behinderungen oder Einschränkungen der Aufgabenwahrnehmung durch die Gleichstellungsbeauftragte geführt hatte, zum anderen wäre begründet darzulegen gewesen, weshalb der mildere Eingriff einer Auskunftserteilung aus den Akten nicht ausreichte.

Die in mehreren Sitzungen geleistete Überzeugungsarbeit hatte Erfolg: Das verabschiedete Gesetz sieht vor, daß in Zukunft den hauptamtlichen Gleichstellungsbeauftragten aus den Personalakten Auskünfte in erforderlichem Umfang erteilt werden; Bewerberunterlagen können bei Bedarf ohne Einwilligung eingesehen werden. Letzteres erscheint im Hinblick darauf, daß der Bewerber ein bestimmtes, für ihn nachlesbares gesetzlich geregeltes Verfahren durchläuft, sachlich vertretbar.

18.4 Führung von Personalakten

Ein Mitarbeiter einer Landesbehörde, der sein abgebildetes Paßfoto neben einem Presseartikel über ihn in einem Nachrichtenmagazin wiederfand und über den darüber hinaus in mehreren Zeitungen im Zusammenhang mit seiner dienstlichen Tätigkeit berichtet worden war, bat den Landesbeauftragten um Überprüfung.

Die Überprüfung des vom Petenten geschilderten Sachverhaltes ergab, daß das Paßfoto in seiner Personalakte seit geraumer Zeit fehlte. Zeitraum und Bildvergleich sprachen durchaus für eine direkte Verbindung zur Veröffentlichung in der Presse. Ob das Foto des Betroffenen rechtswidrig an Dritte übermittelt worden ist, mußte im Ergebnis aber offen bleiben. Bei der Überprüfung wurde aber deutlich, daß die Personalakte von mehreren (leitenden) Personen seiner Beschäftigungsbehörde (berechtigt) empfangen und tagelang genutzt worden war. Die verantwortliche Personalstelle hatte jedoch bei der wiederholten Ausgabe weder die zeitlichen Ausgabeabschnitte und die jeweiligen Nutzer dokumentiert noch bei der Rückgabe die Vollständigkeit der Personalakte geprüft. Dies und die Tatsache, daß das Bild ohne Wissen der dafür verantwortlichen öffentlichen Stelle aus der Personalakte entfernt wurde und nicht mehr auffindbar war, stellt bereits einen schwerwiegenden Verstoß gegen den Grundsatz der Vertraulichkeit der Personalakte, wie er in § 56 BRRG (§ 90 BG-LSA) verankert ist, dar.
Der datenschutzrechtliche Verstoß wurde förmlich beanstandet.

18.5 Wohin mit den Gauck-Bescheiden?

In den Personalämtern und -referaten der öffentlichen Stellen des Landes wurde und wird diese Frage bis heute häufig gestellt. Eindeutige landesweite Regelungen fehlen.
Der Landesbeauftragte hat bei seinen Kontrollen wohl auch deshalb sehr unterschiedliche Verfahrensweisen festgestellt.

Der Landesbeauftragte legt Wert auf die Feststellung, daß die sog. Gauck-Bescheide Teil der Personalakten sind. Sie sind deshalb in den Personalstellen mit den Personalakten gesichert aufzubewahren.
Die vorläufigen und später auch die endgültigen Bescheide sollten allerdings in einem gesondert verschlossenen Umschlag zu den Akten genommen werden. Zugriffsberechtigt sollte nur ein kleiner, festgelegter Personenkreis sein. Soweit der Umschlag geöffnet werden muß, sollte der Tag, der Grund für die Öffnung und die öffnende Person schriftlich bei den Akten festgehalten werden.

18.6 Signierblatt (Vergütung)

Eine Petentin wandte sich an den Landesbeauftragten und wies darauf hin, daß an einer Schule durch die Schulleitung Fragebögen an das Lehrpersonal ausgegeben wurden, in denen Angaben zur Person und zur Besoldung (Personal-daten) abgefragt werden sollten, obwohl die Daten schon bei den Regierungspräsidien vorlagen. Die Fragebögen enthielten weder Erhebungszweck, Rechtsgrundlage noch Absender. Nachfragen zum Erhebungszweck wurden mit dem Hinweis auf „statistische Zwecke“ durch die Schulleitung beantwortet.

Nachfragen durch den Landesbeauftragten bei der Schulleitung ergaben, daß es sich um einen Fragebogen des Kultusministeriums handelte.

Das Kultusministerium wies in seiner Antwort darauf hin, daß die erbetenen Daten aufgrund der gesetzlichen Veränderungen für eine regionale Umverteilung des vorhandenen Personals, notwendige Neueinstellungen, Altersstruktur- und Bedarfsanalysen erforderlich seien. Auf die bei den Regierungspräsidien

vorhandenen Daten konnte aufgrund zeitgleicher technischer und personeller Veränderungen nicht zurückgegriffen werden.

Nach § 84a Schulgesetz i.V. mit § 28 Abs. 1 DSG-LSA dürfen Daten von Beschäftigten u.a. zu Zwecken der Personalplanung und des Personaleinsatzes erhoben, verarbeitet oder genutzt werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist. Die Datenerhebung und -verarbeitung war somit gesetzlich gedeckt.

Der Landesbeauftragte hat das Kultusministerium aber gebeten, bei vergleichbaren künftigen Aktionen nach § 9 Abs. 3 DSG-LSA den Erhebungszweck und die Rechtsgrundlage für die Maßnahme gegenüber dem Betroffenen anzugeben. Außerdem muß man aus dem Fragebogen erkennen können, wer Empfänger der personenbezogenen Daten ist. Deshalb kann auch auf die Angabe des Absenders nicht verzichtet werden.

Das Kultusministerium hat zugesagt, bei den Schulleitern zu veranlassen, daß die ausgefüllten Signierblätter an das jeweilige Regierungspräsidium übermittelt werden. Dort werden sie den jeweiligen Personalakten zugeordnet oder nach Auswertung datenschutzgerecht vernichtet. Damit entfällt auch der zunächst zu Recht im Raum stehende Vorwurf der Doppeldatenerhebung.

18.7 Telefonverzeichnis privater Telefonanschlüsse aller Mitarbeiter

Für die Leitung einer Stadtverwaltung sollte ein Telefonverzeichnis mit den privaten Telefonanschlüssen aller Mitarbeiter erstellt werden. Als Begründung wurde die erforderliche Erreichbarkeit der Mitarbeiter auch nach Dienstschluß aufgeführt.

Jedes Erheben, Verarbeiten und Nutzen von personenbezogenen Daten ist nur zulässig, wenn das DSG-LSA oder eine andere Rechtsvorschrift es erlaubt oder anordnet, oder soweit der Betroffene eingewilligt hat.

Da keine Einwilligung der Mitarbeiter vorlag, wäre die Datenerhebung und -verarbeitung nur nach § 28 DSG-LSA möglich gewesen. Kernpunkt dieser Vorschrift ist der in Absatz 1 aufgestellte „Erforderlichkeitsgrundsatz“, der die Verwendung personenbezogener Daten nur für zulässig erachtet, wenn ohne sie die übertragene Aufgabe nicht oder nicht vollständig erfüllt werden kann. Ist die Verwendung personenbezogener Daten nur zweckmäßig, aber nicht zwingend notwendig, dann ist sie **unzulässig**. Auch die Sammlung nicht anonymisierter Daten „auf Vorrat“, ohne augenblickliche Notwendigkeit, zu unbestimmten künftigen Zwecken, ist mit dem Schutzgedanken nicht vereinbar. Deshalb müssen sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken.
Im Hinblick darauf, daß ein ausreichendes Adressenverzeichnis der der Rufbereitschaft unterliegenden Mitarbeiter bei der Leitstelle der Feuerwehr hinterlegt war, bestand aus datenschutzrechtlicher Sicht keine begründbare Notwendigkeit mehr, von allen übrigen Mitarbeitern der Stadtverwaltung deren private Telefonnummern zu erheben.
Darüber hinaus wurde vom Landesbeauftragten darauf hingewiesen, daß es sich bei der vorgesehenen Maßnahme um einen Mitbestimmungstatbestand nach dem Personalvertretungsgesetz handeln dürfte und die erforderliche Zustimmung der Personalvertretung eine datenschutzrechtlich zu beachtende Regelung sei.
Den Empfehlungen des Landesbeauftragten wurde Rechnung getragen.

18.8 Richtlinienentwurf für Schwerbehinderte

Im Entwurf der „Richtlinie über Förderung der Einstellung und Beschäftigung Schwerbehinderter“ (Fürsorgeerlaß für Schwerbehinderte) war vorgesehen, daß die Schwerbehindertenvertretung in Bewerbungsverfahren auch über die persönlichen und leistungsbezogenen Daten der nicht schwerbehinderten Mitarbeiter unterrichtet wird und an Vorstellungsgesprächen teilnehmen sollte.

Der Landesbeauftragte mußte darauf hinweisen, daß das beabsichtigte Verfahren sich rechtlich als Übermittlung personenbezogener Daten darstellt und durch das Schwerbehindertengesetz des Bundes gesetzlich nicht gedeckt ist.

Auch durch im Zusammenhang mit Bewerbungen geforderte Einwilligungen können absolute gesetzliche Erhebungs-, Verarbeitungs- oder Nutzungsverbote nicht zu Lasten der „freien“ Entscheidung der Bewerber überwunden oder gar unterlaufen werden. Eine hierauf gerichtete Einwilligung wäre insofern unwirksam. Der aus Artikel 20 Abs. 3 GG folgende Grundsatz der Rechtmäßigkeit der Verwaltung untersagt in diesem Fall die gesetzlich nicht vorgesehene Ausdehnung von Aufgaben zu Lasten Dritter.

Diese Regelung wurde deshalb nicht in die Richtlinie aufgenommen.

19. Personalvertretung

Einsichtnahme des Personalrates in Gauck-Mitteilungen

Nach § 56 Abs. 1 Satz 2 BRRG gehören zur Personalakte alle Unterlagen, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren Zusammenhang stehen. Ergänzend gilt in Sachsen-Anhalt z.Zt. § 28 DSG-LSA. Im Hinblick darauf, daß der Einigungsvertrag die Tätigkeit für das frühere MfS dann als einen wichtigen Grund für eine außerordentliche Kündigung zuläßt, wenn deshalb ein Festhalten am Arbeitsverhältnis unzumutbar erscheint, ist die nach § 19 StUG vom Bundesbeauftragten versandte Mitteilung eine personenbezogene Unterlage. Diese ist dementsprechend zur Personalakte zu nehmen. Der zuständige Vorgesetzte entscheidet anhand der übermittelten Informationen und Unterlagen im Einzelfall über Beginn, Fortsetzung oder Beendigung eines Arbeitsverhältnisses im öffentlichen Dienst.

Die §§ 56 Abs. 3, 56d BRRG und § 13 BAT enthalten ausdrückliche Regelungen darüber, wem innerhalb und außerhalb der personalführenden Stelle der Inhalt der Personalakten zugänglich gemacht werden darf. Dabei sind hinsichtlich der

Einsichtsrechte in Personalakten vom Gesetzgeber enge Grenzen gesetzt worden.

Der Personalvertretung steht in Sachsen-Anhalt kein eigenständiges Einsichtsrecht in die Personalakte zu. § 57 Abs. 2 Satz 3 PersVG LSA überläßt es dem Bediensteten, selbst zu entscheiden, ob er dem Personalrat ganz oder teilweise Einblick in seine höchstpersönlichen Angelegenheiten gestatten will. Insoweit genießt hier das Recht auf informationelle Selbstbestimmung des Beschäftigten Vorrang vor dem Recht des Personalrates auf kollektive Interessenwahrnehmung. In der Regel wird zwar der einzelne Bedienstete an einer Vorlage der Personalakten an die Personalvertretung schon deshalb interessiert sein, weil diese sich so ein objektives Bild im Zusammenhang mit der beabsichtigten Personalmaßnahme machen kann. Es darf jedoch nicht übersehen werden, daß Personalakten eine Vielzahl von Angaben über höchstpersönliche Angelegenheiten des einzelnen Bediensteten enthalten, auf die es bei der anstehenden Personalentscheidung nicht ankommt. Daher muß ein schutzwürdiges Interesse des Betroffenen an seiner Entscheidungsfreiheit anerkannt werden.

Liegt die Zustimmung des Bediensteten vor, so verstößt die Weitergabe der Mitteilung der Gauck-Behörde an den Personalrat nicht gegen § 29 StUG, weil der Personalrat rechtlich nicht Dritter ist und die Zweckbindung nicht durchbrochen wird, sofern seine Beteiligung nach den §§ 66 und 67 PersVG i.V. mit § 61 PersVG zwingend vorgeschrieben ist.
Verweigert der Betroffene seine Zustimmung, so darf die Mitteilung selbst nicht vorgelegt werden, doch muß der Personalrat im Rahmen des ihm gegenüber der Behörde zustehenden umfassenden Informations- und Auskunftsrechts über den wesentlichen Inhalt der Mitteilung in Kenntnis gesetzt werden, weil er nur so sein gesetzlich gesichertes Mitbestimmungsrecht voll ausüben kann.

20. Polizei

20.1 Aufzeichnung aller Telefonanrufe bei der Polizei

Wie der Landesbeauftragte bereits in seinem II. Tätigkeitsbericht (S. 101) festgestellt hat, beabsichtigt das Ministerium des Innern nicht, die Aufzeichnung aller eingehenden Telefonanrufe bei der Polizei anzuordnen. Ohne Einwilligung der Betroffenen werden nur die über den Notruf 110 zur Polizei gelangenden Anrufe aufgezeichnet.
Zu dem vom Ministerium des Innern angekündigten und jetzt vorgelegten Erlaßentwurf hat der Landesbeauftragte Stellung genommen und in zwei Punkten Änderungsvorschläge unterbreitet. Es wurde angeregt, die maximale Speicherungsdauer der aufgezeichneten Gespräche auf einen Monat zu begrenzen und darüber hinaus auch festzulegen, in welchen Fällen (z.B. zur Gefahrenabwehr oder bei strafrechtlicher Relevanz) Abschriften von dem Tonträger angefertigt werden dürfen und wer die Entscheidung hierüber trifft.

Es erscheint dem Landesbeauftragten vertretbar, in rechtlich zulässigen Einzelfällen, z.B. bei bestimmten Dienststellen der Kriminalpolizei, auch bei Anrufen über die Amtsleitungen Aufzeichnungen zuzulassen.

Das Ministerium des Innern wird den Erlaßentwurf diesbezüglich überarbeiten.

20.2 Fehlerhafter Umgang mit Altdatenbeständen bei einer Polizeidirektion

Der Landesbeauftragte erfuhr davon, daß bei einer Polizeidirektion zu vernichtende amtliche Unterlagen in einem offenen Container vor dem Dienstgebäude auf öffentlicher Straße unbeaufsichtigt Dritten zugänglich waren.
Die Polizeidirektion hatte vertraglich eine Entsorgungsfirma damit beauftragt, Altpapier und dienstliches Schriftgut zu entsorgen.
Wie sich später herausstellte, konnten sich unbefugte Personen amtliche Unterlagen in Form von Fernschreiben, die teilweise sogar den Zusatzvermerk „VS - Nur für den Dienstgebrauch“ enthielten, verschaffen, von deren Inhalt Kenntnis nehmen und der Presse übergeben.

Die Polizeidirektion war für diese personenbezogenen Unterlagen speichernde Stelle. Ihr oblag daher die Pflicht, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, daß die bei ihr vorhandenen personenbezogenen Daten in jeder der gesetzlich definierten Verarbeitungsphasen ausreichend geschützt waren, insbesondere nicht unbeaufsichtigt und nicht unbefugt zur Kenntnis Dritter gelangen konnten (§ 5 DSG-LSA).
Eine besonders sichere Verfahrensweise wäre bei der Vernichtung der Verschlußsachen erforderlich gewesen.

Der Landesbeauftragte hat deshalb gegenüber dem Ministerium des Innern eine förmliche Beanstandung wegen der Verletzung datenschutzrechtlicher Vorschriften ausgesprochen.
Er hält die vom Ministerium in seiner Stellungnahme zur Beanstandung mitgeteilten Maßnahmen für geeignet und ausreichend, um künftig den erforderlichen Schutz personenbezogener Daten sicherzustellen.

20.3 Errichtungsanordnungen zu automatisierten Dateien der Polizei

Für die Errichtungsanordnungen der Polizei findet anstelle des § 25 Abs. 1 Satz 3 DSG-LSA der § 33 Abs. 2 SOG LSA Anwendung. Die Meldung erfolgt durch die Polizeibehörden auf dem Dienstweg über das Ministerium des Innern an den Landesbeauftragten.
Die bis Herbst 1996 übersandten Errichtungsanordnungen weisen erhebliche rechtliche Defizite auf.

Das Ministerium des Innern hat bei der Übersendung der Errichtungsanordnungen bisher stets darauf hingewiesen, daß die übersandten Errichtungsanordnungen noch auf ihre Rechtmäßigkeit hin überprüft und, soweit erforderlich, die Erstellung einer korrigierten Errichtungsanordnung und Dateifestlegung veranlaßt würde.
Der Landesbeauftragte mußte aber feststellen, daß seit mehr als zwei Jahren keine korrigierten Errichtungsanordnungen bei ihm eingegangen waren.
Die vom Ministerium wiederholt genannten akuten Personalprobleme sind für eine derartige Verfahrensweise keine ausreichende Begründung mehr.

Mit Rücksicht auf die Polizeistrukturreform hat der Landesbeauftragte sein bisheriges Register für Errichtungsanordnungen der Polizei mit dem Stichtag 01.11.1995 geschlossen. Meldungen nach dem 01.11.1995 werden in einem neuen Register erfaßt.
Bei einem im November 1996 geführten Gespräch räumte das Ministerium des Innern die genannten Mängel ein und kam mit dem Landesbeauftragten überein, die bisherige Meldepraxis zu verbessern und die Mitarbeiter der Polizeidienststellen nochmals zu schulen.
Der Landesbeauftragte wird diese Schulungen unterstützen.

20.4 Aufbewahrung von Ed-Unterlagen

Eine Polizeidirektion hatte bei einem Bürger im Jahr 1992 wegen des Verdachts des Landfriedensbruches gem. § 125 StGB eine erkennungsdienstliche Behandlung vorgenommen und die dabei gefertigten Lichtbilder im Jahr 1995 bei den Ermittlungen wegen einer vermuteten Diebstahlshandlung Dritten vorgezeigt.

Dies war unzulässig, denn das 1992 zugrundeliegende Ermittlungsverfahren wurde von der Staatsanwaltschaft bereits im Jahr 1993 gem. § 170 Abs. 2 StPO eingestellt. Damit entfiel mangels anderer Gründe auch die Berechtigung der Polizei, die Ed-Unterlagen des Betroffenen aufzuheben.

Die Polizeidirektion erfuhr aber erst im Dezember 1995 aufgrund der Prüfung durch den Landesbeauftragten von dieser Sachlage und hat daraufhin die Ed-Unterlagen des Bürgers vernichtet.

Mit dem zur Stellungnahme aufgeforderten Ministerium des Innern konnte Einvernehmen darüber erzielt werden, daß die kriminalaktenführenden Dienststellen künftig in solchen Fällen für die Aufbewahrung zunächst nur kurze Speicherungsfristen ansetzen, damit das Ergebnis der staatsanwaltschaftlichen Rechtsbewertung für die Festsetzung einer Aufbewahrung und ihrer Dauer berücksichtigt werden kann.
Der Polizei kommt darüber hinaus als datenspeichernde Stelle auch die Verantwortung für die laufende Aktualisierung und Richtigkeit der bei ihr gespeicherten

Daten zu. Deshalb muß sie den Rücklauf von Rückmeldungen der Staatsanwaltschaft zum Ausgang eines Verfahrens überwachen und ggf. daran erinnern.

20.5 Abfrage aus ZEVIS

Ein Bürger beschwerte sich beim Landesbeauftragten darüber, daß die Polizei seine Kfz-Halterdaten an den Tankwart einer Tankstelle übermittelt hatte, dem bei der Herausgabe von Wechselgeld ein Fehler unterlaufen war.

Die Anfrage des Landesbeauftragten beim Kraftfahrtbundesamt (KBA) erbrachte aufgrund der dortigen Protokollierung der ZEVIS-Abfragen als Teilergebnis, daß die Halterfeststellung durch Streifenbeamte einer Polizeiinspektion veranlaßt worden war. Die Beamten hatten dem Tankwart, menschlich verständlich, aber rechtlich nicht ganz lupenrein, helfen wollen.
Da nach dem Sachverhalt weder eine Straftat noch eine Ordnungswidrigkeit vorlag, sondern der Tankwart lediglich einen zivilrechtlichen Anspruch geltend machen konnte, waren die Polizeibeamten zu keiner ZEVIS-Abfrage befugt. Zwar gehört nach dem SOG-LSA zu den Aufgaben der Polizei auch der Schutz privater Rechte, aber nur dann, wenn die allgemein zuständigen Ordnungsbehörden oder gerichtlicher Rechtsschutz nicht rechtzeitig zu erreichen sind, und wenn ohne behördliche Hilfe die Verwirklichung des Rechts vereitelt oder wesentlich erschwert werden würde.
Da ein solcher Eilfall nicht vorlag, hätten die Beamten den Tankwart an die zuständige Verwaltungsbehörde der Gefahrenabwehr (z.B. an das Ordnungsamt der Gemeinde oder des Landkreises) verweisen müssen.

