Landtag von Sachsen-Anhalt **Drucksache 3/4565**
Dritte Wahlperiode **16.05.2001**

Unterrichtung

Präsident des Landtages von Sachsen-Anhalt

Magdeburg, 16. Mai 2001

Fünfter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Zeit vom 1. April 1999 bis 31. März 2001

Sehr geehrte Damen und Herren,

mit Schreiben vom 10. Mai 2001 hat der Landesbeauftragte für den Datenschutz Sachsen-Anhalts gemäß § 22 Abs. 4 Satz 3 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) vom 12. März 1992 (GVBl. LSA S. 152), zuletzt geändert durch § 29 des Gesetzes über den Öffentlichen Gesundheitsdienst und die Berufsausübung im Gesundheitswesen im Land Sachsen-Anhalt (Gesundheitsdienstgesetz – GDG LSA) vom 27. November 1997 (GVBl. LSA S. 1023), dem Landtag seinen Fünften Tätigkeitsbericht übermittelt. Er schließt an den Vierten Tätigkeitsbericht an, der als Drucksache 3/1587 vorliegt und in den Ausschüssen für Inneres und für Recht und Verfassung beraten wurde.

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

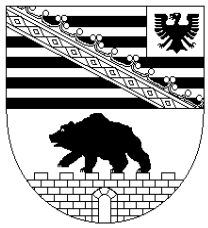
Gemäß § 40 Abs. 1 i. V. m. § 54 Abs. 1 Satz 3 GO.LT überweise ich den Tätigkeitsbericht zur Beratung und zur Berichterstattung an die Ausschüsse für Inneres (federführend) sowie für Recht und Verfassung.

Mit freundlichen Grüßen

Wolfgang Schaefer

(Ausgegeben am 17.05.2001)

Landesbeauftragter
für den Datenschutz
Sachsen-Anhalt



V. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

**für die Zeit
vom
1. April 1999 bis 31. März 2001**

V. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Landesbeauftragter für den Datenschutz - Postfach 1947 - 39009 Magdeburg

Telefon	(0391) 8 18 03 - 0
Bürgertelefon	(0800) 9 15 31 90
Fax	(0391) 8 18 03 33
Internet	http://www.datenschutz.sachsen-anhalt.de

Dienstgebäude: Berliner Chaussee 9 - 39114 Magdeburg

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
ALB	Verfahren Automatisiert geführtes Liegenschaftsbuch
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS - Innere Sicherheit
ArchG-LSA	Landesarchivgesetz
AuslG	Ausländergesetz
a.F.	alte Fassung

B

BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesarbeitsgericht
BArchG	Bundesarchivgesetz
BAT	Bundesangestelltentarifvertrag
BAT-O	Bundesangestelltentarifvertrag-Ost
BauGB	Baugesetzbuch
BauO LSA	Bauordnung des Landes Sachsen-Anhalt
BBiG	Berufsbildungsgesetz
BDSG	Bundesdatenschutzgesetz (neue Fassung)
BDSG 77	Bundesdatenschutzgesetz (alte Fassung)
BevStatG	Bevölkerungsstatistikgesetz
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
BMVBW	Bundesministerium für Verkehr, Bau- und Wohnungswesen
BND	Bundesnachrichtendienst

BNotO	Bundesnotarordnung
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz

C

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

D

DEVO	Datenerfassungsverordnung
DIHT	Deutscher Industrie- und Handelstag e.V.
DNS	Domain Name Service
DONot	Dienstordnung für Notare
DORA	Dialogorientiertes Recherche- und Informationssystem
DÖV	Die öffentliche Verwaltung
Drs.	Drucksache
DSG-LSA	Datenschutzgesetz des Landes Sachsen-Anhalt
DV	Datenverarbeitung

E

ED	Erkennungsdienst
Ed-Behandlung	Erkennungsdienstliche Behandlung
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
E-Mail	Electronic-Mail
EStG	Einkommenssteuergesetz
EU	Europäische Union
EUROCAT	Europäisches Register über große Fehlbildungen
EUROPOL	Europäisches Polizeiamt

F

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

G

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

H

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

I

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

J

JAPrO	Ausbildungs- und Prüfungsordnung für Juristen
JBeitrO	Justizbeitreibungsordnung
JGG	Jugendgerichtsgesetz
JuMiG	Justizmitteilungsgesetz

K

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

L

LAN	Lokal Area Network
LBA	Luftfahrt-Bundesamt
LFI	Landesförderinstitut
LKA	Landeskriminalamt
LKO LSA	Landkreisordnung des Landes Sachsen-Anhalt
LRZ	Landesrechenzentrum (in Halle)
LSA	Land Sachsen-Anhalt
LSA-NET	Bezeichnung für das interne Landesverwaltungsnetz (Intranet) bzw. für die Domain des Landes „lsa-net“ **L**and **S**achsen-**A**nhalt-**Net**z
LuftVG	Luftverkehrsgesetz
LuftVZO	Luftverkehrs-Zulassungs-Ordnung
LVerf	Verfassung des Landes Sachsen-Anhalt
LWG	Landeswahlgesetz

M

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

MRRG	Melderechtsrahmengesetz
MTA	Message Transfer Agent
MWV	Ministerium für Wohnungwesen, Städtebau und Verkehr

N

NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NNTP	Network News Transfer Protocol; Protokoll zum Austausch von Nachrichten in sog. Newsgroups - öffentlichen, thematisch gegliederten Diskussionsforen
NotVO	Verordnung über die Tätigkeit von Notaren in eigener Praxis
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NUB-Richtl.	neue Untersuchungs- und Behandlungsmethoden
n.F.	neue Fassung

O

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

P

PBefG	Personenbeförderungsgesetz
PC	Personal Computer
PersVG LSA	Landespersonalvertretungsgesetz Sachsen-Anhalt
PET	Privacy enhancing technology
PKH	Prozeßkostenhilfe
PKI	Public Key Infrastruktur
PKZ	Personenkennziffer
POLAS	Polizeiliche Auskunftssysteme
POLIS	**Pol**izeiliches **I**nformations**s**ystem Sachsen-Anhalt
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
SG	Schulgesetz des Landes Sachsen-Anhalt
SGB	Sozialgesetzbuch
SGB X	Sozialgesetzbuch - Verwaltungsverfahren (10. Buch)
SGSA	Städte- und Gemeindebund Sachsen-Anhalt
SigG	Signaturgesetz
SigV	Signaturverordnung
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	Strafverfahrensänderungsgesetz
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
StVollzG	Strafvollzugsgesetz
StVZO	Straßenverkehrszulassungsordnung

T

TCP/IP	Transmission Control Protocol/Internet Protocol
TDG	Teledienstegesetz
TESTA	**T**rans-**E**uropean **S**ervices für **T**elematics between **A**dministrations
TPA	Technisches Polizeiamt
TÜV	Technischer Überwachungs-Verein

U

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

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
VermG	Vermögensgesetz
VermKatG	Vermessungs- und Katastergesetz des Landes Sachsen-Anhalt
VO	Verordnung
VONot	Verordnung über die Tätigkeit von Notaren in eigener Praxis
VRZ	Verbindungsstelle zum Finanzrechenzentrum
VV	Verwaltungsvorschrift
VwGO	Verwaltungsgerichtsordnung
VwKostG LSA	Verwaltungskostengesetz des Landes Sachsen-Anhalt
VwVfG	Verwaltungsverfahrensgesetz
VZR	Verkehrszentralregister

W

WAN	Wide Area Network
WoGG	Wohngeldgesetz
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

Was die Entwicklung des Datenschutzes und seine Bedeutung für die Bürgerinnen und Bürger des Landes anbetrifft, so kann nahtlos an die Darstellungen im IV. Tätigkeitsbericht angeknüpft werden. Die Tendenz zur „Grenzüberschreitung“ in fast jeder Hinsicht setzt sich fort. Die Entwicklung der technischen Möglichkeiten vollzieht sich in immer kürzeren Zeitabständen.

Was dem Menschen bei der Vielgestaltigkeit seines täglichen Lebens helfen kann, ihm oft auch nur als Hilfe „verkauft“ wird, kann sich ebenso schnell gegen ihn wenden. Das alte Handy, der alte PC ist tot, schon stehen ganz neue technische Angebote vor der Tür. Im Privat- wie im Berufsleben kann derjenige, der sich gerne mit Neuem umgibt, froh sein, wenn er noch die notwendigsten Bedienungsfunktionen erkennt, die tatsächlichen Abläufe und Auswirkungen der Technik überschauen selbst die Fachleute kaum noch. Die neue WAP-Handy-Generation führt elektronisch den Kalender des Besitzers, ermöglicht ihm aus weiter Ferne das Schließen der heimischen Rollos oder das Einschalten der Waschmaschine, aber es zeichnet auch alles auf, was er tut, wo er sich bewegt, und es überträgt auch ohne sein Wissen - indem es sich von außen aktivieren läßt - was er wo gerade mit wem bespricht.

Ein Click über den heimischen PC verbindet den Surfer mit allen Teilen der Welt und versorgt ihn gegen Geld mit allerlei nützlichen und unnützen Informationen. Aber mit dem gleichen Click in die weltweite Vernetzung verrät der Benutzer seine Gedanken, seine Gefühle und seine persönliche Lebensgestaltung auch an Hunderttausende „stiller Nutzer“, die ihn ohne sein Wissen beobachten, analysieren und mißbrauchen können.

Nicht nur die moderne Technik fesselt und umgarnt den Menschen mehr als er ahnt, das Recht in seinem vertrauten Umfeld kann ihn dagegen zunehmend immer weniger schützen. Die Tatsache, daß die EU-Datenschutzrichtlinie aus dem Jahr 1995 erst im Jahre 2001 in Deutschland im Bund und in den meisten Ländern in unser nationales Recht umgesetzt wird, zeigt geradezu exemplarisch, wie weit das Recht schon hinter der Wirklichkeit zurückgeblieben ist.

Auch der Staat nutzt die moderne Datenverarbeitung in doppelter Hinsicht. Unter dem Schlagwort „e-government“ verspricht er dem Bürger nützliche Informationen und schnellen Service, aber er nutzt dieselbe Technik auch gegen den Bürger. So werden heute in umfangreichen Programmen die Steuer- und Sozialdaten eines Bürger gegeneinander abgeglichen, und bei Bedarf kann der Staat mit - und häufig auch ohne - Wissen des Betroffenen weitere Informationen aus dritten (z.B. privaten) Quellen heranziehen und automatisiert auswerten. Mit ihrer Hilfe kann der Bürger schon heute in weiten Bereichen seines Lebens kontrolliert werden. Nicht nur wer telefoniert, Fax oder E-Mail versendet, kann erfaßt werden. Noch sind „englische Verhältnisse“ bei der Überwachung öffentlich zugänglicher Wege und Plätze nicht erreicht, aber wer in der Bundesrepublik in einer größeren Stadt seine Wohnung verläßt, muß damit rechnen, im öffentlichen Straßenbereich, im Bus, in der U-Bahn ebenso wie in der Bank oder im Kaufhaus mit Videotechnik erfaßt und aufgezeichnet zu werden. Wer mit dem Auto über Land fährt, kann in den meisten Bundesländern heute ohne Angaben von Gründen und ohne besonderen Anlaß von der Polizei angehalten werden; dabei können Personalien gespeichert und mitgeführte Sachen und Gegenstände überprüft werden. Dem Bahnreisenden ergeht es nicht besser - in jedem Zug darf der Reisende heute überall ohne Anlaß vom Bundesgrenzschutz überprüft werden. Für den Flugreisenden gilt dies bekanntlich schon lange.

Das alles ist nicht nur lästig und für einen freien Staatsbürger im demokratischen Rechtsstaat auch unwürdig, sondern es kann im Zeitalter der schnellen Datenverarbeitung mit wenigen Schaltungen zu umfassenden Bewegungs- und Gestaltungsprofilen seitens des Staates genutzt werden. George Orwells Visionen sind fast erreicht. Die Mißbrauchsgefahren durch den Staat, aber auch durch privaten Informationsmißbrauch seiner Bediensteten wachsen angesichts dieser verfügbaren Datenfülle gefährlich an.

Keine guten Aussichten für den Datenschutz. Bürgerinnen und Bürgern ist zu empfehlen, den Schutz ihrer Grundrechte mit mehr Eigenverantwortung anzugehen und genau zu überlegen, wem sie was von sich preisgeben. Auch die Datenschutzbeauftragten in Bund und Ländern können ihnen nur noch begrenzt helfen.

2. Der Landesbeauftragte

2.1 Tätigkeit im Berichtszeitraum

Die im letzten Tätigkeitsbericht (S. 3) festgestellte Stabilisierung der Geschäftseingänge hat im Berichtszeitraum leider nicht angehalten. 1999 gab es bereits wieder 3311 schriftliche Eingänge, im Jahr 2000 waren es 3.226. 1999 sind dazu 653, im Jahr 2000 649 schriftliche Stellungnahmen erarbeitet worden. Die Zahl der fernmündlichen Anfragen durch öffentliche und private Stellen liegt unverändert bei 750 bis 800 pro Jahr. Leicht rückläufig sind die Zahlen der persönlichen Anfragen und Vorsprachen der Bürger in der Behörde des Landesbeauftragten (ca. 20 bis 25 im Jahr) und die Zahl der Bürgereingaben (ca. 140 bis 150 pro Jahr).

Rückläufig ist erfreulicherweise die Zahl der formellen Beanstandungen (1) nach § 24 DSG-LSA, in etwa 20 weiteren Fällen hat der Landesbeauftragte von einer Beanstandung absehen können. Dies könnte die Beobachtung aus dem vorangegangenen Berichtszeitraum bestätigen, daß aufgrund der zunehmend verbesserten Aus- und Fortbildung in den öffentlichen Stellen des Landes der Umgang mit den personenbezogenen Daten der Bürger sicherer geworden ist.

Gleichbleibend hoch sind der Bedarf an Besprechungen und die Bitten um Beratungen vor Ort bei den öffentlichen Stellen des Landes. Dabei verteilen sich die Probleme etwa zu gleichen Teilen auf den materiell-rechtlichen und den technisch-organisatorischen Beratungsbereich. Die nachfolgenden Beiträge sollen dazu einen repräsentativen Überblick geben. Die Entwicklung der automatisierten Datenverarbeitung und die besonderen Probleme der Datensicherheit - auch als Folge der zunehmenden Vernetzung - sind in diesem Bericht schwerpunktmäßig unter den Ziffern 6 und 11 abgehandelt.

Fortgesetzt wurden im Berichtszeitraum die ohne besonderen Anlaß vorgenommenen Querschnittskontrollen bei den Ausländer- und Meldebehörden sowie bei den personalaktenführenden Stellen im Lande.

Erstmals wurden im Lande zwei Justizvollzugsanstalten geprüft und Prüfungen im Bereich des Gesundheitswesens wieder aufgenommen. Abgeschlossen wurden die Querschnittskontrollen bei den kriminalaktenführenden Behörden der Polizei.
Trotz vollständiger personeller Besetzung konnte wegen längerdauernder zahlreicher Ausfälle durch Krankheit die Zahl der insgesamt vorgesehenen Kontrollen nicht eingehalten werden.

Auch im Berichtszeitraum unverändert hoch blieb die Bereitschaft der Mitarbeiterinnen und Mitarbeiter zur Teilnahme an Aus- und Fortbildungsveranstaltungen, gleichermaßen als Lehrende und Lernende.
Leider hat der Landesbeauftragte zum März 2001 eine Referatsleiterin durch Wechsel in den Geschäftsbereich des Ministers des Innern verloren, erfreulicherweise aber nach einem Auswahlverfahren auch einen qualifizierten Bewerber wieder aus diesem Geschäftsbereich für die Tätigkeit beim Landesbeauftragten gewinnen können.
Die aktuelle Aufgabenzuweisung in der Geschäftsstelle des Landesbeauftragten ergibt sich aus dem anliegenden Organigramm **(Anlage 1).**

2.2 Zusammenarbeit mit anderen Aufsichts- und Kontrollinstitutionen

Unverändert gut ist die Zusammenarbeit mit dem Landtag im parlamentarischen Bereich. Zahlreiche Anfragen zu Beratungen und Informationen aus den Fraktionen des Landtages hat der Landesbeauftragte gerne aufgegriffen. Ebenso häufig waren Einladungen der Fachausschüsse des Landtages im Zusammenhang mit der Beratung von Gesetzentwürfen und Petitionen mit datenschutzspezifischem Bezug.
Eine kontroverse Sachdiskussion gab es im Verlauf des letzten Berichtsjahres zur Abgrenzung personalrechtlicher Befugnisse zwischen der Landtagsverwaltung und dem Landtagspräsidenten einerseits und dem Landesbeauftragten andererseits (§ 21 Abs. 3 Satz 3 DSG-LSA). Ein dazu erstelltes Rechtsgutachten

durch ein Mitglied des Gesetzgebungs- und Beratungsdienstes und ein externes Rechtsgutachten führten nicht zu einer einvernehmlichen Rechtsauffassung. Die im Mai 2001 vorgesehenen parlamentarischen Beratungen zur Novellierung des DSG-LSA aus Anlaß der Umsetzung der EU-Datenschutzrichtlinie sollen auch dazu genutzt werden, im Landtag die in Art. 28 Abs. 1 Satz 2 der Richtlinie vorgeschriebene völlige Unabhängigkeit des Landesbeauftragten zu erörtern.

Eine gute und sachorientierte Zusammenarbeit gab es im Berichtszeitraum mit den anderen Obersten Landesbehörden. Hervorzuheben ist die enge und konstruktive Zusammenarbeit mit dem seitens der Landesregierung für den Datenschutz verantwortlichen Ministerium des Innern. Trotz sachlicher Differenzen in der Bewertung rechtlicher Regelungen (zuletzt bei der Novellierung des SOG LSA) und einzelner Feststellungen in den Kontrollberichten überwiegen die praxisbezogenen guten datenschutzrechtlichen Lösungen. Bewährt hat sich diese sachorientierte Zusammenarbeit und die Abstimmung der gegenseitigen Schwerpunkte auch wieder bei der im Frühjahr 2001 anstehenden Novellierung des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA).

Erfolgreich und hilfreich für die Arbeit im Lande Sachsen-Anhalt ist auch die dem Landesbeauftragten obliegende Zusammenarbeit mit den datenschutzrechtlichen Kontrollinstitutionen im nationalen und internationalen Bereich. Die enge Abstimmung und sachorientierte Diskussion in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und in ihren Arbeitskreisen sind für einen effektiven Datenschutz in Sachsen-Anhalt und ein abgestimmtes Vorgehen zwischen den Bundesländern und dem Bund auf diesem Gebiet unentbehrlich.

Der Landesbeauftragte hat deshalb auch im Berichtszeitraum an einer europäischen und zwei internationalen Datenschutzkonferenzen teilgenommen, in einem Fall als Referent.

Die ihm seit Oktober 1998 seitens des Bundesrates übertragene Aufgabe als zweiter unabhängiger deutscher Vertreter in der Gemeinsamen Kontrollinstanz für EUROPOL nimmt der Landesbeauftragte im Nebenamt wahr. Seit Oktober 2000 ist er stellvertretender Vorsitzender dieses Gremiums.

2.3 Neue Kommunikationswege mit Bürgern und Behörden

2.3.1 Die Homepage des Landesbeauftragten im Intranet und im Internet

Im zurückliegenden Berichtszeitraum war zu beobachten, daß bedingt durch den weiteren Ausbau des Landesnetzes und die Etablierung von Internettechnologien (z.B. WWW, E-Mail) in der Landesverwaltung, immer mehr öffentliche Stellen des Landes diese neuen Formen zur eigenen Präsentation sowie zur Informationsbeschaffung und zum Informationsaustausch nutzen.

Darüber hinaus stieß auch die Präsenz der Landesregierung im Internet bei interessierten Bürgerinnen und Bürgern auf ein reges Interesse. Das veranschaulicht nicht zuletzt ein Blick in die Statistik der Zugriffe auf diese Adresse des Landes Sachsen-Anhalt im Internet (http://www.sachsen-anhalt.de). Für die zurückliegenden 12 Monate waren ca. 2,3 Mio. Zugriffe auf die Homepage des Landes Sachsen-Anhalt zu verzeichnen.

Der Landesbeauftragte hat deshalb mit Unterstützung des Landesrechenzentrums in Halle ein eigenes Informationsangebot gestaltet und sieht in der Nutzung dieser Informationstechnologie eine weitere Möglichkeit, seinem Beratungsauftrag gegenüber den öffentlichen Stellen aktuell und flexibel nachzukommen und damit eine wesentlich größere Anzahl von Mitarbeiterinnen und Mitarbeitern in der Landes- und Kommunalverwaltung zu erreichen.

Alle Behörden, die über einen Zugang zum Intranet des Landes (LSA-NET) verfügen, können seit dem 14. Dezember 2000 dieses Informationsangebot über das **Eingangsportal** des LSA-NET (http://www.lsa-net.de) oder die Intranet-Adresse (http://www.datenschutz.sachsen-anhalt.de) erreichen.

Für die Bürgerinnen und Bürger und zum anderen auch für die öffentlichen Stellen der Kommunalverwaltung, die bisher noch nicht über einen Zugang zum internen Netzwerk (Intranet) des Landes Sachsen-Anhalt verfügen, besteht die Möglichkeit, sich auf der **Internet-Homepage** des Landesbeauftragten unter der gleichlautenden Internet-Adresse (http://www.datenschutz.sachsen-anhalt.de) ebenfalls über Datenschutz und Datensicherheit zu informieren.

Das Informationsangebot enthält neben einer Vorstellung der Aufgaben des Landesbeauftragten und seiner Geschäftsstelle die wichtigsten Rechtsvorschriften zum Datenschutz und die bisher erstatteten Tätigkeitsberichte des Landesbeauftragten, auch in downloadbarer Form. Außerdem steht eine Fülle von Informationsmaterialien bereit, die teilweise die Ergebnisse der Tätigkeit von Arbeitskreisen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder widerspiegeln sowie weitere Links zu relevanten Seiten anderer Institutionen.

Das Internet-Angebot des Landesbeauftragten ist in das „Virtuelle Datenschutzbüro“ (http://www.datenschutz.de), einem Gemeinschaftsprojekt verschiedener Datenschutzinstitutionen, eingebunden.

Der Landesbeauftragte ist bestrebt, sein Informationsangebot weiter auszubauen und es den Bedürfnissen der öffentlichen Verwaltung nach Beratung und Empfehlungen zu den Themen Datenschutz und Datensicherheit anzupassen. Hierzu ist er an Vorschlägen, aber auch an kritischen Anmerkungen aus der Landes- und Kommunalverwaltung interessiert.

2.3.2 Die neue gebührenfreie Rufnummer für Bürger

Neben seiner Homepage hat der Landesbeauftragte seit dem 01. Dezember 2000 eine neue **gebührenfreie** Telefonservicerufnummer für die Bürgerinnen und Bürger in Sachsen-Anhalt geschaltet. Für deren datenschutzrechtliche Anliegen gegenüber staatlichen Stellen sind der Landesbeauftragte und seine Mitarbeiter zu den üblichen Bürozeiten unter der Rufnummer **0800 - 91 53 190** zu erreichen. Damit steht innerhalb des Landes eine einfache und unkomplizierte Kommunikationsmöglichkeit zur Verfügung.

2.3.3 E-Mail-Adresse des Landesbeauftragten

Der Landesbeauftragte verkennt nicht die zunehmende Bedeutung der Elektronischen Post (E-Mail) für einen Informationsaustausch in Wirtschaft und Verwaltung. Gleichwohl stellt er z.Zt. seine E-Mail-Adresse nicht (mehr) für die öffentliche Kommunikation zur Verfügung. Das hat gewichtige Gründe:

Mehrfach, zuletzt im IV. Tätigkeitsbericht (S. 50 f), wies der Landesbeauftragte auf spezifische Sicherheitsrisiken der E-Mail-Nutzung hin. Er bat deshalb seine Kommunikationspartner, eine Versendung per E-Mail nur vorzusehen, wenn der Inhalt der Schreiben als nicht besonders schutzwürdig oder als für den Empfänger nicht wichtig anzusehen ist. Denn nach wie vor gilt, daß E-Mails ihren bestimmungsmäßigen Empfänger nicht stets erreichen, ihr Inhalt durch Dritte verfälscht werden und einer Vielzahl Unbefugter zur Kenntnis gelangen kann.

Trotzdem erreichten den Landesbeauftragten immer wieder E-Mails mit besonders sensiblem Inhalt und unverschlüsselt.

Bis auf weiteres soll deshalb durch die Zurückhaltung bei der Bekanntgabe der E-Mail-Adresse vermieden werden, daß Bürger ihre Anliegen, die neben sensiblen persönlichen Daten auch sicherheitsrelevante, brisante Vorgänge bei öffentlichen Stellen des Landes Sachsen-Anhalt enthalten können, per E-Mail übermitteln.

Erst wenn neue Verfahren die einfache und sichere Versendung von E-Mails für **jeden** Nutzer des Internets möglich machen, kann diese Form der Kommunikation uneingeschränkt freigegeben werden.

Ein entsprechender Hinweis des Landesbeauftragten findet sich auch auf seiner Homepage.

3. Ausländerangelegenheiten

3.1 Prüfung von Ausländerbehörden

Der Landesbeauftragte hat auch in diesem Berichtszeitraum die Prüfung von Ausländerbehörden fortgesetzt.

Dabei haben sich die bereits gemachten Erfahrungen bestätigt (vgl. III. Tätigkeitsbericht, S. 14 f; IV. Tätigkeitsbericht, S. 11).

Daneben mußte er zum wiederholten Mal feststellen, daß einzelne Ausländerbehörden von den Ausländern eingezogene Pässe **in den Ausländerakten** aufbewahren. Das hält er für nicht datenschutzgerecht.

Er empfiehlt, eingezogene Pässe in einem ständig verschlossenen Safe aufzubewahren und dies in der jeweiligen Ausländerakte zu notieren.

Die Kontrollen gehen weiter.

3.2 Fehlerhafte Ausschreibungen im Schengener Informationssystem

Ein neues Thema für den Landesbeauftragten waren Anfragen von Ausländern zu den über sie im Schengener Informationssystem (SIS) gespeicherten Daten.

Dieses Informationssystem ist auf der Grundlage der Art. 92 ff des Schengener Durchführungsübereinkommens (SDÜ) geschaffen worden und soll einen Ausgleich für den Wegfall der Binnengrenzkontrollen in den beteiligten Staaten darstellen.

Art. 109 SDÜ sieht vor, daß jeder, der sich in einem Schengen-Staat aufhält, Auskunft über die zu seiner Person im SIS gespeicherten Daten verlangen kann. Zu diesem Zweck wendet er sich an die zuständige Kontrollinstanz seines Aufenthaltslandes, die - falls deutsche (Ausländer-) Behörden die Speicherung vorgenommen haben - den Bundesbeauftragten für den Datenschutz informiert.

Von dort wird das Auskunftsersuchen des Ausländers an den für die speichernde Ausländerbehörde zuständigen Landesbeauftragten weitergeleitet.

Im Berichtszeitraum häuften sich diese Anfragen, und leider mußte der Landesbeauftragte mehrmals feststellen, daß die zuständigen Ausländerbehörden den Ausländer fälschlicherweise im SIS ausgeschrieben hatten.

Nach Art. 96 Abs. 3 SDÜ kann die Entscheidung zur Ausschreibung im SIS insbesondere darauf beruhen, daß der Drittausländer **tatsächlich** ausgewiesen, zurückgewiesen oder abgeschoben worden ist. Daneben kommt im Einzelfall nur dann eine Ausschreibung gem. Art. 96 Abs. 2 SDÜ in Betracht, wenn eine Ausweisung beabsichtigt gewesen, aber mangels Bekanntgabe unterblieben ist, weil der Ausländer ausgereist oder untergetaucht ist.

Diese Voraussetzungen sind bei Ausschreibungen, die lediglich den Zweck der Aufenthaltsermittlung verfolgen, auch wenn die anschließende Festnahme und Abschiebung geplant ist, nicht erfüllt. Demnach darf z.B. ein abgelehnter Asylbewerber, der untergetaucht ist, nur zur Aufenthaltsermittlung im INPOL-System der Polizei und im AZR beim Bundesverwaltungsamt, nicht jedoch im SIS ausgeschrieben werden.

Der Landesbeauftragte empfiehlt den Ausländerbehörden des Landes, ihre Ausschreibungen im SIS zu überprüfen und die nach den obigen Feststellungen unzulässigen zu löschen.

3.3 Besucherdaten in einer Asylbewerberunterkunft

Ein Petent, der einer Familie in einer Asylbewerberunterkunft einen Besuch abstatten wollte, wunderte sich nicht schlecht, als er am Eingang vom Sicherheitspersonal aufgefordert wurde, seinen Personalausweis abzugeben und dann sah, wie daraus seine Daten in ein Besucherbuch übertragen wurden.

Das ging ihm zu weit, und er bat den Landesbeauftragten um Prüfung.

Die Unterbringung von Asylbewerbern in einer Gemeinschaftsunterkunft berechtigt aufgrund der besonderen Gefährdungslage auf der Grundlage des § 15 Abs. 1 Nr. 3 SOG LSA zu geeigneten Sicherheitsmaßnahmen sowohl zum Schutz der Unterkunft selbst als auch der Unterkunftsbewohner. Zu den Vorkehrungen gehört auch eine Kontrolle des Besucherverkehrs, weil dadurch das Entstehen konkreter Gefahren bereits präventiv weitgehend verhindert werden kann. Dabei ist es aber ausreichend, wenn - nach Vorlage eines Passes oder Ausweises - Name und Adresse des Besuchers sowie die Dauer seines Aufenthaltes eingetragen und nach einer überschaubaren Aufbewahrungsfrist auch wieder gelöscht werden. Die Einbehaltung des Personalausweises war nicht erforderlich und somit von der Rechtsgrundlage des § 15 SOG LSA auch nicht gedeckt. Die Verfahrensweise in der Unterkunft wurde entsprechend geändert.

4. Ausweis- und Meldewesen

4.1 Aufbewahrung alter Meldedaten

Ein Stadtarchiv forderte vom Meldeamt, ihm auch die im Melderegister zu löschenden Daten zu überlassen. Die Daten sollten 50 Jahre lang gesammelt werden, um sie anschließend aufzuarbeiten und ggf. in Karteikartenform auszugeben.

Daraufhin wandte sich das Meldeamt ohne eigene rechtliche Prüfung an seinen Softwarehersteller. Der sollte entsprechende Software entwickeln, um die im Meldeamt zu löschenden Daten in einem speziell geschützten Datenverzeichnis für das Archiv aufzufangen.

Dem Softwarehersteller kamen rechtliche Zweifel, und er wandte sich an den Landesbeauftragten.

Das war gut so, denn die rechtlich zulässige Verfahrensweise ist spezialgesetzlich und abschließend in § 26 Abs. 2 und 4 MG LSA geregelt. Danach dürfen dem Stadtarchiv nur bestimmte, nach Ablauf von 50 Jahren beim Meldeamt gesondert weiter aufzubewahrende Meldedaten, wie z.B. Familienname, Vorname, Doktorgrad, Tag und Ort der Geburt, Geschlecht, zur Archivierung übermittelt werden. Alle anderen Meldedaten hat die Meldebehörde zu löschen, d.h., nach der Begriffsbestimmung in § 2 Abs. 5 Nr. 5 DSG-LSA vollständig unkenntlich zu machen und damit eine künftige Kenntnisnahme und Verwendung der Daten für jedermann unmöglich zu machen.

4.2 12.000 falsche Auskünfte aus dem Melderegister

Der Tagespresse mußte der Landesbeauftragte entnehmen, daß in einem Landkreis ein im Rahmen einer Verkehrssicherheitsaktion vorgesehener persönlicher Brief des Innenministers, der eigentlich an junge Autofahrer gerichtet war, an 6 bis 14-jährige Kinder verschickt worden war. In dem Brief wurde davor gewarnt, nach Partys angetrunken Auto zu fahren.

Ursache der teuren und peinlichen Panne war die fehlerhafte Gruppenauskunft eines Meldeamtes.

Keinen Zweifel gab es in diesem Fall am für eine Gruppenauskunft erforderlichen öffentlichen Interesse. Allerdings, so ergab die Prüfung des Auswahlverfahrens, fehlte ein gutes Qualitätssicherungsmanagement. Bei einer so großen Zahl Betroffener waren hohe Ansprüche an die richtige Eingabe der Daten des betroffenen Personenkreises in die automatisierte Auswertung zu stellen und eine entsprechende Zwischenkontrolle durch Ausdruck vorzunehmen. Diese Prüfung unterblieb. So wurde nicht bemerkt, daß die zur Selektion eingegebenen Geburtsdaten falsch waren.

Nach der Intervention des Landesbeauftragten wurde in der Stadtverwaltung sofort eine entsprechende Dienstanweisung erlassen. Wird diese beachtet, sollte sich eine solche Panne zukünftig nicht wiederholen.

4.3 Übermittlungen aus dem Einwohnermelderegister bei der Umbenennung von Straßen

In einer Gemeinde wurden Umbenennungen von Straßen beschlossen. Aus diesem Anlaß übermittelte die Verwaltungsgemeinschaft automatisiert den ortsansässigen Versorgungsunternehmen (Energieversorgung, Wasserversorgung, Gasversorgung, Abfallentsorgung) Namen und Vornamen aller betroffenen Einwohner aus dem Melderegister, wobei sie die bisherigen Anschriftsdaten der künftigen Anschrift gegenüberstellte.

Als Rechtsgrundlage für diese Datenübermittlung bezog sich die Verwaltungsgemeinschaft auf § 33 Abs. 1 MG LSA. Dies war falsch, die Vorschrift gilt nur für Einzelauskünfte zu Einzelanfragen.

Im Fall der Umbenennung von Straßen ist die Einwohnermeldebehörde auf der Grundlage von § 25 MG LSA verpflichtet, die Daten der betroffenen Einwohner von Amts wegen zu berichtigen. Eine automatisierte Unterrichtung über die im Einwohnermelderegister berichtigten Daten aber ist gem. § 25 Abs. 3 MG LSA **nur** an die Stellen zugelassen, denen Daten im Rahmen der regelmäßigen Datenübermittlung nach der MeldDÜVO-LSA übermittelt worden sind. Im konkreten Fall sind also Einwohnermeldedaten an mehrere Empfänger ohne Rechtsgrundlage übermittelt worden.

Die Verwaltungsgemeinschaft hätte sich darauf beschränken müssen, den Versorgungsunternehmen lediglich den (geänderten) neuen Straßennamen mitzuteilen.

5. Europäischer Datenschutz

5.1 Richtlinie der Europäischen Union

Von Anfang an hat der Landesbeauftragte über wichtige datenschutzrechtliche Entwicklungen in der EU berichtet (vgl. I. Tätigkeitsbericht, S. 40; II. Tätigkeitsbericht, S. 30; III. Tätigkeitsbericht, S. 22 ff; IV. Tätigkeitsbericht, S. 18 f).

Gegenstand des letzten Berichtes war insbesondere die neue EG-Datenschutzrichtlinie, deren dreijährige Umsetzungsfrist in deutsches Recht im Oktober 1998 verstrichen war. Trotz der Ankündigung der Bundesregierung, bis Sommer 1999 die Regelungen der Richtlinie in deutsches Recht umzusetzen, ist es bis heute zu keiner Novellierung des Datenschutzgesetzes im Bund gekommen. Unter dem Druck eines Zwangsverfahrens vor dem Europäischen Gerichtshof beabsichtigt die Bundesregierung eine Angleichung des BDSG auf kleinem Änderungsniveau noch im Frühjahr 2001.

In Sachsen-Anhalt ist die Anpassung des DSG-LSA zwar rechtzeitig im Ministerium des Innern vorbereitet worden, doch hatte man hier wegen der möglichst weitgehenden inhaltlichen Übereinstimmung mit den Bestimmungen des BDSG die gesetzliche Änderung noch zurückgestellt.

Zwischenzeitlich hat die Landesregierung ihren Änderungsentwurf dem Landtag zur Beratung zugeleitet.

5.2 Charta der Grundrechte der Europäischen Union

Anfang Dezember 2000 ist in Nizza die feierliche Proklamation der Charta der Grundrechte der Europäischen Union erfolgt.

Unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder sowie ihrer Kollegen in den anderen europäischen Mitgliedsstaaten ist in die Charta auch das **Grundrecht auf Datenschutz** aufgenommen worden:

> Art. 8 [Schutz personenbezogener Daten]
> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Personen oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden.

Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Damit ist eine Grundlage für ein europaweites Grundrecht auf Datenschutz geschaffen worden, das als Teil einer künftigen europäischen Verfassung sogar - ohne Änderung des Wortlautes - rechtlich verbindlich werden könnte.

5.3 EUROPOL

Der Landesbeauftragte greift seine Berichterstattung zu EUROPOL (zuletzt IV. Tätigkeitsbericht, S. 19 ff) wieder auf. Das Europäische Polizeiamt hat seine Tätigkeit offiziell zum 01. Juli 1999 aufgenommen. Die Behörde wird für fünf Jahre von dem Deutschen Jürgen Storbeck geleitet, der bereits Koordinator der Vorläuferinstitution EDU war.

Die von den unabhängigen Mitgliedern der Gemeinsamen Kontrollinstanz festgelegte eigene Geschäftsordnung vom 22. April 1999 ist zwischenzeitlich durch den Rat der EU-Länder ratifiziert worden und im Amtsblatt der Europäischen Gemeinschaft 1999 abgedruckt (Info-Nr. 1999/C 149/01). Die Geschäftsordnung regelt in den Artikeln 11 ff auch das Verfahren im Beschwerdeausschuß zu den rechtskräftigen Entscheidungen. Bislang liegen keine Beschwerden betroffener Bürger vor.

Als derzeit wichtigstes Standbein bei der Arbeit von EUROPOL haben sich erneut die in einem Büro bei EUROPOL angegliederten - nicht eingegliederten - Verbindungsbeamten aus den nationalen Stellen der Mitgliedsländer erwiesen. Über sie erfolgt der Informationsaustausch in aktuellen Fahndungs- und Ermittlungsfällen, weil das als umfassende Datensammlung vorgesehene automatisiert geführte Informationssystem (Art. 7 EUROPOL-Übereinkommen) bis heute nicht einsatzfähig ist. Zur Zeit wird ein vorläufiges System aufgebaut, das noch in diesem Jahr seine Arbeit aufnehmen soll.

Die Behörde hat inzwischen im zweistelligen Bereich automatisiert geführte Analysedateien (Art. 10 EUROPOL-Übereinkommen) zur Auswertung eingerichtet. Die Informationen und personenbezogenen Daten zur Verarbeitung werden direkt über die nationalen Stellen aus den Mitgliedsländern angeliefert und von Analyseteams aufgearbeitet. Die inzwischen abgeschlossenen ersten Analysen werden hinsichtlich der Qualität ihrer Ergebnisse unterschiedlich beurteilt.

Ein weiterer Schwerpunkt der EUROPOL-Tätigkeiten liegt z.Zt. beim Aufbau der Zusammenarbeit mit Drittstaaten und Drittstellen. Die Gemeinsame Kontrollinstanz (GKI) hat in bisher acht Fällen Stellungnahmen zu den von EUROPOL geplanten Verhandlungen abgegeben. Zusätzlich erstellt die GKI datenschutzrechtliche Voten zu den Errichtungsanordnungen für die Analysedateien. Im November 2000 hat sie eine erste datenschutzrechtliche Kontrolle bei EUROPOL durchgeführt. Die Ergebnisse werden z.Zt. ausgewertet und mit EUROPOL diskutiert.

6. Entwicklung der automatisierten Datenverarbeitung

6.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Seit seinem I. Tätigkeitsbericht im März 1993 gibt der Landesbeauftragte in kurzer Form einen Überblick über die wesentlichen Entwicklungen beim Einsatz der Informations- und Kommunikationstechnik (IuK) aus datenschutzrechtlicher Sicht. Besondere Bedeutung kommt dabei dem Gefährdungspotential neuer IuK-Technologien für das Persönlichkeitsrecht der Bürgerinnen und Bürger zu. Deshalb sind gerade beim Einsatz modernster IuK durch die Landesverwaltung, bei dem in vielfältiger Weise personenbezogene Daten automatisiert verarbeitet werden, die Rechte der Bürgerinnen und Bürger wirksam zu schützen (§ 1 DSG-LSA).

Lagen in der ersten Hälfte der 90er Jahre die Problembereiche bei der Ausrüstung und Ausstattung der Landesverwaltung mit PC-Technik, dem Beginn einer lokalen Vernetzung in den Behörden und der Schaffung der Grundlagen für den

Aufbau eines Landesnetzes, so haben sich die Schwerpunkte zum Übergang ins Zeitalter der „globalen Informationsgesellschaft“ und des „Internets“ für die Landesverwaltung und damit auch für den Landesbeauftragten wesentlich geändert. Ein gutes Beispiel für diese Entwicklung ist das Projekt TESTA Deutschland (vgl. IV. Tätigkeitsbericht, S. 23 f), an dem auch das Land Sachsen-Anhalt beteiligt ist. TESTA Deutschland ist ein bundesweites Intranet für die öffentliche Verwaltung in Deutschland mit der Möglichkeit eines länderübergreifenden Zugriffs im Rahmen der EU. Ziel dieses europäischen Projektes ist letztendlich die Vernetzung von Standorten der öffentlichen Verwaltung aller EU-Länder (vgl. die folgende Ziff. 6.4).

Zukünftig werden sich die Landesverwaltung, aber auch die Städte und Gemeinden, verstärkt Fragestellungen und Konzepten zum sog „Electronic Government“ (kurz auch **e-government**) zuwenden. Vorbereitungen laufen hierzu allerorten, und heute sind neben dem Land Sachsen-Anhalt und vielen Landesbehörden auch die Landkreise, viele Städte und Gemeinden mit einer Homepage im Internet vertreten. Mit dieser „Serviceorientierung“ der Verwaltung soll neben dem bereits bestehenden Informationsangebot die Nutzung der modernen Kommunikationstechnologien durch aktive Interaktionsmöglichkeiten für die Bürgerinnen und Bürgern über das Internet zur Inanspruchnahme von Verwaltungsdienstleistungen der Behörden wesentlich erweitert werden.

Aber nur Serviceangebote der Verwaltung, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen den Bürgerinnen und Bürgern letztendlich. Deshalb hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe im Oktober 1999 beauftragt, sich mit dieser Form der Modernisierung der Verwaltung zu befassen. Als Ergebnis dieser Arbeitsgruppe verabschiedete die Konferenz am 12./13.10.2000 eine Entschließung, in der grundsätzliche Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung gegeben wurden **(Anlage 19).** Ausführlich sind die Ergebnisse und Wertungen der Arbeitsgruppe in der Broschüre „Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung“ dargestellt. Diese ist vom Landesbeauftragten in alle Bereiche der Landes- und Kommunalverwaltung verteilt worden und kann natürlich auch von den Bürgerinnen und Bürgern abgefordert werden.

Zuletzt hat der Landesbeauftragte in seinem IV. Tätigkeitsbericht (S. 21 ff) auf die wesentlichen Aspekte und die Entwicklung des Einsatzes von Informations- und Kommunikationstechnik in Sachsen-Anhalt hingewiesen. Mittlerweile verfügt das Land über eine moderne Kommunikationsinfrastruktur, die sich auf der Basis des ITN-LSA entwickelt hat und die heute für die Landesverwaltung die Möglichkeit bietet, unter Nutzung der Internetdienste (wie z.B. WWW, E-Mail, NNTP (NEWS), FTP) sowohl im internen Verwaltungsnetz des Landes (Intranet), im TESTA-Deutschland-Netz als auch im Internet zu arbeiten bzw. zu kommunizieren.

Im aktuellen Berichtszeitraum hat die Landesverwaltung große Anstrengungen bei der Ausstattung der Mitarbeiterarbeitsplätze mit Informations- und Kommunikationstechnik, bei der Schaffung einer modernen Kommunikationsinfrastruktur in den Behörden und beim weiteren Um- bzw. Ausbau des ITN-LSA unternommen. Hervorzuheben ist das Konzept zur Inbetriebnahme weiterer neuer leistungsfähiger Netzknotentechnik (Einsatz von dynamischen Bandbreitenmultiplexern - dBBM) bei gleichzeitiger Integration der Sprachkommunikation sowie der Aufbau eines sog. Backbone-Bereiches. Die Erneuerung der Netzknotentechnik in Verbindung mit der Umstellung auf ein dynamisches Routingkonzept im Backbone-Bereich des ITN-LSA soll voraussichtlich bis Ende 2002 abgeschlossen werden.

Neben dem ITN-LSA bestehen nunmehr zwei weitere virtuelle Netze: das Telekommunikation-Sondernetz der Polizei für Telefonie (TKSoNe-Pol) und das Telekommunikation-Netz der Landesverwaltung für Telefonie (TK-Verw.). Das zuständige Ministerium des Innern als Netzbetreiber benutzt deshalb auch die Bezeichnung "Corporate Network der Polizei und der Verwaltung des Landes Sachsen-Anhalt" (CNPV LSA).

Das Konzept der Trennung von Sprach- und Datenverkehr durch getrennte Bussysteme in den dBBM und die Übertragung in getrennten Basiskanälen (sog. B-Kanälen) klingt plausibel. Das für die Sicherheit im CNPV LSA verantwortliche übergeordnete Managementsystem der dBBM-Netzknoten erkennt nach Aussage des Ministeriums des Innern eventuelle Manipulationen an den dBBM und verwirft diese durch die eigene, zentrale Konfiguration. Eine Überprüfung dieser

Mechanismen und deren Implementierung muß im Rahmen der anstehenden Erstellung eines Sicherheitskonzepts für das ITN-LSA durch das zuständige Ministerium des Innern mit in Erwägung gezogen werden.

Der 6. Gesamtplan der Informationstechnik - 2000, den das Ministerium des Innern jährlich auf der Grundlage der Ressortpläne erstellt, beziffert die Anzahl der an das ITN-LSA angeschlossenen Behörden und Dienststellen mittlerweile auf über 400. Die Anzahl der Arbeitsplatz-PC in den Ressorts und deren nachgeordneten Einrichtungen hat sich gegenüber 1999 (17.754) auf 20.552 Ende des Jahres 2000 erhöht. Damit sind die Ausstattung der obersten Landesbehörden mit PC-Technik und ihre ausreichende Vernetzung im wesentlichen abgeschlossen. In 9 von 11 Obersten Landesbehörden wird ein PC-Ausstattungsgrad zwischen 90 und 100 % erreicht. Lediglich das Kultusministerium und das Ministerium der Justiz liegen erst bei ca. 80 %. Bei 8 von 11 Obersten Landesbehörden liegt der Vernetzungsgrad bei 100 %. Nur das Ministerium des Innern, das Ministerium der Justiz mit jeweils ca. 80 % und der Landesrechnungshof mit ca. 40 % Vernetzungsgrad haben noch Nachholbedarf.

6.2 Das IT-Leitbild der Landesregierung

Die Landesregierung hat im zurückliegenden Berichtszeitraum einen Schwerpunkt ihrer Arbeit auf die konzeptionelle Gestaltung zur zukünftigen Entwicklung des IT-Einsatzes in der Landesverwaltung gelegt.

Ausgangspunkt dieser Aktivitäten bildete das im Auftrag des Ministerium des Innern erstellte Gutachten zur „Organisations- und Wirtschaftlichkeitsuntersuchung der Informationstechnik im Land Sachsen-Anhalt“ vom 31.3.1999. Die Untersuchung umfaßte die großen Infrastruktureinrichtungen der Informationstechnik der Ressorts Inneres, Finanzen, Justiz und Landwirtschaft. Nach Auswertung dieses Gutachtens erfolgte durch die Landesregierung die Bildung einer Projektorganisation mit einer Steuerungsgruppe auf der Ebene der Staatssekretäre

sowie die Einsetzung einer Projektgruppe KIT LSA („Konzeption für die Informations- und Kommunikationstechnik des Landes Sachsen-Anhalt“). Das durch die Projektgruppe KIT LSA erarbeitete **IT-Leitbild LSA** wurde am 20.03.2000 durch die Steuerungsgruppe verabschiedet und veröffentlicht.

Als ein Ziel soll bei der Bereitstellung von Diensten zur umfassenden Kommunikation, Kooperation und Information die Verfügbarkeit, Vertraulichkeit und die Integrität der Information gewährleistet werden.

Inwieweit der Begriff „Information“ auch die personenbezogenen Informationen über die Bürgerinnen und Bürger einschließt und damit auch der im Grundgesetz geschützte und zusätzlich in der Verfassung des Landes Sachsen-Anhalt verankerte Schutz des Persönlichkeitsrechts gewährleistet wird, ist dem IT-Leitbild nicht weiter zu entnehmen.

Die Beachtung der datenschutzrechtlichen Grundsätze der Datensparsamkeit, der Erforderlichkeit, der Verhältnismäßigkeit sowie die Realisierung wirksamer Maßnahmen der Datensicherheit erachtet der Landesbeauftragte als unabdingbare Voraussetzung auf dem Weg in die Informationsgesellschaft. Die Erwähnung des Datenschutzes im IT-Leitbild hätte hier ein Zeichen setzen können.

Wiederholt hat der Landesbeauftragte in den zurückliegenden Jahren auf Defizite beim Datenschutz und bei der Datensicherheit hingewiesen. Regelungsbedarf bzw. Nachholbedarf sieht er bei zentralen Themen wie:

- dem Sicherheitskonzept für das Landesnetz (ITN-LSA),
- dem Projekt TESTA-Deutschland,
- der Neufassung der IT-Grundsätze für die Landesverwaltung,
- der einheitlichen Regelung zur Nutzung des E-Mail-Dienstes,
- dem Aufbau eines zentralen Verzeichnisdienstes einschließlich der Public Key Infrastruktur (PKI) des Landes sowie der zukünftigen Anwendungen beim e-government.

Der Rechtsverantwortung der Obersten Landesbehörden nach § 14 Abs. 1 DSG-LSA kommt gerade bei der Planung und Einrichtung landesweiter Verfahren zur Verarbeitung personenbezogener Daten bzw. bei der umfassenden Vernetzung

zur Schaffung landes- bzw. weltweiter Kommunikationsbeziehungen eine Schlüsselrolle zu.

Im Rahmen der Erfüllung eigener Aufgaben trifft diese Verantwortung nach § 14 Abs. 1 DSG-LSA auch die Gemeinden und Landkreise.

6.3 Fehlendes Sicherheitskonzept für das Landesnetz (ITN-LSA)

Bereits im März 1995 (vgl. II. Tätigkeitsbericht S. 37) hatte der Landesbeauftragte auf das fehlende, bis heute noch nicht vorliegende Sicherheitskonzept für das ITN-LSA hingewiesen. Ab September 1995 wurde vom Netzbetreiber die verschlüsselte Datenübertragung von Sozialdaten im Landesnetz in den Regelbetrieb überführt.

Im März 1997 stellte der Landesbeauftragte in seinem III. Tätigkeitsbericht (vgl. S. 31 f) fest, daß das Ministerium des Innern nicht über einen Entwurf für das Sicherheitskonzept hinausgekommen war. Allerdings wurde für den Anschluß des ITN-LSA an das Internet die Zertifizierung der eingesetzten Firewalltechnik vorbereitet, die ein wesentlicher Bestandteil des Gesamtsicherheitskonzeptes für das Land sein sollte. Die Zertifizierung sollte durch das BSI erfolgen. Dabei kam es durch das starke Engagement des Herstellers der Firewallsoftware bei der Einführung des Informationsverbundes Bonn-Berlin (IVBB) zu einer erheblichen Verzögerung. Die spätere Grundsatzentscheidung des Ministeriums des Innern, eine weitere Verzögerung bei der Ausarbeitung des Sicherheitskonzepts zugunsten einer höherwertigen Zertifizierung in Kauf zu nehmen, wurde auch vom Landesbeauftragten mitgetragen.

Im März 1999, beim Abschluß des IV. Tätigkeitsberichtes, begründete die Landesregierung das weitere Fehlen eines Sicherheitskonzepts für das ITN-LSA mit personellen Engpässen beim Ministerium des Innern.

Auch im März 2001 liegt dem Landesbeauftragten **kein** prüffähiges Sicherheitskonzept für das ITN-LSA vor. Dabei wäre dies - angesichts der vielfältigen Aktivitäten der Landesverwaltung im Internet bzw. auf dem von seiten der Politik

propagierten Weg in die sog. „Informationsgesellschaft“ dringender erforderlich denn je.

Für die Nutzung der von der Landesregierung so gerne als modernen Kommunikationsweg herausgestellte „Datenautobahn“ muß es Verkehrsregeln geben! Im übrigen steht die Landesregierung unter den gesetzlichen Forderungen des § 6 DSG-LSA.

Aus den Protokollen der regelmäßig stattfindenden Netzberatungen im TPA hat der Landesbeauftragte entnehmen können, daß das Ministerium des Innern mit der Telekom AG im Dezember 2000 die Erstellung eines Sicherheitskonzepts für das ITN-LSA vereinbart hat. Das ist nach langer Zeit eine gute Nachricht. Allerdings fehlt bisher dem Landesbeauftragten die dazu gesetzlich vorgeschriebene umfassende Information durch die Landesregierung (§ 22 Abs. 4 Satz 2 DSG-LSA).

Für bedenklich hält der Landesbeauftragte die Tatsache, daß in den News-Gruppen des Intranets die zum Teil vertraulichen Informationen zu Sicherheitsfragen des Landesnetzes für **jeden** Intranet-Nutzer abrufbar sind. Bereits da muß eigentlich schon das Sicherheitskonzept des ITN-LSA einsetzen. Detaillierte Informationen zur Struktur und den Diensten sollten nur einem begrenzten Personenkreis zugänglich sein. Eine allgemeine Information der Ressorts im IMA-IT zur Entwicklung des Landesnetzes dürfte ausreichend sein.

Ziel muß es nun sein, daß das Ministerium des Innern schnellstmöglich dieses Sicherheitskonzept für das ITN-LSA einschließlich der Regelungen zur Nutzung der Internetdienste ausarbeitet, mit den anderen Ressorts abstimmt und bis zum Jahresende auf dem Erlaßwege für die Landesverwaltung verbindlich festlegt.

Als ein positives Beispiel ist das „Sicherheitskonzept Kommunikation NRW“ vom 25.01.2000 (MBl. NRW S. 152) des Landes Nordrhein-Westfalen zu nennen.

Ein solches Konzept kann ohnehin nur Mindestsicherheitsstandards festlegen. Die Ressorts haben im Rahmen ihrer eigenen Rechtsverantwortung nach § 14 Abs. 1 in Verbindung mit § 6 Abs. 2 DSG-LSA für sich und ihren nachgeordneten Bereich weitere Schutzvorkehrungen bei der Verarbeitung personenbezogener

Daten zu treffen, wenn dies die Sensibilität der personenbezogenen Daten, die Einsatz- und Verarbeitungsbedingungen sowie das damit verbundene Gefährdungspotential zur Sicherung schutzwürdiger Interessen der Betroffenen erfordern.

Für notwendig hält der Landesbeauftragte auch die Schaffung eines ständigen Gremiums, das sich mit der **zukünftigen** konzeptionellen Gestaltung der IT-Sicherheit und der Fortschreibung des Sicherheitskonzepts des ITN-LSA unter den sich immer schneller verändernden Bedingungen in der IT-Entwicklung auseinandersetzt.

Der Landesbeauftragte verweist im Rahmen seines gesetzlichen Beratungsauftrages auch auf die aktuelle **Broschüre** zum Thema „Datenschutz bei der Nutzung von Internet und Intranet“ (Redaktionsschluß 15.12.2000). Sie wurde vom Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder erstellt und vom Landesbeauftragten an die Landesverwaltung und die Kommunen verteilt. Der Text ist auch auf der Homepage des Landesbeauftragten im Intranet und Internet eingestellt und so für jedermann online verfügbar.

6.4 Projekt TESTA Deutschland

Der Landesbeauftragte hatte erstmalig in seinem IV. Tätigkeitsbericht (vgl. S. 23 f) über dieses europäische Projekt, an dem sich auch das Land Sachsen-Anhalt unter dem Begriff „TESTA Deutschland“ seit Dezember 1999 beteiligt, berichtet. Das Land ist dem Rahmenvertrag im Januar 2000 beigetreten. Ziel dieses ehrgeizigen Projektes ist die Realisierung einer einheitlichen Kommunikationsplattform für den Datenaustausch

- zwischen den Bundesländern, den obersten Bundesbehörden und den Bundeseinrichtungen,
- der Bundesländer mit dem Bundesrat und dem Bund,
- der Bundesländer zu ihren Landesvertretungen in Brüssel, sowie

- zukünftig zu den EU-Mitgliedstaaten und der EU und auch
- mit und zwischen kommunalen Einrichtungen.

Hierzu erfolgt für das jeweilige Landesverwaltungsnetz (hier das ITN-LSA) der Anschluß an TESTA Deutschland über **einen** Lokationszugang.
Bereits im September 2000 verfügten alle 16 Bundesländer über entsprechende Lokationzugänge (mit Bandbreiten zwischen 64 bis 256 kBit/s). Auch die obersten Bundesbehörden über den IVBB sowie weitere Bundeseinrichtungen, wie das Statistische Bundesamt, das Bundesamt für Finanzen, das Zentrale Staatsanwaltschaftliche Verfahrensregister beim Generalbundesanwalt, das Rechenzentrum für die Finanzverwaltung der Oberfinanzdirektionen der Bundesländer sowie das Kraftfahrtbundesamt, Dienstleister wie die juris GmbH, das FISCUS TESTA-Subnetz, das Netz des Verbandes der Rentenversicherer und auch Kommunen verfügen über eine Kommunikationsverbindung zu TESTA Deutschland.

Bereits die Aufzählung der bisher Beteiligten läßt leicht erkennen, daß in diesem Projekt Sicherheitskriterien wie Verfügbarkeit, Integrität und natürlich die Vertraulichkeit des Datenaustausches eine wesentliche Rolle spielen.

Nach den Informationen, die dem Landesbeauftragten durch Recherchen im Intranet des Landes zur Verfügung stehen, sind durch das IP-Konzept und die Leitungsverschlüsselung in TESTA-Deutschland bereits Sicherheitsmaßnahmen durch den Netzprovider, d.h. die Deutsche Telekom AG und durch die beteiligten Nutzer getroffen worden, die vom Landesbeauftragten begrüßt werden. Hierzu gehören die Umsetzung von Maßnahmen wie:

- kein Zugang zum Internet über TESTA Deutschland,
- Routing nicht öffentlicher IP-Adressen in TESTA Deutschland,
- Network-Adress-Translation (NAT) am Local Domain-Zugang beim Nutzer,
- Leitungsverschlüsselung zwischen den Lokationsstandorten durch Installation von Krypto-Boxen zwischen der Nutzer- und Providerschnittstelle am Standort des Nutzers.

Eine offizielle Information über den bisher erreichten Sicherheitsstandard des Anschlusses des Landesverwaltungsnetzes an TESTA Deutschland und weitere Vorhaben hat den Landesbeauftragten allerdings vom zuständigen Ministerium des Innern noch nicht erreicht. Die gesetzliche Verpflichtung dazu besteht auch hier nach § 22 Abs. 4 Satz 2 DSG-LSA.

Viele Problembereiche sind noch ungelöst. Der Landesbeauftragte hält z.B. die derzeitige Realisierungsform der Nutzerschnittstelle nur über einen Nutzer-Router mit NAT trotz dazwischengeschalteter Krypto-Box und der Übertragung der nicht öffentlichen 192er IP-Adresse vom Router des Netzproviders zukünftig für **nicht** ausreichend. Die nicht öffentlichen 192er IP-Adressen sind zwar im Internet nicht routbar. Wie aber die Deutsche Telekom AG als Netzprovider dem Mißbrauch **innerhalb** des bundesweiten Intranets TESTA Deutschland begegnet, wurde dem Landesbeauftragten noch nicht erläutert.

Deshalb sollte das Ministerium des Innern die jetzige Anbindung an TESTA Deutschland im Rahmen der Untersuchungen zum Sicherheitskonzept des ITN-LSA, als Übergang in ein Fremdnetz, mit in die Untersuchungen einbeziehen. Der Landesbeauftragte hält als Nutzerschnittstelle den Einsatz eines Proxy-Servers oder einer weiteren Firewall für erforderlich. Er geht davon aus, daß er über den Fortgang der Untersuchungen und deren Ergebnis zeitnah unterrichtet wird.

Mit dem Einsatz von TESTA kommen aber auf die öffentlichen Stellen des Landes auch materielle datenschutzrechtliche Probleme zu. Das vom Deutschen Bundestag am 15.02.2001 verabschiedete Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) bildet dabei nur den Anfang.

Neben dem SigG wird der Bundesgesetzgeber in naher Zukunft im Privatrecht neue Formvorschriften zur Erleichterung des elektronischen Rechts- und Geschäftsverkehrs hinsichtlich der elektronischen Unterschrift als Substitut der eigenhändigen Unterschrift und die elektronische Form als Option zur Schriftform sowie hinsichtlich der Vereinfachung des Rechtsverkehrs durch die Zulassung einer Textform für unterschriftslose Erklärungen einführen. Vorgesehen sind

Änderungen im BGB (z.B. Einfügung der §§ 126a u. 126b) und der ZPO (z.B. §§ 130a, 292a, 299a) sowie weiterer 31 Gesetze und Verordnungen (vgl. BT-Drs. 14/4987).

6.5 Verzeichnisdienste

Die vom Landesbeauftragten vorstehend dargestellte rasante Entwicklung bei der Vernetzung im Intranet des Landes und darüber hinaus bundesweit (TESTA Deutschland) und die Verbindung zum Internet macht für moderne Kommunikationsformen (z.B. E-Mail) auch neue Arten der Verbreitung der Kommunikationsadressen notwendig. Dies geschieht durch Verzeichnisdienste.

Vereinfacht dargestellt handelt es sich bei einem Verzeichnisdienst um ein ständig aktuelles „elektronisches Adreßbuch“, welches, ähnlich dem bekannten Telefonbuch, Auskunft zu Kommunikationsadressen von Organisationen und Personen ermöglicht.

Durch die Internationale Organisation für Standardisierung (ISO) wurde bereits 1988 für die Beschreibung eines solchen Verzeichnisdienstes ein Referenzmodell geschaffen und unter der Bezeichnung **X.500** bzw. **X.509** eingeführt.

Der X.500-Verzeichnisdienst ist ein hierarchisch aufgebautes Datenbanksystem, bestehend aus lokalen Informationen in den sog. Directory System Agents (DSA) und der Directory Information Base (DIB). Ist bei der Anfrage eines Directory User Agent (DUA) an einen DSA die Information nicht bekannt, wird diese Anfrage an andere Datenbanken (DSA) weitergeleitet. Diese Prozedur wird solange wiederholt bis die Information gefunden ist.

Verzeichnisdienste nach dem X.500/X.509 Standard bieten die Möglichkeit, durch ein standardisiertes Protokoll beliebige Informationen zu Objekten und Personen zu speichern. Damit besteht die Möglichkeit, in einem einzigen zentralen Verzeichnis (Directory) alle wichtigen Daten über einen Nutzer, also auch **personenbezogene Daten**, zu speichern und diese allen angeschlossenen Systemen zugänglich zu machen. Der Zugriff auf die Daten des Directory erfolgt durch ein eigenes Zugangsprotokoll, dem Directory Access Protocol (DAP).

Überwiegend wird aber heute eine vereinfachte Form dieses Protokolls, das Lightweight Directory Access Protocol (LDAP), auf den Clients eingesetzt. Es bietet die Möglichkeit, eine Authentifizierung von Benutzern gegenüber dem Directory festzulegen.

Als fortentwickeltes Modell hat sich heute der X.509 Standard in der Praxis durchgesetzt. Vor allem in der Version **X.509 Teil 3** (X.509v3; 1996) als Authentifizierungsstandard für Kommunikationsnetze (sog. X.509-Zertifikate).
Dieser Teil 3 beschreibt ein Format für digitale **Zertifikate,** die von einer dritten, vertrauenswürdigen, unabhängigen Instanz (Trust Third Party) signiert werden und ein Format für Sperrlisten. Eine solche dritte, unabhängige Instanz kann z.B. ein sog. Trust Center sein. Dabei hat das digitale Zertifikat eines Trust Centers die Funktion, den Namen und den öffentliche Schlüssel eines Anwenders miteinander sicher in Verbindung zu bringen.

Nach Inkrafttreten des Signaturgesetzes (SigG vom 22.07.1997, BGBl. I S. 1870) und der Signaturverordnung (SigV vom 22.10.1997, BGBl. I S. 2498) wurde der X.509v3-Standard durch das BSI in Zusammenarbeit mit der Gesellschaft für Mathematik und Datenverarbeitung vor allem um rechtliche Inhalte erweitert. Dazu gehören folgende Zertifikatsfelder:

- Nutzungsbeschränkungen (sog. Attribut-Zertifikat des Trust Centers)
- Erstellungsdatum (des Zertifikats)
- Vertretungsvollmacht (für Dritte)
- Zulassung (Bescheinigung des Trust Centers für Zulassung z.B. als Anwalt, Notar u.ä.)
- Beschränkungen (z.B. bis zu welchem Geldbetrag der Anwender mit seinem Zertifikat bürgt).

Mit der sog. **Sperrliste** (auch schwarze Liste genannt) kann ein Trust Center ausgegebene Zertifikate, z.B. bei Verlust des geheimen Schlüssels durch den Anwender, für ungültig erklären (sperren).

Das Vorhalten bzw. das zum Abruf bereithalten dieser Zertifikate der Anwender und der Sperrliste durch das Trust Center bildet eine der wesentlichen Voraussetzungen zum Aufbau einer Public Key Infrastruktur (PKI).

Dem Vorteil eines Verzeichnisdienstes stehen aber auch Nachteile gegenüber. So sind die Administratoren solcher Verzeichnisdienste in der Lage, alle zu einer Person gespeicherten Daten einzusehen. Schwache Authentifizierungsmechanismen und die oberflächliche Nutzung der Zugriffskontrollmechanismen, was anderen Nutzern möglicherweise Mißbrauch erleichtert, sind weitere Risikofaktoren, die zu einer Verletzung des Datenschutzrechtes in diesem Bereich führen können.

Weitergehende Informationen finden sich in der vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgegebenen Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten“ (Stand: September 2000). Auch diese Orientierungshilfe ist auf der Homepage des Landesbeauftragten eingestellt und kann auch bei ihm abgefordert werden.

7. Finanzwesen

7.1 Änderung der Abgabenordnung

Der Landesbeauftragte hat in seinen bisherigen Tätigkeitsberichten (zuletzt IV. Tätigkeitsbericht, S. 28 f) stets auf die Erforderlichkeit von datenschutzrechtlichen Verbesserungen in der Abgabenordnung (AO) hingewiesen.

Die bisher über die Erhebung, Verarbeitung und Nutzung von Daten vorhandenen Regelungen in der AO erfassen nicht alle datenschutzrechtlich relevanten Sachverhalte, wie z.B. die Frage des Auskunfts- und Akteneinsichtsrechts, des Berichtigungsanspruchs, des Löschungsanspruchs, des Anspruches auf Sperrung von Daten und auf Schadenersatz bei datenschutzrechtlichen Verstößen.

Die Bemühungen der Datenschutzbeauftragten des Bundes und der Länder scheiterten aber bisher an der mangelnden Bereitschaft der obersten Finanzbehörden des Bundes und der Länder zu datenschutzrechtlichen Verbesserungen.

In dieser Hinsicht scheint sich nun ein Sinneswandel anzubahnen. Nach entsprechenden Signalen aus dem Bundesministerium der Finanzen (BMF) haben die Datenschutzbeauftragten des Bundes und der Länder die wünschenswerten und notwendigen Änderungen der Abgabenordnung in einem gemeinsamen Schreiben an das BMF zusammengestellt. Dieses Schreiben soll bei den vorgesehenen Gesprächen mit dem BMF als Gesprächsgrundlage dienen.

Der Landesbeauftragte erwartet zur gebotenen Novellierung der Abgabenordnung auch eine entsprechende Unterstützung durch die Landesregierung.

7.2 Fahrtenbücher von Ärzten mit Patientendaten

Zwischen den obersten Finanzbehörden des Bundes und der Länder und den Datenschutzbeauftragten des Bundes und der Länder wurde die Frage kontrovers diskutiert, ob die Finanzverwaltung für Zwecke der ertragsteuerlichen Behandlung der Nutzung betrieblicher Kraftfahrzeuge für Privatfahrten Ärzte verpflichten kann, in einem Fahrtenbuch Name und Anschrift der aufgesuchten Patienten aufzuführen.

Die Datenschutzbeauftragten des Bundes und der Länder haben dabei die Auffassung vertreten, daß es den Ärzten als einer der in § 102 Abs. 1 Nr. 3c AO genannten Berufsgruppen aufgrund der ihnen obliegenden Verschwiegenheitspflicht verwehrt ist, ein Fahrtenbuch nach den Vorstellungen der Finanzverwaltung zu führen. Die Vorschrift räumt dieser Berufsgruppe ein Auskunftsverweigerungsrecht ein, das auch Name und Anschrift der behandelten Patienten mit umfaßt.

Nach langwierigen Verhandlungen mit dem Bundesbeauftragten für den Datenschutz hat das Bundesministerium der Finanzen nunmehr folgende Regelung getroffen:

Zu Reisezweck, Reiseziel und Reiseroute reicht neben der Angabe des Datums, des Kilometerstands und des Zielorts grundsätzlich die Angabe „Patientenbesuch“ aus, wenn Name und Adresse der Patienten vom Arzt in einem vom Fahrtenbuch getrennt zu führenden Verzeichnis festgehalten werden. Die Vorlage dieses Verzeichnisses darf dann nur verlangt werden, wenn tatsächliche Anhaltspunkte vorliegen, die Zweifel an der Richtigkeit oder Vollständigkeit der Eintragungen im Fahrtenbuch begründen und die Zweifel anders nicht auszuräumen sind.

Die bisher strittige Frage, ob ein Arzt im Hinblick auf § 102 Abs. 1 Nr. 3c AO die Bekanntgabe von Name und Anschrift seiner Patienten in einem Fahrtenbuch verweigern darf, wird damit zwar noch nicht grundsätzlich gelöst, aber die praktische datenschutzrechtliche Bedeutung deutlich reduziert.

Das Ministerium der Finanzen des Landes hat hierzu auf Anfrage mitgeteilt, daß es die Entscheidung des Bundesministeriums der Finanzen der OFD mit der Bitte übersandt habe, die Finanzämter des Landes in geeigneter Weise zu unterrichten.

7.3 Verfahrensmängel bei der Versendung von Beitragsbescheiden

Gegen die ihrer Meinung nach falschen Bescheide über Anschlußbeiträge hatten eine Vielzahl betroffener Bürger bei ihrer Stadt Widerspruch eingelegt. Aus Gründen der Kostenersparnis ließen sie sich dabei von **einem** Rechtsanwalt vertreten.

Die Stadt sah ihren Fehler ein und erließ einen neuen (korrekten) Bescheid und fügte dem gleichen Schreiben auch den Abhilfebescheid für den eingelegten Widerspruch bei. Dabei unterlief ihr ein datenschutzrechtlich pikanter Fehler:

Der in allen Fällen gleichlautende Abhilfebescheid war mit einer Sammeladressatenliste versehen. Jeder Empfänger konnte nun Namen und Anschrift aller anderen Widerspruchsführer lesen und - im Umkehrschluß auch erkennen - wer keinen Widerspruch eingelegt hatte.

Ein aufmerksamer Betroffener beschwerte sich deshalb beim Landesbeauftragten.

Der mußte dem Bürger Recht geben, denn eine Rechtsgrundlage für die Übermittlung der Sammeladressen ergibt sich weder aus einer bereichsspezifischen Regelung (z.B. Verwaltungsverfahrensgesetz) noch aus dem DSG-LSA. Auch eine Einwilligung (§ 4 Abs. 1 DSG-LSA) zur Datenübermittlung aller Namen und Anschriften hat nicht vorgelegen. Daran änderte auch nichts, daß das Widerspruchsverfahren nur von einem Rechtsanwalt für alle betrieben wurde.