Der Landesbeauftragte hat diesen Fall zum Anlaß genommen, das aufsichtführende Ministerium des Innern zu bitten, künftig - etwa im Rahmen der Aus- und Fortbildung der Polizeibeamten - Vorkehrungen zu treffen, die eine Wiederholung eines vergleichbaren Falles in der Zukunft möglichst ausschließen.
Darüber hinaus hat der Landesbeauftragte dem Ministerium des Innern vorgeschlagen, künftig auch ZEVIS-Abfragen bei der Polizei zu protokollieren, um eine bessere nachträgliche Rechtskontrolle zu gewährleisten.

Leider ließ schon eine erste Stellungnahme des Ministeriums rund 7 Monate auf sich warten, und bis heute hat es sich zu diesen Vorschlägen noch nicht abschließend geäußert.

20.6 Private Personalcomputer in einem Polizeirevier

Dem Landesbeauftragten war aus einer Presseverlautbarung vom Juli 1996 bekannt geworden, daß in einem Polizeirevier des Landes das Computerzeitalter damit begann, daß seinerzeit einer der Beamten zur Arbeitserleichterung seinen privaten PC mit aufs Revier brachte. Die Eigeninitiative ist verständlich, stößt aber rechtlich in verschiedener Hinsicht auf Probleme.
Formal ist festzustellen, daß es sich hierbei um einen Verstoß gegen die „Dienstanweisung für die Polizei des Landes Sachsen-Anhalt zur Nutzung der Informations- und Kommunikationstechnik (IuK-Technik/ADV)“ handelt, denn unter Ziff. 4.1 der Dienstanweisung steht, daß die Nutzung privater Hard- und/oder privater Software zu dienstlichen Zwecken untersagt ist.
Dies hat reale Gründe: Was passiert mit den auf diesem PC gespeicherten personenbezogenen Daten aus dem Polizeivollzug, wenn der betreffende Beamte als Eigentümer des PC in eine andere Dienststelle versetzt wird oder aus dem aktiven Polizeidienst ausscheidet? Wer ist Herr dieser Daten? Sind die gespeicherten personenbezogenen Daten für den Fall eines Hardwaredefektes ordnungsgemäß gesichert worden? Verfügt dieser PC über die in Polizeidienststellen übliche Sicherheitssoftware, wem gehört diese und besteht möglicherweise ein Lizenzverstoß? Werden die Daten auf der Festplatte ausreichend gelöscht? Beim Gebrauch privater Disketten besteht darüber hinaus die Gefahr wechselseitiger Verwendung im privaten und dienstlichen Gebrauch und damit das Risiko einer Verletzung der Amtsverschwiegenheit.

Das Ministerium des Innern räumte auf Anfrage des Landesbeauftragten zunächst ein, daß eine solche Verfahrensweise jedenfalls erlaßwidrig sei, egal, ob es sich außerdem noch um einen datenschutzrechtlichen Verstoß handele oder nicht. Zur Frage, ob es noch in anderen Polizeidienststellen private PC gäbe, ist wegen der noch laufenden Sachverhaltsaufklärung des Ministeriums des Innern bis zum Redaktionsschluß nichts mitgeteilt worden.

20.7 Übertriebene Öffentlichkeitsarbeit in einer Polizeidirektion

In einer Tageszeitung wurde im Juli 1996 in einem mehrspaltigen Artikel über die Ausstattung eines Polizeireviers mit Computern berichtet. Der interessierte Leser erfuhr unter der Überschrift „Kommissar Computer erleichtert die Arbeit“ vom Pressesprecher der Polizeidirektion nicht nur, wieviele Computer welcher Leistungsklassen zu welchen Zwecken im betreffenden Polizeirevier betrieben werden, sondern auch, welche Sicherheitssoftware installiert wurde und wie die Rechner überregional vernetzt sind.
Der Landesbeauftragte mußte dem zuständigen Fachressort daraufhin mitteilen, daß es nicht mit § 6 Abs. 2 Ziff. 10 DSG-LSA vereinbar sei, die IT-Sicherheitsarchitektur in derart ausführlicher Weise an die breite Öffentlichkeit zu geben, denn das Ziel der dort vorgeschriebenen Organisationskontrolle soll sein, die getroffenen technischen und organisatorischen Maßnahmen des Datenschutzes zu unterstützen und zu ergänzen und nicht, sie zu publizieren.
Durch das Ministerium des Innern wurde dem Landesbeauftragten bisher nur mitgeteilt, daß die Auskünfte in der Zeitung zwar richtig seien, so aber von dem Polizeisprecher sicherlich nicht erteilt worden wären.
Der Landesbeauftragte wartet nun auf die abschließende Stellungnahme.

20.8 KpS-Richtlinien

Nach der mit Wirkung vom 01.01.1995 erfolgten Privatisierung und dem Inkrafttreten des Postneuordnungsgesetzes können Beamte des Betriebssicherungsdienstes der neuerrichteten Deutschen Post AG nicht mehr zu Hilfsbeamten der Staatsanwaltschaft bestellt bzw. als solche tätig werden, da die Deutsche Bundespost als Körperschaft des öffentlichen Rechts nicht mehr besteht.
Die durch die Hilfsbeamtenverordnung verliehenen Befugnisse und Zuständigkeiten bestimmter Beamtengruppen der ehemaligen Bundespost sind ebenso entfallen wie sonstige Rechte, Pflichten, Befugnisse und Zuständigkeiten, die den Unternehmen der Bundespost früher allein aufgrund ihrer öffentlich-rechtlichen Organisationsform als Behörde zustanden.

Bei der Änderung der KpS-Richtlinien des Landes aufgrund der Polizeistrukturreform übersah das Ministerium des Innern diese Tatsache und bezog die „Mitarbeiter des Postermittlungsdienstes“ weiter in den Kreis der öffentlichen Stellen mit ein, denen nach Ziff. 4.5.4 der KpS-Richtlinien Daten aus kriminalpolizeilichen Sammlungen übermittelt werden dürfen. Das geht nicht mehr.

Das Ministerium des Innern hat den entsprechenden Erlaß nach Hinweis des Landesbeauftragten inzwischen korrigiert, benötigte dafür aber rund 8 Monate.

20.9 Wahllichtbildvorlagen im strafrechtlichen Ermittlungsverfahren

Der Landesbeauftragte hat bereits in seinem I. (S. 110) und II. Tätigkeitsbericht (S. 100) auf die derzeit bestehenden rechtlichen Zweifel an der Zulässigkeit des Verfahrens der Wahllichtbildvorlage im strafrechtlichen Ermittlungsverfahren hingewiesen.

Auch bei der Wahllichtbildvorlage muß das Grundrecht auf informationelle Selbstbestimmung der Beteiligten beachtet werden. Dieses Recht darf nur durch ein Gesetz oder aufgrund eines Gesetzes eingeschränkt werden. Weder die StPO, das SOG-LSA noch das KunstUrhG enthalten diese Rechtsgrundlage.

Der in der Stellungnahme der Landesregierung zum II. Tätigkeitsbericht angekündigte Erlaßentwurf für eine Übergangsregelung zur landeseinheitlichen Durchführung von Wahllichtbildvorlagen ist dem Landesbeauftragten leider bisher nicht zur Stellungnahme vorgelegt worden.
Diese Übergangslösung könnte überflüssig werden, wenn der Gesetzentwurf eines Strafverfahrensänderungsgesetzes der Bundesregierung vom Dezember 1996 mit den dort vorgesehenen Bestimmungen in absehbarer Zeit Gesetz werden sollte. Das kann nach den bisherigen Erfahrungen mit dieser Rechtsmaterie aber noch lange dauern. Bis dahin bleiben in Sachsen-Anhalt die Ministerien des Innern und der Justiz in der Pflicht zu eigenen Regelungen.

20.10 Duplikatakten

Der Landesbeauftragte hatte sich bereits in seinem I. (S. 109) und II. Tätigkeitsbericht (S. 106) mit der datenschutzrechtlichen Problematik befaßt, die bei der Verwendung von Duplikatakten durch Dienststellen der Polizei besteht.

Hierzu hatte er zuletzt angeregt, bis zur Schaffung der erforderlichen datenschutzrechtlichen Regelungen in der StPO, eine landesweite gemeinsame Regelung von Ministerium der Justiz und Ministerium des Innern auf dem Erlaßwege zu treffen und darin die Anlegung von Duplikatakten auf Ausnahmefälle zu beschränken.

Das Ministerium der Justiz hat jetzt gebeten, von einer entsprechenden Regelung Abstand zu nehmen, da diese bisher in keinem anderen Bundesland getroffen worden sei. Dieser Auffassung des Ministeriums der Justiz hat sich das Ministerium des Innern angeschlossen. Beide wollen es bei diesem ungeregelten Zustand belassen.
Der Landesbeauftragte hält wegen der Gefahr für die Rechte Betroffener - keineswegs nur Beschuldigte und Täter, sondern auch Geschädigte, Zeugen und andere Unbeteiligte - daran fest, daß zumindest ein Grundrahmen für die Ausnahmefälle erarbeitet werden sollte, der den in § 10 Abs. 1 DSG-LSA geforderten Erforderlichkeitsgrundsatz für die übergangsweise Anwendung der Vorschrift durch die polizeiliche Praxis deutlicher herausarbeitet.

21. Rechtspflege

21.1 Justizmitteilungsgesetz

Sowohl in seinem I. (S. 117) als auch in seinem II. Tätigkeitsbericht (S. 111) hat der Landesbeauftragte die Schaffung einer Rechtsgrundlage für das Justizmitteilungswesen angemahnt. Denn die Gerichte und Staatsanwaltschaften des Landes übermitteln in Verfahren der streitigen Zivilgerichtsbarkeit, in der freiwilligen Gerichtsbarkeit und in Strafsachen eine Vielzahl von personenbezogenen

Daten aus und über eingeleitete Verfahren und Maßnahmen an die unterschiedlichsten Stellen.
Die Landesregierung hat in ihren beiden Stellungnahmen zu den Tätigkeitsberichten der Forderung nach einer gesetzlichen Grundlage grundsätzlich zugestimmt, aber die weitere Anwendung der bundeseinheitlichen Verwaltungsvorschriften (Mitteilungen in Strafsachen - MiStra und Mitteilungen in Zivilsachen - MiZi) auf den sog. „Übergangsbonus“ gestützt.
Der Landesbeauftragte ist jedoch nach wie vor der Auffassung, daß spätestens seit der Geltung des Artikels 6 Abs. 1 der Landesverfassung die genannten Verwaltungsvorschriften in Sachsen-Anhalt nicht mehr ohne gesetzliche Grundlage hätten angewendet werden dürfen. Die hilfsweise Stützung auf die Vorschriften des DSG-LSA reicht in vielen Fällen nicht mehr aus.

Die Bundesregierung hat im Berichtszeitraum nunmehr einen weiteren Entwurf für ein Justizmitteilungsgesetz (JuMiG-E) vorgelegt, der im Bundesrat im ersten Durchgang beraten wurde.

Die Kritik des Landesbeauftragten konzentriert sich im wesentlichen auf folgende Punkte:

- Der im Vorentwurf noch enthaltene Anordnungsvorbehalt für Richter, Staatsanwälte und Beamte des gehobenen Justizdienstes wurde aufgegeben.
  Dies ist in all den Fällen nicht sachgerecht, in denen es einer sorgfältigen Abwägung und/oder juristischen Wertung bedarf, u.a. weil solche Mitteilungen erhebliche Auswirkungen für den Betroffenen haben können, und die Wahrung von Grundrechten der Bürgerinnen und Bürger ein Gebot jedes staatlichen Handelns ist.
- Die im Vorentwurf noch vorgesehene Unterrichtungspflicht des Betroffenen über Inhalt und Adressaten der ihn betreffenden Datenübermittlung wurde durch ein schwächeres Auskunftsrecht ersetzt. Daneben beschränkt sich das Gesetz auf allgemeine Übermittlungsbefugnisse und verlagert die Regelung, wann, in welchen Fällen und zu welchem Zweck eine Übermittlung erfolgen soll, auf die Ebene von Verwaltungsvorschriften.

Auch diese Lösung ist aus datenschutzrechtlicher Sicht nicht akzeptabel. Auf eine Unterrichtungspflicht des Betroffenen von Amts wegen kann nur dann verzichtet werden, wenn für ihn aus dem Gesetz unmittelbar zu ersehen ist, daß und welche Daten zu welchen Zwecken an wen übermittelt worden sind. Da die vorgesehenen Regelungen lediglich einen Rahmen für zulässige Übermittlungen abstecken, die Einzelheiten aber in Verwaltungsvorschriften geregelt werden sollen, die dem Bürger im Normalfall nicht zugänglich sind, sind die vom Bundesverfassungsgericht aufgestellten Kriterien, daß jeder Bürger klar und deutlich aus dem Gesetz erkennen können muß, wer was wann und bei welcher Gelegenheit über ihn weiß, in keiner Weise erfüllt.

Die kritische Stellungnahme des Landesbeauftragten wurde vom Ministerium der Justiz nicht aufgegriffen. Auch ein Schreiben des Vorsitzenden der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. November 1995 an die Ministerin der Justiz als damalige Vorsitzende der Justizministerkonferenz, das die o.g. zentralen datenschutzrechtlichen Anliegen nochmals nachdrücklich formulierte, führte zu keinem besseren Ergebnis.

Statt dessen hat der Bundesrat in seiner jetzigen Stellungnahme zum Gesetzentwurf weitere datenschutzrechtliche Verschlechterungen beschlossen, die überwiegend „weichere“ Formulierungen enthalten, und damit den verfassungsrechtlich gebotenen Erforderlichkeitsgrundsatz aushebeln.

Der Gesetzentwurf wird nunmehr im Rechtsausschuß des Bundestages beraten. Ein Ende ist noch nicht abzusehen.

Unabhängig davon haben sich auch im Berichtszeitraum beim Landesbeauftragten Eingaben von Bürgern gehäuft, die sich darüber beschwert haben, daß zu ihren Lasten Datenübermittlungen auf der Grundlage der MiStra und der MiZi vorgenommen worden sind, die zu schweren Nachteilen für sie geführt haben.

Lediglich in einem Fall ist der Bundesgesetzgeber vorauseilend tätig geworden. Die bisher in der MiZi zu findende Vorschrift, wonach bei Wohnraumräumungsklagen, ohne Rücksicht auf die Erforderlichkeit im Einzelfall, generell pauschale

Datenübermittlungen vorsorglich zum Zwecke der Vermeidung von Obdachlosigkeit an die Gemeinden erfolgen, ist in § 15a BSHG auf eine gesetzliche Grundlage gestellt worden. Auch hiergegen bestehen noch datenschutzrechtliche Bedenken, da nicht jede Räumungsklage auf einem Zahlungsverzug, ausgelöst durch eine wirtschaftliche Notlage des Mieters, beruht. Dann aber geht eine solche Kündigung keine öffentliche Stelle etwas an.

21.2 Aufbewahrungsbestimmungen im Bereich der Justiz

Sowohl im I. (S. 120) als auch im II. Tätigkeitsbericht (S. 111) mahnte der Landesbeauftragte die Schaffung von gesetzlichen Regelungen zur Aufbewahrung von Schriftgut im Bereich der Justiz an, die bisher nur in bundeseinheitlichen Verwaltungsvorschriften geregelt ist. Besonderer Wert wurde dabei auf eine Verkürzung der Aufbewahrungsfristen gelegt. Die Landesregierung vertrat in ihren Stellungnahmen bisher die Auffassung, daß eine gesetzliche Regelung nicht erforderlich sei und aus Zweckmäßigkeitsgründen Verwaltungsvorschriften ausreichend seien.

Mittlerweile sind die Aufbewahrungsbestimmungen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden in zahlreichen Punkten geändert worden. Vielfach wurden dabei auch datenschutzgerechte Verkürzungen der Aufbewahrungsdauer vorgenommen. Dem Anliegen einer **gesetzlichen** Regelung der Aufbewahrung wurde jedoch bisher nicht entsprochen.

In einem anderen Bundesland ist inzwischen das dortige Justizministerium seinem Landesbeauftragten in der Auffassung gefolgt, daß die Aufbewahrungsbestimmungen einer gesetzlichen Grundlage bedürfen. Von daher ist der Landesbeauftragte erneut an das Ministerium der Justiz mit der Bitte um eine Überprüfung der bisher vertretenen Auffassung herangetreten. Eine Antwort des Ministeriums lag bei Redaktionsschluß noch nicht vor.

21.3 Strafverfahrensänderungsgesetz

Zum Jahresende 1996 legte die Bundesregierung einen weiteren Entwurf für ein Strafverfahrensänderungsgesetz 1996 (StVÄG-E) vor. Mit dem Entwurf sollen endlich bereichsspezifische Rechtsgrundlagen für die strafprozessuale Ermittlungstätigkeit und die Verwendung personenbezogener Informationen, die in einem Strafverfahren erhoben worden sind, geschaffen werden. Schwerpunkte sind dabei Regelungen über die Öffentlichkeitsfahndung und die Inanspruchnahme der Medien, Regelungen über die Erteilung von Aktenauskünften und Akteneinsichten für Justizbehörden, andere öffentliche Stellen und Private sowie die Übermittlung von Erkenntnissen für Forschungszwecke. Darüber hinaus finden sich Regelungen, unter welchen Voraussetzungen die Polizeibehörden künftig personenbezogene Informationen, die zunächst allein für die Zwecke der Strafverfolgung erhoben worden sind, auch für präventiv-polizeiliche Zwecke verwenden dürfen. Nicht aufgenommen wurde in den Gesetzentwurf, entgegen ursprünglichen Überlegungen der Bundesregierung, die Einführung der Zulässigkeit des Abhörens von Wohnungen mit technischen Mitteln (sog. „Großer Lauschangriff“, vgl. hierzu Ziff. 21.4).

Der Landesbeauftragte hatte Gelegenheit, zu dem Gesetzentwurf Stellung zu nehmen. Seine Bedenken konzentrieren sich im wesentlichen auf folgende Punkte:

- die mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung sowie eine fehlende Differenzierung zwischen Beschuldigten und Zeugen und die nicht ausreichende Berücksichtigung von Zeugnis- und Auskunftsverweigerungsrechten bei der Durchführung einer Öffentlichkeitsfahndung,
- unverhältnismäßig weite Auskunftserteilungsmöglichkeiten aus den Ermittlungs- und Strafakten an Privatpersonen und Stellen, die nicht Verfahrensbeteiligte sind,
- unzureichende Regelungen über Inhalt, Ausmaß und Umfang der personenbezogenen Dateien und Informationssysteme bei den Staatsanwaltschaften, mit der Folge, daß nahezu unbeschränkt Zentraldateien oder gemeinsame Dateien eingerichtet werden können,

- zu weitgehende Zugriffsmöglichkeiten auf diese Sammeldateien durch alle Strafverfolgungs- und Strafjustizbehörden,
- eine Außerkraftsetzung von Maßnahmen des technischen und organisatorischen Datenschutzes, die in allen sonstigen staatlichen Tätigkeitsbereichen zum Standard gehören (z.B. Protokollierung, interne Zugriffsbeschränkungen etc.).

Dem Ministerium der Justiz wurden die Kritikpunkte mit der Bitte um Unterstützung bei den Beratungen des Bundesrates übermittelt. Eine Stellungnahme des Ministeriums lag bei Redaktionsschluß noch nicht vor.
Dafür hat der Bundesrat inzwischen in seiner Stellungnahme zum Gesetzentwurf einige weitere datenschutzrechtliche Verschlechterungen beschlossen.

Beispielhaft seien hier nur genannt:
- die Streichung des Richtervorbehaltes für die Anordnung der Öffentlichkeitsfahndung und der längerfristigen Observation,
- die Streichung der Verwendungsbeschränkungen für Daten, die mit besonderen Erhebungsmethoden nach dem Polizeirecht erhoben wurden, für Zwecke der Strafverfolgung,
- die Aufhebung der allgemeinen Zweckbindungsregelungen der Datenverarbeitung für öffentliche Stellen gegenüber Strafverfolgungsbehörden,
- eine erhebliche Erweiterung der Auskunfts- und Akteneinsichtsrechte auch für andere öffentliche Stellen,
- die Streichung der im Gesetzentwurf noch vorhandenen detaillierten Regelungen, in welchen Fällen Strafverfolgungs- und Strafjustizbehörden personenbezogene Daten von Amts wegen an andere Stellen übermitteln dürfen, die im weitesten Sinne mit der Strafrechtspflege zu tun haben,
- die ersatzlose Streichung der im Entwurf noch vorhandenen Streichungs- und Löschungsfristen für personenbezogene Daten in Dateien,
- die Beseitigung der im Entwurf noch vorgesehenen Kontrollverfahren für automatisierte Abrufverfahren nebst Wegfall der Verwendungsbeschränkungen der Protokolldaten.