Unter Berücksichtigung der Stellungnahme der Stadt hat der Landesbeauftragte ausnahmsweise von einer förmlichen Beanstandung nach dem DSG-LSA abgesehen, weil dieses Fehlverhalten nicht bewußt, sondern durch Unachtsamkeit geschehen war, die übermittelten Einzeldaten inhaltlich überschaubar blieben und durch die verbundenen Vorverfahren Grundzüge der gemeinsamen Widersprüche bereits einem größeren Personenkreis bekannt waren.

Der Landesbeauftragte hat die betreffende Stadt aber aufgefordert, künftig die gesetzlichen Vorgaben zur Datenübermittlung genau zu beachten.

7.4 Fehlerhafte Mahnbescheide einer Landeskasse

Wie der Landesbeauftragte zunächst Presseberichten entnahm, wurden Ende Juni 1999 durch eine Landeskasse rund 57.000 Mahnbescheide verschickt. Das ist an sich ein alltägliches Verfahren, aber in einer Vielzahl von Fällen ergingen die Mahnbescheide, obwohl die angeforderten Beträge längst entrichtet worden waren.

Die daraufhin vom Landesbeauftragten bei der Kasse getroffenen Feststellungen ergaben ein peinliches Bild:

Die Mahnbescheide waren automatisiert erstellt und verschickt worden, obwohl zum Zeitpunkt der Mahnung die Kasse noch ca. 64.000 Zahlungseingänge nicht buchungsmäßig zugeordnet hatte.

Zum Zeitpunkt der Feststellungen zogen sich diese Mängel bereits seit Ende 1998 hin, ohne daß ausreichende Anstrengungen zu erkennen waren, den Zustand in den Griff zu bekommen.

Der Landesbeauftragte hat das Ministerium der Finanzen darauf hingewiesen, daß es aus datenschutzrechtlicher Sicht nicht vertretbar sei, Bürger - zumal in dieser Vielzahl - mit fehlerhaften Mahnbescheiden zu überziehen. Der Bürger habe einen Rechtsanspruch darauf, daß nur richtige bzw. richtig zugeordnete Daten verarbeitet werden (§ 16 Abs. 1 DSG-LSA), er nicht wegen von öffentlichen Stellen zu vertretender Fehler und Mängel unzutreffend in Anspruch genommen werde und bei ihm amtshaftpflichtrelevante neue Kosten entstünden. Der Landesbeauftragte hat außerdem angekündigt, künftige Betroffene nicht nur auf die allgemeinen Regeln des Schadenersatzes wegen Amtspflichtverletzungen, sondern auch auf die spezielle Vorschrift des § 18 DSG-LSA (Schadenersatz) hinzuweisen, die bekanntlich auch eine Haftung ohne Verschulden vorsieht.

Dem Ministerium der Finanzen war die hohe Anzahl der nicht zugeordneten Zahlfälle nicht bekannt. Eine Kassen- und Geschäftsprüfung bei der Kasse hat die beschriebenen Mängel bestätigt. Mit zusätzlichem Personal wurden die Rückstände abgearbeitet.

Der Landesbeauftragte hat in diesem Fall ausnahmsweise auf eine förmliche Beanstandung verzichtet, weil das Ministerium der Finanzen für eine schnelle Beseitigung der Mängel sorgte.

8. Forschung

Es bestehen weiterhin Probleme bei der Erhebung personenbezogener Daten im Rahmen von Forschungsvorhaben, wie sie auch schon im IV. Tätigkeitsbericht (S. 37 f) angesprochen wurden.

Nach § 9 Abs. 1 DSG-LSA ist das Erheben der personenbezogenen Daten nur zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

Erforderlich im datenschutzrechtlichen Sinne sind personenbezogene Daten nur dann, wenn die Aufgabe ohne Kenntnis der Daten nicht oder nur mit einem unverhältnismäßig hohen Aufwand zu erledigen ist. Das gilt auch für die Erhebung personenbezogener Daten im Rahmen der Freiwilligkeit, also mit Einwilligungserklärung.

Generell ist der Betroffene auf die Rechtsvorschrift, die zur Auskunft verpflichtet, oder auf die Freiwilligkeit seiner Angaben hinzuweisen. Gleiches gilt für eventuelle Folgen der Verweigerung von Angaben und die Möglichkeit des jederzeitigen Widerrufs für die Zukunft (§ 4 Abs. 2 DSG-LSA).

8.1 Ausgewählte Forschungsprojekte:

1. Erfassung nationalsozialistischer Gewaltverbrechen:

   Für die Durchführung dieses Forschungsvorhabens benötigte ein Professor aus den Niederlanden personenbezogene Daten und wandte sich mit seinem Anliegen an das zuständige Ministerium. Das Ministerium bat den Landesbeauftragten um datenschutzrechtliche Bewertung, mit dem Hinweis, man halte eine Datenübermittlung für unzulässig, da der Professor die Daten in die Niederlande übermittelt haben wollte.

   Der Landesbeauftragte bestätigte die Einschätzung des Ministeriums und verwies auf § 13 DSG-LSA. Hiernach ist eine Datenübermittlung ins Ausland nur unter besonders engen Voraussetzungen zulässig, die aber lagen nicht vor.

2. PISA-Studie der OECD:

Die in mehreren europäischen Ländern durchgeführte Studie sah vor, auch an verschiedenen Schulen in der Bundesrepublik Daten bei Schülern und Eltern zu erheben. Einerseits mußte bedacht werden, daß Eltern ihre Einwilligung zu den bei ihnen selbst abgefragten Daten erteilen, andererseits sollten sie ihre Einwilligung für die Befragung ihrer Kinder in den Schulen erteilen. Hierbei mußte berücksichtigt werden, daß Schülerinnen und Schüler mit zunehmendem Alter ein eigenständiges Zustimmungsrecht (je nach Einsichtsfähigkeit) haben.

Die Datenschutzbeauftragten der Länder konnten ihre Forderungen durchsetzen, daß das den Schülerinnen und Schülern zustehende Recht auf informationelle Selbstbestimmung in die Studie aufgenommen wurde. Schülerinnen und Schüler können ihre eigenen personenbezogenen Daten preisgeben (wenn die Eltern eingewilligt haben) aber auch ihre Daten verweigern, obwohl die Eltern eingewilligt haben.

3. Medizinische Netzwerke:

Der Arbeitskreis Wissenschaft und Forschung der Datenschutzbeauftragten des Bundes und der Länder hat sich auch mit den neuen Medizinischen Netzwerken zu befassen. Diese sollen künftig Datenbanken über verschiedene Erkrankungen miteinander verbinden. Die personenbezogenen Daten der Betroffenen sind innerhalb einer Datenbank durch technisch organisatorische Maßnahmen geschützt und stehen nur den behandelnden Ärzten zur Verfügung. Gleichwohl soll unter bestimmten Voraussetzungen auch anderen Ärzten der Zugang zu den personenbezogenen Daten ermöglicht werden (z.B. bei Einwilligung des Patienten). Da dieser Komplex sehr umfangreich ist, konnte er bisher nicht abschließend behandelt werden. Die Landesbeauftragten

haben als vorbereitende Maßnahme eine Arbeitsgruppe gebildet, die sich mit den weiteren speziellen Problemen befaßt.

Des weiteren wurden folgende Forschungsprojekte/Studien in Sachsen-Anhalt datenschutzrechtlich bewertet:

- Organisationskontrolle: Befragung von Publikum im Steueramt,
- Schülerbefragung: Lebenssituationen, Einstellungen, Erfahrungen mit Konflikten,
- Organisationskontrolle: Befragung von Absolventen der Burg Giebichenstein,
- Herzforschung „s.a.p.i.e.n.s.“,
- Forschungsprojekt zum Arztstrafrecht.

8.2 Begleitforschung zur Umsetzung der Kindschaftsrechtsreform

Erst durch Stellungnahmen seiner Kollegen in anderen Bundesländern erhielt der Landesbeauftragte Kenntnis davon, daß dieses Forschungsvorhaben auch in Sachsen-Anhalt durchgeführt wurde.

Das zuständige Ministerium der Justiz wurde daraufhin gebeten, Unterlagen des Forschungsvorhabens zur datenschutzrechtlichen Überprüfung zu übersenden. Das dauerte fünf Monate trotz Erinnerungen. Zu diesem Zeitpunkt lagen bereits 4000 Datensätze bei dem durchführenden Institut vor.

Die kurzfristig erstellte Stellungnahme des Landesbeauftragten mit Hinweisen zur Änderung des Anschreibens an die Teilnehmer der Studie übermittelte das Ministerium an das Institut, allerdings ohne die Umsetzung der datenschutzrechtlichen Hinweise zu überwachen. Nachfragen und Erinnerungen des Landesbeauftragten wurden durch das Ministerium mit dem Hinweis beantwortet, daß das Projekt wohl bereits erledigt sei.

Zwei Monate später - es lagen bereits 7000 Datensätze vor - teilte das Institut dem Landesbeauftragten mit, daß die Änderungen nunmehr eingearbeitet worden seien, was aber nur teilweise zutraf.

Da die Erhebungsphase kurz vor dem Abschluß stand, war es dann nicht mehr möglich, die datenschutzrechtlichen Hinweise vollständig umzusetzen.

Der Landesbeauftragte rügt bei diesem Fall nicht nur die unangemessen lange Reaktionszeit des Ministerium der Justiz, sondern weist erneut darauf hin, daß nur bei rechtzeitiger Beteiligung ein solches Vorhaben auf eine datenschutzgerechte Basis hätte gebracht werden können.

9. Gesundheitswesen

9.1 Auskunftsrechte des Patienten

Im IV. Tätigkeitsbericht (vgl. S. 42 f) hatte der Landesbeauftragte darauf hingewiesen, daß § 10 Abs. 2 der Berufsordnung der Ärztekammer Sachsen-Anhalt nicht mit höherrangigem Recht zu vereinbaren ist, weil diese Vorschrift das uneingeschränkte Auskunftsrecht des Patienten gegenüber dem behandelnden Arzt durch die bisherige Formulierung „ausgenommen sind diejenigen Teile, welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten“ in unzulässiger Weise verkürzt.

Nach intensiver und kooperativer Erörterung dieser besonderen Problematik mit der Ärztekammer Sachsen-Anhalt hat die Kammerversammlung der Ärztekammer Sachsen-Anhalt die strittige Passage der Berufsordnung geändert und die Aufsichtsbehörde die geänderte Berufsordnung der Ärztekammer Sachsen-Anhalt zwischenzeitlich genehmigt.

9.2 Übermittlung medizinischer Daten an die gesetzliche Krankenversicherung

Eine gesetzliche Krankenversicherung forderte von einer Klinik die Kopie der Todesbescheinigung einer dort verstorbenen Patientin, um Schadensersatzansprüche prüfen und durchsetzen zu können.

Der entscheidende Arzt hatte Bedenken und wandte sich an den Landesbeauftragten mit der Bitte um rechtliche Würdigung des Auskunftsverlangens.

Der Landesbeauftragte wies darauf hin, daß neben § 301 SGB V die Vorschrift des § 35 Abs. 5 SGB I die hier problematisierte Übermittlung von Daten Verstorbener regelt. Satz 2 erlaubt die nach § 100 Abs. 1 Ziff. 1 SGB X vorgesehene Auskunft an den Leistungsträger (hier: Krankenversicherung), soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe des Leistungsträgers. Zu den Aufgaben gehört auch die Prüfung und Durchsetzung von Schadenersatzansprüchen.

§ 100 Abs. 1 Ziff. 1 SGB X erlaubt allerdings nur die Übermittlung der für die Durchführung der Tätigkeit **erforderlichen** personenbezogenen medizinischen Daten.

Erforderlich war demzufolge nicht die Übersendung der Todesbescheinigung, sondern nur eine Auskunft über das für den Tod kausale Ereignis und die handelnde(n) Person(en).

Pikanterweise hatte in der Zwischenzeit - ohne Wissen des anfragenden Arztes - eine andere Stelle der Klinik schon die Todesbescheinigung der Krankenversicherung übersandt. Die Bescheinigung wurde auf Aufforderung des Landesbeauftragten bei der Krankenversicherung sofort vernichtet.

9.3 Kontrolle in einer Apotheke

Eine Apothekerin teilte dem Landesbeauftragten mit, daß die staatliche Überwachungsbehörde im Rahmen einer Betriebskontrolle gefordert habe, Rezepte zu kopieren und der Behörde zur Verfügung zu stellen.

Die Apothekerin war mit dieser Forderung so nicht einverstanden und hatte auf den Kopien die Daten von Arzt und Patient unkenntlich gemacht. Dies wiederum stieß auf das Unverständnis der Überwachungsbehörde.

Die datenschutzrechtliche Prüfung des Landesbeauftragten ergab, daß **in diesem Fall** die Anforderung von Rezeptkopien berechtigt war, weil die Überwachungsbehörde ein Bußgeldverfahren wegen eines Verstoßes gegen die

Apothekenbetriebsordnung eingeleitet hatte. Allerdings waren für dieses Verfahren keine personenbezogenen Angaben zu Arzt und Patienten erforderlich. Deshalb war die Schwärzung dieser Daten durch die Apothekerin richtig.

Die vom Landesbeauftragten durchgeführte Beratung hatte Erfolg.

Die Überwachungsbehörde hat durch Dienstanweisung ihre Mitarbeiter angewiesen, künftig in solchen Fällen nur Kopien ohne die Daten von Patient und Arzt zu fordern.

10. Gewerbe, Handwerk und Wirtschaft

10.1 Industrie- und Handelskammern

Die Industrie- und Handelskammern des Landes erheben und verarbeiten personenbezogene Daten in erheblichem Umfang. Eine der größten Datengruppen sind die Daten tausender Kammermitglieder, unter ihnen eine Vielzahl natürlicher Personen.

Die Kammern dürfen die Daten ihrer Kammerzugehörigen nach Maßgabe von § 9 Abs. 6 IHK-G i.V.m. § 11 DSG-LSA an andere öffentliche Stellen, hauptsächlich die Industrie- und Handelskammern in den anderen Bundesländern, übermitteln, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Dabei bedienen sich die Kammern Sachsen-Anhalts und der anderen Bundesländer zur Durchführung dieser Datenübermittlung eines automatisierten Abrufverfahrens, das von einer Gemeinschaftseinrichtung der Kammern, der IHK-GfI, durchgeführt wird (vgl. IV. Tätigkeitsbericht, S. 47 f).

Ein solches **automatisiertes** Abrufverfahren darf in Sachsen-Anhalt jedoch nach § 7 Abs. 1 DSG-LSA nur eingerichtet werden, soweit ein Gesetz dies ausdrücklich zuläßt. Der Landesbeauftragte bemüht sich deshalb seit Jahren beim für die Kammeraufsicht zuständigen Ministerium für Wirtschaft und Technologie darum, eine solche gesetzliche Grundlage für das automatisierte Abrufverfahren zu schaffen.

Nicht zuletzt durch das permanente „Bohren“ des Landesbeauftragten hat der DIHT inzwischen die Initiative übernommen und den Entwurf einer Verordnung über die Einrichtung eines automatisierten Abrufverfahrens der Industrie- und Handelskammern zur gegenseitigen Datenübermittlung vorgelegt.

Allerdings reicht dies noch nicht aus, da nach Art. 80 Abs. 1 GG für den Erlaß einer Rechtsverordnung eine Ermächtigungsgrundlage in einem Gesetz erforderlich wäre. Diese Verordnungsermächtigung soll nun durch Änderung des § 9 Abs. 6 IHK-G geschaffen werden.

Möglicherweise wird - zumindest in Sachsen-Anhalt - das Problem der fehlenden Rechtsgrundlage in Kürze dadurch entschärft, daß der Landesgesetzgeber bei der Novellierung des DSG-LSA u.a. aufgrund der Entwicklung der Informations- und Kommunikationstechnik, insbesondere der zunehmenden Vernetzung, auch den § 7 ändert und erleichterte Zulassungsvoraussetzungen für automatisierte Abrufverfahren schafft.

Nach wie vor ungeklärt ist auch die Vertragsbeziehung zwischen allen Industrie- und Handelskammern und ihrer Gemeinschaftseinrichtung, dem AKB e.V.. Der Verein spielt u.a. bei der Ermittlung der Kammerbeiträge der Mitglieder eine maßgebliche Rolle. Da es sich bei dieser Tätigkeit um eine Datenverarbeitung im Auftrag nach § 8 DSG-LSA handelt, sind bei dem zwischen den beiden Seiten zu schließenden Vertrag bestimmte Formvorschriften einzuhalten. Daran fehlt es bisher, dem Landesbeauftragten liegen aber inzwischen Vertragsentwürfe vor.

Der DIHT verhandelt diese z.Zt. mit der Landesbeauftragten Nordrhein-Westfalen, die freundlicherweise von Seiten der Datenschutzbeauftragten die Federführung übernommen hat. Ziel soll sein, einen einheitlichen, d.h., für alle 16 Bundesländer anzuwendenden Vertragstext zu entwickeln. Dann hätte der AKB e.V. angesichts vieler Kammern im Bundesgebiet nicht viele verschiedene Verträge zu beachten.

Der Landesbeauftragte hofft auf ein baldiges solides Vertragsergebnis.

10.2 Aktualisierung des Datenbestandes einer IHK

Eine IHK hatte die Straßenverkehrsbehörden in ihrem Zuständigkeitsbereich angeschrieben und darum gebeten, sie bei der Aktualisierung ihrer Unternehmensdatei zu unterstützen.

Hintergrund waren u.a. die Änderung gesetzlicher Grundlagen im Güterverkehr, der damit verbundenen neuen Zuordnung der Zuständigkeiten für die Erlaubnis- und Lizenzerteilung (von den Regierungspräsidien auf die Landkreise) und strukturelle Veränderungen des Güterkraftverkehrsgewerbes. Außerdem wollte die IHK ihre Unterlagen des Personenverkehrsgewerbes mit den Daten der Landkreise abgleichen.

Ein Landkreis hatte dagegen datenschutzrechtliche Bedenken.

Der Landesbeauftragte mußte nach Prüfung der Rechtslage der IHK mitteilen, daß die gewünschte Datenübermittlung, zumindest für die Fälle, in denen es sich bei den Gewerbeunternehmen um natürliche Personen handelt, unzulässig wäre.

Der IHK stehen zur Erfüllung ihrer Aufgaben bereits nach § 14 Abs. 5 Nr. 1 GewO sämtliche Daten aus der Gewerbeanzeige, außer dem Feld Nr. 33 (Unterschrift), zu. Diese werden ihr von den Ordnungsämtern übermittelt.

Also müßten bei der IHK unter den genannten Daten aus den Gewerbeanzeigen sämtlicher Gewerbeunternehmen ihres Zuständigkeitsbereiches auch die Daten der Unternehmen des Güterkraftverkehrsgewerbes vorliegen.

Eine erneute Erhebung dieser Daten, und auf eine solche liefe der gewünschte Datenabgleich mit den Straßenverkehrsämtern hinaus, wäre damit schon wegen des Verbotes der Doppeldatenerhebung unzulässig.

Im übrigen wäre seitens der Straßenverkehrsbehörden eine solche Datenübermittlung nur aufgrund einer bereichsspezifischen gesetzlichen Grundlage möglich. Diese fehlt im Straßenverkehrsgesetz.

Der Landesbeauftragte sah auch keine Anhaltspunkte dafür, daß der Gesetzgeber hierfür ein Bedürfnis gesehen hatte. Die IHK konnte auch keine gesetzliche Aufgabe nennen, die ohne die genannten Daten nicht erfüllbar gewesen wäre.

Damit entfiel auch die Prüfung des Rückgriffes auf die allgemeinen Vorschriften des DSG-LSA.

10.3 Öffentliche Bestellung von Sachverständigen

Durch einen Petenten, der bei der Ingenieurkammer des Landes die Ernennung und Bestellung zum Sachverständigen beantragt hatte, ist dem Landesbeauftragten folgender Sachverhalt vorgelegt worden:

Zwischen dem Petenten und der Kammer kam es zu keiner Einigung in bezug auf Umfang und Inhalt der von ihm vorzulegenden Unterlagen zum Sachkundenachweis. Nach Ansicht des Petenten sollte es zum Sachkundenachweis auch möglich sein, die von ihm erstellten und vorzulegenden Gutachten aus Gründen des Persönlichkeitsschutzes der Auftraggeber und anderer Betroffener in **anonymisierter Form** bei der Kammer vorzulegen.

Dagegen argumentierte die Kammer, eine allumfassende Prüfung der besonderen Sachkunde, Zuverlässigkeit und Eignung des Antragstellers sei nur möglich, wenn sie ausschließen könne, daß z.B. vorgelegte Unterlagen von anderen Personen als dem Antragsteller gefertigt worden seien, oder es überhaupt nicht zur Auftragserteilung für ein Gutachten gekommen sei. Eine Prüfung sei insofern nur möglich, wenn ihr Name und Anschrift des Auftraggebers bekannt seien.

Datenschutzrechtlich läuft dies, zumindest für die Fälle, in denen die genannten Gutachten personenbezogene Daten natürlicher Personen, z.B. der Auftraggeber oder Dritter, enthalten, auf eine Datenerhebung und -speicherung durch die Kammer hinaus. Für diese gilt als Körperschaft des öffentlichen Rechts § 4 Abs. 1 DSG-LSA. Weder die Gewerbeordnung noch andere für Kammern geltende spezialgesetzliche Regelungen, wie z.B. das Ingenieurgesetz oder das IHK-Gesetz, enthalten eine gesetzliche Grundlage für eine solche Datenerhebung und -speicherung.

Zwischen der betroffenen Kammer und dem Landesbeauftragten ist deshalb folgende Lösung vereinbart worden:

Den Sachverständigen, die die öffentliche Bestellung beantragen wollen, wird durch die Kammer zukünftig empfohlen, eine Einwilligung der betroffenen Auftraggeber, soweit es sich um natürliche Personen handelt, zur Übermittlung ihrer personenbezogenen Daten an die Kammer und zur Datenerhebung und -speicherung durch die Kammer einzuholen. Sollte diese nicht erteilt werden, wären vorzulegende Gutachten zu anonymisieren. Die Kammer prüft sodann, ob die vorgelegten Unterlagen einschließlich der ggf. anonymisierten Gutachten für die Bewertung von Sachkunde und Zuverlässigkeit des Antragstellers ausreichen, oder ob dies nicht der Fall ist.

Das für die Aufsicht über die Kammern zuständige Ministerium für Wirtschaft und Technologie teilt die Rechtsauffassung des Landesbeauftragten und hält das vereinbarte Verfahren für praktikabel.

10.4 Unzulässige Datenerhebung über Flohmarktteilnehmer

Seit Jahren veranstaltet ein Bürger in Sachsen-Anhalt Flohmärkte ohne rechtliche Probleme. Ein Landkreis aber erteilte ihm die Genehmigung nur mit der Auflage, nach jedem Flohmarkt eine Liste aller Teilnehmer/Aussteller beim Landkreis vorzulegen. Diese Liste sollte dann auch an das Finanzamt weitergeleitet werden.

Dagegen hatte der Bürger Bedenken und wünschte eine datenschutzrechtliche Untersuchung, vor allem, weil unter den Marktbeschickern auch nichtgewerbliche Anbieter sind. Diese bieten z.B. in der Hobbywerkstatt selbst hergestellte Gegenstände in geringer Stückzahl an.

Der Landkreis begründete die erteilte Auflage dem Landesbeauftragten gegenüber damit, daß Märkte gewerbliche Veranstaltungen seien und die Marktteilnehmer gewerberechtliche Vorschriften einzuhalten hätten, wie z.B. das

Anbringen von Name und Firma am Verkaufsstand gem. § 15 GewO, was aber oft unterlassen werde. Im übrigen müßten die Marktbeschicker gem. § 14 Abs. 5 GewO bzw. § 138 AO dem Finanzamt gemeldet werden.

In beiden Punkten irrte der Landkreis und wurde vom Landesbeauftragten auf die auch vom zuständigen Ministerium für Wirtschaft und Technologie geteilte richtige Rechtslage hingewiesen:

Nach § 69a Abs. 2 GewO kann die zuständige Behörde nur im öffentlichen Interesse, insbesondere wenn dies zum Schutz der Veranstaltungsteilnehmer vor Gefahren für Leben oder Gesundheit oder sonst zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und Ordnung erforderlich ist, die Festsetzung eines Marktes mit Auflagen verbinden. Solche Gefahren lagen jedoch unstreitig nicht vor. Die Auflage war deshalb mangels einer Rechtsgrundlage unzulässig. Eventuell fehlende Angaben nach § 15 GewO hat der Landkreis direkt beim Standbetreiber zu bemängeln. Dafür gibt es die Marktaufsicht.

Im übrigen bestand auch keine Rechtspflicht für den Landkreis, dem Finanzamt alle Marktteilnehmer zu nennen. Zu melden hatte der Landkreis dem Finanzamt nur den Veranstalter selbst gem. § 8 Abs. 3 i.V.m. § 6 Ziff. 5 der Mitteilungsverordnung.

Der Landkreis korrigierte seinen Fehler, und das Regierungspräsidium informierte darüber hinaus auch alle anderen Landkreise seines Zuständigkeitsbereiches über die Rechtslage.

10.5 Anforderung einer Betriebsleitererklärung durch eine Handwerkskammer

Eine Handwerkskammer forderte von den Betriebsleitern aller Handwerksbetriebe ihres Zuständigkeitsbereiches eine umfangreiche Erklärung ab. Unter anderem sollten die Betriebsleiter sich damit einverstanden erklären, daß die Handwerkskammer berechtigt sei, bei den zuständigen Stellen (Krankenkasse, Finanzamt u.ä.) Auskünfte über die Art der Beschäftigung und die Höhe des Entgeltes einzuholen. Ziel war, jeweils festzustellen, ob die eingetragenen Unternehmen einen Betriebsleiter beschäftigen, der die Voraussetzungen für die Eintragungen in die Handwerksrolle erfüllt.

Sicherlich hatten viele betroffene Betriebsleiter, die diese Erklärung unterschreiben sollten, Bedenken. Ein Handwerksmeister trug diese dem Landesbeauftragten vor. Das war gut so, denn die Prüfung ergab, daß zwar das Ziel der Kammer dem Gesetz entsprach, aber nicht das Verfahren.

Die Handwerkskammer hatte erkannt, daß die vorgesehene Datenerhebung wegen fehlender gesetzlicher Grundlagen allenfalls durch Einwilligung der Betroffenen möglich war, aber übersehen, daß dies nach den Grundsätzen rechtsstaatlichen Handelns für eine **öffentliche** Stelle nicht ohne weiteres möglich ist.

Selbst eine rechtsgültige Einwilligung befreit die Kammer nicht von der Anforderung, daß die vorgesehene Erhebung der personenbezogenen Daten nur zulässig ist, wenn ihre Kenntnis zur Erfüllung ihrer Aufgaben erforderlich ist.

Aufgaben der Handwerkskammer, die sie nicht ohne diese Daten von Krankenkasse oder Finanzamt erfüllen kann, waren dem Landesbeauftragten bisher nicht bekannt, im übrigen hätte auch das Finanzamt vom Steuergeheimnis befreit werden müssen, um Auskünfte zu erteilen.

Selbst wenn man dies außer Betracht gelassen hätte, so war auch die Einwilligungserklärung nicht rechtsgültig, weil sie weder den Zweck der Datenerhebung genau beschrieb noch die weiteren gesetzlichen Voraussetzungen des § 4 Abs. 2 DSG-LSA erfüllt waren.

Die Handwerkskammer mußte eingestehen, daß zwar ihre Idee von der Kontrolle der Betriebsleiter gut, das gewählte Mittel jedoch untauglich war, weil datenschutzrechtlich unzulässig. Es änderte seine Betriebsleitererklärung entsprechend ab.

10.6 Korruptionsregister

Zu diesem Thema hatte sich der Landesbeauftragte bereits in seinem IV. Tätigkeitsbericht (S. 46 f) geäußert. In ihrer Stellungnahme zum Tätigkeitsbericht hatte damals die Landesregierung erklärt, daß sie die Auffassung des Landesbeauftragten teile, ein Korruptionsregister bedürfe einer bundesgesetzlichen Regelung.

Im Berichtszeitraum hat nun das Ministerium der Finanzen einen erneuten Vorstoß unternommen, eine sog. Melde- und Informationsstelle für Vergabesperren mit einem solchen Register in Sachsen-Anhalt einzurichten. Begründet wird dies mit Erfahrungen anderer Bundesländer, nach denen die Einrichtung einer solchen Melde- und Informationsstelle für Vergabesperren ein wichtiges Instrument zur Korruptionsprävention und -bekämpfung darstellt. Das Ministerium des Innern wurde deshalb vom Ministerium der Finanzen gebeten, die Federführung für das weitere Verfahren zu übernehmen.

Der Landesbeauftragte nahm dazu im Sinne seiner Äußerungen im IV. Tätigkeitsbericht erneut Stellung und erläuterte dem Ministerium der Finanzen ausführlich die Rechtslage, nach der in das Recht auf Schutz der personenbezogenen Daten nur durch oder aufgrund eines Gesetzes, nicht aber durch Ministerialerlaß oder durch eine sonstige Verwaltungsvorschrift, eingegriffen werden darf.

Zu den in den anderen Bundesländern eingerichteten Korruptionsregistern war festzustellen, daß diese entweder auf gesetzlicher Grundlage oder ohne personenbezogene Daten geführt werden, einzelne allerdings auch unter Hinwegsetzen über geltende datenschutzrechtliche Anforderungen ins Leben gerufen worden sind.

Das Ministerium der Finanzen präsentierte schließlich dem Landesbeauftragten einen in Niedersachsen aufgegriffenen Weg. Der Bieter hat dort eine Eigenerklärung abzugeben, mit der er u.a. darin einwilligt, daß seine Daten im Fall seines Wettbewerbsausschlusses wegen Unzuverlässigkeit in ein entsprechendes Register eingestellt und dort befristet gespeichert werden.

Der Landesbeauftragte teilte dem Ministerium der Finanzen mit, daß er seine grundsätzlichen Bedenken gegen ein Korruptionsregister in der vorstehenden Art bis zu einer bundesgesetzlichen Lösung zurückstellen könnte, wenn die Eigenerklärung der Bieter eine ausdrückliche Einwilligung in die beabsichtigte Datenverarbeitung enthält, die Zweckbindung der Daten festgelegt ist und die Erklärung den Formvorschriften des § 4 Abs. 2 DSG-LSA entspricht.

11. Hinweise zum technischen und organisatorischen Datenschutz

11.1 Neue Regelungen zur Datensicherheit

Die derzeitigen Bestimmungen zu technischen und organisatorischen Maßnahmen in den Datenschutzgesetzen von Bund und Ländern - bekannt auch als die „10 Gebote der Datensicherheit“ stammen aus den 70er Jahren. Auch in das DSG-LSA vom 12.03.1992 sind diese Regelungen zur Datensicherheit in § 6 Abs. 2 DSG-LSA übernommen worden.

Nach nunmehr über 20 Jahren ihrer Geltung ist durch die rasante Entwicklung im Bereich der Informations- und Kommunikationstechnik eine Anpassung dieser Regelungen geboten. Nicht zuletzt bedingt durch die schnelle Entwicklung der Informationstechnologie selbst vollzieht sich ein Paradigmenwechsel im Datenschutz. Nicht die zentral ausgerichtete Datenverarbeitung steht mehr im Vordergrund, sondern dezentralisierte und verteilte Strukturen vernetzter multimedialer Systeme, die, wie z.B. das Internet, die Welt zum „globalen Dorf“ verwandeln und vielfältige Möglichkeiten zur Teilnahme an dieser globalen Kommunikation bieten. Dabei werden die Innovationszyklen in der Informationstechnologie immer kürzer, die Entwicklungen immer dynamischer und die Technik selbst immer komplexer.

Deshalb ist es notwendig, künftig neben dem Schutz der Informations- und Kommunikationstechnik den Schutz der personenbezogenen Daten selbst sicherzustellen und hierfür technologieunabhängige **Sicherheitsziele** zu definieren.

Angesichts dieser Entwicklungen wurden durch den ständigen Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der 57. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25./26.03.1999) Empfehlungen für die Vereinheitlichung der Regelung zum technischen und organisatorischen Datenschutz vorgelegt. An den Vorarbeiten einer Arbeitsgruppe war auch der Landesbeauftragte beteiligt.

Ziel dieser Empfehlungen ist es, ein Hilfsmittel für alle am Novellierungsprozeß Beteiligten in Bund und Ländern zu geben und einen Beitrag dazu zu leisten, möglichst **einheitliche**, dem Stand der Technik entsprechende Regelungen zum technischen und organisatorischen Datenschutz zu finden.

Der Landesbeauftragte nahm Kontakt zum Ministerium des Innern auf und leitete diesem die „Empfehlungen für die Vereinheitlichung der Regelungen zum technischen und organisatorischen Datenschutz“ mit der Bitte um Berücksichtigung bei der Novellierung des DSG-LSA zu.

Die Landesregierung hat in ihrem Entwurf eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 27.03.2001 diese Empfehlungen aufgegriffen und für **§ 6 Abs. 2** des Gesetzentwurfes diesen neuen Ansatz vorgesehen.

Die neuen Sicherheitsziele sind:

- **Vertraulichkeit**, d.h. nur Befugte dürfen Daten zur Kenntnis nehmen,
- **Integrität**, d.h. Daten müssen während der Erhebung, Verarbeitung und Nutzung unversehrt, vollständig und aktuell bleiben,
- **Verfügbarkeit**, d.h. Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet oder genutzt werden können,
- **Authentizität**, d.h. Daten müssen jederzeit ihrem Ursprung zugeordnet werden können,
- **Revisionsfähigkeit**, d.h. es muß feststellbar sein, wer wann welche Daten in welcher Weise erhoben, verarbeitet oder genutzt hat,
- **Transparenz**, d.h. die Verfahren zur Erhebung, Verarbeitung und Nutzung müssen nachvollziehbar und aktuell dokumentiert sein.

Diese Sicherheitsziele sind technologieunabhängig und bieten damit einen Sicherheitsrahmen, der auch bei neuen Formen der Datenverarbeitung Bestand haben wird. Auch die EU-Datenschutzrichtlinie bedient sich dieser Begriffe.

Datenschutzkontrollinstanzen und Anwender, d.h. Hard- und Softwareentwickler, Sicherheitsexperten, Systembetreiber, sprechen damit künftig die „gleiche“ Sprache.

11.2 Telefax

Bereits seit seinem II. Tätigkeitsbericht wiederholt der Landesbeauftragte regelmäßig seine Warnungen vor der gewohnheitsmäßigen Verwendung des Telefaxgerätes zur Übertragung personenbezogener Daten. Bekanntermaßen ist das Telefax aus vielerlei Gründen eines der unsicheren Medien zur Datenübermittlung. Ebenso regelmäßig muß er jedoch auch darüber berichten, daß diese Warnungen immer wieder von sorglosen Beschäftigten im Landesdienst ignoriert werden.

Der markanteste Fall im zurückliegenden Berichtszeitraum fand in einem Regierungspräsidium statt. Bei einer Dienstbesprechung mit den Bediensteten der in seinem Zuständigkeitsbereich liegenden Wohngeldstellen und Sozialämter wurde angeordnet, - ausgerechnet im Bereich der besonders geschützten Sozialdaten - zur Geltendmachung von Ansprüchen auf Erstattung von Sozialleistungen gegenüber vorrangig Leistungspflichtigen die Telefaxübermittlung einzusetzen. Besondere dienstliche Gründe dafür gab es nicht.

Einer der Teilnehmer an der Besprechung erinnerte sich an zurückliegende Tätigkeitsberichte des Landesbeauftragten und hinterfragte noch einmal die datenschutzrechtliche Problematik.

Aufgrund der folgenden Intervention des Landesbeauftragten korrigierte das Regierungspräsidium seine Anordnung zur Telefaxverwendung und wies die betreffenden Stellen an, normalerweise den Postweg und nur in absoluten Ausnahmefällen das Telefax zu verwenden. In diesen Fällen sollen dann die im III. Tätigkeitsbericht des Landesbeauftragten (S. 62 ff) genannten Sicherheitsvorkehrungen angewendet werden.

11.3 E-Mail

11.3.1 Generelle Sicherheitsprobleme

Mit der stetigen Zunahme des Anschlußgrades öffentlicher Stellen des Landes an das Internet beobachtet der Landesbeauftragte seit längerem auch die Zunahme des E-Mail-Verkehrs. Mit der Zahl der Benutzer ist aber leider nicht das Wissen um die besonderen Datensicherheitsrisiken bei dieser Übertragungsspielart gestiegen.