Es bleibt nunmehr abzuwarten, ob der Gesetzentwurf bei den kommenden Beratungen im Bundestag noch einige datenschutzrechtliche Verbesserungen erfahren wird.

21.4 Einführung des sog. „Großen Lauschangriffs“

Im Vorfeld der Beratungen zu einem StVÄG 1996 wurde innerhalb der Bundesregierung auch eine Verfassungsänderung diskutiert, die eine akustische Überwachung von Wohn- und Geschäftsräumen zum Zweck der Beweismittelgewinnung im Strafverfahren (sog. „Großer Lauschangriff“) vorsieht. Eine solche Änderung des Artikels 13 Grundgesetz (GG) und die dazugehörige gesetzliche Regelung in der Strafprozeßordnung (StPO) würden einen erheblichen Eingriff in das Persönlichkeitsrecht jedes einzelnen Bürgers darstellen. Von daher haben die Datenschutzbeauftragten des Bundes und der Länder bereits im Jahre 1993 (vgl. II. Tätigkeitsbericht, S. 110) mehrheitlich den „Großen Lauschangriff“ aus grundsätzlichen Erwägungen abgelehnt.

Das Grundgesetz gewährleistet aus den geschichtlichen Erfahrungen Deutschlands heraus jedem Bürger einen unantastbaren Bereich privater Lebensgestaltung, in dem die öffentliche Gewalt nichts zu suchen hat. Dem einzelnen muß, nach der Rechtsprechung des Bundesverfassungsgerichtes ein privates Refugium, ein persönlicher Bereich garantiert werden, der staatlicher Ausforschung - insbesondere heimlicher - entzogen ist. Das gilt insbesondere gegenüber Maßnahmen der Strafverfolgung, weil davon auch unverdächtige und unschuldige Bürgerinnen und Bürger betroffen sein können. Dieses Refugium vor heimlicher staatlicher Ausforschung zum Zwecke der Strafverfolgung war bisher die von Artikel 13 GG geschützte Wohnung.
Mit der Einführung des „Großen Lauschangriffs“, wie er offenbar von der Bundesregierung nunmehr geplant wird, würde dieser letzte unantastbare Bereich privater Lebensgestaltung zum Zwecke der Strafverfolgung geöffnet bzw. hier in Ostdeutschland fast sieben Jahre nach der Wende wiedereröffnet. Dabei täuscht die Verpackung im „biederen“ rechtsstaatlichen Gewande über die damit verbundenen gravierenden menschlichen und rechtlichen Probleme der Maßnahmen hinweg.

Es geht nicht darum, besondere Formen der Schwerstkriminalität der gewünschten und auch vom Bundesverfassungsgericht stets bestätigten, effektiven Strafverfolgung zu entziehen, sondern um die rechts- und gesellschaftspolitisch

richtige Entscheidung, ob man für Ermittlungsansätze - nicht einmal Ergebnisse sind garantiert - in einigen wenigen Fällen, die massive Beeinträchtigung, ja Auflösung der Intimsphäre einer Vielzahl unbeteiligter und unschuldiger Bürger in Kauf nehmen will. Dabei bestehen die Schwierigkeiten nach Ansicht des Landesbeauftragten nicht im rechtlichen, sondern im praktischen Anwendungsbereich. Täter und Tatbeteiligte sind im Ermittlungsverfahren von unschuldigen Bürgern anfangs kaum zu unterscheiden. Der gesuchte Täterkreis verwendet ein hohes Maß an Energie und Phantasie auf die Verschleierung von Personen und Tatabläufen mit der Folge, daß schon heute, mit den vorhandenen Eingriffsmitteln (z.B. Brief- und Telefonkontrolle, polizeiliche Beobachtung), im Normalfall Ermittlungsansätze der Strafverfolger in diesem Milieu immer eine Vielzahl unbeteiligter Personen mit Eingriffsmaßnahmen erfassen und in ihren Rechten beeinträchtigen. Dies ist den unschuldig Betroffenen in einem Rechtsstaat nicht plausibel zu machen und kann mit den vom Staat zu leistenden Geldentschädigungen allenfalls dürftig kompensiert werden. Um so mehr muß eine freie, auf die individuelle Persönlichkeit und Würde ihrer Bürger gegründete Gesellschaft sich fragen, ob sie sich mit den neu geplanten Eingriffsmaßnahmen in den Offenbarungseid einer (praktisch) unbegrenzten Öffnung der Intimsphäre aller Bürgerinnen und Bürger treiben lassen will. Deshalb sollten insbesondere alle diejenigen, die in Staat und Gesellschaft Verantwortung tragen, ihre Bewertung noch einmal kritisch prüfen, ob sie die Bundesrepublik Deutschland schon derart kriminell unterwandert sehen, daß deren staatliche Institutionen und die Freiheit ihrer Bürger im Kern gefährdet sind.

Für den Fall, daß man sich auf Bundesebene dennoch für das Abhören von Wohnungen entscheiden will, erfordert der Schutz der Privatsphäre mindestens eine klare Begrenzung und verfahrensmäßige Sicherung der Maßnahmen. Diese müssen vom Grundsatz her im Grundgesetz selbst und nicht in der StPO festgelegt werden. Die Datenschutzbeauftragten des Bundes und der Länder haben daher einvernehmlich Maßnahmen zur Sicherung der Privatsphäre für den Fall der Einführung der akustischen Wohnraumüberwachung erarbeitet **(Anlage 10)**, die den vorgenannten Grundsätzen Rechnung tragen sollen.

21.5 Länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Aufgrund der durch das Verbrechensbekämpfungsgesetz vom 28.10.1994 geschaffenen gesetzlichen Grundlagen für ein bundesweites Zentrales staatsanwaltschaftliches Verfahrensregister (ZStV), das der Speicherung aller im Bundesgebiet anhängigen Ermittlungs- und Strafverfahren dienen soll, hatte das Bundesministerium der Justiz in Abstimmung mit den Landesjustizverwaltungen eine Errichtungsanordnung zu erstellen. Der Landesbeauftragte hat bereits in seinem II. Tätigkeitsbericht (S. 118) auf zum Teil erhebliche datenschutzrechtliche Mängel in der Errichtungsanordnung hingewiesen. Die Kritikpunkte sind vom Ministerium der Justiz nicht aufgegriffen worden. Die Errichtungsanordnung wurde zwischenzeitlich vom Bundesministerium der Justiz im Einvernehmen mit den Landesjustizverwaltungen nahezu unverändert erlassen.

Neu in die Diskussion kamen während des Berichtszeitraumes die technisch-organisatorischen Leitlinien für das ZStV, die auch seitens des Landesbeauftragten kritisch überprüft worden sind. Bedenken ergaben sich insbesondere gegen die darin vorgesehene Möglichkeit, Auskünfte auch telefonisch, fernschriftlich oder per Telefax anzufordern und auf gleichem Weg zu erhalten.
Auch dazu hat der Landesbeauftragte wiederholt deutlich gemacht, daß Auskünfte über das Telefon oder per Telefax mit erheblichen Sicherheitsrisiken für die übermittelten Daten verbunden sind (vgl. hierzu auch Ziff. 13).
Nicht unproblematisch ist auch die Regelung, wonach immer dann, wenn bei der Einspeicherung eines Ermittlungsverfahrens ein Beschuldigter mit „gleichen“ Personendaten im ZStV bereits registriert ist, das neue Ermittlungsverfahren dem bereits gespeicherten Datensatz des Beschuldigten zugespeichert wird. Aufgrund der in den Leitlinien vorgesehenen weiten Voraussetzungen für die Beantwortung der Frage, wann „gleiche“ Personendaten vorliegen, ist es nicht auszuschließen, daß Datensätze auch dann einer (falschen) Person zugeordnet werden, wenn die Personenmerkmale nicht vollständig übereinstimmen und es sich tatsächlich um zwei verschiedene Personen handelt.
Um hierbei Fehlerquellen zu vermeiden, hat der Landesbeauftragte empfohlen, grundsätzlich nur dann ein neu gemeldetes Ermittlungsverfahren einer bereits

erfaßten Person zuzuspeichern, wenn **alle** Personenmerkmale (Geburts- und Familienname, alle Vornamen, das Geburtsdatum, Geburtsort und Geschlecht) vollständig angegeben sind und jeweils völlig übereinstimmen.

Des weiteren hat der Landesbeauftragte darauf hingewiesen, daß bei einer Auskunftserteilung über Eintragungen von „ähnlichen“ Personen (Ähnlichen-Service) stets klar und deutlich darauf hingewiesen werden muß, daß die Auskunft aufgrund „ähnlicher“ und/oder nur „partiell übereinstimmender“ Personenmerkmale zustande gekommen ist und die Identität der genannten Personen nur zu vermuten ist, nicht aber feststeht.

Schließlich enthielten die technisch-organisatorischen Leitlinien in dem Abschnitt, der mit „Datenschutz und Datensicherheit“ überschrieben wurde, anstelle einer vollständigen und systematischen Übersicht über die einzelnen erforderlichen Maßnahmen lediglich die Ankündigung, daß eine Bedrohungs- und Risikoanalyse durchgeführt werden soll, die Grundlage für kurz-, mittel- und langfristig zu verwirklichende Sicherheitsmaßnahmen bilden soll.
Aus der Sicht des Landesbeauftragten ist nicht nachvollziehbar, warum diese Analyse nicht so rechtzeitig erarbeitet werden kann, daß die Ergebnisse schon vor Inbetriebnahme des Registers (voraussichtlich 1999) vorliegen. Der Beginn einer automatisierten Verarbeitung der besonders sensiblen personenbezogenen Daten, ohne detaillierte Kenntnis der zu erwartenden Risiken, ist mehr als bedenklich. Anders als in den technisch-organisatorischen Leitlinien vorgesehen, hält der Landesbeauftragte auch von Anfang an besondere Maßnahmen zur Sicherung der Vertraulichkeit und Integrität der übertragenen Daten für erforderlich.
An dieser Stelle sei auf die Entschließung der Datenschutzbeauftragten von Bund und Ländern vom 9. Mai 1996 (**Anlage 6)** hingewiesen, die Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten beinhaltet.

Eine Antwort des Ministeriums der Justiz auf die Bedenken und Empfehlungen des Landesbeauftragten vom August 1996 lag bis Redaktionsschluß nicht vor.

21.6 Öffentlichkeitsfahndung im Strafverfahren

Bei an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und auch Zeugen) ist stets auch das Recht der Betroffenen auf informationelle Selbstbestimmung berührt. Jedoch finden sich gegenwärtig nur punktuell gesetzliche Regelungen, die Einzel-aspekte der öffentlichen Fahndung nach Personen behandeln. So sind in verschiedenen Vorschriften der StPO zwar die Voraussetzungen und der Inhalt eines Steckbriefes gegen einen Beschuldigten/Verurteilten geregelt. Einschränkungen, die sich mit Blick auf den Grundsatz der Verhältnismäßigkeit, insbesondere auch auf die Auswahl des Veröffentlichungsmittels und den Adressatenkreis der Fahndungsmaßnahme beziehen, sind bislang lediglich in Verwaltungsvorschriften wie den bundeseinheitlichen „Richtlinien über die Inanspruchnahme von Publikationsorganen zur Fahndung nach Personen bei der Strafverfolgung“ enthalten. Keine Regelungen enthält die geltende Strafprozeßordnung für die Fahndung nach bekannten Zeugen.

Unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts zum Grundrecht auf informationelle Selbstbestimmung sind die vorhandenen gesetzlichen Regelungen über die Voraussetzungen der Öffentlichkeitsfahndung unzureichend. Verwaltungsvorschriften genügen nicht.
Da alle Maßnahmen der öffentlichen Personenfahndung eine Einschränkung des Grundrechts bedeuten, muß sie der Bürger nur dann hinnehmen, wenn eine gesetzliche Grundlage besteht, aus der sich die Voraussetzungen und der Umfang der Einschränkungen klar ergeben. Diese muß nachgeholt werden.

Der nunmehr vorliegende Regierungsentwurf eines StVÄG 1996 hat sich in den §§ 131 - 131c des Themas angenommen. Wie vorstehend bereits unter Ziffer 21.3 dargelegt wurde, bestehen erhebliche Zweifel, ob diese Regelungsvorschläge den verfassungsrechtlichen Anforderungen genügen.
Die 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Grundsätze für die öffentliche Fahndung in Strafverfahren erarbeitet **(Anlage 7)**, die der Landesbeauftragte dem Ministerium der Justiz mit der Bitte um Stellungnahme übersandt hat.

In seiner Antwort hat das Ministerium mitgeteilt, daß es diese Grundsätze in die Überlegungen zur ersten Stellungnahme des Bundesrates zum StVÄG 1996 mit einbeziehen wolle.
Leider fanden sie dort (vgl. Ziff. 21.3) keinen Niederschlag. Die weitere Entwicklung wird von den Beratungen des Bundestages zum StVÄG 1996 abhängen. Dann hat der Bundesrat erneut das Wort.

21.7 Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden an die Medien

Schon die Öffentlichkeitsfahndung in Strafverfahren nach Beschuldigten oder unbekannten Tatverdächtigen bedeutet eine erhebliche Beeinträchtigung der Persönlichkeitsrechte der Betroffenen. Deshalb sind Übermittlungen personenbezogener Daten über strafrechtliche Ermittlungsverfahren an die Medien mit allergrößter Vorsicht zu handhaben. Da ein Ermittlungsverfahren bereits auf Verdacht eröffnet wird, ist der juristisch nicht vorgebildete Bürger allzuleicht geneigt, die Eröffnung eines solchen Verfahrens schon mit dem Nachweis der zur Last gelegten Tat gleichzusetzen. Das wird der Wirklichkeit nicht gerecht, denn die Mehrzahl der Ermittlungsverfahren wird eingestellt, weil sich z.B. der Verdacht nicht bestätigt oder keine Schuld des Betroffenen vorliegt.
Die Medien, deren tägliche Berichterstattung in erheblichem Umfange von laufenden Ermittlungs- und Strafverfahren lebt, haben naturgemäß ein erhebliches Interesse an möglichst detaillierten Informationen über Täter und Opfer von Straftaten. Demgegenüber haben die jeweils Betroffenen regelmäßig ein grundlegendes Interesse daran, daß ihre personenbezogenen Daten nicht an die Öffentlichkeit gelangen.

Jede Bekanntgabe personenbezogener Daten an die Medien durch die Strafverfolgungsbehörden ist rechtlich eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereiches und bedarf als Eingriff in das Grundrecht auf informationelle Selbstbestimmung einer bereichsspezifischen gesetzlichen Grundlage. Eine derartige Regelung existiert jedoch weder im Landespressegesetz noch in

der StPO. Lediglich die bundeseinheitlichen „Richtlinien für das Straf- und Bußgeldverfahren“ (RiStBV) enthalten als Verwaltungsvorschriften allgemeine Abwägungsregelungen für die Zusammenarbeit der Justiz mit Presse und Rundfunk. Daneben besteht im Lande Sachsen-Anhalt auch noch eine Verwaltungsvorschrift über die „Zusammenarbeit zwischen der Polizei und den Medien bei der Strafverfolgung und der Gefahrenabwehr“, die, wenn auch in der Form nicht den verfassungsrechtlichen Vorgaben entspricht, so doch zumindest inhaltlich ansatzweise datenschutzrechtliche Mindestforderungen enthält.

Ein Entwurf des Ministeriums der Justiz vom Oktober 1994 zu „Richtlinien für die Zusammenarbeit der Justiz mit Presse und Rundfunk“ ist seinerzeit vom Landesbeauftragten überprüft worden. Dabei zeigten sich erhebliche datenschutzrechtliche Lücken.
Ende Februar 1997 hat das Ministerium der Justiz - ohne erneute Beteiligung des Landesbeauftragten - nun diese Richtlinien im Justizministerialblatt veröffentlicht. Eine zunächst kursorische Überprüfung hat ergeben, daß auch die jetzt überarbeitete Fassung teilweise nicht den datenschutzrechtlichen Anforderungen genügt und zumindest in einem Punkt nicht mit Art. 6 der Landesverfassung vereinbar sein dürfte, weil die Nutzung personenbezogener Daten für Zwecke der Pressearbeit ohne gesetzliche Grundlage erfolgt.
Der Landesbeauftragte wird diese Punkte im einzelnen noch mit dem Ministerium erörtern.

Die 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung den Bundesgesetzgeber aufgefordert, bereichsspezifische Regelungen für die Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden an die Medien (außerhalb der Öffentlichkeitsfahndung) zu schaffen **(Anlage 8)**. Diese Regelungen sollen - entsprechend der Forderung des Bundesverfassungsgerichtes - für die Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen und ausgewogen die verschiedenen Interessen und Rechte berücksichtigen.

21.8 Staatliche Eingriffsbefugnisse in der modernen Informationsgesellschaft

Die tiefgreifende Entwicklung der modernen Telekommunikation (insbesondere durch Privatisierung der Netze, weite Verbreitung von Mobilfunkgeräten, Digitalisierung der Kommunikation), die rasche Fortentwicklung der weltweit vernetzten Informationstechnologie zu Kommunikationszwecken (z.B. Mailboxen, Internet) und zu Zwecken der Informations- und Güterbeschaffung (z.B. Online-Datenbanken, Teleshopping) sowie die neuen Medien, lassen die traditionellen Grenzen zwischen Medien-, Kommunikations- und Informationstechnik verschwinden und führen - jedenfalls tendenziell - zu einem grundlegend veränderten Kommunikationsverhalten des Bürgers. Traditionelle Büroarbeiten werden über Teleworking Gegenstand digitalisierter Übertragung und damit überwachbar, Telebanking ermöglicht auch überwachbare Banktransaktionen, Tele-shopping kann zu einem transparenten Konsumverhalten führen, die Nutzung von Fernsehen mit Rückkanal oder der Informationsangebote von Rundfunk und Fernsehen im Internet führen zur elektronischen Überprüfbarkeit der Mediennutzung. Mit dieser Entwicklung zur „Informationsgesellschaft“ gehen auch neue Gefahren durch die Nutzung der neuen Technik zu kriminellen Zwecken einher.

Es ist deshalb nicht nur legitim, sondern geboten, daß die Strafverfolgungsbehörden in die Lage versetzt werden, ihre gesetzlichen Überwachungs- und Zugriffsrechte wahrzunehmen, um Mißbräuchen wirksam begegnen zu können.

Die dahingehenden gesetzgeberischen und technischen Anstrengungen dürfen jedoch aus datenschutzrechtlicher Sicht nicht zur Folge haben, daß in die Grundrechte unbeteiligter Bürger, insbesondere in ihr informationelles Selbstbestimmungsrecht, aber auch in das Fernmeldegeheimnis und das Recht auf unbeobachtete Kommunikation mehr eingegriffen wird, als unabdingbar erforderlich. Die verfassungsrechtlich garantierten Freiheitsräume des einzelnen müssen auch bei Nutzung der neuen Technik erhalten bleiben.
Daher hat die 52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder Thesen beschlossen **(Anlage 9)**, die diesen Grundsätzen Rechnung tragen sollen.

21.9 Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVASt)

Sowohl im I. (S. 118) als auch im II. Tätigkeitsbericht (S. 120) hatte der Landesbeauftragte darauf hingewiesen, daß es für die nach den RiVASt vorgenommenen Übermittlungen personenbezogener Daten an der erforderlichen gesetzlichen Grundlage fehlt.
Die Landesregierung hat in ihren Stellungnahmen zu den beiden Tätigkeitsberichten die Auffassung vertreten, daß die RiVASt auf den gesetzlichen Grundlagen der StPO, des BKAG und des Gesetzes über die internationale Rechtshilfe in Strafsachen (IRG) beruhen. Im übrigen wolle sie die Bemühungen der Bundesregierung unterstützen, das IRG im Hinblick auf das Recht auf informationelle Selbstbestimmung zu novellieren und dem folgend die RiVASt entsprechend zu ändern. Die Frage hat auch Bedeutung für die bisher zwischen dem Landesbeauftragten und dem Ministerium der Justiz streitige Frage über die in den RiVASt niedergelegte Meldepflicht bei Auslandsstraftaten von Ausländern (I. Tätigkeitsbericht, S. 32 und II. Tätigkeitsbericht, S. 21).

In der Angelegenheit hat es im Berichtszeitraum keine neuen Entwicklungen gegeben. Namentlich ein Entwurf zur Novellierung des IRG liegt nicht vor. Eine Datenübermittlung dürfte daher nur in Einzelfällen übergangsweise auf der Grundlage des DSG-LSA zulässig sein, soweit nicht bereichsspezifische Rechtsgrundlagen greifen (z.B. § 8 Abs. 3 Asylverfahrensgesetz, §§ 68, 73 SGB X).

21.10 Postbedienstete als Hilfsbeamte der Staatsanwaltschaft?

In der (Landes-)Verordnung über die Hilfsbeamten der Staatsanwaltschaft aus dem Jahre 1991 werden bestimmte Beamtengruppen der inzwischen umgewandelten Deutschen Bundespost in ihrer Eigenschaft als Beamte des Betriebssicherungsdienstes als „Hilfsbeamte der Staatsanwaltschaft“ aufgeführt.
Mit Inkrafttreten des Postneuordnungsgesetzes zum Jahresbeginn 1995 besteht

jedoch keine Grundlage mehr für die Bestellung von Mitarbeitern des Betriebssicherungsdienstes der nunmehr privatisierten Deutschen Post AG zu Hilfsbeamten der Staatsanwaltschaft. Denn seit der Privatisierung der Post gehört der Betriebssicherungsdienst nicht mehr zum öffentlichen Dienst. Mit Artikel 33 Abs. 4 GG ist es nicht vereinbar, wenn hoheitliche Befugnisse im Bereich der Strafverfolgung auf Private übertragen werden.

Der Landesbeauftragte hat daher dem Ministerium der Justiz bereits im November 1995 empfohlen, die notwendigen Änderungen der Verordnung über die Hilfsbeamten der Staatsanwaltschaft des Landes Sachsen-Anhalt vorzunehmen. Eine Antwort des Ministeriums der Justiz bzw. eine Änderung der Verordnung lag bis Redaktionsschluß noch nicht vor.

21.11 Geldwäschegesetz - Registermäßige Behandlung von Verdachtsanzeigen

Bereits in seinem II. Tätigkeitsbericht hat der Landesbeauftragte über das Geldwäschegesetz (GwG) berichtet, welches Identifizierungs- und Aufzeichnungspflichten bei Finanztransaktionen, insbesondere für Banken und andere Gewerbetreibende sowie eine Verpflichtung der Meldung von Verdachtsfällen der Geldwäsche an die Strafverfolgungsbehörden enthält.
Dazu hat das Ministerium der Justiz unter Mitwirkung des Landesbeauftragten „Richtlinien für die Zusammenarbeit von Staatsanwaltschaft und Polizei bei Ermittlungen im Rahmen der Geldwäsche“ erarbeitet, welche im wesentlichen organisatorische Maßnahmen für die Bearbeitung von Anzeigen nach dem GwG und die Bearbeitung der aufgrund von GwG-Anzeigen eingeleiteten Ermittlungen regeln.
Nicht geregelt wurde in dem Erlaß jedoch die Frage, wie die GwG-Anzeigen in den staatsanwaltschaftlichen Verfahrensregistern behandelt werden sollen. Bedeutung hat dies insbesondere für solche Anzeigen, bei denen die Vorprüfung den Verdacht einer Geldwäsche nicht bestätigt hat.
Nach der o.g. Verwaltungsvorschrift werden GwG-Anzeigen als „Strafanzeigen“ nach § 158 Abs. 1 StPO behandelt, auf deren Grundlage die Staatsanwaltschaft prüft, ob ein Ermittlungsverfahren eingeleitet werden soll. Als „Strafanzeigen“

werden sie gem. § 47 Abs. 1 b) der Aktenordnung für die Gerichte der ordentlichen Gerichtsbarkeit und die Staatsanwaltschaften (AktO-oG) in das Js-Register (eingehende Anzeigen, die sich gegen eine bestimmte Person richten) eingetragen.
Nach Auffassung des Landesbeauftragten unterscheiden sich jedoch Verdachtsanzeigen nach dem GwG grundsätzlich von den Strafanzeigen, die in § 47 AktO-oG angesprochen sind. Während Strafanzeigen nach § 47 AktO-oG vom Willen des Anzeigeerstatters getragen sind, daß der von ihm Beschuldigte für ein bestimmtes Verhalten strafrechtlich zur Verantwortung gezogen wird, sind die im GwG genannten Institute und Behörden stets zu reinen Verdachtsanzeigen verpflichtet, die ohnehin rechtsstaatlich problematisch sind. Denn der sonst stets erforderliche strafrechtliche Anfangsverdacht wird nicht von der dazu berufenen Staatsanwaltschaft festgestellt, sondern von dafür nicht ausgebildeten Mitarbeitern der meldepflichtigen Banken und Wechselstuben. Dieser Sach- und Rechtslage muß nach Ansicht des Landesbeauftragten auch bei der registermäßigen Behandlung der GwG-Anzeigen Rechnung getragen werden.

Vor diesem Hintergrund erscheint es datenschutzrechtlich geboten, die eingehenden Verdachtsanzeigen nach dem GwG differenziert zu behandeln:
Leitet die Staatsanwaltschaft aufgrund einer Verdachtsanzeige nach dem Geldwäschegesetz ein Ermittlungsverfahren ein und ist der Beschuldigte schon bekannt, so steht einer Eintragung in das Js-Register nichts entgegen. Besteht jedoch gegen den Beschuldigten kein Anfangsverdacht einer Straftat, so sollte das Verfahren entweder in ein neu zu errichtendes besonderes Geldwäscheregister oder zumindest in das allgemeine AR-Register eingetragen werden.

Der Landesbeauftragte hat sich nachdrücklich bereits im Frühjahr 1995 mit einer entsprechenden Empfehlung an das Ministerium der Justiz gewandt und die derzeitige Verfahrensweise - nicht zuletzt im Hinblick auf eine künftige bundesweite Speicherung solcher Anzeigen im Zentralen staatsanwaltschaftlichen Verfahrensregister - aus datenschutzrechtlicher Sicht für nicht akzeptabel erachtet.
Eine Stellungnahme des Ministeriums lag bis Redaktionsschluß nicht vor.

21.12 Datenschutz beim Täter-Opfer-Ausgleich

Bereits in seinem II. Tätigkeitsbericht (S. 129) hatte der Landesbeauftragte zu den datenschutzrechtlichen Problemen bei der Datenübermittlung im Rahmen der Durchführung des Täter-Opfer-Ausgleiches Stellung genommen und darauf hingewiesen, daß, mangels einer bereichsspezifischen Regelung im Bundesrecht, eine Datenübermittlung ohne vorherige Einwilligung aller Betroffenen (Täter und Opfer) an einen privaten Verein für Straffälligen- und Bewährungshilfe zur Konfliktschlichtung nicht zulässig ist.

Das Ministerium der Justiz hat zwischenzeitlich unter Mitwirkung des Landesbeauftragten eine Verwaltungsvorschrift erlassen, die eine Einwilligung aller Betroffenen zur Voraussetzung der Durchführung des Täter-Opfer-Ausgleichs macht. Gleichzeitig wurde datenschutzkonform geregelt, daß privaten Konfliktschlichtungsstellen nicht die gesamten Verfahrensakten zu übersenden sind, sondern nur Namen und Anschriften von Tätern und Opfern sowie eine kurze Sachdarstellung.

Kürzlich beschwerte sich ein Bürger beim Landesbeauftragten darüber, daß man sich in einer Staatsanwaltschaft nicht daran gehalten und ohne seine vorherige Einwilligung die ihn betreffende Strafakte an einen privaten Konfliktschlichtungsverein übersandt hatte.
Angesichts der offenkundig gewordenen erheblichen Mängel beim Schutz der personenbezogenen Daten und der besonderen Verantwortung einer Staatsanwaltschaft zur Beachtung gesetzlicher Vorschriften beim Umgang mit amtlich geheimzuhaltenden Unterlagen und bei der Einhaltung anderer datenschutzrechtlicher Vorschriften sprach der Landesbeauftragte eine formelle Beanstandung gegenüber dem Ministerium der Justiz aus.
Die daraufhin vom Ministerium der Justiz inzwischen ergriffenen Maßnahmen hält er für geeignet und ausreichend, um künftig bei der Durchführung des Täter-Opfer-Ausgleichs den erforderlichen Schutz personenbezogener Daten sicherzustellen.
Im übrigen unterstützt auch das Ministerium eine bundesgesetzliche Regelung für erwachsene Straftäter im StVÄG 1996.

21.13 Überprüfung der Staatsanwaltschaften

Im Berichtszeitraum hat der Landesbeauftragte seine bereits in den Vorjahren begonnenen schwerpunktmäßigen Überprüfungen der Staatsanwaltschaften fortgesetzt und abgeschlossen. Besonderes Augenmerk legte er dabei insbesondere auf die datenschutzgerechte Führung der Zentralen Namenskartei und der Ermittlungsakten, das Verfahren der Gewährung von Akteneinsicht, die Aufbewahrung von Beweismitteln nach Verfahrenseinstellungen sowie die technischen und organisatorischen Regelungen zur sicheren Aufbewahrung der personenbezogenen Daten.

1. Bei den überprüften Staatsanwaltschaften ist bereits das automatisierte Geschäftsstellenbearbeitungssystem SIJUS-Strafsachen zur automatischen Erfassung aller vorhandenen Ermittlungsakten eingeführt worden. Bei der Eingangserfassung im SIJUS-System werden die persönlichen Daten der Beschuldigten und, bei qualifizierten Sachen mit unbekannten Tätern sowie bei Tötungs- und Selbsttötungsdelikten, die Daten der Opfer gespeichert, unabhängig vom Alter und der Schuldfähigkeit. Darüber hinaus enthält die Bildschirmmaske bei einer Staatsanwaltschaft zur Erfassung auch den Namen der Mutter des Betroffenen.

   Sowohl in seinem I. (S. 131) als auch in seinem II. Tätigkeitsbericht (S. 121) hat der Landesbeauftragte darauf hingewiesen, daß für den Einsatz des SIJUS-Verfahrens keine ausreichende Rechtsgrundlage besteht. In das Grundrecht auf informationelle Selbstbestimmung der betroffenen natürlichen Personen darf aber nur durch oder aufgrund eines Gesetzes eingegriffen werden (Art. 6 Abs. 1 der Landesverfassung Sachsen-Anhalt, Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG).
   Die §§ 152, 160, 161 StPO erfüllen die verfassungsrechtlichen Anforderungen nicht. Der von der Rechtsprechung des Bundesverfassungsgerichts eingeräumte sog. „Übergangsbonus“ kann auch nicht in Anspruch genommen werden, denn er erfaßt nur solche Verfahrensweisen, die 1983 im Zeitpunkt der Entscheidung des Bundesverfassungsgerichts bereits bestanden haben. Das SIJUS-Verfahren ist jedoch erst in den 90er Jahren **neu** geschaffen worden.

Das Ministerium der Justiz des Landes Sachsen-Anhalt hat es bisher abgelehnt, bis zur Schaffung einer bundesgesetzlichen Grundlage, die automatisierte Datenverarbeitung bei den Staatsanwaltschaften zumindest auf eine landesgesetzliche Grundlage zu stellen. Deshalb dürfen die Daten im SIJUS-System - hilfsweise auf § 10 DSG-LSA gestützt - nur insoweit und so lange gespeichert und verarbeitet werden, wie dies zur Aufgabenerledigung unbedingt erforderlich ist.
Gemessen an diesem Maßstab ist die bei einer Staatsanwaltschaft festgestellte Erhebung und Speicherung des Namens der Mutter bei Jugendlichen und Kindern nicht nur nicht erforderlich, sondern dazu fehlt jegliche Rechtsgrundlage. Es handelt sich um ein personenbezogenes Datum einer Person, die im Regelfall in keiner Weise Beteiligte an dem staatsanwaltschaftlichen Ermittlungsverfahren ist und deshalb in den personenbezogenen Datensammlungen der Staatsanwaltschaft nichts zu suchen hat.
Die zur Begründung herangezogene „Bequemlichkeitserfassung“ für das Bundeszentralregister (BZR) trägt keinen rechtswidrigen Eingriff in Grundrechte. Das BZR muß sich eine eigene Rechtsgrundlage beim Bundesgesetzgeber beschaffen.

2. Rechtlich bedenklich ist auch die festgestellte automatische Erstellung eines Einstellungsbescheides an den Geschädigten bei Strafsachen mit unbekannten Tätern; sie erfolgt bereits mit der Eingabe einer neuen Sache in das SIJUS-Verfahren und enthält alle verfahrens- und personenbezogenen Daten einschließlich einer maschinell erstellten Unterschrift des zuständigen Staatsanwaltes. Damit wird ein Rechtszustand schriftlich festgestellt, bevor der zuständige Staatsanwalt sich entschieden hat, ob er Anklage erheben, das Verfahren einstellen oder aber weitere Ermittlungen veranlassen will.
Ein derartiger „Bescheid auf Vorrat“ mag zwar in Massenverfahren, wie bei Strafsachen mit unbekannten Tätern, den Reiz des Praktischen haben, ist aber nicht nur im Hinblick auf die genannten Vorschriften der StPO, sondern auch in bezug auf die Verpflichtung der Staatsanwaltschaft, nur richtige personenbezogene Daten zu verarbeiten (§ 16 Abs. 1 DSG-LSA), in hohem Maße problematisch, wenn nicht gar unzulässig. Die Vorratshaltung provoziert darüber hinaus die ungewollte fehlerhafte Absendung einer materiell-

rechtlich nicht gesicherten Entscheidung und begünstigt die unbemerkte, mißbräuchliche Absendung des Einstellungsbescheides.

Starke Rechtsbedenken waren auch gegen die bei einer Staatsanwaltschaft vorgefundenen, vorgefertigten amtlichen Einstellungsbescheide zu erheben, die schon bei der Polizei als Vordruck vorlagen und ausgefüllt mit dem Ermittlungsvorgang übersandt wurden. Der Vordruck wird mit der Eintragung des Aktenzeichens der Staatsanwaltschaft der Form nach ein fertiger Einstellungsbescheid, ohne daß der zuständige Staatsanwalt eine Entscheidung über den Aus- und/oder Fortgang des Verfahrens getroffen hat.
Damit wird die von § 16 DSG-LSA auch gewährleistete Sicherheit im Rechtsverkehr unterlaufen, weil damit aktenmäßig und ggf. durch unberechtigte Absendung eines inhaltlich nicht gedeckten Einstellungsbescheides falsche Daten verarbeitet werden. Gerade die moderne und automatisierte Datenverarbeitung bietet ausreichende Möglichkeiten einer praktikableren **und** rechtlich besseren Aufgabenlösung.

3. Im Rahmen der stichprobenhaften Überprüfung der Ermittlungsakten wurde festgestellt, daß Unsicherheiten und Unklarheiten über die rechtlichen Grundlagen bei der Entscheidung über die Gewährung von Akteneinsicht an nicht verfahrensbeteiligte Dritte bestehen.
   Hierzu hat der Landesbeauftragte deutlich gemacht, daß es sich auch bei der Gewährung von Akteneinsicht um eine Übermittlung personenbezogener Daten und damit um einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung handelt. Die Regelungen in der StPO erlauben im laufenden Strafverfahren nur die Übermittlung an den Verteidiger des Beschuldigten (§ 147 StPO) oder den Rechtsanwalt des Verletzten (§ 406e StPO). Die Akteneinsicht durch Personen und Stellen, die am Strafverfahren nicht beteiligt sind, erfolgt deshalb zur Zeit, sowohl bei laufenden wie bei abgeschlossenen Strafverfahren, nur auf der Grundlage der Nrn. 183 bis 185 der RiStBV. Diese genügen aber als Verwaltungsvorschriften nicht den verfassungsrechtlichen Anforderungen an einen Eingriff in das Grundrecht. Selbst wenn man mit der Rechtsprechung des Bundesverfassungsgerichts von einem sogenannten „Übergangsbonus“ ausgehen wollte, hat sich der

Umfang der Gewährung von Akteneinsicht an nicht am Verfahren beteiligte Dritte, sowohl während als auch nach Abschluß des Strafverfahrens, in verfassungskonformer Auslegung auf das zu beschränken, was zum Schutze überragender Gemeinwohlinteressen **unerläßlich** ist. Dazu dürfte der beispielsweise bei der Überprüfung festgestellte, häufig von Krankenkassen und von Versicherungen verfolgte Zweck, aufgrund übergegangenen Rechts, das Bestehen zivilrechtlicher Ansprüche gegen den oder die Schädiger zu prüfen, nicht gehören. In jedem Falle ist das „Interesse“ der Krankenkassen an der Gewährung von Akteneinsicht auf ein **rechtliches** Interesse am konkreten Sachverhalt und die Umstände, die beispielsweise zur Schädigung des jeweils Versicherten geführt haben, beschränkt.
Von daher ist die festgestellte Praxis der vollständigen Aktenübersendung sowie der ungeprüften Einsichtsgewährung in **komplette** Aktenvorgänge, datenschutzrechtlich zu beanstanden.

Der Landesbeauftragte hat daher die Empfehlung ausgesprochen, die Akteneinsicht nicht umfassend für die gesamten Akten zu erteilen. Das kann im Einzelfall dazu führen, daß Akten zu trennen oder Auszüge zu erstellen sind. In Fällen, in denen dieses nicht möglich ist, sollte keine Akteneinsicht, sondern auf konkrete Darlegungen eines rechtlichen Interesses seitens der Anfragenden, lediglich eine Auskunft erteilt werden.

4. Daneben wurde bei der stichprobenweisen Überprüfung von Ermittlungsakten auch festgestellt, daß in den Taschen der Akten wiederholt Unterlagen aufbewahrt wurden, die zur Aufgabenerfüllung nicht mehr erforderlich waren. Dies gilt namentlich für aufgefundene handschriftliche Notizen des Gerichts, zusätzliche Ausfertigungen von Urteilen und Beschlüssen, Überstücke von Sachverständigen- und Behördengutachten sowie polizeiinterne Mitteilungen. Die Aufbewahrung dieser Unterlagen ist mit der Verpflichtung der speichernden Stelle aus § 16 DSG-LSA, nur richtige und zur Aufgabenerfüllung erforderliche Daten zu speichern und zu verarbeiten, nicht in Übereinstimmung zu bringen.

Zusätzlich wurden auch Verstöße gegen die Aktenordnung festgestellt, weil, entgegen einer ausdrücklichen Bestimmung, Auszüge des Bundeszentralregisters nicht in einem Sonderheft aufbewahrt wurden.

21.14 Datenschutz bei Notaren

Auch Notare nutzen inzwischen zur Unterstützung ihrer Arbeit in zunehmenden Maße die Vorteile und Möglichkeiten der automatisierten Datenverarbeitung. Dem steht gegenüber, daß in vielen Sachbereichen des Notariats die gesetzlichen Befugnisnormen für die Verarbeitung und Nutzung personenbezogener Daten fehlen. Zwar enthalten die Vorschriften der Bundesnotarordnung (BNotO) und des Beurkundungsgesetzes (BeurkG) sowie der in Sachsen-Anhalt aufgrund des Einigungsvertrages noch fortgeltenden Verordnung über die Tätigkeit von Notaren in eigener Praxis vom 20.06.1990 (NotVO) eine Reihe von datenschutzrelevanten Bestimmungen, aber diese Regelungen erfüllen nicht die vom Bundesverfassungsgericht an einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung gestellten Anforderungen. Sie vermögen auch nicht, wie ein Blick in die Bundesnotarordnung bzw. die Notarverordnung zeigt, das Spektrum der vielen Rechtsgebiete, in deren Bereich notarielle Handlungen vollzogen werden, abzudecken.

Neben den materiell-rechtlichen Defiziten bei Regelungen zur Datenspeicherung und Übermittlung fehlen auch Schutzvorschriften im technisch-organisatorischen Bereich der Datenverarbeitung. Zur Verdeutlichung des Regelungsbedarfes sei nur beispielhaft darauf verwiesen, daß Notare Urkunden mit Hilfe der automatisierten Datenverarbeitung erstellen, die dann auch mit den darin enthaltenen personenbezogenen Daten gespeichert werden. Bereits aus dieser Tatsache ist datenschutzrechtlich (§ 6 Abs. 2 Nr. 1 DSG-LSA) die Forderung nach einem Mindestmaß an Zugangssicherung gegenüber Unbefugten abzuleiten. Zu klären wäre auch, wie der Schutz gegen unbefugte Veränderung, Löschung oder Kenntnisnahme der Daten, z.B. durch Wartungs-, Service- und Dienstleistungsunternehmen, zu gewährleisten ist.

Auch die Frage der Erforderlichkeit einer Vielzahl von Einzelvorgängen bei der Datenverarbeitung durch die Notare bedarf, insbesondere im Hinblick auf die

vielfache Versendung von Abdrucken an öffentliche und nicht-öffentliche Stellen, der kritischen Überprüfung und ggf. auch der gesetzlichen Regelung.

Der Landesbeauftragte hat daher seit Juni 1995 in mehreren Stellungnahmen zu verschiedenen Gesetzentwürfen zur Änderung der BNotO auf den erforderlichen gesetzlichen Regelungsbedarf hingewiesen.