Obwohl der Landesbeauftragte in zurückliegenden Tätigkeitsberichten (zuletzt im IV. Tätigkeitsbericht (S. 25 f und 50 f)) wiederholt auf Sicherheitsrisiken und rechtliche Probleme der E-Mail-Nutzung aufmerksam machte und auch der Fachpresse und Berichten in Funk und Fernsehen zunehmend Warnungen und Hinweise auf die Gefahren von jedermann entnommen werden können, bleibt das von den Anwendern weitgehend unbeachtet. Statt dessen häufen sich die Fälle, in denen auch vertrauliche oder sensible personenbezogene Daten auf diesem Wege übertragen werden. Offensichtlich werden die einen gewissen Schutz bietenden Verschlüsselungsmöglichkeiten als zu kompliziert oder einfach lästig abgelehnt.

Es kann - völlig unbemerkt - zum Verlust der Vertraulichkeit der übersandten Informationen ebenso wie zum Verlust der Integrität kommen, d.h., Absender und/oder Inhalt der Nachricht können unbemerkt ge- oder verfälscht werden. Im übrigen ist weder sicher, daß eine E-Mail den Adressaten stets erreicht, noch ist sie stets schneller als ein Fax. Unter Datensicherheitsaspekten sehr problematisch ist auch die Tatsache, daß einige Provider **alle** E-Mails über zentrale Knoten in den Vereinigten Staaten leiten.

Der Landesbeauftragte hält es deshalb für die öffentlichen Stellen des Landes zwingend erforderlich, Regelungen für den Umgang mit E-Mails zu schaffen.
Einen vielversprechenden Ansatz zur Lösung haben die Kommunalen Spitzenverbände erarbeitet, die der Landesbeauftragte bei der Erarbeitung des Musters einer Dienstanweisung für die Benutzung und Behandlung von E-Mail für ihre Mitglieder beriet.

Die bisher in der auf Beschluß der Landesregierung erlassenen gemeinsamen Geschäftsordnung der Ministerien enthaltenen Regelungen zur Behandlung von E-Mails (§§ 16, 26 Abs. 3) reichen nicht aus. Der Landesbeauftragte hält es für angemessen, wenn die Obersten Landesbehörden in diesem Punkt beispielgebend vorangehen. Denkbar wäre eine entsprechende Ergänzung der gemeinsamen Geschäftsordnung oder eine separate Anweisung zur E-Mail-Behandlung.

11.3.2 E-Mail-Computerviren

In seinem IV. Tätigkeitsbericht (S. 54 f) hatte der Landesbeauftragte kurz den seinerzeit aufgetauchten Computervirus "Melissa" dargestellt und empfohlen, Attachments von unerwartet eingegangenen E-Mails überhaupt nicht oder nur in gesicherter Umgebung, d.h., auf einem unvernetzten PC, zu öffnen.

Der Computervirus "Melissa" und, einige Monate später, der als Liebes-E-Mail getarnte Loveletter-Virus, verwenden beide zur Verbreitung das Adreßbuch des E-Mail-Clients Outlook. Das hat zur Folge, daß ein Nutzer den Liebesbrief oder eine andere Virus-Mail von einer Person oder Stelle erhält, die er kennt und von der er möglicherweise bereits E-Mail erhielt, und der er vertraut.

In erster Linie hilft dagegen ein speicherresidentes Antiviren-Programm, das mittels heuristischer Erkennungsmethoden auch bisher unbekannte Computerviren durch ihr spezifisches Verhalten identifiziert und stoppen kann.

Zum Schutz vor Makro-Viren wie "Melissa" sollte zusätzlich bei Programmen wie Winword oder Excel der Makro-Viren-Schutz aktiviert und z.B. in Word 2000 oder Excel 2000 unter "Extras - Makro - Sicherheit" mindestens die mittlere, besser die hohe Sicherheitsstufe eingestellt werden.

Der Loveletter-Virus war ein Visual-Basic-Script-Virus. Diese Eigenschaft war durch seinen besonderen Dateinamen getarnt (LOVE-LETTER-FOR-YOU.TXT. VBS). Leider wird von Windows die verräterische Dateierweiterung ".VBS" nicht angezeigt. Klickt der ahnungslose Nutzer das Liebesbrief-Attachment mit der Dateierweiterung ".TXT" an, um es zu öffnen, führt dies unter Umständen sofort zur Ausführung des bösartigen Scripts.

Schutz gegen solche Viren bieten außer einem residenten Virenscanner, der verdächtige Aktionen stoppt, ein Speichern des unbekannten E-Mail-Attachments auf der lokalen Festplatte und sein Scannen mit einem Viren-Erkennungsprogramm. Dieses sollte mindestens wöchentlich aktualisiert werden.

Der Landesbeauftragte warnt jedoch davor, sich lediglich auf Virenschutzprogramme zu verlassen. Er hält es vielmehr für erforderlich, die Wachsamkeit der Beschäftigten zu schärfen und sie gründlich mit den Funktionen und Sicherheitsmechanismen der durch sie benutzten Computer vertraut zu machen. Hier sind die Verantwortlichen in den öffentlichen Stellen ebenso gefordert wie das Engagement jedes einzelnen. Der nächste Megavirus kommt bestimmt.

11.4 PC-Diebstähle, Jahr-2000-Problem und die unangenehmen Folgen

Nicht immer sind „aller guten Dinge drei".

Diese Erfahrung mußte ein Regierungspräsidium (RP) machen. Über Jahre hinweg kam es in einem abseits gelegenen Gebäudekomplex wiederholt zu Einbruchsdiebstählen, bei denen auch PC entwendet wurden, auf denen personenbezogene Daten, insbesondere **Personaldaten,** gespeichert waren.

Leider hatten die Verantwortlichen aus den Vorfällen in den Jahren 1996 und 1998 nicht die gesetzlich erforderlichen Konsequenzen gezogen. Ein Rückblick soll die Defizite nochmals verdeutlichen:

Erstmals im April **1996** wurde bei einem Einbruchsdiebstahl unter anderem ein PC entwendet, auf dem sich eine **Personaldatei** von ca. 500 Bediensteten befand. Dieser PC war aber mit einer Sicherheitssoftware für den Zugriffs- und Bootschutz und Sicherheitshardware zur Festplattenverschlüsselung ausgerüstet. Da die Personaldaten verschlüsselt gespeichert waren, konnte ausgeschlossen werden, daß die Daten in lesbarer Form in die Hände von Unbefugten gelangt waren. Gleichwohl hatte der Landesbeauftragte mehr äußere Sicherheit

für das Gebäude angemahnt. Dies unterblieb, weil zunächst der Umzug aus dem baulich maroden Objekt zum Ende des Jahres in Aussicht gestellt wurde.

Im Januar **1998** wiederholte sich ein Einbruch in der gleichen Weise, denn man war weder aus dem Gebäude ausgezogen noch hatte man die Sicherheit verbessert. Die vorhandene PC-Technik war von den Tätern bereits zum Abtransport bereitgestellt worden. Dieser wurde aber noch rechtzeitig verhindert.

Im Februar **2000** wurde dort erneut eingebrochen. Neben dem angerichteten Sachschaden war ein erheblicher Verstoß gegen datenschutzrechtliche Bestimmungen festzustellen. Ursache dafür waren Versäumnisse, die mit Nachlässigkeiten bei der Jahr-2000-Umstellung der PC in Verbindung standen.

Bei diesem PC-Diebstahl waren wieder gespeicherte **Personaldaten** verloren gegangen. Anders als 1996 aber waren diesmal alle personenbezogenen Daten unverschlüsselt und in lesbarer Form in den Besitz von Unbefugten gelangt.

Der Grund für dieses schwerwiegende Datensicherheitsdefizit lag in der mangelhaften Überwachung der Datenverarbeitungsprogramme. In diese nach § 14 Abs. 2 Satz 3 DSG-LSA **gesetzlich** vorgeschriebene Überwachung hätte natürlich auch die installierte PC-Sicherheitssoftware auf den Einzelplatz-PC einbezogen werden müssen. Dies galt 1999 besonders unter dem Gesichtspunkt der Sicherstellung der Jahr-2000-Fähigkeit.

Auf die Gefahren, die sich für die Verarbeitung personenbezogener Datenbestände aus dem sog. Jahr-2000-Problem ergeben könnten, hatte der Landesbeauftragte zuvor in seinem IV. Tätigkeitsbericht (S. 48 f) aufmerksam gemacht. Zudem hatten im Jahr 1999 namhafte Hard- und Softwarehersteller umfangreiche Informationen und Testhinweise über die Jahr-2000-Festigkeit ihrer Produkte bereitgestellt. Auch das Ministerium des Innern des Landes Sachsen-Anhalt hatte rechtzeitig dieses Thema aufgegriffen und Hinweise zur Lösung des Jahr-2000-Problems gegeben und veröffentlicht.

In diesem Arbeitsbereich des Regierungspräsidiums aber vergaß man dies alles. Die Sicherheitssoftware war, nachdem sich Anfang Januar 2000 gezeigt hatte, daß sie nicht mehr funktionierte, einfach deaktiviert worden. Damit gab es auch keine verschlüsselte Speicherung von Personaldaten mehr.

Auch der Einsatz des Betriebssystems Windows NT auf den anderen Einzelplatz-PC bot keine ausreichende Sicherheit für die gespeicherten personenbezogenen Daten. Zwar bietet das Betriebssystem in seinen neueren Versionen Sicherheitsfunktionen an, aber das vermeintlich sichere New Technology File System (NTFS) weist Sicherheitsmängel auf.

So ist ein Zugriff auf NTFS-Partitionen für den Normalanwender zwar nicht ohne genauere Sachkenntnis möglich, doch ist zu beachten, daß es sich beim NTFS nur um ein spezifisches Dateisystem von Windows NT handelt und nicht etwa um eine Verschlüsselung von gespeicherten Daten auf der Festplatte eines PC. Mit im Internet frei verfügbaren Programmen, wie z.B. "NTFSDOS", ist deshalb nach einem Booten des PC unter MS-DOS auch der Zugriff auf vorhandene NTFS-Partitionen möglich.

Im vorliegenden Diebstahlsfall konnte bei einigen gestohlenen PC nicht ausgeschlossen werden, daß die darauf gespeicherten personenbezogenen Daten mit Hilfe solcher Tools lesbar gemacht wurden. Deshalb darf auch bei Verwendung des Betriebssystems Windows NT 4.0 auf einem Einzelplatz-PC nicht auf einen Boot-Schutz und auf eine starke Verschlüsselung der gespeicherten personenbezogenen Daten verzichtet werden.

Der Landesbeauftragte hat das Verhalten des Regierungspräsidiums beim Ministerium des Innern formell nach § 24 Abs. 1 DSG-LSA beanstandet.

Gerade bei der automatisierten Verarbeitung von Personalaktendaten müssen umfassende und geeignete technische und organisatorische Maßnahmen nach § 6 Abs. 2 DSG-LSA getroffen werden.

Bei seiner Abwägung nach § 24 Abs. 3 DSG-LSA hat der Landesbeauftragte berücksichtigt, daß es sich nicht um einen Einzelfall handelte, sonders bereits in der Vergangenheit in Anbetracht der Diebstähle von PC-Technik Versäumnisse

bei der Datensicherheit und der Umsetzung technischer und organisatorischer Maßnahmen festzustellen waren. Des weiteren war zu berücksichtigen, daß es im letzten Diebstahlsfall viele eingespeicherte Personen gab, deren datenschutzrechtliche Belange betroffen waren. Die schwerwiegenden Verstöße gegen die Bestimmungen zur Datensicherheit hätten ohne größeren finanziellen und personellen Aufwand vermieden werden können und nach § 6 DSG-LSA auch vermieden werden müssen.

Das für die Aufsicht zuständige Ministerium des Innern räumte die Versäumnisse ein und sah die Beanstandung als berechtigt an. Es veranlaßte neben der umgehenden Installation von PC-Sicherheitssoftware weitere Maßnahmen zur Sicherung des Gebäudes.

12. Kommunalverwaltung

12.1 Datenschutz in der allgemeinen Dienstanweisung

Anläßlich einer Kontrolle stellte der Landesbeauftragte fest, daß die Allgemeine Dienstanweisung einer Kommunalverwaltung in sensiblen Arbeitsbereichen datenschutzrechtliche Lücken aufwies.

So hatte der Landesbeauftragte bereits im II. Tätigkeitsbericht (vgl. S. 56) darauf hingewiesen, daß an einen in einer Behörde tätigen Arzt gerichtete Briefe diesem ungeöffnet vorzulegen sind. Dennoch enthielt die Allgemeine Dienstanweisung dazu keine Regelung.

Darüber hinaus wurde festgestellt, daß auch die besonderen Postbehandlungsvorschriften nach § 5 Abs. 3 der GemKVO (die an die Gemeindekasse gerichteten Sendungen sind ihr ungeöffnet vorzulegen) und nach § 22 Abs. 2 der Dienstanweisung für Standesbeamte (der Dienstvorgesetzte des Standesbeamten ist nicht befugt, an den Standesbeamten gerichtete Post zu öffnen) keinen Niederschlag in der Allgemeinen Dienstanweisung gefunden hatten.

Im Hinblick auf die besondere Sensibilität der Sozialdaten sind auch die Vorschriften nach § 35 SGB I und § 16 SGB I beachtlich. Briefe, die erkennbar an einen Leistungsträger (vgl. §§ 18 ff SGB I) gerichtet sind und bei einer Gemeinde eingehen, sind dem Leistungsträger unverzüglich ungeöffnet zur weiteren Bearbeitung zuzuleiten.

Die Kommunalverwaltung ergänzte nach Aufforderung ihre Allgemeine Dienstanweisung datenschutzgerecht.

12.2 Öffentliche Zustellung nach dem Verwaltungszustellungsgesetz

Eine behördliche Datenschutzbeauftragte stellte fest, daß ein Amt ihrer Behörde einen Verpflichtungsbescheid nach dem SGB offen mit Namen, Anschrift und Grund des Bescheides sowie weiteren Sozialdaten im für jedermann zugänglichen Informationskasten der Behörde zur öffentlichen Zustellung ausgehängt hatte.

Dieses Verfahren war ihrer Ansicht nach nicht mit dem geltenden Sozialgeheimnis nach § 35 SGB I zu vereinbaren und sie bat aus diesem Grunde um fachlichen Rat.

Der Landesbeauftragte gab ihr Recht. § 15 Abs. 2 Satz 2 VwZG-LSA sieht für solche sensiblen Fälle vor, daß anstelle des Schriftstückes eine Benachrichtigung ausgehängt wird. In der ist allgemein anzugeben, daß und wo das Schriftstück eingesehen werden kann. Nr. 15 Buchstabe d der dazu ergangenen Verwaltungsvorschrift schreibt darüber hinaus ausdrücklich vor, daß diesem Verfahren im Interesse des Persönlichkeitsschutzes der Vorrang zu geben ist. Eine Abweichung ist nur zulässig, wenn sonst die Zustellung beeinträchtigt wird.

Die Behörde hat umgehend reagiert und durch eine interne Dienstanweisung das Verfahren nach Nr. 15 VV-VwZG-LSA verbindlich festgelegt.

12.3 Einsichtnahme von Stasi-Akten durch Mitglieder eines Gemeinschaftsausschusses

Ein Petent hatte sich u.a. mit der Frage an den Landesbeauftragten gewandt, ob der Gemeinschaftsausschuß einer Verwaltungsgemeinschaft, bei der er beschäftigt ist, befugt war, seine sog. Stasi-Akte einzusehen.

Für diesen Fall gilt als bereichsspezifische Rechtsgrundlage das Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz - StUG) in Verbindung mit den Bestimmungen der Gemeindeordnung des Landes Sachsen-Anhalt (GO LSA).

Aus der Stellungnahme der Verwaltungsgemeinschaft ergab sich, daß ein Beschluß des Gemeinschaftsausschusses vorlag, alle Bediensteten der Verwaltungsgemeinschaft auf eine Mitarbeit beim oder auf eine Zusammenarbeit mit dem Staatssicherheitsdienst der ehemaligen DDR zu überprüfen und dazu eine Aktenauskunft bei der sog. Gauck-Behörde einzuholen.

Dieser Beschluß war rechtmäßig. Nach § 79 Abs. 1 Nr. 5 GO LSA beschließt der Gemeinschaftsausschuß über die Ernennung, Einstellung und Entlassung der Bediensteten im Einvernehmen mit dem Leiter des Gemeinsamen Verwaltungsamtes. Folglich waren die Mitglieder des Gemeinschaftsausschusses rechtlich befugt, bei der Gauck-Behörde die entsprechenden Unterlagen zur Person des Petenten anzufordern (§ 19 Abs. 2 StUG) und nach deren Eingang die Unterlagen auszuwerten (§ 20 Abs. 1 Nr. 6d StUG). Weder die Überprüfung selbst noch die Einsichtnahme in die übersandten Unterlagen war vom Einverständnis des Petenten abhängig. Dazu war auch nicht erforderlich, daß tatsächliche Anhaltspunkte für eine Zusammenarbeit mit dem Staatssicherheitsdienst vorlagen.

Es war auch datenschutzrechtlich nicht zu beanstanden, daß in diesem Fall jedes Mitglied Einsicht in die zu bewertenden Unterlagen nehmen konnte. Es stand allein im Ermessen des entscheidenden Gremiums selbst, ob es jedem Mitglied die Einsichtnahme ermöglichen wollte, oder ob nur der Vorsitzende oder beispielsweise ein Dreiergremium mit der Einsichtnahme und einer Berichterstattung beauftragt wurde.

12.4 Auskünfte an Bürgermeister und Gemeinderäte über säumige Abgabenschuldner

Eine Verwaltungsgemeinschaft fragte bei dem Landesbeauftragten an, ob datenschutzrechtliche Bedenken dagegen bestünden, den Bürgermeistern der Mitgliedsgemeinden eine vierteljährliche Aufstellung über säumige Abgabenschuldner ihrer jeweiligen Gemeinde auszuhändigen. Die Daten dazu waren in der Kasse des Gemeinsamen Verwaltungsamtes gespeichert.

Die Bürgermeister beriefen sich dabei auf ihr Kontroll- und Informationsrecht nach § 44 GO LSA. Zu Recht, denn die jeweiligen Gemeinden bleiben „Herr ihrer Daten“.

Allerdings ist wegen der den Vorschriften des Steuergeheimnisses unterliegenden Daten besondere Vorsicht angebracht. Die Aufstellungen mit den Daten sind von den Bürgermeistern besonders sicher zu verwahren. Sobald die Listen zur Aufgabenerfüllung nicht mehr benötigt werden, sind sie nach § 16 Abs. 2 Nr. 2 DSG-LSA **sicher** zu vernichten, am besten sollten sie zur Vernichtung an das Gemeinsame Verwaltungsamt zurückgegeben werden.

Mit der Aushändigung der Schuldnerliste steht den Bürgermeistern nicht das Recht zu, persönlich Einfluß auf die Zahlungspflichtigen zu nehmen. Vollstreckungsaufgaben stehen nach dem Verwaltungsvollstreckungsgesetz nur dem Aufgabenträger, d.h. in diesem Fall der Verwaltungsgemeinschaft, zu.

Die Gemeinderäte dürfen keine Einsicht oder Auskünfte zu den personenbezogenen Daten der Schuldner erhalten. Die Bürgermeister können aber die Gemeinderäte über die Anzahl der Schuldner und die Höhe der Rückstände informieren.

12.5 Auskunft über die Betreiber von Kohleheizungen an Bürgermeister

„Im Interesse des Umweltschutzes“ wollte ein Ortsbürgermeister Hauseigentümer ansprechen und auffordern, ihre alten Kohleheizungen auf moderne Gasheizungen umzurüsten.

Er konnte sein Vorhaben aber so nicht durchführen, weil sowohl der Bezirksschornsteinfeger als auch das Ordnungsamt des Landkreises „aus Gründen des Datenschutzes“ keine Auskunft über die Betreiber von Kohleheizungen erteilten. Darüber beklagte sich der Bürgermeister beim Landesbeauftragten.

Dieser mußte ihm bestätigen, daß es für die gewünschte Auskunft - datenschutzrechtlich eine Übermittlung personenbezogener Daten - an der erforderlichen gesetzlichen Erlaubnis mangelt.

Deshalb hat der Landesbeauftragte dem umweltbewußten Ortsbürgermeister vorgeschlagen, sich an alle Bürger des Ortes zu wenden, um für sein Anliegen zu werben und Einzelgespräche auf freiwilliger Basis (datenschutzrechtlich: mit Einwilligung der Betroffenen) anzubieten.

12.6 Meldung der Betreiber von Öllageranlagen durch den Schornsteinfeger

Eine Petentin beschwerte sich, daß sie als Betreiberin einer Öllageranlage durch den Schornsteinfeger an den Landkreis gemeldet wurde.

Der Landesbeauftragte klärte sie darüber auf, daß es dafür eine gesetzliche Grundlage gab, denn der Landkreis war als untere Wasserbehörde im Rahmen der Gefahrenabwehr tätig geworden und nach der bereichsspezifischen Rechtsgrundlage des § 15 Abs. 1 Nr. 3 i.V.m. Abs. 5 Satz 2 SOG LSA auch berechtigt gewesen, ihre Daten beim Schornsteinfeger zu erheben.

Auch die Datenübermittlung durch den Schornsteinfeger war zulässig, denn § 19 Abs. 3 Satz 1 des Schornsteinfegergesetzes erlaubt dem Schornsteinfeger, personenbezogene Daten aus seinen Aufzeichnungen an öffentliche Stellen zu übermitteln, soweit das für die Bekämpfung der Luft-, Boden- und Gewässerverschmutzung erforderlich ist.

12.7 Beschaffung einer Geburtsurkunde

Eine Petentin wandte sich an den Landesbeauftragten mit der Bitte um Hilfe. Als junge Frau wurde sie zu Unrecht zur zwangspsychiatrischen Behandlung in ein Krankenhaus eingewiesen. Zu dieser Zeit war sie schwanger und wurde für die Geburt ihres Kindes in ein Allgemeinkrankenhaus verlegt, das sie nicht kannte. Anschließend kam sie zur weiteren Behandlung zurück in die Psychiatrie - ohne ihr Kind. Die Wege von Mutter und Kind trennten sich und erst nach langer Zeit konnte sie nach der Wiedervereinigung Rehabilitationsansprüche geltend machen - aber da fehlten ihr viele Unterlagen. So hatte sie über verschiedene Institutionen versucht, den Geburtsort ihres Kindes, die Geburtsklinik und das zuständige Standesamt zum Zwecke der Ausstellung einer Geburtsurkunde zu ermitteln. Darüber hinaus versuchte sie, eine Auskunft über einen weiteren Klinikaufenthalt zu bekommen, der über 30 Jahre zurücklag.

Als sie schließlich ein Standesamt fand und eine Geburtsurkunde anforderte, wurde ihr mitgeteilt, daß die Geburt am Ort der Klinik nicht verzeichnet sei und demzufolge auch keine Geburtsurkunde ausgestellt werden könne. Auch weitere ihrerseits angestellte Nachforschungen führten zu keinem anderen Ergebnis.

Der Landesbeauftragte konnte ihr teilweise helfen. Er führte eine Kontrolle bei dem Standesamt durch, das angeblich keine Geburtsunterlagen besaß und konnte an Hand der im dortigen Archiv befindlichen Unterlagen den Geburtseintrag und die Entbindungsklinik ermitteln. Bei der anschließenden Kontrolle in dieser Entbindungsklinik konnte gerade noch rechtzeitig der Bestand der medizinischen Unterlagen, der schon zur Vernichtung anstand, gesichert werden. Damit hatte die Petentin noch die Möglichkeit, Einsicht in die sie betreffenden medizinischen Unterlagen zu nehmen und diese für die Beweisführung zu sichern.

Im weiteren Fall konnte leider nicht mehr geholfen werden. Immerhin waren seitdem mehr als 30 Jahre vergangen, so daß trotz aller Sucharbeiten in verschiedenen Archiven keine Dokumente aufgefunden werden konnten. Es muß davon

ausgegangen werden, daß diese Unterlagen - durchaus fristgerecht - vernichtet wurden.

13. Landtag

Öffentliche Vorstellung von Petitionen in den Medien

Der Landesbeauftragte hat sich wiederholt in den früheren Tätigkeitsberichten (vgl. II. Tätigkeitsbericht, S. 85 ff, III. Tätigkeitsbericht, S. 71 f und IV. Tätigkeitsbericht, S. 65 ff) mit Problemen des Datenschutzes bei der Arbeit des Petitionsausschusses auseinandergesetzt. Auch im Berichtszeitraum ist wieder eine Frage aus diesem Bereich aufgeworfen worden. Das macht deutlich, wie sehr dem Petitionsausschuß an einer die Persönlichkeitsrechte wahrenden Verfahrensweise liegt.

An den Petitionsausschuß wurde die Überlegung herangetragen, einen Fernsehbericht über die Arbeit des Ausschusses zu senden und dabei einzelne Petitionen öffentlich vorzustellen. Dazu bat die Vorsitzende um datenschutzrechtliche Beratung.

Der Landesbeauftragte hat dazu folgende Auffassung vertreten:
Das Bundesverfassungsgericht hat aus Artikel 2 Abs. 1 i.V. mit Artikel 1 Abs. 1 GG das (Grund-)Recht auf informationelle Selbstbestimmung entwickelt. Es beinhaltet die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbaren will (Urteil vom 15.12.1983, BVerfGE 65, 1). In der Verfassung des Landes Sachsen-Anhalt ist dieses Grundrecht in Artikel 6 Abs. 1 festgeschrieben und bindet alle öffentlichen Stellen, damit auch den Petitionsausschuß des Landtages.
Um diesen verfassungsrechtlichen Vorgaben zu entsprechen, bestimmt § 4 Abs. 1 DSG-LSA, daß für die Erhebung, Nutzung und Verarbeitung (dazu gehört

auch die Übermittlung an Dritte, z.B. über die Medien) personenbezogener Daten eine gesetzliche Grundlage vorhanden sein muß, es sei denn, der oder die Betroffene haben ihre Einwilligung dazu wirksam erklärt oder bleiben völlig anonym.

Im Lande Sachsen-Anhalt gibt es derzeit keine Rechtsgrundlage, die es in den jetzt diskutierten Fällen dem Petitionsausschuß erlaubt, mit Bezug zu betroffenen Personen öffentlich zu verhandeln. Deshalb bedarf es für solche Fälle einer schriftlichen Einwilligung der Betroffenen. Diese sind zuvor über die Art der Daten, die Form ihrer Verarbeitung und die vorgesehenen Empfänger detailliert aufzuklären (sog. informierte Einwilligung nach § 4 Abs. 2 DSG-LSA).

Die Petentin oder der Petent sollte dabei auch darauf hingewiesen werden, daß bei einer öffentlichen Erörterung in den Medien Sachverhalte bekanntermaßen eine Eigendynamik entwickeln, die durch den Ausschuß nicht mehr gesteuert werden kann. Damit können neue Gefahren für das Persönlichkeitsrecht des Betroffenen heraufbeschworen werden.

Rechtlich nicht unproblematisch ist bei einer öffentlichen Falldiskussion auch der Schutz der Entscheidungsträger auf Seiten der beteiligten Behörden oder öffentlichen Stellen. Zwar hat ein solcher behördlicher Entscheidungsträger datenschutzrechtlich hinzunehmen, daß er namentlich bekannt wird, doch geht dies nicht soweit, daß er sich auch in jedem Fall persönlich vor einer Kamera rechtfertigen muß.

Alternativ bietet sich an, geeignete Fälle anonymisiert darzustellen. Dabei wäre ein Verfahren zu wählen, das unter Verzicht auf die Nennung personenbezogener Daten den Sachverhalt umfassend tatsächlich und rechtlich, aber so abstrakt darstellt, daß die Person nicht bestimmbar wird. Anderenfalls würde wieder der volle Schutz des Gesetzes greifen.

Sollte der Petitionsausschuß ein solches Verfahren ins Auge fassen, hat der Landesbeauftragte angeboten, die Präsentation der Petitionen datenschutzrechtlich beratend zu begleiten.

14. Personalwesen

14.1 Verwendung von privaten Telefonnummern für Alarmierungszwecke

Anläßlich eines vom Landesbeauftragten durchgeführten Fortbildungsseminars zum Thema „Personalaktenführung“ wurde die Frage erörtert, unter welchen Voraussetzungen die Erhebung, Speicherung und weitere Verwendung von privaten Telefonnummern durch den Arbeitgeber/Dienstherrn statthaft ist.

Als Beispiel wurde eine Behörde genannt, bei der in einer Dienstanweisung das Verhalten der Beschäftigten bei Unfällen und im Feuer- und Gefahrenfall geregelt ist. In einer Anlage zu dieser Dienstanweisung ist der Kreis der im Brandfall außerhalb der Dienstzeit fernmündlich zu informierenden leitenden Mitarbeiterinnen und Mitarbeiter festgelegt.

Rechtsgrundlage für die Datenerhebung bei Dienst- und Arbeitsverhältnissen ist § 90 Abs. 4 Satz 1 BG LSA i.V.m. § 13 BAT-O; ergänzend gilt § 28 DSG-LSA. Danach darf der Dienstherr personenbezogene Daten über Bedienstete erheben, soweit dies u.a. zu Zwecken des Personaleinsatzes erforderlich ist. Die Auswahl der zu alarmierenden Personen war im Hinblick auf deren jeweilige herausgehobene Funktion und die zu schützenden beträchtlichen Sachwerte sachlich gerechtfertigt, so daß gegen die Datenerhebung und Speicherung rechtlich keine Bedenken bestanden.

Da die komplette Dienstanweisung - also auch einschließlich der Anlage mit den privaten Telefonnummern - allen Mitarbeiterinnen und Mitarbeitern zur Verfügung gestellt wurde, bedurfte die erweiterte Verwendung der privaten Telefonnummern einer eigenen Bewertungsgrundlage. Diese ergibt sich aus § 90 Abs. 1 Satz 3 BG LSA.

Der Dienstherr war danach berechtigt, für Zwecke des Personaleinsatzes auch die privaten Telefonnummern zu nutzen. Allerdings hatte der Dienstherr dem Umstand, daß die privaten Telefonnummern mit einem Sperrvermerk versehen waren, bei der dienstlichen Nutzung angemessen Rechnung zu tragen. Damit war ein genereller Verteiler an jeden Bediensteten nicht vereinbar und auch

nicht zulässig. Datenschutzgerecht wäre beispielsweise, die in der Anlage enthaltenen Telefonnummern in einem verschlossenen Umschlag beim Pförtner oder der Einsatzzentrale der Feuerwehr zu hinterlegen.

14.2 Übersendung einer Nettolohnbescheinigung

Einem öffentlichen Arbeitgeber wurde ein Pfändungs- und Überweisungsbeschluß durch einen Gerichtsvollzieher zugestellt. Die Lohnbuchhaltung war - rechtsirrig - nach Rücksprache mit dem Schuldner der Ansicht, daß der Titel nicht zu Recht bestehe und überwies im Verhältnis zur Gesamtforderung des Gläubigers nur einen geringen Betrag. Als der Rechtsanwalt des Gläubigers daraufhin den geringen Überweisungsbetrag reklamierte, übersandte das Lohnbüro zur Rechtfertigung kurzerhand eine Nettolohnabrechnung.

Der Landesbeauftragte mußte feststellen, daß die Übermittlung von (überschüssigen) Personaldaten des Beschäftigten mit der Nettolohnabrechnung ohne Rechtsgrund erfolgte und gegen § 90d Abs. 2 BG LSA i.V.m. § 13 BAT-O verstieß. § 840 ZPO, der die Auskunftserteilungspflicht des Drittschuldners regelt, beinhaltet weder eine Verpflichtung noch ein Recht, überschüssige Personaldaten den Gläubigern zur Kenntnis zu geben.

Im Hinblick auf die nicht ganz einfache Bewertung der Sach- und Rechtslage für eine in diesem Fall kleine Verwaltungseinheit und die nicht absichtlich mißlungene Rechtsgüterabwägung zwischen Persönlichkeitsrecht und Schadensabwendung hat der Landesbeauftragte ausnahmsweise von einer förmlichen Beanstandung abgesehen.

14.3 Einsichtnahme in Personalakten durch eine Wirtschaftsberatungsgesellschaft

Der Personalrat eines Landkreises hatte die Frage aufgeworfen, ob zur Vorbereitung betriebsbedingter Kündigungen eine außerhalb der Behörde stehende private Einrichtung herangezogen werden dürfe. Vorausgegangen war ein

Beschluß des Kreistages, ein Wirtschaftsberatungsunternehmen mit der Umsetzung von Haushaltskonsolidierungsmaßnahmen zu betrauen. Dazu sollte das Beratungsunternehmen auch die Personalakten auf kündigungsschutzrechtlich relevante soziale Daten auswerten.

Der Landkreis stützte sich bei der Zulässigkeit der Datenübermittlung auf § 12 Abs. 1 DSG-LSA (Datenübermittlung an nicht-öffentliche Stellen) i.V.m. § 10 Abs. 2 DSG-LSA (Zweckänderung). Das war falsch, denn da es dabei um persönliche Daten aus Personalakten ging, waren die bereichsspezifischen Bestimmungen der §§ 90 ff BG LSA i.V.m. § 28 DSG-LSA zu beachten. Die Datenübermittlung durch die Einsichtnahme der privaten Prüfer war dementsprechend rechtlich stark eingeschränkt und hätte der Einwilligung der Bediensteten gem. § 90d Abs. 2 BG LSA bedurft.

Eine legale Möglichkeit, wie der Landkreis ohne rechtliche Schwierigkeiten das Wirtschaftsberatungsunternehmen hätte einbeziehen können, bietet demgegenüber § 8 DSG-LSA. Danach bleibt der Landkreis als Auftraggeber Herr der Daten und weiterhin für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich, insbesondere für die Zulässigkeit der Verarbeitung und Nutzung der personenbezogenen Daten, die Wahrung der Rechte der Betroffenen sowie die Einhaltung der nach § 6 DSG-LSA erforderlichen Datensicherungsmaßnahmen. Rechtlich findet dabei keine Datenübermittlung statt.

Der Landesbeauftragte schlug dem Landkreis deshalb vor, bis zur schriftlichen Ausgestaltung eines entsprechenden Vertrages (§ 8 Abs. 2 DSG-LSA) dem Wirtschaftsberatungsunternehmen die Personaldaten der Mitarbeiterinnen und Mitarbeiter lediglich anonymisiert oder mit deren Einwilligung zur Verfügung zu stellen.

Der Landkreis hat prompt reagiert und einen die gesetzlichen Vorgaben umfassenden schriftlichen Vertrag mit der privaten Gesellschaft geschlossen.

14.4 Personaldaten in Verzeichnisdiensten

Den Aufbau von Verzeichnisdiensten und die damit verbundenen grundsätzlichen datenschutzrechtlichen Probleme hat der Landesbeauftragte bereits in Ziff. 6.5 dargelegt. Neben der dort beschriebenen technischen Absicherung sind aber auch materielle Datenschutzbestimmungen zu beachten, insbesondere wenn in diese Verzeichnisdienste **Personaldaten** eingestellt werden sollen.

Werden Verzeichnisdienste nur im **Intranet** des Landes angeboten, handelt es sich **nicht** um einen Tele- bzw. einen Mediendienst, denn es liegt kein „Angebot“ im Sinne des § 2 Abs. 2 Teledienstegesetz (TDG) bzw. § 2 Abs. 2 Mediendienstestaatsvertrag (MDStV) vor. Die datenschutzrechtliche Zulässigkeit der Einstellung von Personaldaten in solche Verzeichnisdienste richtet sich dann nach § 90g i.V.m. § 90d BG LSA, ergänzend gilt § 28 DSG-LSA. Diese Bestimmungen gelten auch für Tarifpersonal.

Sollen Verzeichnisdienste mit solchen personenbezogenen Daten der Bediensteten über das Intranet des Landes **hinaus** genutzt werden, z.B. im bundesweiten TESTA Deutschland oder im **Internet**, hält der Landesbeauftragte diese Veröffentlichung (rechtlich: Übermittlung) von Bedienstetendaten generell nur mit **Einwilligung** der Betroffenen gem. § 90d Abs. 2 BG LSA für zulässig.