Das Ministerium der Justiz hat diese Auffassung nicht geteilt und es abgelehnt, sich für eine bereichsspezifische gesetzliche Regelung des Datenschutzes im notariellen Bereich (z.B. in der BNotO) einzusetzen. Auch die dem Landesbeauftragten bekannte Auffassung, daß die Bestimmungen der Landesdatenschutzgesetze einschlägig und ausreichend für den notariellen Bereich seien, übersieht, daß das Bundesverfassungsgericht in der bekannten Entscheidung zum Volkszählungsgesetz ausdrücklich **bereichsspezifische** Regelungen gefordert hat.
Die vom Ministerium angebotenen Regelungen in Verwaltungsvorschriften (z.B. der DONot) reichen nicht aus.

21.15 Schuldnerverzeichnis

Bereits in seinem II. Tätigkeitsbericht (S. 112 f) hatte der Landesbeauftragte darauf hingewiesen, daß der Bundesgesetzgeber zwischenzeitlich mit einer Änderung der Zivilprozeßordnung (ZPO) und der Einführung einer Schuldnerverzeichnisverordnung (SchuVVO) eine ausreichende Rechtsgrundlage für Führung, Eintragung, Löschung, Auskunftsersuchen und die Erteilung von Abdrucken und Listen aus dem Schuldnerverzeichnis geschaffen hat. Danach ist eine Auskunftserteilung im automatisierten Abrufverfahren jedoch nur durch Bezieher von Abdrucken aus dem Schuldnerverzeichnis möglich, nicht für Bezieher von Listen. Ihnen steht nach § 915 f ZPO nur eine Auskunftserteilung im nicht automatisierten Verfahren zu.

Das Bundesministerium der Justiz hat sich im Berichtszeitraum an die Landesjustizverwaltungen mit der Bitte um Stellungnahme gewandt, ob durch eine gesetzliche Änderung der Vorschriften der ZPO die Möglichkeit geschaffen werden

soll, daß in Zukunft auch die Listenbezieher, denen die Bewilligung zum Bezug von Abdrucken für wenigstens ein Schuldnerverzeichnis erteilt worden ist, Daten im automatisierten Abrufverfahren abrufen dürfen.
Der Landesbeauftragte hat dazu gegenüber dem Ministerium der Justiz keine grundsätzlichen Bedenken erhoben. Er hat jedoch darauf hingewiesen, daß es nicht ausreicht, eine zusätzliche Regelung in die ZPO aufzunehmen, die den automatisierten Abruf auch im Listenverfahren ermöglicht. Vielmehr ist auch zwingend eine Anpassung der SchuVVO erforderlich, da sich ansonsten die Datensicherheitsregelungen nur auf das automatisierte Verfahren beim Abruf aus Abdrucken und nicht auch auf das automatisierte Verfahren beim Abruf aus Listen beziehen würden.
Das Ministerium der Justiz hat die Anregung des Landesbeauftragten aufgegriffen und gegenüber dem Bundesministerium der Justiz ebenfalls aus datenschutzrechtlichen Gründen eine entsprechende Anpassung der SchuVVO gefordert.

21.16 Veröffentlichung personenbezogener Daten im Zwangsversteigerungsverfahren

Ein Amtsgericht hatte in einem Zwangsversteigerungsverfahren die personenbezogenen Daten der betroffenen Eigentümer (einschl. des Geburtsdatums) veröffentlicht. Das mißfiel einer Eigentümerin, die sich deshalb beim Landesbeauftragten beschwerte. Der konnte ihr nur in einem Punkt Recht geben.

Nach dem Gesetz über die Zwangsversteigerung und Zwangsverwaltung (ZVG) wird für jede Zwangsversteigerung ein Versteigerungstermin bestimmt, der öffentlich bekannt zu machen ist. Gem. § 38 Satz 1 ZVG **soll** in der Terminsbestimmung auch die Bezeichnung der z.Zt. der Eintragung des Versteigerungsvermerkes eingetragenen Eigentümer enthalten sein.

Der Landesbeauftragte kennt allerdings datenschutzfreundliche Gerichte, die auf die Bezeichnung der Eigentümer in der Veröffentlichung verzichten. Er hat beim Ministerium der Justiz des Landes Sachsen-Anhalt angeregt, in Sachsen-Anhalt einheitlich so zu verfahren.

Dies hat das Ministerium der Justiz unter Hinweis auf die gesetzlichen Vorschriften abgelehnt. Es hat aber bestätigt, daß jedenfalls die Veröffentlichung des Geburtsdatums nicht von den Vorschriften des Gesetzes über die Zwangsversteigerung und Zwangsverwaltung gedeckt war. Wie sich herausstellte, handelte es sich dabei um ein Versehen, das nicht wieder vorkommen soll.

21.17 Übersendung von Gerichtsakten, einschließlich Prozeßkostenhilfe-Unterlagen, an die Regierungsbezirkskassen

Aus einem anderen Bundesland ist der Landesbeauftragte auf ein Problem aufmerksam gemacht worden, wonach die dortige Landesbezirkskasse als Justizkasse zur Erfüllung ihrer Vollstreckungsaufgaben von einem Gericht die vollständigen Gerichtsakten nebst der dazugehörigen Prozeßkostenhilfe (PKH)-Unterlagen angefordert hat. Dies ist aus datenschutzrechtlicher Sicht nicht unproblematisch, da insbesondere die PKH-Unterlagen wegen ihres sensiblen Inhaltes über die persönlichen und wirtschaftlichen Verhältnisse des Betroffenen im Regelfall als Sonderakten zu den normalen Prozeßakten geführt werden. Zum anderen ist auch zu beachten, daß im Falle der Übersendung der gesamten Gerichtsakten an die Justizkasse diese Daten auch für einen anderen Zweck verarbeitet werden als für den sie einst erhoben worden sind. Eine Zweckänderung ist nach § 10 Abs. 2 Nr. 1 DSG-LSA ohne Einwilligung des Betroffenen u.a. nur zulässig, wenn eine Rechtsvorschrift diese vorsieht oder zwingend voraussetzt.

Der Landesbeauftragte hat sich wegen dieser Problematik an das Ministerium der Justiz mit der Bitte um eine Information über die Verfahrenspraxis in Sachsen-Anhalt und zum Verhältnis Gerichte und Regierungsbezirkskassen gewandt.
Das Ministerium der Justiz hat dem Landesbeauftragten mitgeteilt, daß bei der Tätigkeit der Regierungsbezirkskassen grundsätzlich wie folgt differenziert wird: Bei der Tätigkeit als Staatskasse hat sie nach § 127 ZPO ein Beschwerderecht. Dazu obliegt ihr die Prüfung, ob die bewilligte Prozeßkostenhilfe zutreffend ohne Raten angeordnet worden ist. Hierzu ist mindestens die Übersendung des die Prozeßkostenhilfe bewilligenden Beschlusses erforderlich; die Übersendung

des Prozeßkostenhilfeheftes hält das Ministerium deshalb **für diesen Zweck** vertretbar.
Soweit allerdings die Gerichtskasse gem. der Justizbeitreibungsordnung (JBeitrO) als Vollstreckungsbehörde tätig wird, hält das Ministerium die Übersendung von Unterlagen aus dem Prozeßkostenhilfeheft oder die Übersendung desselben mit dem Datenschutz für unvereinbar. Es hat daher den nachgeordneten Geschäftsbereich auf die Problemstellung aufmerksam gemacht und eine entsprechende Differenzierung angewiesen.

21.18 Ausbildungs- und Prüfungsordnung für Juristen in Sachsen-Anhalt

Bereits in seinem II. Tätigkeitsbericht (S. 130) hatte der Landesbeauftragte darauf hingewiesen, daß es bei der Durchführung von praktischen Studienzeiten nach der Ausbildungs- und Prüfungsordnung für Juristen (JAPrO) auch zu Übermittlungen oder nur zur Kenntnisnahme personenbezogener Daten an bzw. durch die Praktikanten kommen könnte. Zwar wäre es wünschenswert, die Jurastudenten während ihrer Praktikantenzeit nur mit den personenbezogenen Daten in Berührung zu bringen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen, jedoch wird sich dies nicht in jedem Fall einhalten lassen. Schließlich soll den Studenten im Praktikum eine anschauliche Vorstellung von dem breiten Spektrum juristischer Tätigkeit vermittelt werden.

Der Landesbeauftragte hat daher gegenüber dem Ministerium der Justiz vorgeschlagen, in § 11 der zur Novellierung anstehenden JAPrO einen Passus einzufügen, wonach die Studenten entweder durch das Landesjustizprüfungsamt oder die jeweilige Ausbildungsstelle zu Beginn des Praktikums nach dem Verpflichtungsgesetz förmlich zu belehren, zur Verschwiegenheit zu verpflichten und insbesondere auf die strafrechtlichen Folgen einer Pflichtverletzung hinzuweisen sind.

Das Ministerium der Justiz hat diesen Vorschlag aufgegriffen und dies in der neuen JAPrO vom 21.01.1997 ausdrücklich so geregelt.

21.19 Telefaxverkehr im Rahmen des Geldwäschegesetzes

Das Ministerium des Innern hat sich an den Landesbeauftragten mit der Frage gewandt, inwieweit Verdachtsanzeigen nach dem Geldwäschegesetz zwischen den beteiligten öffentlichen Stellen, namentlich den Staatsanwaltschaften und den Polizeibehörden, per Telefax versendet werden dürfen und inwieweit hierfür eine Verschlüsselung erforderlich sei.

Bei Verdachtsanzeigen nach dem Geldwäschegesetz handelt es sich um hochsensible personenbezogene Daten, die als solche prinzipiell nicht geeignet sind, auf dem unsicheren Übertragungsweg mittels Telefax versandt zu werden (vgl. Ziff. 13.4).

Im Rahmen seiner Beteiligung zur Erarbeitung der „Richtlinien für die Zusammenarbeit zwischen Staatsanwaltschaft und Polizei bei Ermittlungen im Rahmen des Geldwäschegesetzes“ wurde deshalb durch den Landesbeauftragten darauf hingewirkt, daß in diesem Bereich eine regelmäßige Übermittlung per Telefax nicht vorgesehen wird.

Gleichwohl verkennt der Landesbeauftragte nicht, daß aufgrund der kurzen Prüffristen des Geldwäschegesetzes in Eilfällen die Telefaxübermittlung zwischen den beteiligten Stellen erforderlich sein kann. In diesen Fällen ist aber ein hoher Sicherheitsstandard für die Datenübermittlung zu fordern. Dieser kann wirksam durch den Einsatz von Verschlüsselungssystemen gewährleistet werden, die einen entsprechenden Schutz vor unbefugter Kenntnisnahme, z.B. bei einer Fehlleitung der Telefaxnachricht, ermöglichen.

Der zunächst vom Ministerium des Innern dazu vertretenen Auffassung, der personelle und finanzielle Aufwand für eine Neuanschaffung oder Umrüstung aller Faxgeräte sei zu hoch, hat der Landesbeauftragte widersprochen.
Zum einen ist in Sachsen-Anhalt die Zuständigkeit für die Bearbeitung von Geldwäscheanzeigen auf zwei Schwerpunktstaatsanwaltschaften und das Landeskriminalamt beschränkt. Verschlüsselungstechnik, etwa z.B. durch Zusatzgeräte auf Chipkartenbasis, wäre daher im Geschäftsbereich des Ministeriums des

Innern nur für eine Behörde und im Geschäftsbereich des Ministeriums der Justiz nur für zwei Behörden zu vertretbaren Preisen zu beschaffen. Ein überbordender personeller und finanzieller Aufwand auf seiten der drei genannten Behörden, der es unverhältnismäßig erscheinen ließe, den Forderungen des Landesbeauftragten nachzukommen, ist daher nicht zu erkennen.

Ergänzend weist der Landesbeauftragte hierzu auf § 6 Abs. 1 Satz 3 DSG-LSA hin, wonach sich technisch-organisatorische Maßnahmen nach dem jeweiligen Stand der Technik zu richten haben. Verschlüsselungshard- und -software ist mittlerweile Stand der Technik.

Eine abschließende Stellungnahme des Ministeriums des Innern lag bei Redaktionsschluß noch nicht vor, eine prinzipielle Bereitschaft zum Einsatz solcher Technik wurde jedoch bereits signalisiert.

22. Öffentlich-rechtliche Rundfunkanstalten

22.1 Die Fahndung nach Schwarzhörern und -sehern

Zur Frage, ob die von den öffentlich-rechtlichen Rundfunkanstalten betriebene gemeinsame Gebühreneinzugszentrale (GEZ) in Köln regelmäßig Datenübermittlungen aus allen Einwohnermelderegistern des Landes erhalten soll, hat der Landesbeauftragte in seinem I. (S. 136 f) und II. Tätigkeitsbericht (S. 132 ff, S. 175) bereits Stellung genommen. Zwischenzeitlich hat dazu eine gemeinsame Besprechung zwischen der juristischen Direktion des MDR und den Landesbeauftragten für den Datenschutz der beteiligten Länder Sachsen, Thüringen und Sachsen-Anhalt stattgefunden. Der Landesbeauftragte hat dabei erneut herausgestellt, daß die derzeitige Rechtslage eine **regelmäßige** Datenübermittlung nicht zuläßt und die Erforderlichkeit und die Geeignetheit solcher Massendatenübermittlungen für die Gebührenerhebung im übrigen auch nicht ausreichend begründet worden ist.

Der für den demokratischen Rechtsstaat richtige Weg führt nur über den Landesgesetzgeber. Er muß nach Abwägung **aller** tatsächlichen Gesichtspunkte

und der Verfassungsrechtslage entweder den Rundfunkgebührenstaatsvertrag ändern oder eine Ergänzung des Landesmeldegesetzes vornehmen.

22.2 Befreiung von der Rundfunkgebührenpflicht aus sozialen Gründen

Auch ein weiterer Datenfluß zwischen den Bürgern und Bürgerinnen des Landes und dem MDR harrt noch einer endgültigen Entscheidung:
Es sind die Fälle, in denen Bedürftige die Befreiung von der Rundfunkgebührenpflicht aus sozialen Gründen beantragen. Der Sachstand ist - trotz Vorlage eines Formulierungsvorschlages zu einer novellierten Rundfunkbefreiungsverordnung durch die Landesbeauftragten für den Datenschutz Sachsens, Thüringens und Sachsen-Anhalts sowie einer gemeinsamen Besprechung mit dem MDR - unverändert. Es kann deshalb nahtlos an die Ausführungen im II. Tätigkeitsbericht (vgl. S. 134 f) angeknüpft werden.

Die Landesbeauftragten der beteiligten Länder vertreten im Ergebnis weiterhin die Auffassung, daß die ohnehin maßgeblich beteiligten Sozialämter auch abschließend über die Befreiungsanträge entscheiden sollten. Dadurch könnte vermieden werden, daß ein unnötiger Datenfluß zum MDR erfolgt und nebenbei könnten dessen (Überprüfungs-) Kosten vermindert werden.
Die Auffassung der Datenschutzbeauftragten stützt sich auf Aussagen des MDR, wonach dessen bisherige Aufhebungsquote lediglich zwischen zwei und drei Prozent liegt. Bei einer monatlichen Zahl von ca. 10 000 Befreiungsanträgen im Sendegebiet des MDR setzt der MDR derzeit dafür zehn Mitarbeiter ein. Gemessen an dem Verfahrensaufwand und der geringen „Erfolgsquote“ erscheint es unangemessen, die Vorlagepraxis an den MDR künftig beizubehalten.
Die Staatskanzlei unseres Landes hat sich dieser Auffassung jetzt angeschlossen.

23. Schulen

23.1 Durchführung „jugendärztlicher Reihenuntersuchungen an Schulen“ durch das Gesundheitsamt

Von Schülern wurde der Landesbeauftragte darüber informiert, daß in den 9. Klassen sogenannte „jugendärztliche Reihenuntersuchungen“ durchgeführt worden sind bzw. unmittelbar bevorstünden. Hierzu wurde den Schülerinnen und Schülern ein Fragebogen ausgehändigt, mit dem eine Fülle medizinischer Daten über sie selbst und ihre Eltern erhoben und anschließend gespeichert werden sollten.

Das war in dieser Form unzulässig. Die §§ 37 und 38 des Schulgesetzes regeln abschließend, was an amtsärztlicher Schulgesundheitspflege möglich ist. Diese spezielle Form der Reihenuntersuchung gehört nicht dazu.

Damit wäre für das Gesundheitsamt nur die Möglichkeit des freiwilligen Angebotes an die Schüler und deren Eltern geblieben (§ 84a Abs. 2 SchulG i.V. mit § 4 Abs. 2 DSG-LSA).
Der vom Gesundheitsamt übersandte Fragebogen erfüllte aber die Voraussetzungen des § 4 Abs. 2 DSG-LSA nicht.
Da die Befragung nicht den gesetzlichen Voraussetzungen entsprach, handelte es sich nicht nur um eine unzulässige Datenerhebung, sondern es lag bei den bereits ausgefüllt zurückgegebenen Fragebögen auch eine unzulässige Speicherung personenbezogener Daten vor. Nach § 16 Abs. 2 Nr. 1 DSG-LSA waren diese Bögen zu vernichten.

Das Ministerium für Arbeit, Gesundheit und Soziales wurde über den Sachverhalt informiert und gebeten, allen Gesundheitsämtern die datenschutzrechtliche Problematik bei der Durchführung von Reihenuntersuchungen an Schulen aufzuzeigen. Gleichzeitig wurde das Kultusministerium gebeten, die Schulleiterinnen und Schulleiter daran zu erinnern, daß sie für die Beachtung der Rechtsvorschriften an ihrer Schule verantwortlich sind.
Beide Ministerien haben inzwischen die erforderlichen Maßnahmen ergriffen.

23.2 Veröffentlichung personenbezogener Daten ehemaliger Schüler im Internet

Die Anfrage eines Petenten, ob personenbezogene Daten ehemaliger Schüler im Internet veröffentlicht werden dürfen, beantwortete der Landesbeauftragte wie folgt:

Gemäß Artikel 6 Abs. 1 der Verfassung des Landes Sachsen-Anhalt vom 16.07.1992 hat jeder das Recht auf Schutz seiner personenbezogenen Daten durch die öffentlichen Stellen des Landes. In dieses Recht darf nur durch oder aufgrund eines Gesetzes eingegriffen werden.
Dies gilt natürlich auch für die Verarbeitung (dazu zählt auch eine Übermittlung an Dritte) personenbezogener Daten ehemaliger Schüler. Da das Schulgesetz des Landes dafür keine Erlaubnisregelung enthält, wäre eine Datenübermittlung ins Internet nur mit Einwilligung des/der Betroffenen möglich. Form und Inhalt der Einwilligungserklärung sind in § 4 Abs. 2 DSG-LSA geregelt.

23.3 Wahlen zum Landeselternrat 1995

Im Schulverwaltungsblatt wurden gem. § 20 Abs. 5 ElternWO die Wahlen zum Landeselternrat durch das Kultusministerium bekanntgegeben. Hierbei wurden eine Vielzahl personenbezogener Daten (Name, Vorname, Anschrift, Schultyp) der Eltern veröffentlicht.

Dazu hat der Landesbeauftragte die Auffassung vertreten, daß die Privatanschrift mit der Ausübung der Elternvertretung in keinem Zusammenhang steht, zumal der Landeselternrat über eine eigene Geschäftsstelle verfügt (§ 75 Schulgesetz).
Der Landesbeauftragte hat daher empfohlen, für künftige Fälle die Veröffentlichungspraxis zu überprüfen.
Das Kultusministerium hat diese Rechtsauffassung bestätigt. Es ist vorgesehen, Einzelheiten über den Umfang bekanntzumachender Daten in die ElternWO aufzunehmen.

23.4 Anfertigen von Schülerfotos durch private Fotofirmen

Im II. Tätigkeitsbericht (S. 138) hatte der Landesbeauftragte von einer Empfehlung an das Kultusministerium und das zuständige Regierungspräsidium berichtet, alle Grundschulen darauf hinzuweisen, daß für die Anfertigung von Schülerfotos die Einwilligung der Erziehungsberechtigten erforderlich ist. Ergänzend bat der Landesbeauftragte darum, die dabei für weiterführende Schulen noch verbleibenden Probleme (z.B. Kauf solcher Bilder bei eingeschränkter Geschäftsfähigkeit der Schüler) nicht ungeregelt zu lassen.

Das Kultusministerium hat die Regierungspräsidien als obere Schulbehörden auf diese Sachverhalte hingewiesen. Unabhängig hiervon ist beabsichtigt, Einzelheiten für künftige Fälle im Erlaßverfahren zu regeln. Daran fehlt es aber bis jetzt.

23.5 Datenerhebung und -übermittlung im Rahmen polizeilicher Ermittlungen

Nach einem Verkehrsunfall, bei dem zwei Schüler einer Grundschule verletzt wurden, hat die Schulleitung die ihr zu einem anderen Zweck überlassene Telefonnummer des Arbeitgebers der nicht am Unfall beteiligten Ehefrau des Unfallverursachers auf Anforderung telefonisch der Polizei übermittelt. Darüber ging eine Beschwerde beim Landesbeauftragten ein.

Nach Artikel 6 Abs. 1 der Verfassung des Landes Sachsen-Anhalt hat jeder das Recht auf Schutz seiner personenbezogenen Daten. In dieses Recht darf nur durch oder aufgrund eines Gesetzes eingegriffen werden. Damit hätten die für einen anderen Zweck in der Schule gespeicherten personenbezogenen Daten der Ehefrau nur dann von der Schulleitung übermittelt werden dürfen, wenn eine gesetzliche Regelung die Übermittlung an die Polizei zuließ.
Die Verarbeitung (dazu gehört auch die Übermittlung) personenbezogener Daten durch Schulen ist in § 84a Abs. 2 und Abs. 3 des Schulgesetzes geregelt. Diese verweisen für den vorliegenden Fall auf die Bestimmungen des DSG-LSA. Nach § 11 Abs. 1 DSG-LSA i.V. mit § 10 Abs. 2 Nr. 7 DSG-LSA wäre die

Übermittlung der Daten an die Polizei zulässig gewesen, wenn sie zur Verfolgung einer Straftat oder Ordnungswidrigkeit erforderlich gewesen wäre. Rechtlich problematisch war hier, daß die Ehefrau weder Unfallverursacherin noch Zeugin war. Da der Polizei auch bereits Name, Anschrift und Telefonnummer des Unfallverursachers bekannt waren, bestand zwischen der Polizei und der Ehefrau keine rechtlich relevante Verbindung. Die in der Schule über die Ehefrau zu anderen Zwecken gespeicherten Daten hätten deshalb nicht an die Polizei übermittelt werden dürfen. Der Grundrechtsschutz der Ehefrau gewährleistete in diesem Fall, als Unbeteiligte nicht bei ihrem Arbeitgeber mit der Polizei in Verbindung gebracht zu werden.
Demgegenüber wäre es rechtlich unbedenklich und ausreichend gewesen, wenn die Schulleitung selbst die Ehefrau angerufen und gebeten hätte, sich ggf. mit der Polizei in Verbindung zu setzen.

24. Sozialwesen

24.1 Elternbeiträge zu Kindertagesstätten

Wesentliche Änderungen des Gesetzes zur Förderung von Kindern in Tageseinrichtungen (KiBeG) sind zum 01.01.1997 in Kraft getreten. Die neue Regelung sieht vor, daß der Träger der Einrichtung die Elternbeiträge sozialverträglich gestaltet und diese nach dem Elterneinkommen, dem Alter und der Zahl von Geschwistern staffeln kann. Die Beitragspflichtigen haben die Möglichkeit, beim Träger der öffentlichen Jugendhilfe eine Ermäßigung bzw. den Erlaß der Beiträge zu beantragen.

Durch die Eingaben mehrerer Petenten wurde der Landesbeauftragte darauf hingewiesen, daß einige Träger der öffentlichen Jugendhilfe bei der Umsetzung der neuen Regelungen weit über das nach dem Gesetz zugelassene Maß hinausgegangen sind. Die Eltern wurden zum Teil mit sechs- bis neunseitigen Antragsbögen voller überflüssiger und rechtlich nicht zulässiger Fragen traktiert.

Die datenschutzrechtliche Überprüfung der Antragsbögen ergab, daß die Ermäßigung des Elternbeitrages vielfach mit dem Antrag zur Erlangung von Sozialhilfe gleichgestellt wurde. Nicht erkannt wurde, daß mit § 18 KiBeG eine spezielle Grundlage für die Erhebung, Ermäßigung und den Erlaß der Elternbeiträge in Tageseinrichtungen vorliegt. Der Begriff „Eltern“ ist in § 90 Abs. 2 KJHG definiert. Lebt das Kind vor Entstehung der Beitragspflicht nur mit einem Elternteil zusammen, so tritt dieser an die Stelle der Eltern. Auch das Zusammenleben in einer eheähnlichen Gemeinschaft bleibt unberücksichtigt, wenn der Partner nicht Erziehungsberechtigter ist.

Ein weiterer kritischer Punkt in den Antragsbögen waren die Abfragen zu vorhandenem Vermögen. Nach § 18 Abs. 3 KiBeG i.V. mit § 93 KJHG gelten für die Anrechnung des Vermögens die Beschränkungen des § 88 BSHG und des § 93 Abs. 6 KJHG. Nur in diesem Rahmen sind Fragen zum Vermögen erforderlich und zulässig, soweit der damit verbundene Verwaltungsaufwand in einem angemessenen Verhältnis zum Kostenbeitrag steht.

Der Landesbeauftragte hat den Trägern der öffentlichen Jugendhilfe empfohlen, ihre Vordrucke den gesetzlichen Bestimmungen anzupassen und die Datenerhebung auf das Erforderliche zu beschränken.
Soweit bereits mehr Daten als erforderlich erhoben und gespeichert wurden, sind sie nach § 16 Abs. 2 DSG-LSA zu löschen. Zur Zeit findet die Überarbeitung der Erhebungsbögen bzw. deren Vernichtung oder die Rückgabe an die Antragsteller statt.

24.2 Besuch im Altenheim

Mehrere Senioren eines Altenheimes beschwerten sich darüber, daß ihre Besucher bei jedem Besuch ihren Namen, den Namen des/der Besuchten, die Zimmernummer und die Besuchszeit anzugeben hätten. Als Begründung gab die örtliche Heimleitung an, daß diese Daten bei Bombendrohungen, Havarien u.ä. benötigt würden.

Unabhängig von der anzuzweifelnden Erforderlichkeit solcher Datensammlung und einer fehlenden Rechtsgrundlage schreibt § 2 des Heimgesetzes ausdrücklich vor, daß die Selbständigkeit und Selbstverantwortung der Heimbewohner zu wahren sind.
Zumindest die Selbstverantwortung der Heimbewohner wurde in unzulässiger Art und Weise eingeschränkt, weil ihre Kontakte zu anderen Personen von der Altenheimleitung lückenlos registriert wurden. Aber auch die Verordnung über die Mitwirkung der Heimbewohner in Angelegenheiten des Heimbetriebes läßt eine derartige Einschränkung des Grundrechts auf informationelle Selbstbestimmung nicht zu.

Der Einrichtungsträger hatte nach einer durchgeführten Kontrolle des Landesbeauftragten umgehend dafür Sorge getragen, daß die unzulässige Gängelung der Bewohner und ihrer Besucher abgestellt wurde.

24.3 Die „tote“ Altenheimbewohnerin

Eine Bürgerin zog aus ihrer Wohnung in eine Altenpflegeeinrichtung, ohne ihren Betreuungsverein darüber zu informieren.
Dieser begann nach einer gewissen Zeit mit eigenen Nachforschungen über ihren Verbleib. Bei diesen Nachforschungen erfuhr der Verein von verschiedenen Personen, daß die Bürgerin wohl nach einem Umzug verstorben sei. Ohne den Wahrheitsgehalt dieser Aussagen zu überprüfen, teilte der Verein den Tod der betreuten Frau der zuständigen Versorgungsbehörde mit. Diese forderte - ebenfalls ohne nähere Prüfung - eine Sterbeurkunde beim zuständigen Standesamt an. Das Standesamt stellte - ebenfalls ohne genaue Prüfung der Personalien - eine Sterbeurkunde über eine bereits vor 2 Jahren Verstorbene mit gleichem Vor- und Familiennamen aus. Schließlich forderte die Versorgungsbehörde von dem Sohn die „zuviel gezahlte Rente“ zurück.
Erst die Reaktion des Sohnes, daß seine Mutter noch lebe, sich einer altersgerechten Gesundheit erfreue und sich aus diesen Gründen keine Rückforderung ergebe, führte zu einer internen Prüfung bei den beteiligten Behörden und zu einer Korrektur der Entscheidung.

Der Landesbeauftragte nahm den Fall zum Anlaß, auf die Pflicht jeder öffentlichen Stelle hinzuweisen, nur wahrheitsgemäße und geprüfte personenbezogene Daten zu verarbeiten, damit derartige Fälle von Amtsunsinn ausgeschlossen bleiben. Es bleibt zu hoffen, daß die von ihm angeregten und von den Behörden umgesetzten zusätzlichen Sicherungsmaßnahmen in Zukunft ähnliche unangenehme Vorfälle verhindern werden.

24.4 Verarbeitung von Sozialdaten durch private Prüfungseinrichtungen

Aus der lokalen Presse erfuhr der Landesbeauftragte, daß das Sozialministerium beabsichtigte, die vorgeschriebenen Geschäftsprüfungen der gesetzlichen Krankenkassen und Pflegekassen, der Kassenärztlichen und der Kassenzahnärztlichen Vereinigung, sowie des Medizinischen Dienstes der Krankenkassen nach §§ 274, 281 SGB V und § 46 SGB XI an **private** Anbieter zu übertragen. Dazu führte es eine Ausschreibung durch.

Diese Ausschreibung fiel auf und führte zu einer Anfrage im Deutschen Bundestag. Das Bundesministerium für Gesundheit wies in seiner Antwort darauf hin, daß die Absicht, die Prüfung auf eine private Prüfungseinrichtung zu übertragen, dem geltenden Recht widersprechen würde. Gleichwohl schloß das Sozialministerium des Landes mit einer privaten Prüfungsinstitution einen entsprechenden Vertrag.
In wiederholten Gesprächen mit dem Ministerium wies der Landesbeauftragte darauf hin, daß die Prüfung jedenfalls nur ohne Einblick in die Sozialdaten der Mitglieder erfolgen dürfe, weil für deren Übermittlung keine gesetzliche Grundlage vorhanden sei.
Die Überprüfung des ersten, dem Landesbeauftragten zugeleitete Prüfungsberichtes ergab, daß die Prüfung ohne Einbeziehung der Sozialdaten erfolgte.

24.5 Fehler bei der Übermittlung von Sozialdaten

- Ein Petent hatte mit seiner Lebenspartnerin einen Untermietvertrag abgeschlossen. Diesen Vertrag legte seine Partnerin dem Sozialamt als Nachweis zur Erlangung von Sozialhilfe vor. Der Sachbearbeiter des Sozialamtes setzte sich daraufhin unmittelbar mit der Wohnungsbaugesellschaft in Verbindung, ohne der Antragstellerin vorher Gelegenheit zur Beantwortung der offenen Fragen zu geben.
  Dadurch erfuhr die Wohnungsbaugesellschaft unzulässigerweise Sozialdaten der Lebenspartnerin und, daß der Petent ein nicht genehmigtes Untermietverhältnis abgeschlossen hatte; sie kündigte ihm fristlos.

  Erst der Hinweis auf die rechtsfehlerhafte Verhaltensweise führte zur Korrektur bei der Stadt. Deren schnelle Reaktion zur Schadensbegrenzung und die Rücknahme der Kündigung durch die Wohnungsgesellschaft bewahrten die Stadt vor einer Beanstandung durch den Landesbeauftragten und vor einer Schadenersatzforderung des Geschädigten.

- Ein Sozialversicherungsträger hatte in einem Regreßverfahren einem Schädiger zum Nachweis der Rechtmäßigkeit seiner Forderung eine Rechnung in Kopie zur Verfügung gestellt. Auf der Rechnung befanden sich aber auch die personenbezogenen Daten dritter, nicht am Verfahren beteiligter Personen. Auf diese Art und Weise wurden personenbezogene Daten Unbeteiligter unzulässig übermittelt.
  Der Sozialversicherungsträger hatte sich sofort nach Bekanntwerden bei den Betroffenen entschuldigt.

24.6 Vorlage von Kontoauszügen bei Sozialhilfeleistungen

Nach § 2 BSHG erhält nur derjenige Sozialhilfe, der sich nicht selbst helfen kann oder von anderen die erforderliche Hilfe nicht bekommt. Daher muß das Sozialamt in den Fällen, in denen bei ihm eine Leistung beantragt wird, die Einkommens- und Vermögensverhältnisse des Antragstellers überprüfen und ggf.

im Einzelfall Bankauskünfte einholen oder sich Kontoauszüge vorlegen lassen. Die Antragsteller haben dabei nach den §§ 60 ff SGB I eine Mitwirkungspflicht.

Ein Leistungsempfänger, der eine Erhöhung der Hilfe zur Pflege nach den Vorschriften des BSHG beantragte, wurde aufgefordert, **alle** Kontoauszüge der letzten 3 Monate vorzulegen.
Das hielt der Landesbeauftragte im konkreten Fall für überzogen, da aus der gesamten Leistungszeit keine konkreten Anhaltspunkte für einen Mißbrauch vorlagen. Er empfahl deshalb unter Hinweis auf die Rechtsprechung, sich in Stichproben auf die Vorlagen für jeweils einen Monat zu beschränken. So hat der Hessische Verwaltungsgerichtshof entschieden, daß das pauschale Verlangen nach **Bankauskünften** eine überflüssige Ermittlungstätigkeit darstellt, wenn nicht weitere Anhaltspunkte für die Erforderlichkeit dieser Forderung gegeben sind (vgl. RDV 95, S. 175).

Der Landkreis wurde auf die Rechtslage hingewiesen und hat sein pauschales Verfahren geändert.

24.7 Der „gläserne“ Patient

Ein Krankenhaus beabsichtigte, die übliche Dokumentation der Pflegedienstleistungen und die medikamentöse Therapie der Patienten deutlich sichtbar am jeweiligen Krankenbett auf dem Krankenblatt offen anzubringen.
Man wollte sich so ersparen, die jeweils kompletten Patientenakten, z.B. bei Visiten, mitzunehmen.

Der dazu vorsorglich befragte Landesbeauftragte riet im Hinblick auf die Rechtslage davon ab. Das Krankenhaus folgte dem Rat.

24.8 Werbemaßnahmen durch gesetzliche Krankenkassen

Einem Bürger wurde von einer gesetzlichen Krankenkasse unaufgefordert Informations- und Werbematerial übersandt, das auf die bevorstehende Gründung einer Betriebskrankenkasse in seiner Firma hinwies. Der Bürger, der nicht bei dieser gesetzlichen Krankenkasse versichert war, wandte sich an den Landesbeauftragten für den Datenschutz mit der Bitte um Auskunft über die Herkunft seiner Daten.
Durch eine Kontrolle des Landesbeauftragten konnte festgestellt werden, welchen Weg seine Daten genommen haben:
Außer den Aufgaben einer Krankenversicherung haben die gesetzlichen Krankenkassen nach § 28i SGB IV auch die Pflicht, die Beiträge für die übrigen Sozialversicherungsträger einzuziehen. Dabei wurden die vom Arbeitgeber zu entrichtenden Beiträge der übrigen Versicherungszweige (Renten- und Arbeitslosenversicherung) weitergeleitet. Die bei dieser Gelegenheit bekanntgewordenen Daten nutzte in diesem Fall die Krankenkasse für eigene Werbemaßnahmen.

Noch im Zuge der Kontrolle änderte die Krankenkasse ihre Dienstanweisung und stellte klar, daß auf Daten, die die Krankenkasse als Einzugsstelle für andere Zwecke erhält, nicht zugegriffen werden darf.

Darüber hinaus regte der Landesbeauftragte beim Bundesbeauftragten für den Datenschutz an, daß Zugriffsbeschränkungen in dem vom Bundesverband der Krankenkassen entwickelten EDV-Programm installiert werden, damit unberechtigte Zugriffe (und damit eine anderweitige Verwendung der Daten) auch von der technischen Seite her ausgeschlossen sind.

24.9 Auskunft von Unterhaltsverpflichteten

Ein Petent, der für ein Jugendamt einen Vordruck ausfüllen sollte, wandte sich an den Landesbeauftragten. In dem Formular sollten z.B. Fragen nach dem erlernten Beruf beantwortet werden, auch eine Befreiung vom Bankgeheimnis und pauschale Auskünfte über sein Vermögen wurden gefordert.

Der Landesbeauftragte wies darauf hin, daß seitens des Amtes der in § 1605 BGB dargelegte Erforderlichkeitsgrundsatz nicht berücksichtigt wurde.

Im Ergebnis verzichtete das Amt auf die Daten, und es wurde eine Überarbeitung der Vordrucke in die Wege geleitet.

25. Statistik

25.1 Landesstatistikgesetz

Der Landesbeauftragte hatte bereits in seinem II. Tätigkeitsbericht (S. 150) über seine Mitwirkung am Prozeß der Schaffung eines Landesstatistikgesetzes berichtet und an den Landtag appelliert, den damals bereits vorliegenden Gesetzentwurf im Hinblick auf die Erwartungen der Bürgerinnen und Bürger und der betroffenen öffentlichen Stellen zügig zu beraten, auch wegen der noch im Jahre 1995 beginnenden flächendeckenden Gebäude- und Wohnungszählung (GWZ).

In seiner Sitzung am 15.03.1995 beriet der Innenausschuß des Landtages über den Entwurf des Landesstatistikgesetzes. Dabei gelang es dem Landesbeauftragten noch, die Ausschußmitglieder für einige wichtige Änderungen am Gesetzestext zu gewinnen.
Im April 1995 wurde der Gesetzentwurf einstimmig beschlossen. Damit verfügt das Land Sachsen-Anhalt über ein auch datenschutzrechtlich gelungenes, modernes Gesetz für die Durchführung von Statistiken. Dadurch wurde u.a. § 30 DSG-LSA entbehrlich und deshalb aufgehoben.

25.2 Gebäude- und Wohnungszählung (GWZ)

Mit Stichtag 30.09.1995 war in den neuen Bundesländern nach dem WoStatG eine Gebäude- und Wohnungszählung als Totalerhebung durchzuführen. Dabei war der Landesbeauftragte bereits im Vorfeld durch das Statistische Landesamt (SLA) in vorbildlicher Weise beteiligt worden, um durch sachkundigen Rat bei

der Lösung der Aufgabe zu helfen. So war eine datenschutzgerechte Ausgestaltung eines der wichtigsten Arbeitsmittel in den Erhebungsstellen, der Erhebungsstellenanleitung, möglich.
Außerdem war der Landesbeauftragte an der Gestaltung eines Vertrages zwischen dem SLA und einer Druckerei beteiligt, die im Rahmen einer Auftragsdatenverarbeitung nach § 8 DSG-LSA für die Verteilung der Erhebungsbögen alle Adressen von Eigentümern bzw. Auskunftspflichtigen in Sachsen-Anhalt zu verarbeiten hatte.
Im Rahmen von Kontrollen und Beratungen im Vorfeld der GWZ war der Landesbeauftragte vielfach mit Problemen bei der Durchführung des § 8 WoStatG „Datenübermittlung an die Erhebungsstellen“ konfrontiert worden, vor allem, wenn in den Erhebungsstellen festgestellt werden mußte, daß die von den in § 8 WoStatG genannten Stellen gelieferten Eigentümeranschriften unvollständig oder falsch waren.
So mußte der Landesbeauftragte darauf aufmerksam machen, daß die Aufzählung der Stellen, die gem. § 8 WoStatG den Erhebungsstellen Daten zuzuarbeiten hatten, abschließend ist, und Daten anderer Stellen nur verwendet werden durften, wenn sich bei einem Gebäude in keiner anderen Weise der Eigentümer feststellen ließ. Dann hätten ausnahmsweise bei der Erhebung - natürlich anonym - ersatzweise auch die Hausbewohner oder Nachbarn befragt werden dürfen.

In diesem Zusammenhang ergab sich auch die Rechtsfrage, ob es auf dem umgekehrten Weg zulässig sei, z.B. dem Stadtsteueramt durch die Erhebungsstelle wenigstens mitzuteilen, welche der von dort genannten Eigentümeradressen falsch sind.
Im Hinblick auf das strikte Abschottungsgebot zwischen Statistik und Verwaltungsvollzug mußte der Landesbeauftragte mitteilen, daß eine derartige Datenweitergabe unzulässig wäre.

Bereits in seinem II. Tätigkeitsbericht (S. 150) hat der Landesbeauftragte zu Fragen der Zulässigkeit von sog. „Tabelleneinsen oder -zweien“ Stellung bezogen. Auch im Zusammenhang mit der GWZ gab es zu diesem Problem zwischen dem SLA und dem Landesbeauftragten Beratungen. Ergebnis der Gespräche war

wiederum, daß im **Einzelfall** zu entscheiden sei, ob dieser als solcher reanonymisierbar wird, oder ob eine Geheimhaltung im Sinne von § 16 Abs. 1 Ziffn. 3 und 4 BStatG unterbleiben kann, weil die Daten anonymisiert als statistische Ergebnisse vorliegen und dem Befragten oder Betroffenen nicht mehr zuzuordnen sind.

25.3 Mikrozensusgesetz 1996

Auch in den letzten zwei Jahren hatte der Landesbeauftragte wieder eine Vielzahl von telefonischen oder persönlich vorgetragenen Anfragen und Auskunftsersuchen besorgter Bürgerinnen und Bürger zum Mikrozensus zu beantworten. Besonders häufig wurde gefragt, ob die Erhebung überhaupt rechtsstaatlich sei, ob die personenbezogenen Daten für den Mikrozensus wirklich in solch umfassender Weise erhoben werden dürfen, wie ernst die Auskunftspflicht zu nehmen sei und vor allem, was mit den preisgegebenen Daten passieren würde.
Der Landesbeauftragte mußte im Zusammenhang mit diesen Auskünften in keinem Fall die Verfahrensweise des Statistischen Landesamtes im Umgang mit den ausgewählten Bürgern und deren Daten beanstanden.