Folgende weitere **Grundsätze** sind beim Einsatz von Verzeichnisdiensten bei öffentlichen Stellen des Landes zu beachten:

- der Verzeichniseintrag ist auf die **erforderlichen** Angaben zu beschränken, die für die Aufgabenerledigung notwendig sind,
- die Zugriffsmöglichkeiten auf die Verzeichnisse sind eng zu fassen, starke Authentifizierungsmechanismen (digitale Signatur, biometrische Verfahren) sind einzusetzen, Verfahren, die lediglich dem X.500 Standard entsprechen, sind nicht einzusetzen,
- eine zeitnahe Aktualität der Daten des Verzeichnisdienstes muß sichergestellt werden (auch für Kopien, die sog. Repliken),

- vor Veröffentlichung des Eintrags im Verzeichnisdienst sind die einzutragenden Daten dem Betroffenen zur Einsichtnahme/Korrektur vorzulegen.

Neben den vorstehend genannten technischen und organisatorischen Maßnahmen ist auch die Sicherheit bei der Übertragung, d.h. bei sog. Replikationen der Daten, durch Verschlüsselung zu gewährleisten.

Zum Thema „Verzeichnisdienst“ hat das Ministerium des Innern bereits Kontakt zum Landesbeauftragten aufgenommen. Welche Institution in Sachsen-Anhalt die Funktion eines Trust Centers übernehmen wird, oder ob auf Dritte aus der Privatwirtschaft zurückgegriffen wird, ist noch nicht entschieden. Nach Abschluß der Meinungsbildung im Ministerium soll dem Landesbeauftragten der Entwurf zu Inhalt und Struktur eines Verzeichnisdienstes für die Landesverwaltung Sachsen-Anhalt zur Stellungnahme zugeleitet werden.

14.5 Einsichtnahme Dritter in archivierte Personalakten

Ein pauschal - ohne nähere Eingrenzung - bevollmächtigter Antragsteller begehrte bei einem Landkreis Einsicht in dessen archivierte Personalunterlagen, um eventuell vorhandene Ansprüche im Zusammenhang mit Ereignissen nach der Machtergreifung der Nationalsozialisten und in den Folgejahren nach dem Vermögensgesetz auszuwerten. Da der Landkreis aus mehreren Gründen Bedenken hatte, dem Antrag zu entsprechen, bat er den Landesbeauftragten um die rechtliche Beurteilung des Begehrens.

Zunächst war formalrechtlich festzuhalten, daß eine per Telefax übermittelte „Vollmacht“ ohne die nachgereichte Originalvollmacht rechtlich unbeachtlich ist. Unabhängig davon war auch die Auffassung des Rechtsamtes des Landkreises zu teilen, daß die Vollmacht inhaltlich zu unpräzise war und zu einer pauschalen Ausforschung der im Kreisarchiv befindlichen personenbezogenen Unterlagen führen würde. Dies war aus mehreren Gründen rechtlich unzulässig. Die daten-

schutzrechtliche Prüfung erstreckte sich auf das Vermögensgesetz, auf archivrechtliche Bestimmungen und auf Regelungen des Personalaktenrechts.

1. Das Vermögensgesetz enthält keinerlei Rechtsgrundlagen für die Ausforschung von Personalakten und die damit verbundenen Grundrechtseingriffe. § 31 Vermögensgesetz verpflichtet den Anspruchsteller nur, bei den **amtlich** durchzuführenden Ermittlungen mitzuwirken, beinhaltet aber für diesen keinerlei eigene Eingriffsgrundlage in die Rechte Dritter. Möglich wäre ein eventuelles Datenübermittlungsersuchen des Amtes zur Regelung offener Vermögensfragen nach § 11 i.V.m. § 10 DSG-LSA im Rahmen seiner Amtsermittlungen.

2. Wird die Einsicht in bereits abgeschlossene Personalunterlagen begehrt, wäre die Zulässigkeitsprüfung nach den Vorschriften des Archivrechts vorzunehmen. Soweit es dabei um Archivgut geht, das vor Inkrafttreten des Landesarchivgesetzes (ArchG-LSA) am 28.06.1995 entstanden ist, sind grundsätzlich die damals geltende Verordnung über das staatliche Archivwesen sowie die Zweite Durchführungsbestimmung vom 19.03.1976 und vom 16.03.1990 heranzuziehen. Da bekanntermaßen nach den Festlegungen im Einigungsvertrag das Recht der ehemaligen DDR nur Anwendung finden kann, soweit es mit den heute geltenden Vorschriften des Grundgesetzes übereinstimmt, wäre dabei auch die grundlegende Entscheidung des Bundesverfassungsgerichts vom 15.12.1983 (NJW 1984 S. 419 ff) zum Recht auf informationelle Selbstbestimmung zu beachten. Deshalb empfiehlt es sich, bei der Rechtsprüfung das in solchen Fällen höhere Schutzniveau des Landesarchivgesetzes zur Prüfung heranzuziehen.

   Nach § 10 Abs. 2 Nr. 2 ArchG-LSA ist die Nutzung von Archivgut unzulässig, soweit Grund zu der Annahme besteht, daß schutzwürdige Belange Betroffener oder Dritter entgegenstehen. Dementsprechend hat der Gesetzgeber in § 10 Abs. 3 Satz 2 ArchG-LSA vorgesehen, daß derartiges Archivgut grundsätzlich erst 30 Jahre nach dem Tode der Betroffenen genutzt werden darf.

3. Handelt es sich um personenbezogene Unterlagen aus Personalvorgängen, die noch nicht abgeschlossen sind, gelten die Bestimmungen des BG LSA i.V. mit § 13 BAT-O. Nach § 90f BG LSA sind Personal- und Versorgungsakten unterschiedlich lange als nicht abgeschlossene Vorgänge zu behandeln. Daraus folgt, daß solche personenbezogenen Akten, auch wenn sie schon im Archiv gelagert sein sollten, noch der laufenden Verwaltung zuzurechnen sind und damit nicht den archivrechtlichen Benutzungsregelungen unterfallen. Auskunft an Dritte - dazu zählt auch die Einsichtnahme - bedarf in diesen Fällen der Einwilligung des Betroffenen (§ 90d BG LSA).

14.6 Private Benutzung von Telekommunikationsanlagen

Der Gesamtpersonalrat einer Universität des Landes Sachsen-Anhalt hatte den Landesbeauftragten gebeten, ihn mit datenschutzrechtlichen Empfehlungen bei der Verwendung von personenbezogenen Daten im Zusammenhang mit dem Betrieb von Telekommunikationsanlagen zu unterstützen.

Im Vorfeld waren personenbezogene Daten bei der Telekommunikation ausgewertet worden, die zu dienstrechtlichen und arbeitsrechtlichen Maßnahmen führten.

Es wurde herausgearbeitet, daß rechtliche Unterschiede bei der dienstlichen Benutzung einer Telekommunikationsanlage und der privaten geduldeten Nutzung der Anlage bestehen. Für den Dienstherren/Arbeitgeber muß es Instrumentarien der Mißbrauchskontrolle dienstlicher Anlagen geben. Grundsätzlich ist für solche Mißbrauchskontrollen ein Einverständnis der entsprechenden Teilnehmer gem. § 89 Abs. 10 TKG einzuholen. Die früheren Rundschreiben der Universität zur Telefonbenutzung sahen eine Kontrolle durch den Dienstvorgesetzten nicht vor. Deshalb bestanden seitens des Personalrates Zweifel an der Zulässigkeit der seitens der Universitätsverwaltung vorgenommenen Auswertungen zur mißbräuchlichen privaten Benutzung der Telekommunikationsanlage.

Im Ergebnis wurde von der Universität eine Dienstanweisung vorgelegt, die eine rechtlich zulässige Verwendung von Verbindungsdaten im Sinne der Mißbrauchskontrolle regelt, und auch die dann mit dem Gesamtpersonalrat abgestimmte Gebührenerfassung privater Telefongespräche entsprach den rechtlichen Vorgaben.

15. Polizei

15.1 Novellierung des SOG LSA

Am 26.07.2000 ist nach engagierter, teilweise erbitterter rechtspolitischer Diskussion die Novellierung des SOG LSA in Kraft getreten. Der Landesbeauftragte hat dazu wiederholt mündliche und schriftliche Stellungnahmen abgegeben, die dem Landtag bekannt sind. Es besteht deshalb aus seiner Sicht z.Zt. kein Anlaß, diese Diskussion erneut aufzugreifen.

Für die Bürgerinnen und Bürger des Landes und die Öffentlichkeit aber ist es wichtig, sich darauf einzustellen, daß es auch in Sachsen-Anhalt künftig zwei wesentliche Einschränkungen der persönlichen Bewegungsfreiheit auf öffentlichen Wegen und Plätzen geben wird:

1. An sog. Kriminalitätsschwerpunkten kann künftig eine Videoüberwachung angeordnet werden (§ 16 Abs. 2 SOG LSA). Sie ist durch Hinweisschilder deutlich zu machen. Im Normalbetrieb findet dabei nur eine allgemeine Beobachtung statt, die Kameras senden nur Übersichtsaufnahmen. Erst bei einer besonderen Gefahrensituation oder dem Verdacht einer Straftat werden Bildausschnitte herangezoomt, so daß Personen erkannt und aufgezeichnet werden.

   Im Berichtszeitraum gab es ab dem Jahr 2000 solche Beobachtungen am Marktplatz in Halle und im Stadtpark von Dessau.

2. Personenkontrollen im öffentlichen Raum (§ 14 Abs. 3 SOG LSA)

Zur Bekämpfung der grenzüberschreitenden Kriminalität sind Personenkontrollen auf Bundesfernstraßen und eine Inaugenscheinnahme mitgeführter Gegenstände möglich, wenn besondere Lageerkenntnisse diese Maßnahmen zur Verhütung von Straftaten von erheblicher Bedeutung angezeigt sein lassen und ein Behördenleiter die Maßnahme angeordnet hat.

Aus den Zeitungen war zu entnehmen, daß eine solche Maßnahme bisher einmal Anfang 2001 angeordnet worden ist.

Der Landesbeauftragte wird die Entwicklung und den Einsatz dieser neuen Eingriffsmittel beobachten und von seinen Interventionsmöglichkeiten Gebrauch machen, wenn er dies nach der Rechtslage für erforderlich hält.

15.2 Überprüfung der Kriminalakten

Der Landesbeauftragte hat im Berichtszeitraum die 1997 begonnene Prüfung der Kriminalaktenhaltung, die Nutzung der Informationstechnik und die Einhaltung der Datensicherheit bei den Polizeidirektionen zum Abschluß gebracht. Dabei ergaben sich vergleichbare Feststellungen, wie sie zuvor im IV. Tätigkeitsbericht (S. 79) aufgeführt worden sind.

Überwiegend wurden die vorgesehenen Prüffristen für die Aussonderung der Kriminalakten beachtet. Soweit Fehler festgestellt wurden, lag dies daran, daß die Festsetzung nicht an das Datum der Haftentlassung oder der Tat anknüpfte, die Aussonderungsprüffrist bei Jugendlichen von zwei Jahren unbegründet überschritten wurde oder die weitere Erforderlichkeit der Kriminalakte nach dem Ergebnis der Rückmeldung der Staatsanwaltschaft nicht erkennbar war. Diese Unsicherheit in der Rechtsanwendung führte in etlichen Fällen zu verkürzten oder längeren Prüffristen.

Auch wiederholte vollständige Ed-Behandlungen innerhalb kurzer Zeiträume, die nicht erforderlich und damit nicht von § 81 StPO gedeckt waren, wurden festgestellt. In einigen Fällen war auch die Anordnung zur Ed-Behandlung fehlerhaft, weil sie nicht erkennen ließ, ob der Betroffene der Ed-Behandlung freiwillig zugestimmt hat oder sie auf gesetzlicher Grundlage durchgesetzt wurde.

Unvollständig und teilweise nicht nachvollziehbar wurden die Lichtbildnachweise geführt. In Einzelfällen waren bedingt durch nicht erforderliche mehrfache Ed-Behandlungen mehr Lichtbilder vorhanden als erforderlich.

Bei der zuletzt geprüften Polizeidirektion wurde eine nicht ordnungsgemäße Aktenführung festgestellt, weil auch umfangreiche Kriminalakten ungeheftet in Loseblatt-Form geführt wurden und eine Übersicht über wichtige Einzelunterlagen (z.B. Haftbefehle, Mitteilungen der Staatsanwaltschaften und der Gerichte) fehlte. Eine unübersichtliche Aktenführung eröffnet leicht die Möglichkeit der Entfernung oder des Vertauschens einzelner Blätter und entspricht nicht den Anforderungen der Rechtsprechung.

15.3 Überprüfung der TÜ-Maßnahmen

In seinem letzten Tätigkeitsbericht hatte der Landesbeauftragte über die Einführung des sogenannten „Großen Lauschangriffs“ informiert (vgl. IV. Tätigkeitsbericht, S. 90 ff).

Weil er dieses Thema für datenschutzrechtlich äußerst sensibel hält, hat er im Berichtszeitraum mit der Prüfung von Telekommunikationsüberwachungsmaßnahmen (TÜ-Maßnahmen) begonnen. Die stichprobenweise Überprüfung bei einer Polizeidirektion des Landes hat keine gravierenden datenschutzrechtlichen Verstöße ergeben.

Was den Landesbeauftragten wie seine Kollegen im Bund und den Ländern jedoch beunruhigt, ist der zunehmende Gebrauch dieses einschneidenden Eingriffsmittels und der geradezu formelhafte Umgang damit bei den Staatsanwalt-

schaften und Gerichten. Dadurch fühlt er sich mit den Kollegen in der grundsätzlichen Kritik bestätigt, daß die gesetzlichen Voraussetzungen der Überwachung zu leicht belegt werden können. Das ist aber der datenschutzrechtlichen Sensibilität dieses Themas nicht angemessen. Deshalb ist es gut, daß das Bundesverfassungsgericht in der letzten Zeit begonnen hat, die Gerichte von Verfassungs wegen zur genaueren Prüfung der tatsächlichen und rechtlichen Anforderungen anzuhalten.

15.4 INPOL-Neukonzeption

Die Polizeidienststellen des Bundes und der Länder verarbeiten in erheblichem Umfang personenbezogene Daten zur Kriminalitätsbekämpfung. Um einen schnellen und effektiven Informationsaustausch zwischen den verschiedenen Polizeidienststellen zu gewährleisten, wird beim Bundeskriminalamt (BKA) das bundesweite polizeiliche Informationssystem „INPOL“ geführt (vgl. die Beiträge im I. Tätigkeitsbericht, S. 102 ff, und im II. Tätigkeitsbericht, S. 107 f).

Zur Erweiterung und grundlegenden Neustrukturierung des bisherigen Systems wurde beim BKA schon 1996 eine Projektgruppe eingesetzt. Anlaß für die Neukonzeption dieses Verfahrens waren neben neuen technischen Möglichkeiten der Auswertungen auch veränderte Anforderungen aus polizeifachlicher Sicht zur Bewältigung des immens gestiegenen Datenaufkommens und dessen elektronischer Verarbeitung. Ende 2001 sollte das neue System seinen Betrieb aufnehmen, daran darf aber gezweifelt werden, weil die technische Realisierung mehr Tücken zeigt als erwartet.

Die Datenschutzbeauftragten des Bundes und der Länder haben zur datenschutzrechtlichen Begleitung des Projekts eine Arbeitsgruppe gebildet, der auch ein Vertreter des Landesbeauftragten angehört.

Probleme bei der abschnittsweisen Entwicklung des Projektes haben sich aus der Tatsache ergeben, daß INPOL-neu eine Verbundanwendung für die Daten

aller Länderpolizeien beinhaltet, aber aufgrund der unterschiedlichen Polizeigesetze der Länder unterschiedliche Vorschriften abdecken muß.

Der wichtigste Bestandteil von INPOL-neu ist dabei die Zusammenführung aller Erkenntnisse zu einer Person in einer Gesamtdatenbank im Gegensatz zu dem gegenwärtigen Verfahren einer Vielzahl von geschlossenen Dateien. Die Zugriffe auf diese neue Datenbank sollen dann entweder gezielt auf die Einzelinformation oder umfassend je nach Berechtigungsgrad der abfragenden Person oder Stelle möglich sein. Dies soll durch ein umfassendes Berechtigungssystem gewährleistet werden, das die datenschutzrechtlichen Grundsätze der Zweckbindung und der Erforderlichkeit berücksichtigt.

Im Rahmen dieser Neukonzeption und der damit verbundenen Anpassung der Länderinformationssysteme wird von einigen Ländern angestrebt, die Länderpolizeidaten künftig im Wege der Auftragsdatenverarbeitung an das BKA zu übertragen. Eine solche Datenverarbeitung im Auftrag war zunächst nur übergangsweise für die Länder vorgesehen, die keinen zeitgerechten technischen Anschluß an das Verfahren INPOL-neu gewährleisten konnten. Inzwischen liebäugeln aber eine ganze Reihe von Ländern aus Gründen der Kosteneinsparung damit, eine dauerhafte Verarbeitung ihrer polizeilichen Daten beim BKA vornehmen zu lassen.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine Auslagerung der Verarbeitung wesentlicher Teile der Datenbestände der Landespolizei zum BKA auf der Grundlage des § 2 Abs. 5 BKAG grundsätzlich für unzulässig und darüber hinaus für verfassungsrechtlich bedenklich. Nicht von ungefähr weist das Grundgesetz die Polizeihoheit den Ländern zu!

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen, und die in § 2 Abs. 1 BKAG statuierte Schwelle, daß nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen (vgl. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13.10.2001 **(Anlage 20)**). Damit würde auch ein wesentliches Stück Machtverteilung

zwischen dem Bund und den Ländern zu Lasten der Länder und ihrer Bürger aufgegeben.

Die vom Landesbeauftragten dargelegte Rechtsauffassung wird vom Ministerium des Innern nicht geteilt. Über die künftige Verarbeitung von Polizeidaten des Landes Sachsen-Anhalt beim BKA steht nach Mitteilung des Ministeriums des Innern von Ende März 2001 die abschließende Entscheidung allerdings noch aus.

15.5 Ein Verkehrssünder in der Pressekonferenz

Ein Verkehrsteilnehmer fuhr mit fast 200 km/h über eine Landstraße, dabei fiel er einem Zivilstreifenwagen der Polizei auf. Die folgende Verfolgungsjagd mit Geschwindigkeitsmessung und Videoaufzeichnung wurde zu einem Lehrstück für die nächste Pressekonferenz der Polizei. Dort wurden, um die Angelegenheit lebensnah zu gestalten, Sequenzen aus der Videoaufzeichnung vorgespielt.

Kurz darauf klingelte bei dem Verkehrssünder pausenlos das Telefon, Fernsehen, Rundfunk und die Zeitung hatten Interviewwünsche und überhaupt sprach sich der Vorfall in Windeseile in der Kleinstadt herum.

Daraufhin beschwerte sich der Betroffene über seinen Anwalt beim Landesbeauftragten und rügte die unzulässige Übermittlung seiner persönlichen Daten durch die Polizei an die Medienvertreter.

Die Überprüfung durch den Landesbeauftragten ergab, daß bei der Vorführung der Originalsequenzen in der Pressekonferenz Gelegenheit bestand, Fotos von dem Videoband anzufertigen bzw. dieses abzufilmen. Allerdings sollte bei der polizeilichen Vorführung das Kfz-Kennzeichen nicht zu sehen sein. Es wurde auch später bei der Wiedergabe der abgefilmten Ausschnitte im Fernsehen nicht gezeigt. Dennoch deutete alles darauf hin, daß die Medienvertreter die persönlichen Daten des Mannes nur über das Kfz-Kennzeichen erfahren haben konnten.

Der Landesbeauftragte hat in seiner rechtlichen Würdigung gegenüber der Polizeidirektion und dem Ministerium des Innern noch einmal klargestellt, daß die Vorführung des Videobandes grundsätzlich von § 4 Abs. 1 des Landespressegesetzes gedeckt war. Danach ist die Polizei berechtigt und im gewissen Umfange auch verpflichtet, die öffentlichen Medien über geeignete Vorfälle zu informieren. Allerdings hätte diese Öffentlichkeitsarbeit nicht dazu führen dürfen, daß der Betroffene auch nur indirekt über das Kfz-Kennzeichen als Halter bekannt wurde (§ 4 Abs. 2 Nr. 3 Landespressegesetz). Der Betroffene mußte sich nicht persönlich an den Pranger stellen lassen.

Das Ministerium des Innern hat durch Erlaß bei den Polizeibehörden angeordnet, die gesetzlich gebotene Berücksichtigung schutzwürdiger Interessen des Betroffenen künftig sicherzustellen.

15.6 Falscher Umgang mit Daten verhindert den Berufseinstieg

Jugendlicher Übermut brachte einem 14jährigen Mädchen ein Ermittlungsverfahren bei der Polizei des Landes ein. Der die Sache abschließend bearbeitende Jugendstaatsanwalt sah eine bereits durchgeführte erzieherische Maßnahme als ausreichend an, das Verfahren wurde nach § 45 Abs. 2 JGG eingestellt, und die über die Jugendliche gespeicherten Daten bei der Polizei wurden innerhalb der rechtlich geregelten kurzen Fristen gelöscht. Für die Einspeicherungen bei der Justiz galt bis zur vollständigen Tilgung der staatsanwaltschaftlichen Verfügung ein Verwertungsverbot nach den §§ 51 und 52 BZRG.

Zwei Jahre später bewarb sich die mittlerweile junge Dame für eine Ausbildung bei der Polizei in zwei Bundesländern. Beide Mal erhielt sie eine Absage unter Hinweis darauf, daß sie als 14jährige kurzzeitig Beschuldigte in einem Ermittlungsverfahren gewesen sei.

Die empörte Mutter der Minderjährigen beschwerte sich darüber beim Landesbeauftragten und bat um Aufklärung der Angelegenheit.

Die Überprüfung ergab, daß die junge Dame bei ihrer Bewerbung zusammen mit ihren Eltern darin eingewilligt hatte, daß die Ausbildungsbehörde bei der Polizeibehörde ihres Wohnsitzes auch zu laufenden Ermittlungsverfahren nachfragen durfte. Dies ist ein zulässiges und durchaus übliches Verfahren, um zeitliche Lücken zwischen dem Abschluß eines Strafverfahrens und der Eintragung evtl. Strafen in Registern zu schließen. Es wäre danach auch möglich gewesen, daß die für die Kriminalaktenhaltung des Wohnsitzes zuständige Kriminalpolizei Auskunft zu einer vorhandenen Kriminalakte hätte geben können.

Es gab aber zum Zeitpunkt der Bewerbung weder eine Kriminalakte noch ein **laufendes** Ermittlungsverfahren. Die im Ergebnis also rechtlich unzulässige Auskunft der Polizei des Wohnsitzes beruhte auf einer automatisierten Auswertung ihrer Vorgangsbearbeitungsdatei. Richtig ist dabei, daß die Polizei jeden amtlich zur Kenntnis zu nehmenden Sachverhalt zu registrieren und im Sinne einer ordnungsgemäßen Aktenführung und eines entsprechenden Tätigkeitsnachweises für die Dauer von fünf Jahren vorzuhalten hat.

Dies durfte aber nicht dazu führen, daß aus dieser Vorgangsbearbeitungsdatei entgegen den gesetzlichen Zweckbindungsvorschriften Auskunft zu längst abgeschlossenen und gelöschten Vorgängen gegeben wurde.

Das Ministerium des Innern teilt die Auffassung des Landesbeauftragten und hat die Polizeibehörden des Landes angewiesen, aus Vorgangsverwaltungsdateien keine derartigen Auskünfte zu erteilen. Im übrigen hat es den Fall zum Anlaß genommen, auch den Umfang der in einer Vorgangsverwaltungsdatei gespeicherten Daten auf die für die Erreichung der Zwecke erforderlichen Angaben zu beschränken.

16. Rechtspflege

16.1 Strafverfahrensänderungsgesetz 1999

Mit dem Strafverfahrensänderungsgesetz vom 02.08.2000 ist vorläufig eine jahrelange Diskussion darüber zu Ende gegangen, wie ein Ausgleich zwischen dem Recht auf informationelle Selbstbestimmung des einzelnen und dem Anspruch des Staates auf eine funktionstüchtige Strafrechtspflege aussehen soll.

Das Ergebnis ist ein Kompromiß zwischen den eher datenschutzfreundlichen Vorstellungen des Bundestages und den an einer möglichst einfachen Strafverfolgung interessierten Vorstellungen des Bundesrates. Dies ist deshalb bedauerlich, weil eine Vielzahl unbescholtener Bürger in Ermittlungsverfahren verwickelt werden und dabei erheblich und belastend in ihre Rechte eingegriffen wird.

Aus der Sicht des Landesbeauftragten und der seiner Kollegen und Kolleginnen im Bund und den übrigen Ländern begegnet das Strafverfahrensänderungsgesetz allerdings weiterhin datenschutzrechtlichen Bedenken (vgl. die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 **(Anlage 13)**).

In den §§ 131 bis 131c StPO wurden Fahndungsregeln, auch für die Öffentlichkeitsfahndung, endlich gesetzlich normiert. Diese Umsetzung einer alten datenschutzrechtlichen Forderung wird vom Landesbeauftragten grundsätzlich begrüßt. Allerdings bleibt das Ergebnis der gesetzlichen Normierung (vgl. IV. Tätigkeitsbericht, S. 89 f) in weiten Teilen datenschutzrechtlich bedenklich.

So regelt § 131 StPO die Fahndung zur Festnahme, § 131a StPO die Fahndung zur Aufenthaltsermittlung, § 131b StPO die Fahndung zur Identitätsfeststellung. Die Anordnungskompetenzen sind in § 131 StPO sowie in § 131c StPO für §§ 131a und b StPO geregelt. Dabei ist kritisch anzumerken, daß bei den Anordnungskompetenzen das Richterprivileg für die tief in die Persönlichkeitssphäre eingreifende Öffentlichkeitsfahndung erheblich aufgeweicht wird.

Nicht nur, daß die Hilfsbeamten der Staatsanwaltschaft bei Gefahr im Verzug die Fahndungsmittel der Strafverfolgung in Anspruch nehmen können (§ 131 Abs. 1 und 2, § 131c Abs. 1 Satz 2 StPO), sondern sie dürfen selbst auch Öffentlichkeitsfahndungen zum Zwecke der Aufenthaltsermittlung und Identitätsfeststellung veranlassen, wenn sonst „eine wesentliche Erschwernis der Ermittlungen“ droht. Das ist nach Auffassung des Landesbeauftragten im Lichte des Verhältnismäßigkeitsgrundsatzes ein zu unbestimmter Begriff, um den schwerwiegenden Eingriff in die Persönlichkeitsrechte ohne Richter zu rechtfertigen, denn erfahrungsgemäß sind davon auch immer wieder Unbeteiligte betroffen.

Diese Eingriffe betreffen nicht nur Beschuldigte, sondern auch Zeugen. So muß künftig jedermann damit rechnen, daß er als Zeuge Objekt einer groß angelegten Öffentlichkeitsfahndung wird.

Der faktische Wegfall des Richterprivilegs und damit die Unzulänglichkeit von Schutzregelungen wird in § 131c Abs. 2 StPO deutlich. Diese Vorschrift ermöglicht die Öffentlichkeitsfahndung **ohne** richterliche Bestätigung für längstens eine Woche.

Die erheblichen Gefahren dieser Regelung für das Persönlichkeitsrecht Betroffener werden insbesondere bei Fahndungen im Internet deutlich, weil die in diesem Medium veröffentlichten Fahndungen nicht nur „grenzenlos“, sondern vom Augenblick der Einstellung an faktisch nicht mehr rückholbar sind. Jeder Internetnutzer kann die Fahndungsmeldung herunterladen bzw. verändert wieder ins Netz einstellen. Die öffentliche Fahndung kann also bei neuen Erkenntnissen nicht mehr „zurückgeholt“ werden. Ob ein Richter binnen einer Woche die Anordnung zur Öffentlichkeitsfahndung bestätigt oder ablehnt, spielt dann für die Praxis keine Rolle mehr.

Nicht zufriedenstellen können unter datenschutzrechtlichen Aspekten auch die Regelungen zur Akteneinsicht.

§ 474 Abs. 1 StPO ermöglicht nunmehr die Akteneinsicht zum Zweck der Rechtspflege. Der Landesbeauftragte ist weiterhin der Auffassung (vgl. IV. Tätigkeitsbericht, S. 88 ff), daß der Begriff „zum Zwecke der Rechtspflege“ zu unbestimmt ist.

Bedenklich ist auch, daß künftig für die Akteneinsicht durch Private (§ 475 StPO) bereits ein **berechtigtes** Interesse ausreicht. Datenschutzfreundlicher wäre es gewesen, die Akteneinsicht nur bei einem **rechtlichen** Interesse zu gewähren.

Ein weiterer vom Landesbeauftragten bereits im Gesetzgebungsverfahren angesprochener Kritikpunkt ist der Aufbau von Dateien, in denen die Strafverfolgungsbehörden für Zwecke künftiger Strafverfahren bestimmte Daten speichern dürfen (§ 484 StPO). Da bereits ein zentrales staatsanwaltschaftliches Verfahrensregister aufgebaut wird, kann es zu von Verfassungs wegen verbotenen Doppelspeicherungen kommen. Hinzu kommen Speicherbefugnisse nach Landes- und Bundespolizeirecht, so daß zu erwarten ist, daß künftig Daten aus ein und demselben Verfahren mehrmals in verschiedenen Dateien gespeichert sein werden.

16.2 Parlamentarische Kontrolle von Lauschangriffen

16.2.1 Unzulänglicher Bericht der Bundesregierung

Die Bundesregierung hat zum Ende des Jahres 1999 gem. Art. 13 Abs. 6 Satz 1 GG und § 100e StPO ihren ersten Bericht über die erweiterten Abhörmaßnahmen in Strafverfahren vorgelegt.

Der Bericht soll eine parlamentarische Kontrolle der mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen und den Bundestag in die Lage versetzen, die Angemessenheit und Eignung der neuen Überwachungsmaßnahmen zu überprüfen. Deshalb muß nach § 100e Abs. 1 StPO über den gesamten Umfang der Maßnahmen berichtet werden. Hierzu zählen die Angaben über die Anzahl aller von der Maßnahme betroffenen Personen, denn der sog. Große Lauschangriff greift nicht nur in die Rechte der in einer gerichtlichen Anordnung Genannten, sondern auch in die Grundrechte unverdächtiger Familienangehöriger, Bekannter, Besucherinnen und Besucher ein.

Der 1999 vorgelegte Bericht beschränkt sich demgegenüber nur auf Zahlen zu Wohnungsinhabern und Beschuldigten. Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb in einer Entschließung vom 26. Juni 2000 **(Anlage 15)** gerügt, daß durch den Bericht in der derzeitigen Form die gesetzliche vorgesehene Berichtspflicht nicht erfüllt wird. Sie halten es darüber hinaus für wünschenswert, wenn - wie in den „Wire-tap-Reports“ der USA - die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren im Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahmen, die Anzahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahmen beigetragen haben, angegeben werden.

Nur dann wäre der Bundestag in der Lage, Angemessenheit und Zweckmäßigkeit der Maßnahmen tatsächlich zu überprüfen. Diese Auffassung teilt auch das Kontrollgremium des Deutschen Bundestages. Im Schreiben des Vorsitzenden vom 05. Februar 2000 an den Bundesbeauftragten für den Datenschutz wird ausgeführt, daß „der erste Bericht der Bundesregierung keine effektive parlamentarische Kontrolle ermöglicht“, weil „wesentliche Informationen fehlen, um die Rechtmäßigkeit eines Grundrechtseingriffs beurteilen zu können“.

16.2.2 Parlamentarische Kontrolle von Lauschangriffen auf Landesebene

In seinem IV. Tätigkeitsbericht (S. 92 ff) hat der Landesbeauftragte bereits eine effektive parlamentarische Kontrolle von Lauschangriffen gem. Art. 13 Abs. 6 GG auf Landesebene gefordert.

Die bereits vorstehend zitierte Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26. Juni 2000 **(Anlage 15)** greift dieses Anliegen auf und fordert für präventiv-polizeiliche und repressive Lauschangriffe eine **gesetzlich** normierte regelmäßige Berichtspflicht der Landesregierungen, um eine wirksame parlamentarische Kontrolle des tiefgehenden Grundrechtseingriffs „akustische Wohnraumüberwachung“ zu gewährleisten. Die Landtage müssen

die Möglichkeit haben, die in anonymisierter Form übermittelten Berichte der Landesregierung öffentlich zu erörtern.

In Sachsen-Anhalt wurde diese Forderung bislang nicht verwirklicht.
Hier haben sich das Ministerium des Innern, das Ministerium der Justiz, die Staatskanzlei und der Ältestenrat des Landtages geeinigt, daß die jeweils zuständigen Fachminister für präventiv-polizeiliche und repressive Lauschangriffe dem jeweils zuständigen Landtagsausschuß für Inneres oder Recht und Verfassung über solche Maßnahmen jährlich berichten.
Eine Erörterung im Landtagsplenum ist bisher nicht vorgesehen.

Der Landesbeauftragte kann damit nur feststellen, daß im Land Sachsen-Anhalt eine gleichwertige parlamentarische Kontrolle, wie sie Art. 13 Abs. 6 Satz 3 GG fordert, nicht gewährleistet ist.
Immerhin ist dem Landesbeauftragten bekanntgeworden, daß es im Ausschuß für Recht und Verfassung Stimmen gibt, die die Einführung eines dem Kontrollverfahren auf Bundesebene gleichwertigem Verfahren befürworten und auch einer gesetzlichen Fixierung nicht ablehnend gegenüberstehen.

16.3 Evaluation der Überwachung der Telekommunikation

Nicht nur eine aussagekräftige Berichtspflicht (vgl. Art. 13 Abs. 6 GG) zu den Auswirkungen des großen Lauschangriffs dient einer Erfolgskontrolle grundrechtsintensiver Eingriffe. Dazu gehört auch die von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderte Evaluation der Überwachung der Telekommunikation schlechthin.

Neben dem 1998 eingeführten sog. Großen Lauschangriff gehört die Überwachung der Telekommunikation nach §§ 100a und 100b StPO zu dem Instrumentarium der Strafverfolgungsbehörden, das gravierende Eingriffe in das durch Art. 10 GG geschützte Fernmeldegeheimnis ermöglicht.

1999 hat auch das Bundesministerium der Justiz die Notwendigkeit effektiver Erfolgskontrollen anerkannt und ein Forschungsvorhaben zur Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation an das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg vergeben.

Allerdings war zunächst wegen einer fehlenden Forschungsklausel in der Strafprozeßordnung ein Beginn der Arbeiten nicht möglich.

Nach Aufforderung der Datenschutzbeauftragten des Bundes und der Länder hat der Bundesgesetzgeber nachgebessert und mit dem Gesetz zur Änderung und Ergänzung des Strafverfahrensrechts - Strafverfahrensänderungsgesetz 1999 (StVÄG 1999) vom 02. August 2000 - in § 476 i.V.m. § 477 Abs. 2 Satz 3 StPO eine gesetzliche Grundlage geschaffen.

Auf das Ergebnis der Studie darf man gespannt sein.

16.4 DNA-Identitätsfeststellung

Zwischenzeitlich ist das Gesetz zur Änderung des DNA-Identitätsfeststellungsgesetzes (DNA-IFG) vom 02. Juni 1999 in Kraft getreten.

Die Gesetzesänderung hat eine Rechtsgrundlage für die Erfassung von bereits verurteilten Straftätern (sog. retrograde Erfassung) geschaffen. Zu diesem Zweck darf das Bundeszentralregister nach den §§ 2a bis 2e DNA-IFG Auswertungen durchführen. Die Anlage zu § 2c DNA-IFG führt z.Zt. 41 Straftatbestände auf, nicht alle sind von erheblicher Bedeutung.

Im Berichtszeitraum hat sich eine Rechtsdiskussion zu folgenden Punkten ergeben:

- Reicht für die Entnahme des Analysematerials (in der Regel eine Speichelprobe) die Einwilligung des Betroffenen aus?
- Kann auch für die retrograde molekulargenetische Untersuchung und die Speicherung in der Gendatei eine Einwilligung ausreichen?