In den Berichtszeitraum fiel auch die Diskussion um die Novellierung des jeweils nur für wenige Jahre geltenden Mikrozensusgesetzes, dessen Gültigkeit zuletzt bis 1995 befristet war. Vom (Bundes-)Gesetzgeber war in ersten Änderungsentwürfen noch eine erhebliche Ausweitung der Auskunftspflicht auf vorher freiwillig zu beantwortende Fragen beabsichtigt, andere umfangreiche Fragenkataloge sollten - zum großen Teil ebenfalls mit Auskunftspflicht - neu aufgenommen werden. Dank der gemeinsamen Bemühungen der Datenschutzbeauftragten des Bundes und der Länder konnte ein Ausufern des Fragekataloges verhindert werden, da eine eingehende, auch wissenschaftlich unterlegbare Begründung zur Erforderlichkeit der beabsichtigten Ausweitung der Fragen vom Gesetzgeber letztendlich nicht erbracht werden konnte.

In diesem Zusammenhang konnte auch für die Zukunft eine bessere Unterscheidung durch besondere Markierung und farbliche Hervorhebung der in den Erhebungsbögen gemischt vorhandenen freiwillig zu beantwortenden Fragen von den Pflichtangaben erreicht werden.

25.4 Bevölkerungsstatistik in der Kommune

Von einer Gemeinde wurde dem Landesbeauftragten der Entwurf einer Satzung über eine kommunale Bevölkerungsstatistik mit der Bitte um datenschutzrechtliche Prüfung vorgelegt. Anfragende Stelle war dabei nicht etwa das zuständige Amt für Statistik, sondern das zur Mitzeichnung des Satzungsentwurfes aufgeforderte Einwohnermeldeamt.

Tatsächlich mußte der Landesbeauftragte die dort vorhandenen Bedenken teilen. Zwar kann die Gemeinde Angelegenheiten des eigenen Wirkungskreises nach § 6 Abs. 1 GO LSA, wie z.B. Kommunalstatistiken gem. § 6 StatG-LSA, durch Satzung regeln, dabei sind ihr jedoch verfassungsrechtliche Grenzen gesetzt. So können - auch zu Zwecken der Statistik - unter bestimmten Voraussetzungen die in § 22 Abs. 1 MG LSA aufgeführten Daten aus dem Melderegister weitergegeben werden, „wenn dies zur Erfüllung der in der Zuständigkeit ... des Empfängers liegenden Aufgaben erforderlich ist“. Aber auch wenn das Gesetz grundsätzlich eine Empfängeraufgabe als hinreichende Legitimationsgrundlage anerkennt, bedeutet das nicht, daß als „Aufgabe“ jeder selbstgesetzte Handlungszweck zu verstehen ist.
Nach der Rechtsprechung des Bundesverfassungsgerichts darf der einzelne Bürger über die Fülle der Aufgaben nicht zum bloßen Informationsobjekt werden.
Den daraus resultierenden Anforderungen an den Schutz der Persönlichkeit bei der Datenverarbeitung für statistische Zwecke wurde der vorgelegte Satzungsentwurf nicht gerecht.
So wurden auf Intervention des Landesbeauftragten aus dem Katalog der Erhebungsmerkmale für alle beabsichtigten Statistiken die Daten „Tag der Geburt“ und „Religionszugehörigkeit“ gestrichen und für die Statistik der Eheschließun-

gen entfielen mehrere nicht relevante Erhebungsmerkmale. Die Namensstatistik, für die neben Vor- und Familiennamen die Erhebung der „Staatsangehörigkeit, Jahr und Ort der Geburt, Wohnungsstatus und der statistischen Gliederung der Wohnung“ beabsichtigt war, entfiel ganz.
In den überarbeiteten Satzungsentwurf wurden dann noch Begriffsbestimmungen und eine Vorschrift über die Geheimhaltung und den Veröffentlichungsmodus aufgenommen.

25.5 Kommunale Statistikstellen

Das StatG-LSA sieht in seinem § 7 vor, daß Kommunalstatistiken von kommunalen Statistikstellen durchzuführen sind. Diese Stellen sind, so das Gesetz weiter, räumlich und organisatorisch - und letztendlich natürlich auch personell - von den anderen Verwaltungsbereichen zu trennen (Abschottung). Dazu haben die Bürgermeister bzw. Landräte in einer Dienstanweisung die entsprechenden Regelungen zu erlassen. Sie haben dabei die Einrichtung einer kommunalen Statistikstelle ortsüblich bekanntzugeben und dem Statistischen Landesamt, der zuständigen Kommunalaufsichtsbehörde und dem Landesbeauftragten schriftlich anzuzeigen.

Mit Stand vom 01.01.1997 lagen dem Landesbeauftragten insgesamt sieben derartige Anzeigen vor. Es dürften noch deutlich mehr werden. Der Landesbeauftragte wird wegen der Fülle der in kommunalen Statistikstellen verarbeiteten personenbezogenen Daten und der damit einhergehenden Gefahren für die Rechte der betroffenen Bürgerinnen und Bürger in nächster Zeit Beratungen und Kontrollen durchführen.

Werden in Statistikstellen statistische Einzelangaben in EDV-Anlagen verarbeitet, sind nach dem StatG-LSA zusätzliche Maßnahmen zur Gewähr der Abschottung und der Sicherung ihrer Zweckbestimmung zu treffen.
Das Ministerium des Innern hat in diesem Zusammenhang von seiner Ermächtigung aus § 7 Abs. 2 StatG-LSA bereits Gebrauch gemacht und dem Landesbeauftragten den Entwurf einer Verordnung über die Abschottung der DV-Anlagen

in kommunalen Statistikstellen zugeleitet. Nach kontroverser Diskussion gab es ein einvernehmliches Ergebnis.

25.6 Bundesstatistik über Schwangerschaftsabbrüche

Nach den §§ 15 ff, hier insbesondere § 18 Abs. 3 Schwangerschaftskonfliktgesetz, führt das Statistische Bundesamt eine Statistik über die unter den Voraussetzungen des § 218a Abs. 1 bis 3 StGB vorgenommenen Schwangerschaftsabbrüche. Dabei werden allerdings nur anonymisierte Angaben der Schwangeren verwendet.
Auskunftspflichtig sind die Inhaber der Arztpraxen und die Leiter der Krankenhäuser, in denen Schwangerschaftsabbrüche durchgeführt wurden. Um die Erhebung möglichst vollständig durchführen zu können, ist das Statistische Bundesamt gesetzlich berechtigt, von den Landesärztekammern die Anschriften der Ärzte anzufordern, in deren Einrichtungen Schwangerschaftsabbrüche vorgenommen worden sind oder vorgenommen werden sollen.

Anders als in anderen Bundesländern liegt in Sachsen-Anhalt diese Information bei der Landesärztekammer dadurch vor, daß die interessierten Ärzte entsprechend der vom Ministerium für Arbeit, Soziales und Gesundheit erlassenen „Richtlinie für die Anerkennung von Einrichtungen zur Durchführung eines Schwangerschaftsabbruches“ ihre Zulassung beim Landesamt für Versorgung und Soziales zu beantragen haben. Das Landesamt hat von seiner (positiven) Entscheidung die Landesärztekammer zu unterrichten.
Damit ist in Sachsen-Anhalt eine Möglichkeit geschaffen, die es dem Statistischen Bundesamt erlaubt, gezielt von seinem gesetzlichen Auftrag Gebrauch zu machen, ohne übermäßig Daten unbeteiligter Ärzte erheben zu müssen.
Das Verfahren ist datenschutzrechtlich nicht zu beanstanden.

26. Strafvollzug

26.1 Entwurf eines Gesetzes zur Änderung des Strafvollzugsgesetzes

Den jahrelangen Forderungen der Datenschutzbeauftragten des Bundes und der Länder, auch im Bereich des Strafvollzuges durch eine Änderung des Strafvollzugsgesetzes (StVollzG) bereichsspezifische Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu schaffen, hat das Bundesministerium der Justiz nunmehr in einem zweiten Anlauf nach 1991 durch einen vorläufigen Referentenentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes zu entsprechen versucht.
Leider ist auch dieser Entwurf aus datenschutzrechtlicher Sicht nicht frei von Bedenken. Zwar ist als deutliche datenschutzrechtliche Verbesserung vorgesehen, die Gefangenen über ihr Recht aufzuklären, die Vernichtung der angefertigten erkennungsdienstlichen Unterlagen z.B. bei der Entlassungsverhandlung verlangen zu können. Vorzuziehen wäre jedoch eine Lösung, wonach die erkennungsdienstlichen Unterlagen unaufgefordert nach Entlassung des Gefangenen aufgrund einer festen gesetzlichen Regelung zu vernichten sind.

Darüber hinaus hat der Landesbeauftragte empfohlen, eine klare Regelung der Fälle vorzunehmen, in denen eine erkennungsdienstliche Behandlung im Strafvollzug nicht stattfinden darf. So sollte aus Gründen der Verhältnismäßigkeit von einer generellen erkennungsdienstlichen Behandlung zumindest bei kurzen Freiheitsstrafen sowie bei Ersatzfreiheitsstrafen abgesehen werden.
Des weiteren hat der Landesbeauftragte angeregt, daß, neben den allgemeinen Regelungen zur Verarbeitung und Nutzung der personenbezogenen Daten der Gefangenen, in § 180 des Gesetzentwurfs eine spezielle Regelung über die Führung der Gefangenenpersonalakten getroffen werden sollte, da diese die wichtigsten und umfangreichsten Datensammlungen in den Justizvollzugsanstalten enthalten. Im Gesetz selbst oder einer Rechtsverordnung sollte festgelegt werden, welchen Inhalt die Gefangenenpersonalakte hat und wie sie geführt werden soll. Außerdem sollte eine weitere Unterteilung der Gefangenenpersonalakte vorgesehen werden, um zu verhindern, daß für jede Form der Verarbeitung und Nutzung die gesamte Gefangenenpersonalakte herangezogen werden muß. Denkbar wären z.B. Sonderhefte für Erkenntnisse aus der Überwachung

des Besuchs- und Schriftverkehrs, für die Unterlagen über Bezugspersonen, für die Unterlagen über die erkennungsdienstliche Behandlung und für die Vorgänge bezüglich der Gefangenenarbeit. Auch bei der Auskunftserteilung ließen sich mit Teilakten Eingriffe in das Grundrecht auf informationelle Selbstbestimmung der Gefangenen einschränken.
Die vorgesehenen Aufbewahrungsfristen für Altakten von 30 Jahren sind nach Ansicht des Landesbeauftragten in vielen Fällen deutlich zu lang bemessen. Statt dessen hält der Landesbeauftragte eine zehnjährige Aufbewahrungsfrist nach der Entlassung, zumindest für die Gefangenenpersonalakten, die Gesundheitsakten und die Krankenblätter für ausreichend.
Zur fraglichen Übermittlung von Gefangenendaten für Forschungszwecke hat sich der Landesbeauftragte dafür ausgesprochen, daß diese angesichts der Sensibilität der Daten im Grundsatz nur mit Einwilligung der Gefangenen erlaubt sein soll. Für Ausnahmefälle wäre eine Erlaubnis durch die Oberste Landesbehörde vorzusehen. Die in § 186 des Gesetzentwurfs vorgesehene Übersendung von Akten erhöht unnötig das Risiko einer zweckfremden Verwendung. Insbesondere die besonders sensible Daten enthaltenden Gefangenenpersonalakten sollten zur Akteneinsicht nur ausnahmsweise an Forschungseinrichtungen versandt werden, wenn der Forschungszweck anderweitig nicht erfüllt würde. Im übrigen würde eine Aktenversendung vielfach die Anfertigung von Aktendoppeln oder Retenten bedingen, um einen geordneten Anstaltsbetrieb ununterbrochen zu gewährleisten. Damit würde auch das generelle Verbot der Doppeldatenerhebung berührt.
Erhebliche Bedenken erhob der Landesbeauftragte gegenüber einer im Gesetzentwurf vorgesehenen Bestimmung, eine beabsichtigte Veröffentlichung von Gefangenendaten anläßlich einer Forschungsarbeit allein davon abhängig zu machen, daß die Darstellung von Forschungsergebnissen über die Ereignisse der Zeitgeschichte unerläßlich ist. Zumindest muß angesichts des erheblichen Eingriffs in das Grundrecht des Gefangenen eine Abwägung mit eventuell überwiegenden schutzwürdigen Interessen des Betroffenen stattfinden.

Das Ministerium der Justiz unterstützt die Empfehlungen des Landesbeauftragten gegenüber dem Bundesministerium der Justiz nur teilweise, so bezüglich einer gesetzlichen Bestimmung zur Vernichtung der Ed-Unterlagen des Gefangenen bei seiner Entlassung und des Absehens von der Aktenversendung zu

Forschungszwecken.
Die weitere Entwicklung des Gesetzesvorhabens wird zunächst von den Beratungen zwischen den Landesjustizverwaltungen im Bundesministerium der Justiz abhängen und kritisch zu beobachten sein.

26.2 Entwurf eines Untersuchungshaftvollzugsgesetzes

Das Bundesministerium der Justiz hat einen vorläufigen Referentenentwurf eines Gesetzes über den Vollzug der Untersuchungshaft (UVollzG) vorgelegt und den Landesjustizverwaltungen zur Stellungnahme übersandt. Dieses Gesetz soll nicht nur die bisher lediglich in einer bundeseinheitlichen Verwaltungsvorschrift geregelte Untersuchungshaftvollzugsordnung ablösen, sondern auch bereichsspezifische Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Gefangenen im Untersuchungshaftvollzug schaffen. Da dieser Entwurf bezüglich seiner Regelungen zum Datenschutz im wesentlichen auf die Regelungen im StVollzG verweist, sind auch hierzu seitens des Landesbeauftragten im wesentlichen identische Kritikpunkte (vgl. Ziff. 26.1) erhoben worden.
Darüber hinaus hat der Landesbeauftragte in seiner Stellungnahme zum Gesetzentwurf empfohlen, die Versagung von Besuchserlaubnissen und die Überwachung eines Besuches, von den Fällen einer Verdunklungsgefahr abgesehen, an das Vorliegen von konkreten Anhaltspunkten für eine Gefährdung des Haftzweckes oder der Anstaltsordnung und -sicherheit anzuknüpfen. Dies würde nicht nur dem angesichts der Unschuldsvermutung besonders zu beachtenden Verhältnismäßigkeitsgrundsatz genügen, sondern auch den vom Bundesverfassungsgericht daraus entwickelten Kriterien für zulässige Beschränkungsmaßnahmen während der Untersuchungshaft.
Für die Überwachung des Schriftverkehrs des Untersuchungsgefangenen und seiner Telefongespräche hat der Landesbeauftragte eine Vorabinformation des Gefangenen empfohlen, damit dieser selbst entscheiden kann, ob er den Schriftverkehr aufnehmen bzw. ein Telefongespräch führen möchte und, da auch Grundrechte des Gesprächspartners betroffen sind, entscheiden kann, ob

er diesen über die Überwachung und damit über die Tatsache seiner Inhaftierung unterrichten möchte. Daneben sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach in den Fällen, in denen der Untersuchungsgefangene rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren gegen ihn nicht nur vorläufig eingestellt wird, die öffentlichen Stellen, die von seiner Inhaftierung informiert worden sind, über den Ausgang des Verfahrens in Kenntnis gesetzt werden. Zumindest sollte dem Betroffenen in diesen Fällen ein Recht zu einer solchen Nachberichtigung eingeräumt und eine Pflicht zu seiner Belehrung über dieses Recht in den Gesetzentwurf aufgenommen werden.

Der Landesbeauftragte hat diese Empfehlungen gegenüber dem Ministerium der Justiz mit der Bitte um Unterstützung bei den anstehenden Beratungen auf Bund-/Länderebene unterbreitet. Eine Antwort aus dem Ministerium lag bei Redaktionsschluß noch nicht vor.

27. Umwelt und Natur

Umweltinformationsgesetz

In seinem II. Tätigkeitsbericht (S. 157 f) hatte der Landesbeauftragte von der Verabschiedung des Umweltinformationsgesetzes (UIG) berichtet und gemutmaßt, daß es zu Anwendungsschwierigkeiten in der Praxis führen und Anlaß zu Rechtsstreitigkeiten geben werde.

Aus einem anderen Bundesland wurde nun der Fall eines Rechtsanwaltes bekannt, der unter Berufung auf das UIG von der zuständigen Behörde die Vorlage eines Verzeichnisses aller Unternehmen verlangte, die ökologischen Landbau betreiben.
Der Landesbeauftragte, nach seiner Meinung gefragt, konnte dem betreffenden Kollegen deutlich machen, daß es sich bei dem geforderten Unternehmensverzeichnis weder um Daten über den **Zustand** der Gewässer, der Luft, des Bodens, der Tier- und Pflanzenwelt und der natürlichen Lebensräume (§ 3 Abs. 2

Nr. 1 UIG) noch um Daten über **Tätigkeiten oder Maßnahmen**, die diesen Zustand beeinträchtigen oder beeinträchtigen können (§ 3 Abs. 2 Nr. 2 UIG), handelt. Genauso wenig handelt es sich um Daten über **Tätigkeiten oder Maßnahmen** zum Schutz dieser Umweltbereiche (§ 3 Abs. 2 Nr. 3 UIG).
Eine Übermittlung dieser personenbezogenen Daten kam auf der Grundlage des UIG also nicht in Frage.

28. Verfassungsschutz

Auch in diesem Berichtszeitraum hat der Landesbeauftragte das Landesamt für Verfassungsschutz wiederholt bei der Umstellung von Karteikartensystemen auf die automatisierte Datenverarbeitung, insbesondere bei der Einrichtung von Dateien sowie beim Erlaß von Dienstanweisungen zur Anwendung des Nachrichtendienstlichen Informationssystems (NADIS) (vgl. II. Tätigkeitsbericht, S. 159) beraten.
Einzelheiten können hierzu, wegen der Einstufung der Vorgänge nach der Verschlußsachenanweisung des Landes Sachsen-Anhalt, nicht dargestellt werden.

29. Verkehr

29.1 Automatische Gebührenerhebung (AGE) auf Autobahnen

Zu den sich daraus ergebenden datenschutzrechtlichen Fragestellungen und Anforderungen berichtete der Landesbeauftragte bereits in seinem II. Tätigkeitsbericht (S. 162 f und Anlage 17).
Im November 1995 veröffentlichte der TÜV Rheinland in einem Abschlußbericht die Ergebnisse seines im Auftrag des Bundesministeriums für Verkehr durchgeführten mehrjährigen Feldversuches „Autobahntechnologien A 555“.
In seinem Abschlußbericht stellte er fest, daß die Anforderungen des Datenschutzes erfüllt werden können. Voraussetzungen hierfür seien ein anonymes Erhebungsverfahren für diese Autobahnmaut in Verbindung mit einem Kontrollsystem, das davon befreite sowie ordnungsgemäß zahlende Verkehrsteilnehmer

nicht erfaßt (Grundsatz der „datenfreien Fahrt“) und eine transparente, d.h. für jeden Verkehrsteilnehmer erkennbare und nachprüfbare Gestaltung des gesamten Verfahrens bis hin zur Gebührenabrechnung beinhaltet.
Letztendlich wurden aber die Pläne für eine automatische Gebührenerhebung durch das Bundesministerium für Verkehr aufgegeben.
Als ein positives Fazit wertet der Landesbeauftragte die Tatsache, daß **vor** der Entscheidung über die Einführung eines so umfangreichen automatisierten Verfahrens eine rechtzeitige Beteiligung der Datenschutzbeauftragten möglich war. Deutlich wurde auch, daß Datenschutzanforderungen durch eine entsprechende Technikgestaltung erfüllbar sind und nicht zum „K.o.-Kriterium“ für ein solches Vorhaben werden müssen.

29.2 Schutz und Gefahren in neuen Vorschriften

Über die hierzu bestehenden datenschutzrechtlichen Defizite hat der Landesbeauftragte u.a. bereits in seinem II. Tätigkeitsbericht (S. 165) berichtet.
Mit dem durch die Bundesregierung verabschiedeten Gesetzentwurf für ein „Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze“ (BR-Drucksache 821/96 vom 08.11.1996) haben die seit 1993 andauernden Novellierungsbestrebungen zu verkehrsrechtlichen Vorschriften, insbesondere des Straßenverkehrsgesetzes, des Fahrlehrergesetzes und des Kraftfahrsachverständigengesetzes einen vorläufigen Abschluß gefunden. Diese umfangreichen Änderungen verkehrsrechtlicher Vorschriften dienen der Umsetzung der Zweiten EU-Führerscheinrichtlinie vom 29.07.1991 (91/439/EWG) in nationales Recht, nicht zuletzt aber auch der Anpassung und Einfügung datenschutzrechtlicher Regelungen entsprechend den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts. So fehlt seit langem eine Rechtsgrundlage für die bestehenden örtlichen Fahrerlaubnisregister.
Weiterhin beinhaltet der Gesetzentwurf die datenschutzrechtliche Überarbeitung der Vorschriften über das Verkehrszentralregisters (VZR) beim Kraftfahrt-Bundesamt (KBA) und die der Fahrzeugregister beim KBA (ZFR) und die örtlichen Zulassungsbehörden.