- Streitig war bis vor kurzem, ob für die Einspeicherung in die Gendatei aus laufenden Strafverfahren nach § 81g StPO eine richterliche Prognose notwendig ist.

Für die Entnahme von Analysematerial verweist § 81g Abs. 3 StPO auf § 81a Abs. 2 und § 81f StPO, d.h., für eine Entnahme von Analysematerial gegen den Willen des Betroffenen ist eine richterliche Anordnung notwendig. Im Umkehrschluß hält der Landesbeauftragte die reine Probeentnahme auch für zulässig, wenn der Beschuldigte oder der Verurteilte in diese Probeentnahme **wirksam** eingewilligt hat. Bei inhaftierten Personen ist allerdings sicherzustellen, daß die Verweigerung der Zustimmung keine nachteiligen Wirkungen auf Vollzugsmaßnahmen hat.

Anders beurteilt der Landesbeauftragte die Rechtslage bei der molekulargenetischen Untersuchung entnommenen Materials gem. § 81e, § 81f und § 81g Abs. 3 StPO. Hier ist in jedem Fall eine richterliche Anordnung erforderlich.

Aufgrund der Tiefe des Eingriffs in das Persönlichkeitsrecht durch die molekulargenetische Untersuchung ist der Richtervorbehalt unerläßlich. Für die molekulargenetische Untersuchung wird zwar vielfach der harmlos klingende Begriff "Genetischer Fingerabdruck" verwandt und damit eine Vergleichbarkeit mit der Abnahme von Fingerabdrücken suggeriert, dies ist aber nicht zutreffend. Die DNA-Analyse birgt, auch wenn sie sich im Strafprozeßrecht derzeit auf nicht-codierende Merkmale beschränkt, durch die Speicherung in der Gendatei des BKA die Gefahr und die grundsätzliche Möglichkeit weiterer Verarbeitungsschritte über die Identitätsfeststellung hinaus.

Das Erfordernis der richterlichen Anordnung gilt um so mehr im Rahmen von molekulargenetischen Untersuchungen nach § 81g StPO.

Für die sog. Negativprognose, die allein eine Untersuchung und anschließende Speicherung in der Gendatei begründen kann, darf die richterliche Anordnung nicht durch eine Einwilligung ersetzt werden.

Das würde bedeuten, daß der Betroffene eine Art von Selbstbezichtigung abgeben würde, daß bei ihm die Gefahr künftiger Strafverfahren besteht, denn nur dann dürfen molekulargenetische Untersuchung und Speicherung erfolgen.

In seiner Auffassung sieht sich der Landesbeauftragte durch den Beschluß des Bundesverfassungsgerichtes vom 14. Dezember 2000 (Az.: 2 BvR 1741/99) bestätigt. Danach ist vor einer Einspeicherung in die Gendatei des BKA ein richterlicher Beschluß nach § 81g StPO einzuholen. Darüber hinaus fordert das Bundesverfassungsgericht eine durch Tatsachenfeststellung begründete Einzelfallentscheidung. Eine bloße Wiederholung des Gesetzestextes und eine Aufzählung der Vorstrafen reichen entgegen der bisherigen Praxis einiger Gerichte künftig nicht mehr aus.

Erfreulicherweise wird in Sachsen-Anhalt nach Angaben des Ministeriums der Justiz in jedem Fall bei Maßnahmen nach § 81g eine richterliche Anordnung eingeholt. Das gilt zumindest für die retrograde Erfassung rechtskräftig verurteilter Personen.

Anders, so die bisherigen Erkenntnisse, sieht es aus, wenn in laufenden Ermittlungsverfahren molekulargenetische Untersuchungen angeordnet werden.
Eine Kontrolle im LKA sowie Nachfragen bei Polizeidirektionen haben ergeben, daß in diesen Fällen häufig die Prüfung des § 81g StPO durch die Polizei erfolgt und nicht durch den gesetzlich vorgesehenen Richter. Das ist bedenklich, denn die nach § 81e StPO gewonnenen Datensätze dürfen gem. § 3 Satz 3 DNA-IFG nur unter den Voraussetzungen des § 81g StPO in der DNA-Analysedatei gespeichert werden. Der Gesetzgeber ging dabei davon aus, daß im Zeitpunkt der Speicherung auf jeden Fall eine richterliche Anordnung vorliegt.
Die Intention des Gesetzgebers zielt also auch im laufenden Ermittlungsverfahren auf eine **richterliche** Negativprognose ab.

Die rechtspolitische Diskussion zu Einsatz und Möglichkeiten der DNA-Analyse dürfte noch lange nicht abgeschlossen sein. Die kurze und schrille Diskussion im März 2001, inwieweit nicht bei allen deutschen Männern vorsorglich ein „genetischer Fingerabdruck“ erhoben und gespeichert werden sollte, zeigte neben der Gefahr emotional bedingter „Entgleisungen“ ein hohes Maß an Unwissen über die tatsächlich vorhandenen und rechtlich möglichen Eingriffsmaßnahmen im Rahmen des geltenden Rechts (vgl. dazu auch die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12. März 2001 **(Anlage 27)**), ganz zu schweigen von den praktischen Problemen der Durchführung und der Geeignetheit einer solchen Maßnahme.

16.5 Der gläserne Internetbürger?

Wenn es nach den Innenministern des Bundes und der Länder ginge, wäre es mit der Freiheit der Bürger und Bürgerinnen, unbeobachtet von staatlichen Stellen im Internet zu surfen, bald vorbei. Auf ihrer Konferenz am 24. November 2000 haben die Herren gefordert, Provider und Betreiber von Servern sollten künftig verpflichtet werden, IP-Adresse und Nutzungszeitraum jedes im Internet aktiven Rechners zu protokollieren und diese Daten eine angemessene Zeit aufzubewahren.

Mit Hilfe der IP-Adresse kann bekanntlich jeder Rechner im Internet eindeutig identifiziert werden. Über die Protokolldateien der Server können Provider und Betreiber erkennen, von welchen IP-Adressen aus welche Webseiten aufgerufen werden. Aufzeichnungen darüber sehen die Innenminister als ideale Vorratsdatensammlung für den Fall, daß irgendwann einmal daraus Spuren von Straftaten nachgewiesen werden könnten.

Wollte man diese Idee ernsthaft umsetzen, könnte man auch gleich die Post und andere vergleichbare Dienstleister verpflichten, sämtliche Absender- und Empfängerangaben im Brief- und im Paketverkehr für Zwecke einer möglichen späteren Strafverfolgung zu speichern.

Der Landesbeauftragte hat gemeinsam mit seinen Kolleginnen und Kollegen der übrigen Bundesländer (außer Thüringen) in einer Presseerklärung deutlich gemacht, daß eine solche Vorschrift nicht nur verfassungswidrig wäre, sondern auch für praktische Zwecke der Strafverfolgung schnell ungeeignet werden könnte. Die generelle Protokollierungs- und Aufbewahrungspflicht der personenbezogenen Daten aller Internetbenutzer würde nicht nur unzulässig in das Grundrecht auf informationelle Selbstbestimmung eingreifen, sondern wäre auch angesichts von Millionen rechtstreuer Internetnutzer völlig unverhältnismäßig. Im übrigen hat das Bundesverfassungsgericht schon 1983 im sog. Volkszählungs-
Urteil die Vorratsdatenhaltung verboten.

Es besteht dafür auch aus praktischen Gründen gar kein Bedürfnis. In konkreten Ermittlungsfällen haben Polizei und Justiz schon nach der heutigen Rechtslage jederzeit die Möglichkeit, entsprechende Angaben bei den Providern zu erhalten und in eine konkrete Strafverfolgung einzubringen. Im übrigen würde eine generelle Erfassung aller Internetnutzer nur dazu führen, daß man sich mit Hilfe der weltweiten Möglichkeiten bei Providern im Ausland entsprechende IP-Adressen besorgt, die den deutschen Strafverfolgungsorganen nicht zugänglich sind.

Der Landesbeauftragte ist mit seinen Kolleginnen und Kollegen deshalb der Auffassung, daß es den unbescholtenen Bürgerinnen und Bürgern in Deutschland auch weiterhin möglich sein muß, unbeobachtet im Internet zu surfen.

16.6 Aufbewahrungsbestimmungen im Bereich der Justiz

Auch im abgelaufenen Berichtszeitraum wurde der Forderung nach einer gesetzlichen Grundlage für die Aufbewahrung von Schriftgut der Justiz nicht entsprochen (vgl. zuletzt IV. Tätigkeitsbericht, S. 96).

Die 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher am 07./08. Oktober 1999 zum wiederholten Male eine gesetzliche Grundlage für die Aufbewahrungsbestimmungen des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften angemahnt **(Anlage 6).**

In dieser Entschließung wurde auch auf einen Beschluß des OLG Frankfurt/M vom 16.08.1998 hingewiesen. Darin wird die alsbaldige Schaffung einer gesetzlichen Grundlage für Akten gefordert, weil der für eine Übergangsfrist nach der Verfassungsrechtsprechung hinzunehmende Übergangszustand als abgelaufen bewertet wird.

Schon 1999 hat der damalige Vorsitzende der Konferenz der Justizministerinnen und -minister die Forderung der Datenschutzkonferenz nicht per se abgelehnt, doch seither scheinen die Bemühungen in der von der Justizministerkonferenz einberufenen Arbeitsgruppe, eine gesetzliche Grundlage zu schaffen, nicht voran zu gehen.

16.7 Länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Wie bereits im IV. Tätigkeitsbericht (S. 98 f) angesprochen, stellt die Auskunftserteilung aus dem neuen Register per Telefon oder Telefax eine besondere Schwachstelle dar. Die letzte dem Landesbeauftragten übersandte Zusammenfassung der organisatorisch-technischen Leitlinien (Stand 26.09.2000) sieht in Ziff. 3.2.6 zwar die telefonische Auskunft bzw. die Auskunft per Telefax nur im Ausnahmefall vor und erlaubt diese nur nach Prüfung der Authentizität der anfragenden Behörde, damit sind aber die Bedenken zur technisch sicheren Übermittlung personenbezogener Daten nicht ausgeräumt.

Insbesondere hinsichtlich der Auskunftserteilung per Telefax verweist der Landesbeauftragte auf seine unverändert aktuellen Hinweise im II. (S. 91 f), III. (S. 62 ff) und IV. Tätigkeitsbericht (S. 49 f).

16.8 Täter-Opfer-Ausgleich im Strafverfahren

Die Durchführung des Täter-Opfer-Ausgleichs in Sachsen-Anhalt ist vom Landesbeauftragten im III. (S. 107) und IV. Tätigkeitsbericht (S. 102 f) positiv

gewertet worden. Im Jahresbericht 1999 der sozialen Dienste der Justiz (JMBl. LSA Nr. 17/2000) wird noch ein ständiger Anstieg erfolgreich durchgeführter Täter-Opfer-Ausgleichsverfahren registriert.

Leider ist diese datenschutzfreundliche Praxis durch das Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des Gesetzes über Fernmeldeanlagen vom 20. Dezember 1999 eingeschränkt worden.

Während bisher der Täter-Opfer-Ausgleich nur durchgeführt werden konnte, wenn Täter **und** Opfer mit der Durchführung einverstanden waren, kommt es nunmehr auf die Mitwirkungsbereitschaft des Täters gar nicht mehr an, auf den Willen des Opfers nur bei ausdrücklicher Ablehnung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte zuvor noch in ihrer Entschließung vom 7./8. Oktober 1999 **(Anlage 7)** festgehalten, daß Rechtsfriede und Toleranz sowie die Achtung und wirksame Unterstützung von Opfern nur verwirklicht werden können, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Maßgeblich für einen erfolgreichen Täter-Opfer-Ausgleich sei aber auch die Sicht des Beschuldigten, die daher nicht völlig außer Betracht bleiben könne.

Bedauerlicherweise ist der Gesetzgeber diesem berechtigten datenschutzrechtlichen Anliegen nicht gefolgt. Man wird nun abwarten müssen, ob sich das Verfahren im neuen Gewande so erfolgreich erweist, wie die alte Regelung in unserem Bundesland.

16.9 Mängel bei der Registrierung von Wahlrechtsausschlüssen

Im Berichtszeitraum kam es zu einer Diskussion zwischen den Datenschutzbeauftragten der Länder und den Länderjustizverwaltungen über die Anforderungen an datenschutzgerechte Mitteilungen bei Wahlrechtsausschlüssen im Strafverfahren. Insbesondere fehlende Folgemitteilungen der Staatsanwaltschaften über die Beendigung bzw. den Ablauf von Wahlrechtsausschlüssen an die das

Wählerverzeichnis führenden Meldebehörden hatten in Einzelfällen dazu geführt, daß Wahlrechte nicht wahrgenommen werden konnten.

Seitens einiger Länderjustizverwaltungen wurden Folgemitteilungen rundweg abgelehnt und Meldebehörden darauf verwiesen, daß auch ein Führungszeugnis für den Betroffenen angefordert werden könne.
Diese Verfahrensweise war schon deshalb abzulehnen, weil dabei die Meldebehörden eine Fülle an unzulässigen Überschußinformationen erhalten würden, die sie zu ihrer Aufgabenerfüllung nicht benötigen.

Erfreulicherweise hat das Ministerium der Justiz unseres Bundeslandes hierzu von Anfang an einen datenschutzfreundlichen Standpunkt vertreten und dem Landesbeauftragten mitgeteilt, daß das Ministerium eine Mitteilung über das Ende des Rechtsverlustes für richtig und zulässig halte. Zumindest gelte dies für eine Mitteilung an den letzten bekannten Wohnsitz des Verurteilten. Des weiteren wird in Sachsen-Anhalt auch die ausdrückliche (vorzeitige) Wiederverleihung des aktiven und passiven Wahlrechts den Meldebehörden zum Wählerverzeichnis mitgeteilt.

Wie dem Landesbeauftragten zwischenzeitlich bekannt wurde, sollen sich nunmehr auch die anderen Landesjustizverwaltungen und das Bundesministerium der Justiz auf eine solche Praxis und die entsprechende Änderung der Nr. 12 MiStra verständigt haben.

16.10 Datenschutz bei den Notaren

16.10.1 Dienstordnung für Notare

Bereits in seinem IV. Tätigkeitsbericht (S. 108) hat der Landesbeauftragte über die Entwicklung bei der Neufassung der bundesweit geltenden Dienstordnung für Notare (DONot) durch die Landesjustizverwaltungen berichtet.

Dieses Vorhaben ist mittlerweile zur Veröffentlichungsreife gediehen.

Positiv ist anzumerken, daß § 14 Abs. 1 DONot geändert wird. Künftig können Urkundenrolle und Verwahrungsbuch als Buch mit herausnehmbaren Einlageblättern geführt werden. Nach Ablauf des Kalenderjahres sind die Einlegeblätter unverzüglich gem. § 30 zu heften und zu siegeln. In der alten Fassung des § 14 DONot waren nach Ablauf des Kalenderjahres die Einlageblätter unverzüglich mit Schnur und Siegel zu verbinden und fest einzubinden. Dies hatte zu datenschutzrechtlichen Problemen geführt.

Negativ ist bedauerlicherweise festzustellen, daß die von allen Landesbeauftragten begrüßte Fassung des § 5, die entsprechend der Rechtsprechung des Bundesgerichtshofes klarstellen sollte, daß die Notare in vollem Umfang der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen, im Laufe der Novellierungsarbeiten (als überflüssig) wieder gestrichen wurde.

Mängelbehaftet ist nach wie vor § 17, der die automationsgestützte Führung der Bücher und Verzeichnisse regelt. Auch in der überarbeiteten Fassung fehlen hinreichend konkrete Löschungsregelungen für gespeicherte Daten, auch wenn der Charakter der Daten als Buch gem. § 14 Abs. 1, als Massenkartei gem. § 14 Abs. 2 oder als Verzeichnis festgelegt wurde und entsprechend zu behandeln ist. Außerdem fehlen immer noch Regelungen zu Zugangs- und Bearbeitungsrechten.

Nicht berücksichtigt wurde auch ein Vorschlag des Landesbeauftragten zur Prüfung der Amtsführung der Notare und Notarinnen gem. § 32 DONot. Der Landesbeauftragte hätte es als zweckmäßig angesehen, daß er bei Beanstandungen der Prüfer wegen Nichtbeachtung datenschutzrechtlicher Vorschriften informiert und bei Verstößen und Mängeln im Zusammenhang mit Auskünften oder Abrufen aus Registern darüber hinaus auch die Leiterinnen und Leiter der Registergerichte unterrichtet worden wären.

16.10.2 Ein vorausdenkender Notar

Im Berichtszeitraum hat sich ein Notar an den Landesbeauftragten gewandt, da bei seiner Amtsprüfung durch die Aufsichtsbehörde beanstandet worden war, daß er aus datenschutzrechtlichen Bedenken die Einlageblätter eines Kalenderjahres nicht zum festen Einbinden an eine Druckerei gegeben hatte, sondern "lediglich" geheftet und gesiegelt hatte.

Der Landesbeauftragte hat die datenschutzrechtlichen Bedenken des Notars geteilt und seiner Aufsichtsbehörde empfohlen, in Anbetracht der damals bereits absehbaren Änderung des § 14 Abs. 1 DONot von einer Beanstandung dieser künftig datenschutzfreundlicheren Verfahrensweise abzusehen.

16.11 Staatsanwaltschaftliche Mitteilungen an einen öffentlichen Arbeitgeber

Einem Arbeitnehmer war wegen Trunkenheit im Straßenverkehr durch Strafbefehl eines Amtsgerichts die Fahrerlaubnis entzogen und gleichzeitig eine Geldstrafe gegen ihn festgesetzt worden. Hierüber informierte die Staatsanwaltschaft seinen öffentlichen Arbeitgeber, so daß der Petent, der in einer Kinder- und Jugendeinrichtung als Erzieher tätig war, Nachteile befürchtete und sich deshalb Rat suchend an den Landesbeauftragten wandte.

Rechtsgrundlage für eine diesbezügliche Datenübermittlung ist § 14 Abs. 1 Nr. 5 EGVG. Hiernach ist die Übermittlung von personenbezogen Daten in Strafsachen zulässig, wenn die Kenntnis der Daten aus Sicht der übermittelnden Stelle (also der Staatsanwaltschaft) erforderlich ist für die Entscheidung über eine Kündigung, für andere arbeitsrechtliche Maßnahmen oder für die Untersagung der Einstellung, Beschäftigung oder Beaufsichtigung von Kindern und Jugendlichen.

In der Gesetzesbegründung zu § 14 Abs. 1 EGVG wird klargestellt, daß die übermittelnde Stelle keine inhaltliche Prüfung oder Ermittlung anstellen muß, sondern lediglich eine Art Schlüssigkeitsprüfung durchzuführen hat. Sind die

Daten der zu übermittelnden Art nach den für den Empfänger geltenden Rechtsvorschriften zur Erfüllung seiner Aufgaben grundsätzlich beachtlich, so ist die Kenntnis der Daten im Sinne dieser Vorschrift erforderlich. Ob der Empfänger aufgrund der übermittelten Daten tatsächlich Maßnahmen ergreift, ist unerheblich.

Die Datenübermittlung von der Staatsanwaltschaft an den Arbeitgeber des Petenten war somit rechtlich gedeckt und datenschutzrechtlich nicht zu beanstanden. Der Petent mußte sich mit der Informierung seines Arbeitgebers abfinden.

17. Schulen

17.1 EDV-Einsatz in Schulen und der Anschluß an das Internet

Der Landesbeauftragte begrüßt, daß Schülerinnen und Schüler z.B. im Rahmen der Aktion „Schulen ans Netz“ frühzeitig an die moderne Technik herangeführt werden. Die nachwachsenden Generationen haben damit eine frühe Chance, die neue Technik kennenzulernen und professionell mit ihr umzugehen. Er weist aber auch darauf hin, daß die Nutzung dieser neuen Technik und insbesondere das Internet mit erheblichen Gefahren verbunden sind, weil es sich um ein unsicheres, weltumspannendes Netz handelt, das nicht unter Sicherheitsaspekten entwickelt wurde.

Aus dem Einsatz dieser modernen Kommunikationsmittel ergeben sich aber auch für die Schulen selbst Konsequenzen. So dürfen schulische Echtdaten im Interesse der Schülerinnen und Schüler, ihrer Erziehungsberechtigten und auch der Lehrkräfte nur in lokalen Netzen verarbeitet werden, die vom Internet streng abzuschotten sind.

Der Landesbeauftragte hat den ständig wachsenden Einsatz moderner Kommunikationsmittel zum Anlaß genommen, im Rahmen einer Bekanntmachung **(Anlage 28)** die wichtigsten Aspekte aufzuzeigen (abgedruckt auch SVBl. LSA Nr. 6/2000, S. 153).

17.2 Umgang mit chronischen Erkrankungen von Schülerinnen und Schülern innerhalb des Schulbereiches

Die Bundeszentrale für gesundheitliche Aufklärung beabsichtigt ein Handbuch zu o.a. Thema zu erstellen.
Das Kultusministerium erbat dazu auch datenschutzrechtliche Hinweise des Landesbeauftragten.

Schwerpunkt der Stellungnahme des Landesbeauftragten waren die erforderlichen Einwilligungserklärungen der betroffenen Schüler und ihrer Eltern. Erforderlich ist eine Einwilligungserklärung (§ 4 Abs. 2 DSG-LSA) für die Übermittlung der betreffenden Schülerdaten von einer informierten Lehrkraft (z.B. innerhalb der Schule - an Vertretungskräfte und Mitschüler -) und eine Erklärung zur Entbindung des Arztes von der ärztlichen Schweigepflicht (für den Kontakt des behandelnden Arztes zur Schule).

Der Landesbeauftragte hat hierzu entsprechende MUSTER erstellt und empfohlen, diese ins Handbuch aufzunehmen.
Die Stellungnahme mit den Mustererklärungen wurde an die übrigen Datenschutzbeauftragten der Länder übersandt, da es sich um ein länderübergreifendes Projekt handelt.

17.3 Abrechnungsunterlagen für Klassenfahrt

Nach der Abschlußfahrt einer 10. Klasse wurde der die Reise organisierende Lehrer von seinem Schulamt aufgefordert, alle mit der Reise im Zusammenhang stehenden namentlichen Quittungen und Belege für die Reisekostenabrechnung im Original vorzulegen.
Der Lehrer stellte die Rechtmäßigkeit der Aufforderung in Frage und bat den Landesbeauftragten um seine Rechtsauffassung zur Offenlegung von personenbezogenen Daten im Zusammenhang mit Klassenfahrten.

Alle Lehrerinnen und Lehrer stehen gem. § 30 Abs. 2 Satz 1 SG in einem unmittelbaren Dienstverhältnis zum Land. Schulische Veranstaltungen - wie Klassenfahrten - stehen in einem unmittelbaren rechtlichen Bezug zum Dienstverhältnis.

Daran ändert sich nichts, wenn im Rahmen der Fahrtplanungen durch individuelle Verhandlungen des Lehrers, z.B. mit Reiseunternehmen, Rechnungen solcher Klassenfahrten an die Privatadresse eines Lehrers gehen. Die Rechnung wird auch dann zu einer dienstlichen Unterlage. Enthalten diese Unterlagen personenbezogene Daten, so richtet sich der Umgang mit ihnen nach § 84a Abs. 2 SG i.V.m. § 28 Abs. 1 Satz 1 DSG-LSA.

Danach dürfen Daten von Lehrerinnen und Lehrern von der Schulbehörde erhoben, verarbeitet oder genutzt werden, wenn eine Rechtsvorschrift dies vorsieht. Für die Reisekosten der Lehrer gelten die speziellen Vorschriften des Bundesreisekostengesetzes. Darin ist z.B. nur die Erstattung der **notwendigen** Fahrkosten vorgesehen. Daraus folgt, daß die bei Klassenfahrten häufig von Reiseunternehmen angebotenen Freiplätze bei der Gesamtkostenabrechnung umzulegen sind. Deshalb hat die abrechnende Schulbehörde das Recht und die Pflicht, personenbezogene Kostenbelege im Hinblick auf die Teilnehmer zu prüfen.

Gegen die Pflicht zur Vorlage solcher Unterlagen an das Staatliche Schulamt, zu Prüfungszwecken auch an den Schulleiter, bestehen deshalb aus datenschutzrechtlicher Sicht keine Bedenken.

18. Sozialwesen

18.1 Ermäßigungs-/Erlaßanträge zu Elternbeiträgen in Kindertagesstätten

Im IV. Tätigkeitsbericht (S. 112) hatte der Landesbeauftragte mitgeteilt, daß dieser Problembereich aus datenschutzrechtlicher Sicht als abgeschlossen angesehen werden kann. Leider trog diese Hoffnung, denn aufgrund der Änderung des KiBeG zum 01.08.1999 wurde es erneut erforderlich, Einzelberatungen aufzunehmen, weil die Anpassung der Fragebögen wiederum Probleme bereitete.

Im folgenden sollen einige Problembereiche aufgezeigt werden:

- Bei der Ermittlung der zumutbaren Belastung finden nur die in § 90 Abs. 4 SGB VIII ausgewiesenen §§ des BSHG als Berechnungsgrundlage entsprechende Anwendung.

- Nach § 90 Abs. 2 Satz 2 SGB VIII bleiben Elternteile bei der Berechnung unberücksichtigt, die nicht mit dem Kind oder dem Jugendlichen zusammenleben. Hinweise hierzu und zu eheähnlichen Gemeinschaften hatte der Landesbeauftragte bereits im III. Tätigkeitsbericht (S. 123 f) gegeben.

- In einer Satzung wurden Auskunftspflichten genannt, die durch das SGB VIII nicht gedeckt waren. So sollten die Eltern verpflichtet werden, Angaben zur Arbeitsstelle zu machen.

- In einer Gebührensatzung wurden Abwaschgebühren festgesetzt, wobei weder die Höhe noch die Fälligkeit angegeben waren. Die Festsetzung entsprach nicht den Anforderungen des § 2 Abs. 1 KAG-LSA. In diesem Fall war es sogar erforderlich, die Kommunalaufsicht einzuschalten.

Allerdings waren nicht alle Probleme in der schwierigen gesetzlichen Materie zu suchen:

So versuchte eine Amtsleiterin die fehlerhaften Fragebögen und fehlenden Erläuterungen bzw. Hinweise damit zu rechtfertigen, daß sie „bisher keine Zeit gehabt habe“, sich mit der Rechtsgrundlage (SGB) zu befassen. Dadurch fehlte natürlich die Kenntnis, welche Daten überhaupt zu erheben sind, oder daß nach §§ 13, 14 SGB I eine Aufklärungs- und Beratungspflicht gegenüber Antragstellern besteht.

Sie sah auch nicht ein, daß die Angabe einer Rechtsgrundlage den betroffenen Bürger in die Lage versetzen soll, selbst im Gesetz nachzulesen, zu welchen Angaben er verpflichtet ist.

Um alle Landkreise und kreisfreien Städte mit den Problempunkten zu erreichen, hat der Landesbeauftragte mit dem Landkreistag eine Beratung im Rahmen der regelmäßig stattfindenden Tagung des Arbeitskreises der Jugendamtsleiter durchgeführt. Daraufhin besserte sich die Bearbeitung dieser Fälle deutlich.

18.2 „Vererbbarkeit“ von Persönlichkeitsrechten?

Ein Erbe wandte sich an den Landesbeauftragten, weil ein Sozialleistungsträger ihm den Einblick in die bei ihm vorhandenen Unterlagen über den Verstorbenen verwehrte. Als Begründung für den gewünschten Einblick gab der Erbe an, es seien im letzten Lebensjahr des Verstorbenen erhebliche Summen der Ersparnisse verschwunden und es bestehe der Verdacht, daß ein Vermögensschaden zu Lasten der Erben entstanden sei.

Dem Anraten, bei einem Verdacht auf Vermögensschädigung die Staatsanwaltschaft einzuschalten, folgte er nicht. Vielmehr vertrat der Erbe die Auffassung, daß er als Erbe direkt in die Rechte des Verblichenen eintreten würde.

Die Ablehnung der Akteneinsicht durch den Sozialleistungsträger war rechtens.

Die Persönlichkeitsrechte einer natürlichen Person sind an diese gebunden und gehen - von einzelnen gesetzlich geregelten Ausnahmefällen abgesehen - mit derem Tod unter. Eine Ausnahme ist in § 35 Abs. 5 Satz 2 SGB I enthalten. Danach dürfen Sozialdaten Verstorbener verarbeitet - also auch an Dritte übermittelt - werden, wenn schutzwürdige Interessen des Verstorbenen oder seiner Angehörigen (das sind aber nicht unbedingt die bürgerlich-rechtlichen Erben!) dadurch nicht beeinträchtigt werden können.

Der Begriff der Angehörigen ist nach Sinn und Zweck der Vorschrift in Anlehnung an § 56 SGB I auszulegen. Dort sind nur Ehegatten, Kinder, Eltern und Haushaltsführer genannt. Der hier auftretende Erbe gehörte nicht zu diesem Personenkreis.

Und in diesem speziellen Fall gab es noch ein weiteres Hindernis:

Der Beschwerdeführer war nur Miterbe. Im Falle einer Erbengemeinschaft aber müssen Auskünfte durch alle (Mit)Erben gefordert werden. Auch daran fehlte es.

18.3 Datenübermittlungen bei der öffentlichen Jugendhilfe

Mehrere Gemeinden als Betreiber von Kindertagesstätten hatten sich zu einem Zweckverband zusammengeschlossen. In ihrer Satzung hatten sie dazu festgelegt, daß die für die Gemeinden geltenden Vorschriften zum Zweckverband angewendet werden sollten.

Aufgrund dieser Satzung ging der Landkreis fälschlicherweise davon aus, daß die Jugendhilfeplanung nach § 80 SGB VIII ebenfalls auf den Zweckverband übergegangen ist und übermittelte diesem deshalb personenbezogene Planungsdaten.

Hierbei wurde übersehen, daß der Landkreis die ihm obliegende Jugendhilfeplanung **nicht übertragen** kann, sondern nach § 80 SGB VIII im Rahmen seiner eigenen Planung lediglich den Zweckverband als Träger dieser Einrichtungen frühzeitig zu beteiligen hat.

Auf den Hinweis durch den Landesbeauftragten hat der Landkreis seine bisherige Verfahrensweise sofort eingestellt.

18.4 Auskunft über den Werdegang des „verlorenen“ Sohnes

Die Eltern eines Jungen, der den Kontakt mit ihnen abgebrochen hatte, baten das Jugendamt um Auskunft. Das Jugendamt, daß den Jugendlichen eine Zeitlang ihm Rahmen einer Maßnahme der Hilfe zur Erziehung betreut hatte, lehnte Auskünfte mit dem Hinweis auf die „Verletzung des Datenschutzes“ ab.

Der Landesbeauftragte, an den sich die Eltern wandten, mußte sie darauf hinweisen, daß der Sohn mit Vollendung des 18. Lebensjahres volljährig geworden war und damit ausschließlich allein bestimmt, mit wem er Kontakt pflegen und welche Rechtsgeschäfte er tätigen will. Diese Tatsache war den Eltern so nicht bewußt.

Der Landesbeauftragte schlug als praktische Lösung vor, dem jungen Erwachsenen Post im verschlossenen Umschlag über das Jugendamt zukommen zu lassen. Dann kann er selbst entscheiden, ob und wann er sich mit seinen Eltern in Verbindung setzen will.

18.5 Fehlbelegungsprüfungen in Krankenhäusern

Bereits im IV. Tätigkeitsbericht (S. 117) hat sich der Landesbeauftragte mit der Problematik der Kontrolle der Krankenhäuser durch den Medizinischen Dienst der Krankenversicherungen (MDK) im Zusammenhang mit Fehlbelegungsprüfungen eingehend auseinandergesetzt.

Im jetzigen Berichtszeitraum schlossen die Krankenkassen mit dem Dachverband der Leistungserbringer eine Vereinbarung ab, wie im Streitfall das Verfahren zur Einigung der Vertragsparteien vor einer einzurichtenden Konfliktstelle ausgestaltet werden sollte.

Datenschutzrechtlich bedenklich war dabei die vorgesehene Regelung, daß die Patientenunterlagen in 20facher Ausfertigung der Konfliktstelle vorgelegt werden sollten. Eine Anonymisierung der Krankenunterlagen war nicht vorgesehen. Die Beschaffung einer Einwilligung der Patienten erschien in diesem Zusammenhang wenig praktikabel, auch dürfte dieses Verfahren die ehemaligen Patienten kaum interessieren.

Aufgrund der Intervention des Landesbeauftragten änderten die Vertragsparteien den Vertrag derart, daß nunmehr nur noch anonymisierte Daten der Konfliktstelle vorgelegt werden.

18.6 Daten auf der gesetzlichen Krankenversicherungskarte

Ein aufmerksamer Bürger ließ seine Krankenversicherungskarte auslesen und stellte dabei fest, daß dort Daten enthalten waren, deren Bedeutung ihm

Mitarbeiter seiner gesetzlichen Krankenversicherung nicht erklären konnten. Daraufhin wandte er sich an den Landesbeauftragten.

Dessen Überprüfung ergab, daß über die in § 291 Abs. 2 SGB V enumerativ aufgeführten Angaben unzulässigerweise weitere Angaben, z.B. zum Risikostrukturausgleich nach § 266 SGB V, auf der Versichertenkarte enthalten waren.

Im Zuge der weiteren Nachforschungen wurde festgestellt, daß diese Angaben nicht nur im Bereich der Krankenkasse in Sachsen-Anhalt, sondern sogar bundesweit genutzt wurden. Deshalb war die Zuständigkeit des Bundesbeauftragten für den Datenschutz gegeben, der die Angelegenheit weiter verfolgte.

Zwischenzeitlich werden Überlegungen angestellt, den Umfang der Daten auf der Krankenversicherungskarte zu erweitern. In jedem Fall ist die festgestellte Verfahrensweise geeignet, bei den Versicherten Mißtrauen hinsichtlich des Umgangs mit ihren personenbezogenen Daten zu wecken.

18.7 Anforderung von Patientenunterlagen durch eine Betriebskrankenkasse

Durch Anfragen wurde dem Landesbeauftragten bekannt, daß die Novitas Vereinigte Betriebskrankenkasse auch in Sachsen-Anhalt Patienten- bzw. Unterlagen aus Krankenhausbehandlungen zur Vorlage bei einem von ihr bestimmten Arzt abforderte. Zur rechtlichen Begründung bezog sie sich auf verschiedene gerichtliche Entscheidungen, die dieses Verfahren angeblich zulassen würden. Der Landesbeauftragte fand diese weder rechtlich überzeugend noch gar bindend für andere Fälle.

Richtig ist, daß die Krankenkassen nach § 275 SGB V berechtigt sind, bei individuellen Verdachtsfällen (nicht generell!) Voraussetzungen, Art und Umfang der Leistungen im Krankenhaus zu prüfen. Da die Kassen selbst über keinen medizinischen Sachverstand verfügen, sieht das Gesetz in solchen Fällen vor, Stellungnahmen des Medizinischen Dienstes der Krankenversicherungen (MDK) einzuholen. Die Krankenhäuser sind dementsprechend verpflichtet, die Behandlungsunterlagen zur Prüfung nach § 276 Abs. 2 SGB V unmittelbar an den MDK

zu senden. Eine Pflicht des Krankenhauses, Unterlagen an andere von der Kasse beauftragte Ärzte zu übersenden, gibt es nicht. Auch eine Schweigepflichtentbindungserklärung des betroffenen Patienten ändert nichts an dem gesetzlich vorgesehenen Verfahrensweg über den MDK.

Da diese Betriebskrankenkasse bundesweit tätig ist, hat der Bundesbeauftragte für den Datenschutz in einem Rundschreiben an die Dachverbände der verschiedenen Krankenversicherungen auf diese Rechtslage hingewiesen.

Krankenhäuser tun gut daran, die Regeln zu beachten, da ein Verstoß gegen diese Vorschriften unter Umständen zu einem Strafverfahren nach § 203 StGB führt.

19. Statistik

19.1 Hochbaustatistik

In dem am 01.01.1999 in Kraft getretenen (Bundes-)Hochbaustatistikgesetz (HBauStatG) ist in § 6 auch die Auskunftspflicht neu geregelt worden. Auskunft für Bundesstatistiken ist nach § 15 Abs. 2 BStatG nur gegenüber den mit deren Durchführung betrauten Stellen und Personen zu erteilen. In Sachsen-Anhalt ist dies gemäß § 2 Abs. 2 Ziff. 1 StatG-LSA nur das Statistische Landesamt.