Der Gesetzentwurf beinhaltet auch eine ganze Reihe datenschutzrechtlicher Verbesserungen.
Hierzu gehören u.a. die unentgeltliche Selbstauskunft für Betroffene, die Zweckbindung von Abrufprotokolldaten aus den VZR und dem ZFR mit der Einschränkung der Nutzung durch die Strafverfolgungsbehörden auf den Einzelfall zur Verhinderung oder Verfolgung schwerwiegender Straftaten gegen Leib, Leben und Freiheit einer Person, die Aufgabe der Pläne zur Einrichtung **zentraler** Register für Fahrlehrer und Kraftfahrsachverständige und die Harmonisierung der Verwertungsregel des Bundeszentralregisters (§ 52 Abs. 2 BZRG) mit denen über das Verkehrszentralregister (VZR) bei Verfahren zur Erteilung oder Entziehung einer Fahrerlaubnis. Damit würde auch der Forderung des Landesbeauftragten (II. Tätigkeitsbericht, S. 164) nach einer zeitlich begrenzten Verwertungsfrist im BZR, die sich an der des VZR orientiert, entsprochen.

Problematisch aus verfassungsrechtlicher Sicht ist die vorgesehene Einführung eines Zentralen Fahrerlaubnisregisters (ZFER) beim KBA.
Mit dieser Vorschrift würde eines der umfangreichsten personenbezogenen Register in Deutschland mit ca. 50 Millionen erfaßten Bürgerinnen und Bürgern geschaffen werden. Dafür gibt es bis heute keine hinreichende Begründung für ein **überwiegendes** Allgemeininteresse. Der Verweis auf die Notwendigkeit eines solchen zentralen Registers beim KBA infolge der Umsetzung der Zweiten EU-Führerscheinrichtlinie und den angeblich nur so zu erreichenden schnellen Informationsaustausch zwischen den EU-Mitgliedsstaaten überzeugt nicht.
Eine weitere Möglichkeit der Gefährdung des Grundrechts auf informationelle Selbstbestimmung enthalten die Regelungen des Gesetzentwurfs zur Schaffung automatisierter Anfrage- und Auskunftsverfahren aus den zentralen Registern für öffentliche Stellen im Inland, für die EU-Mitgliedsstaaten und darüber hinaus für dritte Staaten.
Besonders gefährlich für die Grundrechte aller Bürgerinnen und Bürger sind die vorgesehenen Datenabgleichsregelungen zwischen den dann vorhandenen drei zentralen Registern, ohne daß es auf die Erforderlichkeit im Einzelfall ankommt. Es klingt in der Begründung gut, wenn damit nur eine regelmäßige Nutzung der Personendaten zwischen dem VZR, dem FZR und dem ZFER zur Feststellung und Beseitigung von Abweichungen und Fehlern ermöglicht werden soll. Diese

ist aber schon praktisch mit einem erheblichen Arbeitsaufwand verbunden und begründet neue Forderungen nach einer aufgeblähten Bürokratie. Denn wer soll feststellen, welche der bemerkten Abweichungen richtig und welche falsch sind? Im übrigen lassen der so geschaffene gesetzliche Rahmen und die damit verbundenen technischen Möglichkeiten weitere „Begehrlichkeiten“ für eine Erweiterung der Übermittlungs- und Nutzungsmöglichkeiten als sehr wahrscheinlich erscheinen.
Im Ergebnis wird damit für Millionen Menschen eine neue automatisierte Überwachungsmöglichkeit geschaffen, die dem bis heute abgelehnten Zentralen Einwohnermelderegister hinsichtlich der Gefahren für das Grundrecht der Betroffenen in keiner Weise nachsteht.

29.3 Datenschutz bei Verkehrsordnungswidrigkeitenverfahren - Radarfotos -

Bereits in seinem II. Tätigkeitsbericht (S. 168) hat der Landesbeauftragte Kritik an der Versendungspraxis von Frontfotos mit unbeteiligten Mit- bzw. Beifahrern geübt.
Der mangels spezialgesetzlicher Regelung anzuwendende § 12 Abs. 1 DSG-LSA läßt diese Datenübermittlung in den privaten Bereich in den meisten Fällen nicht zu.

Nach eingehender Diskussion mit dem Ministerium des Innern und einer begleitenden Diskussion in der Presse wurde im Juli 1995 eine befriedigende Lösung gefunden. Unter der Überschrift „Auf Fahrer-Fotos sind Beifahrer künftig nicht zu sehen“ erfolgte durch das Ministerium des Innern im August 1995 eine Pressemitteilung über den gefundenen Konsens mit dem Landesbeauftragten. Zum Hintergrund dieser Verständigung gehörte die geplante Einführung einer neuen Auswertungstechnik, die es ermöglicht, durch die Digitalisierung der Foto-Negative und deren Weiterverarbeitung mittels Software-Programm eine entsprechende Bildausschnittwahl zu treffen.

Das neue technische Verfahren ließ aber auf sich warten. Im Herbst 1995 drängte der Landesbeauftragte deshalb im Hinblick auf die nach wie vor zahl-

reichen berechtigten Anrufe und Beschwerden erneut darauf, eine bürgerfreundlichere Zwischenlösung einzuführen.
Allerdings benötigte das Ministerium des Innern noch fast ein halbes Jahr, bis es dann im Mai 1996 Regeln zur sog. „Fahrerkennung“ festlegte.

Erst mit der Einrichtung einer zentralen Auswerte- und Filmentwicklungsstelle des Landes zu Beginn des Jahres 1997 wurden die erwarteten technischen Voraussetzungen geschaffen. Der Landesbeauftragte wird sich demnächst vor Ort darüber informieren.

29.4 Speicherung von Wiederholungsfällen bei Verstößen im ruhenden Verkehr

Mit einem Erlaß vom 05.01.1996 zum o.g. Sachverhalt hat das Ministerium des Innern die Führung manueller Karteien wie auch automatisierter Dateien durch Kommunen zu diesem Zweck für **unzulässig** erklärt. Ebenso unzulässig ist nach diesem Erlaß auch die diesbezügliche systematische Auswertung der aus kassentechnischen Gründen zu Verwarngeldverfahren geführten örtlichen Dateien.
Die Unzulässigkeit ergibt sich aus den bestehenden Regelungen des StVG, die in den §§ 28 bis 30a StVG insoweit abschließende Bestimmungen enthalten.

Im August 1996 setzte das Ministerium des Innern den Landesbeauftragten über eine Vollzugsmeldung der zuständigen Regierungspräsidien von der Umsetzung des o.g. Erlasses in Kenntnis.
Der Landesbeauftragte begrüßt diese datenschutzgerechte Klarstellung.

Wiederholte Anfragen von Ordnungsämtern in der Folgezeit sowie eingegangene Meldungen zum Dateienregister von sog. „OWi-Dateien“ lassen aber beim Landesbeauftragten Zweifel an der wirksamen Umsetzung dieses Erlasses und dessen Kenntnis in der Verwaltungspraxis aufkommen.
Der Landesbeauftragte weist deshalb die Straßenverkehrsbehörden nochmals auf folgende Grundsätze hin:

1. Auch eine automatisiert vorgehaltene „OWi-Datei“ unterliegt dem Zweckbindungsgrundsatz, wie ihn das Bundesverfassungsgericht in seiner Recht-

sprechung zum Volkszählungsurteil entwickelt hat. Das bedeutet, daß eine Speicherung und Auswertung von abgeschlossenen Verwarngeldverfahren bei Verkehrsordnungswidrigkeiten zur Erkennung von sog. „Mehrfachtätern“ unzulässig ist. Eine solche automatisierte „OWi-Datei“ soll lediglich dem Zweck dienen, mittels moderner EDV die einzelnen Verfahren schneller und leichter abzuwickeln.

2. Auch der § 17 Abs. 3 OWiG bildet **keine** Rechtsgrundlage zur Speicherung und Auswertung von Halt- oder Parkverstößen, die als Verwarnung erledigt wurden. Mit der rechtzeitigen Zahlung des Verwarnungsgeldes durch den Betroffenen ist die Sache erledigt und „aus der Welt“.
   Eine Erhöhung bei der Bemessung des Verwarnungsgeldes durch die zuständige Verwaltungsbehörde der Gefahrenabwehr kann daher nur im Einzelfall in Betracht kommen, wenn der Behörde zeitnahe weitere Verstöße vorliegen, die ohne besondere Nachforschung bekannt sind oder sich von selbst im Verfahren ergeben (Göhler, OWiG, 11. Aufl. § 17 Rdnr. 20c).
3. Der § 25a Abs. 1 StVG sieht für die Halt- oder Parkverstöße im ruhenden Verkehr die Halterhaftung vor. Wesentlich dafür war die Tatsache, daß in der Praxis den Verwaltungsbehörden in den allerwenigsten Fällen der Nachweis gelingt, daß der Betroffene (hier der Kfz-Halter) den oder die mehrfachen Verstöße auch tatsächlich selbst begangen hat. Die Bezahlung eines Verwarnungsgeldes ist kein Schuldeingeständnis des Betroffenen, sondern Teil eines mitwirkungspflichtigen Verwaltungsaktes aus Anlaß einer Ordnungswidrigkeit (Göhler, OWiG, 11. Aufl., vor § 56 Rdnr. 4 - 6).

Der Landesbeauftragte wird deshalb im Rahmen seines Kontrollauftrages die datenschutzgerechte Umsetzung dieses Erlasses bei den Behörden überprüfen.

30. Vermögensgesetz

Auskunft an Entwicklungsträger im Städtebau

Eine Stadt wollte vom Landesbeauftragten wissen, ob an den Entwicklungsträger einer städtebaulichen Entwicklungsmaßnahme personenbezogene Daten

von Antragstellern nach dem Vermögensgesetz im Bereich des Entwicklungsgebietes übermittelt werden dürfen.

Nach § 32 Abs. 5 VermG können **jedem** (also jeder natürlichen oder juristischen Person), der ein berechtigtes Interesse glaubhaft darlegt, Name und Anschrift der Antragsteller sowie der Vermögenswert mitgeteilt werden, auf den sich die Anmeldung eines Vermögensanspruches bezieht. Adressaten dieser Vorschrift sind zwar vorrangig private Dritte, jedoch schließt sie das berechtigte Interesse öffentlicher Stellen an der Mitteilung nicht von vornherein aus.

Für das weitere Verfahren gab der Landesbeauftragte aber zwei Hinweise, die auch für andere Ämter zur Regelung offener Vermögensfragen von Interesse sein können:

1. Jeder Antragsteller ist nach § 32 Abs. 5 Satz 3 VermG - soweit dies im Falle früherer Auskunftsersuchen Dritter noch nicht geschehen ist - vor der Datenübermittlung auf sein Widerspruchsrecht bezüglich der ihn betreffenden Angaben hinzuweisen. Im Falle seines Widerspruchs hat die Übermittlung stets zu unterbleiben.

2. Selbst wenn der Betroffene keinen (fristgerechten) Widerspruch einlegt oder eingelegt hat, entbindet das die Behörde nicht von ihrer generellen Verpflichtung, im Rahmen der pflichtgemäßen Ermessensausübung in jedem Einzelfall die schutzwürdigen Interessen des Antragstellers mit den berechtigten Interessen des Auskunftssuchenden abzuwägen.

31. Wasserrecht

Aufgabenübertragung bei Abwasserzweckverbänden

Mit einer Eingabe beim Landesbeauftragten wandte sich eine Petentin gegen die ihrer Meinung nach datenschutzrechtlich unzulässige Übermittlung von Wasserverbrauchswerten von einer Wasserversorgungs-GmbH an einen mit der

Betriebsführung beauftragten Abwasserzweckverband, der wiederum für einen Abwasserzweckverband aus dem Wohnbereich der Petentin handelte. Die Übermittlung der Wasserverbrauchswerte diente der Berechnung der Kanalbenutzungsgebühren.

Wie vom Landesbeauftragten festgestellt wurde, war die Eingabe berechtigt, der Abwasserzweckverband hatte die Verbrauchswerte der Petentin ohne Rechtsgrundlage bei der Wasserversorgungs GmbH abgefordert.

Zwar ist ein Abwasserzweckverband nach dem Kommunalabgabengesetz des Landes berechtigt, selbst oder durch Dritte Abwassergebühren festzusetzen und dafür die personenbezogenen Daten der Abgabepflichtigen zu erheben und zu verarbeiten. Bedient er sich aber - wie im vorliegenden Fall geschehen - der Dienste eines anderen Abwasserzweckverbandes bei der Abgabenerhebung, und ist es dazu erforderlich, daß an Stelle der Beteiligten auch noch andere Dritte Berechnungsgrundlagen (z.B. Wasserverbrauchswerte) für die Abgabenfestsetzung mitzuteilen haben, so sind diese Vorgänge gem. § 10 Abs. 1 und 2 KAG-LSA in die entsprechende **Abgabensatzung** mit aufzunehmen und konkret zu beschreiben.

Da die Abgabensatzung des Abwasserzweckverbandes diese erforderlichen Regelungen nicht enthielt, hat der Landesbeauftragte den gravierenden Rechtsfehler formell beanstandet und den Abwasserzweckverband zur Beseitigung der Rechtsmängel aufgefordert.

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, Offene Vermögensfragen, Natur- und Umweltschutz, Landwirtschaft und Forsten, Ausländer, Aussiedler, Staatsangehörigkeit	Telekommunikation, Netze, Neue Medien, Vermessungs- und Katasterwesen, Dateienregister, Gleichstellungsfragen

Verwaltungsangelegenheiten der Geschäftsstelle, Wahlen, Ausweis-, Meldewesen, Wehrpflicht, Feuerwehr, Katastrophenschutz

Registratur

Bücherei

Dienstgebäude: Berliner Chaussee 9
39114 Magdeburg

Postanschrift: Postfach 1947
39009 Magdeburg

Telefon: (0391) 81803-0

Telefax: (0391) 81803-33

Stand: 01.04.1997

Anlage 2

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995 zur Weiterentwicklung des Datenschutzes in der Europäischen Union

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

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

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10.2.1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u.a. folgende Aussagen enthält: "Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (...) wird gewährleistet".

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

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

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

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

Materielle Datenschutzregelungen

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

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

Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z.B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

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

Europäischer Datenschutzbeauftragter

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

Parlamentarische und richterliche Kontrolle

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

Anlage 3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 - Modernisierung und europäische Harmonisierung des Datenschutzrechts

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

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

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten.

2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung.

3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz.

4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität.

5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen.

6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung.

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung.

8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist.

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

10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z.B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten.

11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen.

12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung.

13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing.

14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau.

Anlage 4

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 zum Transplantationsgesetz

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

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

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

Anlage 5

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995 zu datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 09./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z.B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)
- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z.B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.
- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.
- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. **Besondere Schutzwürdigkeit medizinischer Daten**
   Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. **Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte**
   Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

   - ob Daten auf einer Chipkarte gespeichert werden,
   - welche der Gesundheitsdaten auf die Karte aufgenommen werden,
   - welche Daten auf der Karte wieder gelöscht werden,
   - ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
   - welche Daten im Einzelfall zugänglich gemacht werden.

   Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die KrankenversicherungsNr., gespeichert werden, da andernfalls - zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad - die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z.B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z.B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkarten-vermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte - z.B. mit Hilfe von Schlüsselbegriffen - dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z.B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine "Einwilligung" in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor "billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung,..., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten - einschließlich der Sicherungskopien - übertragen oder nicht.

7. **Leserecht des Karteninhabers**
   Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. **Suche nach datenschutzfreundlichen Alternativen**
   Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Anlage 6

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996 - Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten

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

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

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

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

Anlage 7

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 1996 - Grundsätze für die öffentliche Fahndung im Strafverfahren

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

1. Der Gesetzgeber hat zunächst die Voraussetzungen der öffentlichen Fahndung zu regeln und dabei einen sachgerechten Ausgleich zwischen dem öffentlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen. Die öffentliche Fahndung sollte nur bei Verfahren wegen Verletzung bestimmter vom Gesetzgeber zu bezeichnender Straftatbestände und bei Straftaten, die aufgrund der Art der Begehung oder des verursachten Schadens ein vergleichbares Gewicht haben, zugelassen werden. Sie soll nur stattfinden, wenn weniger intensive Fahndungsmaßnahmen keinen hinreichenden Erfolg versprechen. Der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets ist auch bei der Auswahl des Mediums zu berücksichtigen.

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

Bei Gefahr in Verzug kann eine Eilkompetenz der Staatsanwaltschaft vorgesehen werden; dies gilt nicht bei der öffentlichen Fahndung nach Zeugen. In diesem Falle ist unverzüglich die richterliche Bestätigung der Maßnahme einzuholen. Die öffentliche Fahndung nach Beschuldigten setzt voraus, daß ein Haftbefehl oder Unterbringungsbefehl vorliegt bzw. dessen Erlaß nicht ohne Gefährdung des Fahndungserfolges abgewartet werden kann.

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

   Eine öffentliche Fahndung nach Zeugen darf nach Art und Umfang nicht außer Verhältnis zur Bedeutung der Zeugenaussage für die Aufklärung der Straftat stehen. Hat ein Zeuge bei früherer Vernehmung bereits von seinem gesetzlichen Zeugnis- oder Auskunftsverweigerungsrecht Gebrauch gemacht, so soll von Maßnahmen der öffentlichen Fahndung abgesehen werden.

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

5. Die öffentliche Fahndung zur Sicherung der Strafvollstreckung sollte zur Voraussetzung haben, daß
   - eine Verurteilung wegen einer Straftat von erheblicher Bedeutung vorliegt und
   - der Verurteilte, der sich der Strafvollstreckung entzieht, (noch) eine Restfreiheitsstrafe von in der Regel mindestens einem Jahr zu verbüßen hat, oder ein besonderes öffentliches Interesse, etwa tatsächliche Anhaltspunkte für die Begehung weiterer Straftaten von erheblicher Bedeutung, an der alsbaldigen Ergreifung des Verurteilten besteht.

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

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

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

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

Anlage 8

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09./10. November 1995 zu Forderungen an den Gesetzgeber zur Regelung der Übermittlung personenbezogener Daten durch die Ermittlungsbehörden an die Medien
(außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.

   Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines "überwiegenden Interesses" der Öffentlichkeit anzulegen.

   Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

4. Grundsätzlich sind in Auskünfte und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z.B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

5. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

6. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind, und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

7. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat - auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens - erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

8. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

9. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

10. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

Anlage 9

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996 über Eingriffsbefugnisse zur Strafverfolgung im Informations- und Telekommunikationsbereich

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

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

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

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

Sie hebt insbesondere den Grundsatz der spurenlosen Kommunikation hervor. Kommunkationssysteme müssen mit personenbezogenen Daten möglichst sparsam umgehen.

Daher verdienen solche Systeme und Technologien Vorrang, die keine oder möglichst wenige Daten zum Betrieb benötigen. Ein positives Beispiel ist die Telefonkarte, deren Nutzung keine personenbezogenen Daten hinterläßt und die deshalb für andere Bereiche als Vorbild angesehen werden kann. Daten allein zu dem Zweck einer künftig denkbaren Strafverfolgung bereitzuhalten, ist unzulässig.

Bei digitalen Kommunikationsformen läßt sich anhand der Bestands- und Verbindungsdaten nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Eine staatliche Überwachung dieser Vorgänge greift tief in das Persönlichkeitsrecht der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse (z.B. Arztgeheimnis, anwaltliches Vertrauensverhältnis). Die Datenschutzbeauftragten fordern daher, daß der Gesetzgeber diesen Gesichtspunkten Rechnung trägt.

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

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

Anlage 10

Forderungen der Datenschutzbeauftragten des Bundes und der Länder anläßlich der 52. Konferenz am 22./23.10.1996 in Hamburg -
Maßnahmen zur Sicherung der Privatsphäre für den Fall der Einführung der akustischen Wohnraumüberwachung

1. Im Grundgesetz selbst ist festzulegen, daß

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

   - nur auf Anordnung eines Kollegialgerichts

   erfolgen darf.

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

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

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

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

6. Eine anderweitige Verwendung der erhobenen Daten (Zweckänderung) ist weder zu Beweiszwecken noch als Ermittlungsansatz für andere als Katalogtaten zulässig.

   Personenbezogene Erkenntnisse aus einem Lauschangriff dürfen nur zur Abwehr von konkreten Gefahren für gewichtige Rechtsgüter verwendet werden.

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

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

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

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

Stichwortverzeichnis *

* Fundstelle zitiert nach Tätigkeitsbericht und Seite