Allerdings ist in Sachsen-Anhalt z.Zt. das Verfahren noch so, daß die Bauherren oder die mit der Baubetreuung Beauftragten die zutreffenden Merkmale auf den Erhebungsbögen ausfüllen und die Belege dann zunächst an die Bauaufsichtsbehörden weiterleiten. Diese ergänzen die Belege mit Merkmalen, die nur sie mitteilen können und geben sie dann an das Statistische Landesamt weiter.

Im Gegensatz zum Landesbeauftragten, der in dieser Verfahrensweise eine Durchbrechung des Gebotes der strikten Trennung von Statistik und Verwaltungsvollzug sieht, hält das für Statistik in Sachsen-Anhalt zuständige Ministerium des Innern dieses Verfahren für legal. Es begründet diese Ansicht damit,

daß den Bauaufsichtsbehörden die von den Bauherren zur Statistik mitgeteilten Angaben ohnehin bekannt seien. Deshalb sei der Verfahrensweg in den meisten Bundesländern so üblich.

Das Ministerium des Innern hat inzwischen jedoch mitgeteilt, daß wegen der erfolgten umfassenden Novellierung der Landesbauordnung beabsichtigt sei, von der in § 6 Abs. 2 HBauStatG erteilten Verordnungsermächtigung Gebrauch zu machen und den Verfahrensweg der Auskunftserteilung neu zu regeln. Dabei wird auch auf datenschutzrechtliche Belange zu achten sein.

19.2 Bevölkerungsstatistik

Die Standesämter sind nach §§ 1, 2 und 6 BevStatG verpflichtet, bei Eheschließungen, Geburten, Sterbefällen, Todeserklärungen und gerichtlichen Feststellungen der Todeszeit laufend bestimmte Angaben mit Zählkarten zu erfassen und dem Statistischen Landesamt zu übersenden.

Durch das Ministerium des Innern wurde der Landesbeauftragte um Stellungnahme dazu gebeten, ob Bedenken gegen eine vereinfachte Übersendung dieser Daten auf Diskette an das Statistische Landesamt bestünden.

Bei der Überprüfung durch den Landesbeauftragten zeigte sich, daß bei dem Verfahren mit den bisher verwendeten Zählblättern auch von § 2 BevStatG nicht gedeckte personenbezogene Einzelmerkmale der Betroffenen an das Statistische Landesamt übermittelt wurden.

Das lag an einer Nichtbeachtung der gesetzlichen Grundlagen und einem diesbezüglich falschen Schreiben des Bundesministeriums des Innern aus dem Jahre 1990.

Auf die Hinweise des Landesbeauftragten wurden die Datenerhebungsbögen der z.Zt. geltenden Rechtslage angepaßt und die Standesämter darüber unterrichtet, welche Merkmale zukünftig als Hilfsmerkmale zu verwenden sind.

Diese nun korrekte Datenübermittlung an das Statistische Landesamt kann auch mittels maschinenlesbarer Datenträger erfolgen.

Der Bundesgesetzgeber bleibt aber aufgefordert, bei der nächsten Änderung des BevStatG den Katalog der Erhebungsmerkmale den aktuellen Erfordernissen anzupassen und die Hilfsmerkmale explizit im Gesetz zu nennen.

20. Strafvollzug

20.1 Prüfung von Justizvollzugsanstalten

Im Berichtszeitraum hat der Landesbeauftragte damit begonnen, die Justizvollzugsanstalten des Landes zu kontrollieren. Geprüft wurden in bisher zwei Anstalten als datenschutzrechtlicher Schwerpunkt die Führung der Gefangenenpersonalakten, die Übermittlung der personenbezogenen Daten der Gefangenen nach außen, aber auch der datenschutzgerechte Umgang mit Besucherdaten. Da im modernen Strafvollzug auch die automatisierte Datenverarbeitung stark Einzug gehalten hat, ist ein weiterer Schwerpunkt die Datensicherheit in allen Formen der Verarbeitung.

Gravierende Mängel haben sich bei den Prüfungen bisher nicht ergeben. Die Kontrollen werden fortgesetzt.

20.2 Privatisierung des Maßregelvollzuges

Das Land Sachsen-Anhalt hat mit Wirkung vom 01.01.2000 die Durchführung des Maßregelvollzuges privatisiert. Mit der SALUS gGmbH obliegt nun die Durchführung des Maßregelvollzuges einer 100%igen Landesgesellschaft.

Gemäß § 3 Maßregelvollzugsgesetz des Landes Sachsen-Anhalt ist die SALUS gGmbH zuständig für die Vollziehung strafrechtlicher Entscheidungen nach den §§ 63, 64 StGB sowie für einstweilige bzw. vorbereitende Maßnahmen aufgrund richterlicher Entscheidungen, mit denen Freiheitsentziehungen nach den §§ 7, 73 und 93a JGG sowie nach §§ 81, 126a, 163 und 453c StPO verbunden sind.

Die SALUS gGmbH ist dabei nach dem Beleihungs- und Betriebsübergangsvertrag verpflichtet, die Landeskonzeption für die Durchführung des Maßregelvollzuges sowie die einschlägigen und im einzelnen aufgeführten Erlasse und Dienstanweisungen der Landesregierung anzuwenden.

Im Rahmen der Rechts- und Fachaufsicht hat sich das zuständige Ministerium für Arbeit, Frauen, Gesundheit und Soziales umfassende Zugangs- und Kontrollrechte zu Räumlichkeiten, Einrichtungen wie auch zu Akten und anderen schriftlichen Unterlagen vorbehalten.

Der Landesbeauftragte hat in seiner Stellungnahme darauf Wert gelegt, daß bei personenbezogenen ärztlichen Unterlagen diese nur nach Entbindung von der ärztlichen Schweigepflicht eingesehen werden können, weil das Maßregelvollzugsgesetz diesbezüglich keine Einschränkungen von Grundrechten enthält.

Bei einem Kontrollbesuch des Landeskrankenhauses Uchtspringe konnte sich der Landesbeauftragte davon überzeugen, daß die medizinischen, psychologischen und therapeutischen Bestandteile von Patientenakten getrennt von der allgemeinen Patientenakte geführt werden.

20.3 Einschränkung des Brief- und Postgeheimnisses von Strafgefangenen

Auch für Strafgefangene gilt das Recht auf informationelle Selbstbestimmung - wenn auch mit den Einschränkungen des Strafvollzugsgesetzes (StVollzG). So darf das Brief- und Postgeheimnis nur dann eingeschränkt werden, wenn die Überwachung des Schriftwechsels eines Gefangenen gem. § 29 Abs. 3 StVollzG aus Gründen der Behandlung oder der Sicherheit oder der Ordnung der Anstalt angeordnet worden ist.

Das dies in der Vollzugspraxis nicht immer beachtet wird, erfuhr der Landesbeauftragte von einem Gefangenen, der sich beschwerte, ihm seien Schriftsätze und Mitteilungen von Behörden geöffnet und ohne Umschlag ausgehändigt worden, obwohl sein Schriftverkehr nicht der Überwachung unterliege. Die um

Stellungnahme gebetene Justizvollzugsanstalt bestätigte diesen Sachverhalt und begründete ihn damit, daß amtliche Schreiben von anderen Behörden (insbesondere der Staatsanwaltschaft) gesammelt in Umschlägen an die JVA gesandt würden. Darin befänden sich dann auch - ohne separaten Umschlag - Schreiben für die Gefangenen, die in diesem Zustand ausgehändigt würden.

Die Annahme des Landesbeauftragten, es könne in Sachsen-Anhalt doch gängige Verwaltungspraxis sein, amtliche Schreiben geöffnet und ohne Briefumschlag an Strafgefangene auszuhändigen, wollte das Ministerium der Justiz nicht teilen. Es trug vor, daß in solchen Fällen die jeweilige Behörde gebeten wird, „künftig an Gefangene gerichtete Schreiben zusätzlich zu kuvertieren".
Außerdem habe das Ministerium diesen „Einzelfall" zum Anlaß genommen, die Behörden seines Geschäftsbereiches nochmals auf die Problematik hinzuweisen.

Gleichwohl nimmt der Landesbeauftragte den Fall zum Anlaß, alle Behörden des Landes zu bitten, darauf zu achten, daß Post an Gefangene immer zu kuvertieren ist.

Kurz vor Redaktionsschluß beklagte sich derselbe Strafgefangene erneut über „die öffentliche Zustellung von Behördenpost".
Dieses Mal war die Post jedoch von der öffentlichen Stelle eines benachbarten Bundeslandes gekommen, so daß der Landesbeauftragte seinen dortigen Kollegen beteiligt hat.

21. Verfassungsschutz

Änderungen beim G 10-Gesetz

Das Bundesverfassungsgericht hat in seinem Urteil vom 14.07.1999 zum Verbrechensbekämpfungsgesetz für die Verwendung von privaten Daten, die aus

der Fernmeldeüberwachung durch staatliche Stellen gewonnen wurden, deutliche verfassungsrechtliche Schranken aufgezeigt und die Änderung bzw. Ergänzung von Vorschriften verlangt. Ein Schwerpunkt der Entscheidung liegt beim Umgang der Nachrichtendienste des Bundes und der Länder mit personenbezogenen Daten, die sie unter den besonderen Voraussetzungen des G 10-Gesetzes erheben dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich in der anschließenden rechtspolitischen Diskussion wiederholt zu Wort gemeldet und zunächst in einer Entschließung der 59. Konferenz vom 14./15. März 2000 grundlegende Aussagen zu den Konsequenzen aus dem Urteil des Bundesverfassungsgerichts dargelegt **(Anlage 9).** Schwerpunkte waren dabei die Pflicht zur unverzüglichen Löschung von Daten, die aus Eingriffen in das Fernmeldegeheimnis resultieren und nicht mehr benötigt werden, sowie eine Kennzeichnungspflicht für diese Daten, um die vom Bundesverfassungsgericht als besonders wichtig angesehene Zweckbindung der Daten auf ihrem weiteren Weg zu sichern.

Seit dem 24. Januar 2001 liegt nun ein Gesetzentwurf der Bundesregierung zur Novellierung des G 10-Gesetzes (G-10 E) vor. Dazu haben die Datenschutzbeauftragten des Bundes und der Länder in einer vorläufigen Stellungnahme folgende Kernpunkte herausgestellt:

- Die in § 15 G-10 E vorgesehene Regelung zur notwendigen Personal- und Sachausstattung der G 10-Kommission und deren Kontrollbefugnisse werden einhellig begrüßt.
  Soweit personenbezogene Daten nicht der Kontrolle durch die G 10-Kommission unterliegen (z.B. bei ihrer Übermittlung von den Nachrichtendiensten des Bundes an andere Bundesstellen), bleibt es bei der Zuständigkeit des Bundesbeauftragten für den Datenschutz. Damit ist im G 10-Bereich prinzipiell eine lückenlose Datenschutzkontrolle einerseits durch die G 10-Kommission und andererseits durch den Bundesbeauftragten für den Datenschutz gewährleistet.

- Positiv zu bewerten ist auch die in § 14 Abs. 1 G-10 E vorgesehene Berichtspflicht des zuständigen Bundesministeriums für sämtliche Beschränkungen nach dem G 10-Gesetz.
  Datenschutzrechtlichen Bedenken begegnet allerdings die in § 14 Abs. 1 Satz 2 G-10 E vorgesehene Formulierung, nach der die parlamentarische Kontrollkommission jährlich dem Deutschen Bundestag über „Durchführung“ sowie „Art und Umfang“ der Maßnahme Bericht zu erstatten hat, weil sie nicht konkret genug ist. Berichte an den Bundestag machen nur dann Sinn, wenn diese eine effiziente parlamentarische Kontrolle der Maßnahmen ermöglichen. Daher sollte die gesetzliche Vorschrift in Anlehnung an § 100e StPO so formuliert sein, daß über Anlaß, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen sowie über die Benachrichtigung der beteiligten Personen zu berichten ist.

  Zu den Forderungen des Landesbeauftragten und seiner Kollegen und Kolleginnen in Bund und Ländern gehört seit langem bei intensiven Eingriffen in das Persönlichkeitsrecht eine Evaluation und Erfolgskontrolle der Maßnahmen. Diese kann aber nur dann sachgerecht erfolgen, wenn entsprechend detailliertes Material zur Verfügung steht. Ansonsten liefe jede Verpflichtung des Gesetzgebers zur Evaluation grundrechtstangierender Maßnahmen größtenteils ins Leere.

- Datenschutzrechtlich problematisch ist die in § 3 Abs. 1 Nr. 6 G-10 E vorgesehene Regelung, wonach die Überwachungsbefugnisse auf Einzeltäter außerhalb von Staatsschutzdelikten ausgeweitet werden sollen. Die 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich bereits im Oktober 2000 mit dieser geplanten Erweiterung der Überwachungsbefugnisse befaßt und eine entsprechende Änderung des G 10-Gesetzes abgelehnt. Die Bedenken bestehen bereits deshalb, weil die ohnehin rechtsstaatlich sensiblen Überwachungsbefugnisse des Verfassungsschutzes und des Bundesnachrichtendienstes nunmehr in den Bereich der Strafverfolgung ausgedehnt werden sollen. Die Strafverfolgung muß aber aus rechtsstaatlichen Gründen Sache der Strafverfolgungsbehörden bleiben,

die in einem durch die strafprozessualen Regelungen ausgestalteten rechtsstaatlichen Verfahren agieren, das für die betroffenen Bürger und ihre Bevollmächtigten hinreichend transparent und überschaubar ist und eine gerichtliche Überprüfung getroffener Maßnahmen gewährleistet. Die geplante Einbeziehung der Geheimdienste mit ihren nachrichtendienstlichen Mitteln in die Verfolgung von Straftaten beeinträchtigt diese rechtsstaatlichen Sicherungen.

Die in § 3 Abs. 1 Nr. 6 G-10 E vorgesehene Regelung kann in Verbindung mit der in § 4 Abs. 3 G-10 E vorgesehenen Übermittlungsbefugnis in der Praxis dazu führen, daß die Polizei, die selbst nicht über die im G 10-Gesetz normierten Kompetenzen verfügt, letztendlich einen Großteil der von den Verfassungsschutzbehörden und dem Bundesnachrichtendienst erhobenen Daten erhält.

- Die Wiedereinführung der durch das Verbrechensbekämpfungsgesetz gestrichenen Fünfjahresfrist in § 12 Abs. 1 Satz 3 G-10 E wird abgelehnt. Hier ist eine Frist von drei Jahren völlig ausreichend. Wird auch nach drei Jahren nicht benachrichtigt, so ist die G 10-Kommission zu benachrichtigen.

- Die in § 8 G-10 E vorgesehene Regelung zur Überwachung von internationalen Telekommunikationsbeziehungen hat das datenschutzrechtliche Manko, daß keine Obergrenzen für die zur Kontrolle freigegebene Übertragungskapazität festgelegt wird. Dies kann im Einzelfall dazu führen, daß die gesamte Telekommunikation zwischen der Bundesrepublik und einem anderen Staat erfaßt wird. Hier ist es aus datenschutzrechtlichen Gründen mindestens erforderlich, wenn dauerhaft auf die Festlegung von Obergrenzen verzichtet werden soll, Kriterien zur Evaluation und Erfolgskontrolle der durchgeführten Maßnahmen festzulegen.

- Bei der vorgesehenen Durchbrechung des Zweckbindungsgrundsatzes nach § 4 Abs. 1 G-10 E ist anzustreben, daß die Zweckbindung in Anlehnung an

die derzeit geltende Regelung so zu formulieren ist, daß die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G-10 E genannten Straftaten genutzt werden dürfen.

- Unter datenschutzrechtlichen Gesichtspunkten zu kritisieren ist auch die in § 4 Abs. 2 Satz 3 G-10 E vorgesehene Regelung zur Ausnahme von der Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen. Die Kennzeichnungspflicht gehört zu den Grundaussagen des Bundesverfassungsgerichtes in seinem Urteil vom 14.07.1999. Die vorgesehene Neuregelung enthält in § 4 Abs. 2 Satz 3 die Ausnahme, daß der Behördenleiter oder sein Stellvertreter anordnen kann, daß bei der Übermittlung auf die Kennzeichnung verzichtet wird, wenn dies unerläßlich ist, um die Geheimhaltung einer Beschränkungsmaßnahme nicht zu gefährden, und die G 10-Kommission zugestimmt hat.
  Eine solche Ausnahmeregelung, die auch dazu führen könnte, daß in der Praxis die Kennzeichnungspflicht unterlaufen wird, wäre höchstens hinnehmbar, wenn bei der Evaluation besonders darauf geachtet wird, ob es sich lediglich um Einzelfälle der Ausnahme von der Kennzeichnungspflicht handelt.

Zwischenzeitlich liegen aus dem Rechts- und Innenausschuß des **Bundesrates** Empfehlungen zu dem Gesetzentwurf vor, die nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder die Persönlichkeitsrechte der Bürgerinnen und Bürger erheblich einschränken würden und die über den Gesetzentwurf der Bundesregierung in Teilen weit hinausgehen. Insbesondere wenden sich die Datenschutzbeauftragten dagegen, daß

- die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf der Bundesregierung noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u.a. zur Strafverfolgung nicht nur für die Verfolgung der Schwerkriminalität genutzt werden sollen,

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

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

In der Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001 sind weitere gravierende Kritikpunkte genannt **(vgl. Anlage 25).**

Auch für das Land Sachsen-Anhalt ist eine Novellierung des Ausführungsgesetzes zum G 10-Gesetz erforderlich, da nach dem Urteil des Bundesverfassungsgerichts auch im Bereich der Länder eine lückenlose Kontrolle bestehen muß.
Das Ministerium des Innern hat auf Anfrage des Landesbeauftragten mitgeteilt, daß zuerst die Neufassung des Bundesgesetzes abgewartet werden soll, bevor die Landesbestimmungen novelliert werden. Die Vorgaben des Urteils des Bundesverfassungsgerichts will man dabei dann berücksichtigen.

22. Verkehr

22.1 Videoüberwachung in öffentlichen Verkehrsmitteln

Auch in Sachsen-Anhalt zeigt sich der bundesweit zu beobachtende Trend, in Fahrzeugen öffentlicher Verkehrsunternehmen (Buslinienverkehr und Straßenbahnen) eine Videoüberwachung der Fahrgäste durchzuführen bzw. dies probeweise einzuführen. Begründet werden diese Maßnahmen mit den allgemein zunehmenden Sachbeschädigungen (Vandalismus), Bedrohungen von Fahrgästen und der Notwendigkeit der Aufklärung von Straftaten.
In zwei Fällen erfuhr der Landesbeauftragte aus der Presse über solche beabsichtigten Videoüberwachungsvorhaben kommunaler Nahverkehrsgesellschaften

in Sachsen-Anhalt. Er hat seine Zuständigkeit nach § 3 Abs. 2 Nr. 2 DSG-LSA bejaht und in Rechtsgesprächen vor Ort die nicht ganz einfache Rechtslage mit den Beteiligten erörtert.

Danach ist seitens der Verkehrsunternehmen, die sich ganz im Eigentum der öffentlichen Hand befinden, zu beachten, daß in das Grundrecht auf informationelle Selbstbestimmung der Bus- bzw. Straßenbahnbenutzer nur auf **gesetzlicher** Grundlage eingegriffen werden darf. Ob und wenn ja für welche Fälle eine solche Rechtsgrundlage vorhanden ist, ist in den Bundesländern umstritten. In Hamburg und Nordrhein-Westfalen sind einzelne Pilotprojekte zugelassen worden.

Der Landesbeauftragte hat für Sachsen-Anhalt zunächst festgestellt, daß für die Verkehrsunternehmen die Vorschriften des Personenbeförderungsgesetzes (PBefG) und die von der Genehmigungsbehörde danach erteilte Betriebsgenehmigung zu beachten sind (§§ 37, 43 und 47 i.V.m. § 39 PBefG). Diese sehen z.Zt. keine solche Beobachtungs- und Aufzeichnungsmöglichkeiten vor.

Deshalb wurde zum Thema „Videoüberwachung“ im Ministerium für Wohnungswesen, Städtebau und Verkehr (MWV) unter Beteiligung des Landesbeauftragten, des Ministeriums des Innern und der drei Regierungspräsidien eine Besprechung durchgeführt. Dabei wurden einvernehmlich nachfolgende Grundsätze für die Durchführung von Pilotprojekten mit Videoüberwachung erörtert und als Handlungsrahmen durch das MWV bis zu einer gesetzlichen Regelung durch den Bundesgesetzgeber für verbindlich erklärt:

1. Jede Form der Videoüberwachung - sei es nur als Beobachtung oder Aufzeichnung - stellt einen **Eingriff** in das Recht auf informationelle Selbstbestimmung der Benutzer öffentlicher Verkehrsmittel dar. Dieser bedarf grundsätzlich einer gesetzlichen Grundlage oder der Einwilligung des Betroffenen.
   Derzeit gibt es keine bereichsspezifische gesetzliche Regelung für die Videoüberwachung in öffentlichen Verkehrsmitteln. Dies bedeutet aber nicht,

daß eine Videoüberwachung gänzlich ausgeschlossen ist. Ihr dürfen aber insbesondere keine aus dem allgemeinen Persönlichkeitsrecht herrührenden Abwehrrechte der Fahrgäste entgegenstehen.

2. Eine Videoüberwachung ist **nur** zulässig, wenn im Rahmen einer Güterabwägung festgestellt wird, daß der mit der Maßnahme zu erreichende Schutz der Fahrgäste vor gewalttätigen Übergriffen anderer Fahrgäste und des Schutzes des Eigentums des Beförderungsunternehmens vor Randalieren das Interesse der Fahrgäste am Nichtbeobachtetsein **erheblich** überwiegt. (So z.B. bei überdurchschnittlich vielen und hohen Sachschäden auf bestimmten Linien in den Verkehrsmitteln (Vandalismus) oder bei wiederholter Begehung von Gewalttaten).

3. Öffentliche Verkehrsunternehmen haben regelmäßig eine Monopolstellung und sind grundsätzlich zur Beförderung von Fahrgästen verpflichtet. Die Fahrgäste können nur bedingt auf andere öffentliche Verkehrsmittel ausweichen. Daher sind die Fahrgäste bei einer Videoüberwachung in öffentlichen Verkehrsmitteln in besonderem Maße der Gefahr ausgesetzt, daß sie in ihrem Persönlichkeitsrecht beeinträchtigt werden. Das Risiko steigt mit dem Grad der Überwachung. Der Videoüberwachung sind daher **enge** Grenzen gesetzt.

4. Kriterium für die Güterabwägung ist weiterhin, ob die Videoüberwachung nur zu bestimmten Zeiten erfolgt oder nur bestimmte Bereiche des Verkehrsmittels erfaßt. So ist regelmäßig eine Beeinträchtigung des Persönlichkeitsrechtes von Fahrgästen zu verneinen, wenn nur Teilbereiche des Verkehrsmittels videoüberwacht werden, dem Fahrgast dieses bekannt ist und er die Möglichkeit hat, sich im nicht überwachten Bereich aufzuhalten. Weiter ist entscheidend, ob per Videotechnik nur beobachtet oder auch Aufzeichnungen gefertigt werden und für welche Dauer diese Aufzeichnungen gespeichert bleiben.

5. Modellprojekte zur Videoüberwachung sind **zeitlich befristet** durchzuführen. Die Projekte sollten auf einen Zeitraum von 1 bis 2 Jahren beschränkt werden und eine **Erfolgskontrolle** einschließen.
   Dabei müssen in den Betriebsanweisungen der Verkehrsunternehmen die erforderlichen technischen und organisatorischen Maßnahmen zur Sicherung der Videoaufzeichnungen festgelegt werden.

Der Landesbeauftragte regte an, bei den Pilotprojekten Einzelheiten der Videoüberwachung als Besondere Beförderungsbedingungen nach **§ 39 PBefG** durch die Regierungspräsidien genehmigen und festlegen zu lassen.
Gleiches gilt, soweit ein Verkehrsunternehmen dem Regierungspräsidium unter Vorlage von Unterlagen darlegt, daß eine ordnungsgemäße und vor allem sichere Durchführung der Beförderung aufgrund einer Vielzahl konkreter gravierender Vorfälle nicht mehr ohne weitere Schutzmaßnahmen möglich erscheint.

Nach gegenwärtigem Kenntnisstand sind die Konzepte bei den Genehmigungsbehörden eingereicht worden. Der Landesbeauftragte wird bei Beginn der Pilotversuche wieder beteiligt.

22.2 Medizinische Daten der Privatpiloten in einer Zentraldatei?

Der Landesbeauftragte wurde durch einen Artikel in einer Fachzeitschrift auf ein Rechtsproblem bei **§ 65 Abs. 3 Ziff. 4b** Luftverkehrsgesetz (LuftVG) in der seit 01.03.1999 gültigen Fassung aufmerksam. Das geänderte Gesetz sieht im Gegensatz zur derzeitigen Praxis künftig eine Zentrale Luftfahrerdatei vor. Sie dient der Feststellung, welche Erlaubnisse und Berechtigungen ein Luftfahrer besitzt und wird vom Luftfahrt-Bundesamt (LBA) geführt. Bisher führten die Länder solche Dateien für die von ihnen erteilten Genehmigungen.
In diese Datei sollen künftig u.a. auch medizinische **Einzelbefunde** aus den für die Privatpiloten vorgeschriebenen Tauglichkeitszeugnissen der fliegerärztlichen Untersuchungsstellen gespeichert werden. Damit soll auch eine vergleichende Kontrolle der Arbeit dieser Untersuchungsstellen möglich werden.

Diese Verfahrensweise hält der Landesbeauftragte datenschutzrechtlich für bedenklich, weil unter verfassungsrechtlicher Betrachtung der Zweck der Zentralen Luftfahrerdatei weder die Erforderlichkeit zur Speicherung von medizinischen Einzelangaben aus dem fliegerärztlichen Tauglichkeitszeugnis begründet noch dem Bund nach dem Grundgesetz (GG) die Kontrolle der fliegerärztlichen Tätigkeit zusteht. Gemäß Art. 74 Abs. 1 Nr. 19 GG hat der Bund nur die konkurrierende Gesetzgebungszuständigkeit bei der Zulassung zu ärztlichen und anderen Heilberufen. Die Kontrolle der ärztlichen Tätigkeit unterliegt aber dem **Landes**recht.

Im übrigen bestehen auch erhebliche Zweifel, ob der Bund nach Art. 73 Nr. 6 GG berechtigt ist, eine solche Überwachung durch das Luftfahrt-Bundesamt zu regeln.

Auch aus den neuen europäischen Rechtsvorschriften für den Luftverkehr ergeben sich keine Zwänge zur Übermittlung medizinischer Einzelbefunde an ein solches Zentralregister.

Eine Rückfrage bei der zuständigen Luftfahrtbehörde des Landes ergab, daß auch nach Änderung des LuftVG aus Sachsen-Anhalt bisher **keine** medizinischen Einzeldaten an das Luftfahrt-Bundesamt übermittelt worden sind.

Trotzdem hat der Landesbeauftragte den Bundesbeauftragten um eine Klärung dieser Rechtsfragen beim zuständigen Bundesministerium für Verkehr, Bau- und Wohnungswesen (BMVBW) gebeten. Dort sind zu diesem Thema bereits Gespräche auch mit Vertretern des LBA geführt worden. Bei der geplanten Neufassung des LuftVZO sollen diese datenschutzrechlichen Bedenken Berücksichtigung finden. Tatsächlich spricht einiges dafür, daß sich die im Gesetz vorgesehene Erfassung **nur** auf die Speicherung der Feststellungs**merkmale** der Tauglichkeit und der eingeschränkten Tauglichkeit beschränkt.

Eine solche Auslegung hält der Landesbeauftragte für verfassungskonform.

Sobald die Entscheidungsfindung im BMVBW abgeschlossen ist, wird der Landesbeauftragte informiert.

22.3 Parkerleichterung für Schwerbehinderte

Schwerbehinderten mit **außergewöhnlicher** Gehbehinderung und Blinden werden nach § 6 des Straßenverkehrsgesetz (StVG) Parkerleichterungen gewährt. Diese haben dann bundesweite Gültigkeit. Die Erteilung von Ausnahmegenehmigungen erfolgt gem. § 46 Abs. 1 der Straßenverkehrsordnung (StVO), das Verfahren ist in den Verwaltungsvorschriften zu § 46 StVO geregelt. Zum Nachweis ist vom Berechtigten bei Inanspruchnahme der Genehmigungsbescheid mitzuführen und ein **Ausweis** im Fahrzeug gut sichtbar auszulegen.

Für den Genehmigungsbescheid und den Ausweis nach § 46 StVO sind bundeseinheitliche Formblätter vorgeschrieben. Danach besteht die Möglichkeit, das **Namensfeld** auf dem auszulegenden Ausweis auf Wunsch des/der Berechtigten freizulassen. In diesen Fällen wird der Name auf der **Rückseite** des Ausweises eingetragen.

Für die Gewährung von Parkerleichterungen für behinderte Personen, bei denen **keine** außergewöhnliche Gehbehinderung vorliegt, aber aufgrund der Behinderung oder Krankheit ein Bedarf an Parkerleichterung besteht, hat das Land Sachsen-Anhalt in einem Gemeinsamen Runderlaß des MWV und des MS Regelungen getroffen. Damit wurde im Interesse der Behinderten, allerdings nur für den Gebrauch in Sachsen-Anhalt, diese nach Bundesrecht bestehende Parkerleichterung auf einen größeren Personenkreis erweitert.

Auf die Ausgabe eines Parkausweises, wie in der bundeseinheitlichen Verwaltungsvorschrift zu § 46 StVO vorgesehen, wurde allerdings im Runderlaß verzichtet.

Ein behinderter Bürger beantragte bei seiner zuständigen Straßenverkehrsbehörde die in Sachsen-Anhalt mögliche (erweiterte) Ausnahmegenehmigung. Da die Voraussetzungen vorlagen, erteilte die Behörde die Genehmigung und wies den betroffenen Bürger darauf hin, diese sei **gut sichtbar** im Fahrzeug beim Parken auszulegen.

Das Problem für den Bürger bestand nun darin, daß die Ausnahmegenehmigung eine Fülle von personenbezogenen Angaben enthielt, die bei der geforderten gut sichtbaren Auslegung im Kraftfahrzeug von jedermann im Vorbeigehen zur Kenntnis genommen werden konnten. Zu lesen waren neben seinem Vor- und Zunamen die vollständige Wohnanschrift, und unter der Rubrik „Besondere Bedingungen und Auflagen“ fanden sich auch noch die Gründe für die Ausnahmegenehmigung mit medizinischen Angaben über seine körperliche Behinderung. Der Bürger konnte sich nicht vorstellen, daß dies datenschutzrechtlich zulässig sei und bat den Landesbeauftragten um Überprüfung.

Die Überprüfung ergab Anwendungs- und Umsetzungsprobleme bei der zuständigen Straßenverkehrsbehörde. Diese hatte sich im Geflecht zwischen der bundeseinheitlichen Verwaltungsvorschrift zu § 46 Abs. 1 StVO für Schwerbehinderte mit außergewöhnlicher Gehbehinderung sowie für Blinde und den ergänzenden Regelungen im Runderlaß des MWV und des MS verheddert.

Richtig war natürlich, daß die dem Bürger zu erteilende Ausnahmegenehmigung als Verwaltungsakt alle die genannten personenbezogenen Angaben enthalten mußte. Davon zu trennen war aber der im Fahrzeug gut sichtbar auszulegende Berechtigungsnachweis. Der Gemeinsame Runderlaß des MWV und MS sieht aber **keinen** gesonderten Ausweis vor.

Trotzdem hätte die Straßenverkehrsbehörde mit Rücksicht auf die sensiblen Daten und die negativen Auswirkungen für den Betroffenen eine datenschutzgerechte Lösung finden müssen.

Auf den entsprechenden Hinweis des Landesbeauftragten räumte der Landkreis seine datenschutzrechtlich fehlerhafte Verfahrensweise ein und versorgte den Bürger mit einer datenschutzrechtlich unbedenklichen Ausnahmegenehmigung.

Der Landesbeauftragte hat das Ministerium für Wohnungswesen, Städtebau und Verkehr gebeten, die datenschutzgerechte Bundesregelung auch für die erweiterten Fälle in den Gemeinsamen Runderlaß einzuarbeiten.

23. Wahlen

23.1 Mitteilung der Anschriften zugelassener Wahlvorschläge und der gewählten Mandatsträger zu Kommunalwahlen

Ein Bildungswerk im Land Sachsen-Anhalt, das im Vorfeld von Kommunalwahlen Seminare für spätere Mandatsträger anbietet, wünschte von einem Einwohnermeldeamt die Herausgabe der Namen und Anschriften aller zugelassener Wahlkandidaten und der (später) gewählten Mandatsträger. Die personenbezogenen Daten wollte das Bildungswerk dazu benutzen, die Betroffenen zu kommunalen Bildungsveranstaltungen einzuladen bzw. mit Informationsmaterial zu versorgen. Die Verwaltungsgemeinschaft kam dem Wunsch nicht nach und verwies auf die fehlende Rechtsgrundlage bei der Übermittlung von personenbezogenen Daten der Betroffenen.

Der Landesbeauftragte hat den Sachverhalt wie folgt beurteilt:

Die speziellen Rechtsgrundlagen zum Erheben und Verarbeiten personenbezogener Daten bei Kommunalwahlen finden sich im Kommunalwahlgesetz (KWG LSA) und der Kommunalwahlordnung (KWO LSA). Ein wichtiger Garant für die Gewährleistung des Rechts auf informationelle Selbstbestimmung ist zudem das Prinzip der Zweckbindung.

Der Wahlkandidat darf danach darauf vertrauen, daß seine für die Kommunalwahl zur Verfügung gestellten und rechtlich zulässig erhobenen Daten nicht ohne Rechtsgrundlage zweckentfremdet werden.

Für die vom Bildungswerk gewünschte Liste der Namen und Anschriften enthält das KWG LSA keine Übermittlungsgrundlage. Die Wahlkandidaten haben zudem einen Anspruch darauf, nach Abschluß der Wahl und außerhalb der eigentlichen Wahlabläufe (vgl. § 28 und § 42 KWG LSA) nicht in die Öffentlichkeit gezerrt zu werden.

Der Landesbeauftragte hat deshalb zur praktischen und datenschutzgerechten Lösung das sog. Adreßmittlungsverfahren vorgeschlagen. Das Bildungswerk

leitet der Verwaltungsgemeinschaft frankierte Briefumschläge mit dem zu versendenden Material für die Mandatsträger zu und die Verwaltungsgemeinschaft versieht die Umschläge mit den ihr vorliegenden Adressen. Dann können die Betroffenen selbst entscheiden, ob sie mit dem Bildungswerk Kontakt aufnehmen wollen.

23.2 Unterstützung von Wahlvorschlägen für die Kommunalwahl

Der Landesbeauftragte hatte aufgrund von Eingaben zu prüfen, ob im Melde- und im Wahlamt einer Stadt die Bearbeitung der eingereichten Unterstützungsunterschriften für Wahlvorschläge von Wählergemeinschaften den datenschutzrechtlichen Voraussetzungen entsprach.

Für die Unterstützungsunterschriften werden Formblätter verwendet. Darin ist vorgesehen, daß die Meldebehörde in dem vom Unterstützer unterschriebenen und mit Familien-, Vornamen, Geburtsdatum sowie Anschrift versehenen Vordruck die Wahlberechtigung in der Gemeinde bzw. für den Kreis bestätigt.

In den beanstandeten Fällen hatte die Meldebehörde eine größere Zahl solcher Formblätter mit dem Vermerk „die Bescheinigung kann nicht erteilt werden, da die Personendaten nicht korrekt sind“ an die Wählergemeinschaft zurückgegeben.

Wie die Prüfung ergab, war die verweigerte Bestätigung in mehreren Fällen nicht rechtens. Maßgebendes Kriterium für die Bescheinigung des Wahlrechts war, ob die betroffenen Unterstützer nach Maßgabe der §§ 20 ff GO LSA Einwohner der Gemeinde und dort entsprechend dem Meldegesetz registriert waren. Dabei müssen die für eine Identitätsfeststellung erforderlichen Daten vollständig und richtig sein, wozu jedenfalls das Geburtsdatum und - bei verbleibenden Zweifeln zur Person - im Einzelfall auch der Geburtsort gehören.

Im übrigen ist die Wahlberechtigung der betroffenen Person aber auch bestätigungsfähig, wenn nur einzelne Daten unvollständig oder unrichtig sind, weil es auf das Vorhandensein aller Merkmale des § 22 MG LSA nicht zwingend ankommt.

Das Ministerium des Innern teilt die Auffassung des Landesbeauftragten, daß die Wahlrechtsbestätigung bei Vorliegen der Voraussetzungen nach § 30 Abs. 4 Nr. 2 KWO LSA auch dann auszustellen ist, wenn z.B. die angegebene Straße oder Hausnummer nicht mit den Angaben im Melderegister übereinstimmen, eine eindeutige Identifizierung der Person als Wahlberechtigter in dieser Kommune aber anhand der übrigen Angaben gewährleistet ist. Das Ministerium wird die in diesem Punkt offenen Verwaltungsvorschriften zur Klarstellung ergänzen.

Der Fall zeigte aber noch in einem weiteren Punkt Unzulänglichkeiten bei der betroffenen Verwaltung auf: Die Meldebehörde als für die Bescheinigung des Wahlrechts zuständige Stelle hat in solchen Fällen eine Beratungspflicht nach § 25 VwVfG i.V.m. § 23 GO LSA. Diese Vorschriften sind Ausdruck des Grundsatzes, daß im demokratischen Rechtsstaat niemand aus Unkenntnis wesentlicher staatsbürgerlicher Rechte verlustig gehen soll.

Zur Beratungspflicht gehörte beispielsweise, daß in einem abgestuften Verfahren zunächst den die Formulare ausfüllenden Bürgern hätte Gelegenheit gegeben werden müssen, ihre Angaben ggf. zu vervollständigen oder zu korrigieren.

So hätten auch offenkundige Mängel oder Zweifel wegen divergierender Eintragungen im Melderegister aufgeklärt werden können.

Im Hinblick auf die noch nicht sehr gefestigten Erfahrungen bei der Anwendung verfassungsrechtlicher Grundanforderungen im Zusammenhang mit der Abhaltung von Kommunalwahlen und das Fehlen ergänzender Hinweise in den Verwaltungsvorschriften des Landeswahlleiters zu § 30 Abs. 4 Nr. 3 i.V.m. Nr. 2 KWO LSA wurde von einer förmlichen Beanstandung abgesehen.

24. Wohnungswesen

24.1 Freistellung geförderter Wohnungen von der Belegungsbindung

Das Ministerium für Wohnungswesen, Städtebau und Verkehr teilte dem Landesbeauftragten mit, daß sich aufgrund der entspannten Wohnungsmarkt-

verhältnisse Fälle häuften, in denen belegungsgebundene, also mit erheblichen staatlichen Mitteln geförderte Wohnungen freigestellt werden müssen. Häufigster Grund, dem Antrag des Verfügungsberechtigten auf Befreiung von der Belegungsbindung stattzugeben, ist das fehlende öffentliche Interesse an der Einhaltung dieser Bindung, weil entweder allgemein die Wohnungsnachfrage gedeckt ist oder kein Wohnberechtigter Interesse an der bestimmten Wohnung hat.

Das Ministerium bat um Beratung durch den Landesbeauftragten, wie die zuständigen Stellen datenschutzgerecht den Versuch einer belegungskonformen Vermietung umsetzen können.

Als datenschutzgerechte Lösung empfahl der Landesbeauftragte, daß die zuständige Stelle, unter entsprechender Auslegung der §§ 4 Abs. 4 und 5a des Gesetzes zur Sicherung der Zweckbestimmung von Sozialwohnungen (Wohnungsbindungsgesetz - WoBindG) und unter Berücksichtigung der in Ziff. 5.1.1 der Verwaltungsvorschrift zur Sicherung der Belegungsbindung (BelegWoVV LSA), dem Verfügungsberechtigten mindestens drei Wohnungssuchende mit Namen und Anschrift zur Auswahl benennt.

Dabei sollte die für die Belegungsfreigabe zuständige Stelle die für die Anbahnung eines Mietverhältnisses erforderlichen Daten - und nur diese - dem gem. Ziff. 2.9 BelegWoVV LSA zu führenden Datenpool entnehmen. Dieses Verfahren hat eine gesetzliche Grundlage und ist verhältnismäßig, weil die Anzahl der mitgeteilten Wohnungssuchenden dabei in einem angemessenen Rahmen bleibt und nur nach Bedarf übermittelt wird.

24.2 Wohnungsförderung durch das Landesförderinstitut

Das Landesförderinstitut (LFI) nimmt treuhänderisch für das Land Sachsen-Anhalt Aufgaben mit Schwerpunkten in den Bereichen Wohnungsbau-, Wirtschafts-, Agrar- und Umweltförderung wahr.

In den zurückliegenden Jahren wurden so im Bereich der Wohnungsbauförderung fast 4 Milliarden DM vergeben. Nach den allgemeinen haushaltsrechtlichen Grundsätzen hat das LFI beim Umgang mit diesen Steuermitteln die wirtschaftlichste Handhabung sicherzustellen und die Fördermittel nur im Rahmen der gesetzlichen Vorschriften auszureichen.

Fördermittel erhält, wer die erforderliche Leistungsfähigkeit und Zuverlässigkeit besitzt und die Gewähr für eine ordnungsgemäße und wirtschaftliche Durchführung des Bauvorhabens bietet.

Um dies umfassend und der Höhe der zu bewilligenden Fördermittel entsprechend zu prüfen, muß das LFI in erheblichem Umfang personenbezogene Daten bei den antragstellenden Bürgern erheben. Dies geschieht zunächst mittels eines Selbstauskunftfragebogens bei den Betroffenen selbst. Für Fälle, in denen dem LFI die erteilten Auskünfte nicht ausreichen, läßt es sich vom Antragsteller vorab legitimieren, bei Steuer- und sonstigen Behörden, Kreditinstituten und anderen Stellen weitere Auskünfte über die Vermögens- und Einkommensverhältnisse einzuholen.

Das LFI wollte nun bei **allen** Antragstellern den Umfang der bei Dritten zu erhebenden Daten um Daten über die Schuldverhältnisse und die Zahlungsmoral der Antragsteller erweitern. Vorher bat es dazu beim Landesbeauftragten um datenschutzrechtlichen Rat.

Der Landesbeauftragte mußte dem LFI jedoch § 9 DSG-LSA entgegenhalten. Danach ist das Erheben personenbezogener Daten nur dann zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Dazu war anzumerken, daß das LFI auch ohne diese extra erhobenen Daten einen recht genauen Überblick über die Schuldverhältnisse der Antragsteller erhält.

Zum einen durch deren Angaben auf dem Selbstauskunftfragebogen, zum anderen durch die stets eingeholte Schufa-Auskunft.

Nur wenn im **Einzelfall** diese Daten nicht ausreichend sind oder beim LFI Zweifel an ihrer Richtigkeit bestehen, kann eine weitere Datenerhebung erforderlich

sein. Für diese Fälle empfahl der Landesbeauftragte, eine gesonderte Einwilligungserklärung vom Antragsteller anzufordern. Dieser hat dann auch die Möglichkeit, seinen Fördermittelantrag zurückzuziehen, wenn ihm - aus welchen Gründen auch immer - diese zusätzliche Datenerhebung nicht recht ist.

Anlage 1

Organisationsplan

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Herr Kalk

Referat 1	Referat 2	Referat 3
Grundsatzfragen des Datenschutzes, Internationaler Datenschutz (ohne Europa), Landtag, Öffentlicher Dienst, Personalvertretung Rundfunk- und Presserecht, Geschäftsstellenleitung	Rechtspflege, Justizverwaltung, Justizvollzug, Rechtshilfe, Allgemeines Ordnungswidrigkeitenrecht, Verfassungsschutz, Nachrichtendienste	Grundsatzfragen der Technik und Organisation des Datenschutzes und der Informationstechnik, Wirtschaft, Verkehr, Raumordnung und Landesplanung
Hochschulen, Sozialwesen, Gesundheitswesen, Jugendhilfe	Polizei, Finanzen, Kommunalrecht	Betriebs- und Datenbanksysteme, Statistik, Handwerk und Gewerbe, Wohnungswesen
Personenstandswesen, Kindertageseinrichtungen, Kultur, Denkmalschutz, Archivwesen, Wissenschaft und Forschung, Schulen	Gefahrenabwehrrecht, Bau- und Bodenangelegenheiten, Natur- und Umweltschutz, Landwirtschaft und Forsten, Ausländer, Aussiedler, Staatsangehörigkeit, EUROPOL und Schengen, Europäischer Datenschutz	Telekommunikation, Netze, Neue Medien, Vermessungs- und Katasterwesen, Dateienregister, ---------- Gleichstellungsfragen
Verwaltungsangelegenheiten der Geschäftsstelle, Ausweis-, Meldewesen, Feuerwehr, Katastrophenschutz, Personalaktenrecht, Wahlen,		
Registratur		
Bücherei		

Dienstgebäude: Berliner Chaussee 9
39114 Magdeburg

Postanschrift: Postfach 1947
39009 Magdeburg

Telefon: (0391) 8 18 03 - 0

Telefax: (0391) 8 18 03 33

Internet: http://www.datenschutz.sachsen-anhalt.de

Stand: 01.04.2001

Anlage 2

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. Oktober 1999:

Patientenschutz durch Pseudonymisierung

Im Gesundheitsausschuß des Deutschen Bundestages wird derzeit der vom Bundesministerium für Gesundheit vorgelegte Gesetzesentwurf zur Gesundheitsreform 2000 dahingehend geändert, daß die Krankenkassen künftig von den Leistungserbringern (z.B. Ärztinnen und Ärzte, Krankenhäuser, Apotheken) die Patientendaten nicht in personenbezogener, sondern in pseudonymisierter Form erhalten. Dieses neue Modell nimmt eine zentrale Forderung der Datenschutzbeauftragten auf, für die Verarbeitung von Patientendaten solche technischen Verfahren zu nutzen, die die Persönlichkeitsrechte der Betroffenen wahren und so die Entstehung des „gläsernen Patienten“ verhindern.

Auch anhand von pseudonymisierten Daten können die Krankenkassen ihre Aufgaben der Prüfung der Richtigkeit der Abrechnungen sowie der Wirtschaftlichkeit und der Qualität der Leistungen erfüllen.

Die Konferenz unterstützt den Bundesbeauftragten für den Datenschutz dabei, daß in den Ausschußberatungen die Wirksamkeit der Pseudonymisierung, die gesetzliche Festlegung von Voraussetzungen für die Identifizierung der Versicherten zu bestimmten Zwecken und die Definition strikter Zweckbindung dieser Daten durchgesetzt werden.

Anlage 3

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. Oktober 1999:

DNA-Analysen zur künftigen Strafverfolgung auf der Grundlage von Einwilligungen

In der Strafprozeßordnung ist der Einsatz der DNA-Analyse zur vorbeugenden Verbrechensbekämpfung nur mit richterlicher Anordnung vorgesehen.

In einigen deutschen Ländern werden DNA-Analysen ohne richterliche Anordnung gestützt allein auf die Einwilligung der Betroffenen durchgeführt. Soweit die dabei erhobenen Daten zum Zweck der Identitätsfeststellung in künftigen Strafverfahren genutzt werden sollen, bedürfen DNA-Analysen nach der klaren gesetzlichen Regelung des DNA-Identitätsfeststellungsgesetzes jedoch einer richterlichen Anordnung. Der Richter oder die Richterin hat u.a. die Prognose zu treffen, ob Grund zur Annahme besteht, dass gegen Betroffene künftig erneut Strafverfahren wegen des Verdachts erheblicher Straftaten zu führen sind. Wenn nunmehr auch DNA-Analysen gespeichert und zum Zweck der zukünftigen Strafverfolgung genutzt werden dürfen, die auf freiwilliger Basis – also ohne richterliche Anordnung – erstellt worden sind, und dies sogar durch die Errichtungsanordnung für die DNA-Analyse-Datei beim BKA festgeschrieben werden soll, werden damit die eindeutigen gesetzlichen Vorgaben des DNA-Identitätsfeststellungsgesetzes unterlaufen.

Die von Strafgefangenen erteilte Einwilligung zur Entnahme, Analyse und Speicherung kann keine Grundlage für einen derartigen Eingriff sein. Eine wirksame Einwilligung setzt voraus, dass sie frei von psychischem Zwang freiwillig erfolgt. Da Strafgefangene annehmen können, dass die Verweigerung der Einwilligung Auswirkungen z.B. auf die Gewährung von Vollzugslockerungen hat, kann hier von Freiwilligkeit keine Rede sein. Ausschlaggebend für die Beurteilung der Freiwilligkeit einer Einwilligung ist die subjektive Einschätzung des Betroffenen. Auch wenn im Einzelfall die Weigerung von Strafgefangenen, sich einer

DNA-Analyse zu unterziehen, die Entscheidung über Vollzugslockerungen nicht beeinflußt, ist dennoch davon auszugehen, dass die Befürchtung, die Verweigerung habe negative Folgen, die freie Willensentscheidung beeinträchtigen.

Die Datenschutzbeauftragten des Bundes und der Länder halten deshalb die Praxis einiger Länder, DNA-Analysen – abweichend von den gesetzlich vorgesehenen Verfahren – systematisch auf der Grundlage von Einwilligungen durchzuführen, für eine Umgehung der gesetzlichen Regelung und damit für unzulässig. Die möglicherweise mit der Beantragung richterlicher Anordnungen verbundene Mehrarbeit ist im Interesse der Rechtmäßigkeit der Eingriffsmaßnahmen hinzunehmen. Die Datenschutzbeauftragten fordern daher, DNA-Analysen zum Zweck der Identitätsfeststellung für künftige Strafverfahren nur noch auf der Grundlage richterlicher Anordnungen durchzuführen.

Anlage 4

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. Oktober 1999:

Beschluß des Europäischen Rates zur Erarbeitung einer Charta der Grundrechte der Europäischen Union

Der Europäische Rat hat anläßlich seiner Zusammenkunft am 4. Juni 1999 in Köln die Ausarbeitung einer Charta der Grundrechte der Europäischen Union beschlossen. In dem Ratsbeschluß heißt es: „Im gegenwärtigen Entwicklungszustand der Union ist es erforderlich, eine Charta dieser Rechte zu erstellen, um die überragende Bedeutung der Grundrechte und ihre Tragweite für die Unionsbürger sichtbar zu verankern".

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen nachhaltig die Initiative des Europäischen Rates zur Ausarbeitung einer europäischen Grundrechtscharta. Sie fordern Bundesregierung, Bundestag und Bundesrat auf, sich für die Einfügung eines Grundrechts auf Datenschutz in den zu schaffenden Katalog europäischer Grundrechte und dessen Verankerung in den Verträgen der Europäischen Union einzusetzen. Damit würde der herausragenden Bedeutung des Datenschutzes in der Informationsgesellschaft Rechnung getragen.

Die europäische Datenschutzrichtlinie verpflichtet die Mitgliedstaaten zur Gewährleistung des Schutzes der Grundrechte und Grundfreiheiten und insbesondere des Schutzes der Privatsphäre (Art. 1 Abs. 1). Die Datenschutzbeauftragten weisen darauf hin, dass einige europäische Länder ein Datenschutzgrundrecht in ihre Verfassung aufgenommen haben; in einigen anderen Ländern wurde ihm durch die Rechtsprechung Grundrechtsgeltung zuerkannt. In Deutschland wird das vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) abgeleitete Grundrecht auf Datenschutz als solches von zahlreichen Landesverfassungen ausdrücklich erwähnt.

Anlage 5

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. Oktober 1999:

Eckpunkte der deutschen Kryptopolitik - ein Schritt in die richtige Richtung

Das Brief-, Post- und Fernmeldegeheimnis zählt zu den traditionellen und wichtigsten Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet deshalb die freie Entfaltung der Persönlichkeit durch einen privaten, vor Dritten verborgenen Austausch von Nachrichten, Gedanken und Informationen. Deshalb darf nur in Ausnahmefällen im überwiegenden Allgemeininteresse auf gesetzlicher Grundlage in dieses Grundrecht eingegriffen werden.

Im Zuge der Privatisierung der Telekom hat der Staat sein Post- und Fernmeldemonopol verloren, so daß zum Grundrechtsschutz die bloße Abwehr unrechtmäßiger staatlicher Eingriffe nicht mehr genügt. Darüber hinaus bestehen die Möglichkeiten der staatlichen Datenschutzkontrolle in offenen Netzen nur in eingeschränktem Maße. Der Schutz personenbezogener Daten während der Verarbeitung und Übertragung ist häufig nicht ausreichend gewährleistet. Deshalb sind ergänzende staatliche Maßnahmen zum Schutz Aller gegen neugierige Dritte (z.B. Systembetreiber, Unternehmen mit wirtschaftlichen Interessen, Hacker und Hackerinnen, ausländische Geheimdienste) erforderlich.

Die Privatsphäre läßt sich jedoch nur mit Rechtsvorschriften nicht ausreichend schützen. Neben bestehenden Ge- und Verboten sind wirksame technische Vorkehrungen nötig. Systemdatenschutz und datenschutzfreundliche Technologien sind unverzichtbar. Den Bürgerinnen und Bürgern müssen effektive Instrumente zum Selbstschutz an die Hand gegeben werden. Der Datenverschlüsselung kommt deshalb in einem modernen Datenschutzkonzept eine herausragende Bedeutung zu.

Bislang mußte befürchtet werden, daß auf Betreiben der staatlichen Sicherheitsbehörden in Deutschland das Recht auf Verschlüsselung eingeschränkt würde. Jetzt jedoch hat die

Bundesregierung mit dem Eckpunktepapier vom 2. Juni 1999 die Diskussion auf eine völlig neue Basis gestellt. Richtigerweise wird darin die Kryptographie als „eine entscheidende Voraussetzung für den Datenschutz der Bürger“ besonders hervorgehoben.
Die Position der Bundesregierung, die freie Verfügbarkeit von Verschlüsselungsprodukten nicht einschränken zu wollen, wird von den Datenschutzbeauftragten des Bundes und der Länder ausdrücklich begrüßt. Damit wurde ein erster wichtiger Schritt in die richtige Richtung getan, dem jedoch weitere folgen müssen. Der im Sinne des Artikels 10 des Grundgesetzes legitime und grundrechtlich geschützte Anspruch Aller auf unbeobachtete Telekommunikation und auf den Schutz ihrer personenbezogenen Daten sollte von der Bundesregierung noch stärker unterstützt werden. Um der Bedeutung geschützter Telekommunikation unter den Bedingungen der Informationsgesellschaft gerecht zu werden, sind konkrete Maßnahmen notwendig. Vorrangig sind zu nennen:

- Aktive Förderung des Einsatzes von Verschlüsselungstechniken in der öffentlichen Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen,

- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern,

- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z.B. Ärzte und Ärztinnen, Anwälte und Anwältinnen, Psychologen und Psychologinnen),

- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation,

- Förderung einer neutralen Bewertung von Verschlüsselungsprodukten mit dem Ziel, den Verbrauchern Empfehlungen für ihren Gebrauch zu geben,

- Förderung der Entwicklung europäischer Verschlüsselungsprodukte mit offengelegten Algorithmen.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten die öffentlichen Stellen auf, mit gutem Beispiel voranzugehen. Sie sollten vorbehaltlos die technischen Möglichkeiten des Einsatzes kryptographischer Verfahren zum Schutz personenbezogener Daten prüfen und derartige Lösungen häufiger als bisher einsetzen. Künftig muß Kryptographie der Standard in der Informations- und Kommunikationstechnik werden, auf deren Einsatz nur dann verzichtet wird, wenn wichtige Gründe dagegen sprechen.

Hersteller von Produkten der Informations- und Telekommunikationstechnik werden aufgefordert, die guten Voraussetzungen zur Entwicklung von Verschlüsselungsprodukten in Deutschland zu nutzen, um sichere, leicht bedienbare und interoperable Produkte zu entwickeln und den Anwendern kostengünstig anzubieten. Die Datenschutzbeauftragten des Bundes und der Länder bieten hierfür ihre Kooperation an.

Anlage 6

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. Oktober 1999:

Aufbewahrung des Schriftguts der ordentlichen Gerichtsbarkeit und Staatsanwaltschaften

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits in ihrer Entschließung zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich am 09./10.03.1995 gefordert, dass insbesondere die Dauer der Aufbewahrung von Strafakten nach rechtskräftigem Abschluß eines Strafverfahrens, ihre Aussonderung und Vernichtung einer Regelung durch formelles, den Grundsätzen des Volkszählungsurteils entsprechendes Gesetz bedarf.

Mit Beschluß vom 16.08.1998 hat das Oberlandesgericht Frankfurt am Main festgestellt, dass der derzeitige Zustand zwar für eine Übergangsfrist noch hinzunehmen sei, dass die Schaffung einer gesetzlichen Grundlage für die Aufbewahrung von Akten jedoch nicht als nur mittelfristige Aufgabenstellung des Gesetzgebers betrachtet werden dürfe, sondern alsbald in Angriff zu nehmen sei. In gleicher Weise hat auch das OLG Hamm mit Beschluß vom 17.09.1998 darauf hingewiesen, dass die Aufbewahrung von Strafakten einer gesetzlichen Grundlage bedarf. Auch der Entwurf des Strafverfahrensänderungsgesetzes 1999 enthält insoweit keine Regelung.

Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für dringend geboten, dass unverzüglich mit der Umsetzung dieser Aufgabe begonnen wird. Sie weisen ferner darauf hin, dass auch für die Aufbewahrung von Zivilakten und Akten im Bereich der freiwilligen Gerichtsbarkeit umgehend gesetzliche Regelungen zu schaffen sind, die die Dauer der Aufbewahrung auf das erforderliche Maß festlegen.

Anlage 7

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. Oktober 1999:

Täter-Opfer-Ausgleich und Datenschutz

Kernstück datenschutzrechtlicher Überlegungen zum Täter-Opfer-Ausgleich ist die Frage, ob Institutionen zur Durchführung des Ausgleichsverfahrens umfassende Informationen insbesondere über Opfer von Straftaten erhalten dürfen, ohne dass diese davon Kenntnis erlangt und eingewilligt haben.

Darin wäre ein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen zu sehen. Dies ist nach geltendem Recht unzulässig.

Der nunmehr vorliegende Gesetzentwurf der Bundesregierung (BR-Drs. 325/99 vom 28.05.1999) sieht in § 155a Satz 3 StPO-Entwurf vor, dass nur der ausdrücklich geäußerte entgegenstehende Wille der oder des Verletzten dazu führt, dass keine Datenübermittlungen an Schlichtungsstellen erfolgen sollen. Das bedeutet, dass solche im Einzelfall gleichwohl möglich sind. Dies halten die Datenschutzbeauftragten nicht für ausreichend.

Der Bundesrat ist sogar dem Gesetzentwurf der Bundesregierung nicht gefolgt; er hat vielmehr angeregt, im Gesetz klarzustellen, dass es für solche Datenübermittlungen auf den Willen der Opfer nicht ankommen soll. Folgende Argumente werden dafür genannt: Eine vor der Einschaltung von Schlichtungsstellen durch die Justiz einzuholende Einwilligung führe dazu, dass das kriminalpolitisch wichtige Institut des „Täter-Opfer-Ausgleichs“ nicht ausreichend genutzt werde. Erst die professionelle Tätigkeit der Schlichtungsstellen mit ihrem Selbstverständnis als „objektive Dritte mit dem Gebot der Unterstützung jeder Partei“ könnte wirksame Überzeugungsarbeit leisten; nur dann könne der Rechtsfriede dauerhafter als bei herkömmlichen Verfahren sichergestellt werden, wenn durch die „fachlich geleitete Auseinandersetzung“ der „am strafrechtlich relevanten Konflikt beteiligten Parteien im Idealfall Verständnis und wechselseitige Toleranz geweckt werden“.

Dieser Argumentation widersprechen die Datenschutzbeauftragten entschieden: Die Achtung und wirksame Unterstützung der Opfer ist ein wesentliches Anliegen des Strafverfahrens. Rechtsfriede und Toleranz können nur verwirklicht werden, wenn die Strafverfolgungsbehörden bei Datenübermittlungen an Schlichtungsstellen (z.B. in der Rechtsform von Vereinen) den Willen und die Eigenverantwortung der Opfer uneingeschränkt respektieren. Auch die Sicht der Beschuldigten, ohne deren Mitwirkung der Täter-Opfer-Ausgleich nicht durchgeführt werden kann, sollte von den Strafverfolgungsbehörden dabei berücksichtigt werden. Die Konferenz der Datenschutzbeauftragten fordert deshalb, daß an der Voraussetzung der unzweifelhaften Einwilligung vor solchen Datenübermittlungen festgehalten wird.

Ferner sollte der Gesetzgeber festlegen, daß die Berichte der Schlichtungsstellen an Staatsanwaltschaft und Gericht nur für Zwecke der Rechtspflege verwendet werden dürfen. Das besondere Vertrauensverhältnis zwischen den Schlichtungsstellen und den am „Täter-Opfer-Ausgleich“ Beteiligten muß gesetzlich geschützt werden.

Anlage 8

Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. Oktober 1999:

Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in der Telekommunikation

Die Ausbreitung moderner Telekommunikationsnetze und die Fortentwicklung der Informationstechnologie erfolgen in großen Schritten. Dieser technische Fortschritt hat einerseits zu einer massenhaften Nutzung der neuen Möglichkeiten der Telekommunikation und damit zu einer grundlegenden Veränderung des Kommunikationsverhaltens der Bevölkerung geführt. Andererseits erhalten dadurch die herkömmlichen Befugnisse der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs eine neue Dimension, weil aufgrund der weitreichenden Digitalisierung immer mehr personenbezogene Daten elektronisch übertragen und gespeichert werden.

Die bei der Telekommunikation anfallenden Daten können mit geringem Aufwand in großem Umfang kontrolliert und ausgewertet werden. Anhand von Verbindungsdaten läßt sich nachvollziehen, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen und Neigungen nachgeht. Bereits auf der Ebene der bloßen Verbindungsdaten können so Verhaltensprofile erstellt werden, die die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen. Eine staatliche Überwachung dieser Vorgänge greift daher tief in das Telekommunikationsgeheimnis der Betroffenen ein und berührt auf empfindliche Weise die Informationsfreiheit und den Schutz besonderer Vertrauensverhältnisse.

Die bisherige rechtliche Grundlage für den Zugriff der Strafverfolgungsbehörden auf Verbindungsdaten in § 12 des Fernmeldeanlagengesetzes (FAG) stammt noch aus einer Zeit, in der die analoge Vermittlungstechnik vorherrschte, nicht für jedes Gespräch personenbezogene Verbindungsdaten erzeugt wurden und die Telekommunikationsdienste in

wesentlich geringerem Maße als heute genutzt wurden. Die Vorschrift erlaubt auch Zugriffe auf Verbindungsdaten wegen unbedeutenden Straftaten, bei denen eine inhaltliche Überwachung der Telekommunikation unzulässig wäre. Unter Berücksichtigung der Digitaltechnik, der vollständigen Datenerfassung und der Möglichkeit zur Bildung von Verhaltensprofilen verstößt § 12 FAG daher gegen den Verhältnismäßigkeitsgrundsatz und ist somit nicht mehr geeignet, Eingriffe in das Telekommunikationsgeheimnis zu rechtfertigen.

In einem früheren Gesetzesentwurf war vorgesehen, den Zugriff auf Verbindungsdaten grundsätzlich auf nicht unerhebliche Straftaten zu beschränken. Beschlossen wurde aber lediglich die unveränderte Fortgeltung des § 12 FAG, zuletzt befristet bis zum 31.12.1999. Nunmehr wollen der Bundesrat und die Justizministerkonferenz die Befristung für die Weitergeltung dieser Vorschrift aufheben und es damit beim bisherigen, verfassungsrechtlich bedenklichen Rechtszustand belassen.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen eine Verlängerung der Geltungsdauer des § 12 FAG und fordern statt dessen eine Neufassung der Eingriffsbefugnis unter Beachtung der grundrechtlichen Bindungen und Anforderungen, die sich aus dem von Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis ergeben.

Die gesetzliche Ermächtigung für den Zugriff auf Verbindungsdaten gehört sachlich in die Strafprozeßordnung. Die gesetzlichen Zugriffsvoraussetzungen sollten in Abstimmung mit § 100a StPO neu geregelt werden.

Anlage 9

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000:

Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

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

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

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

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

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

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

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

länger als fünf Jahre zurückgestellt wird.

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

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

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

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

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

- Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist. Das Bundesverfassungsgericht hat gefordert, dass auch im Bereich der Landesverwaltung eine ausreichende Kontrolle existieren muss.

Anlage 10

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000:

Data Warehouse, Data Mining und Datenschutz

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

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

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

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

- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden ist. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.
- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.
- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten „Daten-Lagerhäusern“ rechtswidrig. Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). „Data Mining“ ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

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

Anlage 11

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000:

Für eine freie Telekommunikation in einer freien Gesellschaft

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

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

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

- **Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten**
  Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

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

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

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

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

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

- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern

verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.

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

Forderungen zur Gewährleistung der freien Telekommunikation

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

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

- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.

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

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

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

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

- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäuser oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o.g. Nebenstellenanlagen gilt.

Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.

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

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

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

Anlage 12

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000:

Unzulässiger Speicherungsumfang in „INPOL-neu“ geplant

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

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

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

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

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

Anlage 13

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000:

Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

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

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

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,
- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z.B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,
- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,
- nicht am Verfahren beteiligte Dritte schon bei „berechtigtem Interesse“ Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen.

Statt dessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

Anlage 14

Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000:

Risiken und Grenzen der Videoüberwachung

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

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

Daher müssen

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

strikt sichergestellt werden.

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

Dies bedeutet:

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

- Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. *Dafür kommen – **soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen** – unter Anderem in Betracht[1]:*
  - *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.*
  - *für die Verkehrslenkung nur Übersichtsaufnahmen,*
  - *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.*

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

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

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

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

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

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

Anlage 15

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. Juni 2000:

Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 6 Satz 1 GG zur Strafverfolgung eingesetzten „Großen Lauschangriffe“ zu unterrichten. § 100e StPO konkretisiert die Berichtspflicht dahingehend, daß die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlaß, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

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

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

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

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

Darüber hinaus wäre es wünschenswert, wenn - wie in den „Wire-tap-Reports“ der USA - die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

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

Anlage 16

Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000:

Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

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

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

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine „genetische Diskriminierung“ bei der Gewinnung oder Verwendung

genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der „Entschließung über Genomanalyse und informationelle Selbstbestimmung“ vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

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

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

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

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

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

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

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

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

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

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

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

Anlage 17

Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000:

Entschließung zur Novellierung des BDSG

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (System-datenschutz - § 3a E-BDSG) und die Einführung des Datenschutzaudit (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

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

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

Anlage 18

Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000:

Datensparsamkeit bei der Rundfunkfinanzierung

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

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

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

Anlage 19

Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000:

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

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

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

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

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit

gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

Anlage 20

Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000:

Auftragsdatenverarbeitung durch das Bundeskriminalamt

- Umlaufbeschluss -

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

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

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

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

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

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

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

Anlage 21

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001:

Äußerungsrecht der Datenschutzbeauftragten

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

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

Anlage 22

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001:

Datenschutz beim elektronischen Geschäftsverkehr

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

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

Anlage 23

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001:

Informationszugangsgesetze

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

Anlage 24

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001:

Datenschutz bei der Bekämpfung von Datennetzkriminalität

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

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

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

[2] European Committee on Crimes Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), Draft Convention on Cyber-crime (PC-CY (2000) Draft No. 25)
[3] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 26.01.2001 – KOM (2000) 890 endgültig

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

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

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

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

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

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

Anlage 25

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001:

Novellierung des G 10-Gesetzes

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

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

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

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

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

- Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle

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

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

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

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

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

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

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

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

- Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei "strategischer Überwachung" nach § 5 G10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

Anlage 26

Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09. März 2001:

Novellierung des Melderechtsrahmengesetzes

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

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.

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

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

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

5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen Auskunft über Daten von Gruppen von Wahlberechtigten erteilen, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

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

Bei Enthaltung Thüringens zu Ziffer 6.

Anlage 27

Entschließung der Datenschutzbeauftragten des Bundes und der Länder
vom 12. März 2001:

Anlaßlose DNA-Analyse aller Männer verfassungswidrig

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

Anlage 28

Bekanntmachung des Landesbeauftragten für den Datenschutz vom 10.05.2000:

EDV-Einsatz in Schulen, insbesondere der Anschluss an das Internet

Der Einsatz moderner Kommunikationsmittel ist zwischenzeitlich auch in der öffentlichen Verwaltung weit verbreitet und dort für die tägliche Aufgabenerledigung unverzichtbar geworden.
Dazu gehört auch der Wunsch, neben dem Anschluss an ein lokales Netz oder das Landesnetz auch Zugang zu globalen Datennetzen zu erhalten.
Es ist zu begrüßen, dass diese Entwicklung vor den Schulen nicht Halt macht und mit Hilfe höherer Haushaltsmittel und den Angeboten von Sponsoren die jungen Menschen eine frühere Chance zum professionellen Kennenlernen dieser neuen Technik erhalten.
Deshalb begrüßt der Landesbeauftragte für den Datenschutz die beabsichtigte Ausstattung der Schulen mit Computern, um Anschluss an die technische Entwicklung zu halten und damit auch die sichere Beherrschung dieser neuen Technologien zu fördern.

Bei aller Begeisterung darf aber nicht übersehen werden, dass der Wunsch nach Zugang zu internationalen Kommunikationsdiensten und -angeboten, wie dem weltumspannenden Datennetz Internet, Risiken für jede einzelne Benutzerin und jeden einzelnen Benutzer und ihr und sein Recht auf informationelle Selbstbestimmung, das heißt den selbstbestimmten Umgang mit ihren und seinen persönlichen Daten, beinhalten kann. Diese Risiken resultieren größtenteils daraus, dass das Internet als Datennetz nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung (TCP/IP), in den Implementierungen und der Installation der Programme für die Internet-Dienste und auch den angeschlossenen Rechnersystemen. So stellt zum Beispiel das TCP/IP-Protokoll keine sicheren Mechanismen zur Identifikation und Authentisierung bereit. Deshalb gehört auch das Wissen um Schutzmaßnahmen und Datensicherheit zu diesem Thema.

Die Datenschutzbeauftragten des Bundes und der Länder sind darum bemüht, Benutzerinnen und Benutzer über die nicht unerheblichen, aber zum größten Teil vermeidbaren Gefährdungen und Gefahren im Interesse einer sicheren Nutzung unter Berücksichtigung der weiteren Entwicklung des Internet aufzuklären.
Insbesondere wird darauf hingewiesen, dass zwischen personenbezogenen Daten für schulische Zwecke und den jeweiligen Arbeitsdaten um Unterricht streng zu unterscheiden ist und eine Vermischung dieser Daten unter allen Umständen vermieden werden muss.
Daraus folgt, dass im Interesse der Schülerinnen und Schüler, ihrer Erziehungsberechtigten und auch der Lehrkräfte sogenannte schulische Echtdaten, wie sie sich insbesondere aus den Richtlinien zum Schülerstammblatt (vgl. RdErl. MK vom 20.06.1995, SVBl. LSA S. 208, zuletzt geändert durch RdErl. des MK vom 12.06.1997, SVBl. LSA S. 223) ergeben, nur im lokalen Netz verarbeitet werden dürfen, das vom Internet strikt abzuschotten ist. Das kann durch verschiedene Techniken, zum Beispiel Firewall-Systeme geschehen.
Trotzdem ist zu bedenken und zu beachten, dass selbst wenn Schutzmaßnahmen gegen die bekannten Gefährdungen getroffen werden, ein hundertprozentiger Schutz nur durch Verzicht auf eine Internet-Anbindung realisiert werden kann.

Nähere Hinweise erhalten die Schulen aus den vom Landesbeauftragten für den Datenschutz herausgegebenen Tätigkeitsberichten und weiteren Informationsbroschüren. Darüber hinaus ist die Behörde gerne bereit, im Einzelfall unmittelbare Hilfestellung zu gewähren.

Stichwortverzeichnis *

* Fundstelle zitiert nach Tätigkeitsbericht und Seite